kaspersky

Kaspersky Security для виртуальных сред 5.2 Легкий агент

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 5.2

Уважаемый пользователь!

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

Дата редакции документа: 12.10.2023

Обозначение документа: 643.46856491.00097-04 90 01

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

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

kaspersky

Содержание

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Security для виртуальных сред 5.2 Легкий агент" (далее также "Kaspersky Security", "программа").

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Security, а также поддержка организаций, использующих Kaspersky Security. Документ адресован техническим специалистам, которые имеют опыт работы с операционными системами Microsoft® Windows® и Linux®, системой удаленного централизованного управления программами «Лаборатории Касперского» Kaspersky Security Center и виртуальными инфраструктурами.

Имеются ограничения в установке и работе программы в виртуальных инфраструктурах Enterprise Cloud Platform VeiL и SharxBase. Подробнее см. в Базе знаний (https://support.kaspersky.ru/15719).

О программе

Программное изделие "Kaspersky Security для виртуальных сред 5.2 Легкий агент" (далее также "Kaspersky Security", "программа") представляет собой средство антивирусной защиты типов "Б" и "В" четвертого класса защиты и предназначено для применения на серверах и автоматизированных рабочих местах информационных систем.

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

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- контроль доступа к веб-ресурсам;
- контроль запуска программ;
- контроль доступа программ к защищаемым ресурсам;
- мониторинг файловых операций;
- контроль целостности компонентов.

В этом разделе

Функциональные компоненты Легкого агента

Каждый тип угроз обрабатывается отдельным функциональным компонентом Легкого агента. Вы можете включать, выключать и настраивать функциональные компоненты независимо друг от друга.

К компонентам защиты относятся следующие функциональные компоненты Легкого агента:

- **Файловый Антивирус** (см. раздел "**Защита файловой системы виртуальной машины. Файловый Антивирус**" на стр. 197) позволяет избежать заражения файловой системы операционной системы защищенной виртуальной машины. Компонент запускается при старте программы, постоянно находится в оперативной памяти и проверяет все открываемые,

сохраняемые и запускаемые файлы в операционной системе защищенной виртуальной машины. Файловый Антивирус перехватывает каждое обращение к файлу и проверяет этот файл на вирусы и другие вредоносные программы.

- **Почтовый Антивирус** (см. раздел "**Защита почты. Почтовый Антивирус**" на стр. 224) проверяет входящие и исходящие сообщения электронной почты на вирусы и другие вредоносные программы.
- **Веб-Антивирус** (см. раздел "**Защита веб-трафика виртуальной машины. Веб-Антивирус**" на стр. 237) проверяет входящий и исходящий веб-трафик защищенной виртуальной машины, а также проверяет веб-адреса по базам вредоносных и фишинговых веб-адресов.
- **Мониторинг системы** (на стр. 262) получает данные о действиях программ в операционной системе защищенной виртуальной машины и предоставляет эту информацию другим функциональным компонентам для более эффективной защиты. Мониторинг системы также может защищать папки общего доступа от внешнего шифрования, отслеживая операции, выполняемые с удаленного компьютера.
- **AMSI-защита** (на стр. 221) позволяет программам Microsoft Office и другим сторонним программам запрашивать проверку объектов на вирусы и другие угрозы, используя интерфейс Windows Antimalware Scan Interface (AMSI).

К компонентам контроля относятся следующие функциональные компоненты Легкого агента:

- **Контроль запуска программ** (на стр. 275) отслеживает попытки запуска программ пользователями и регулирует запуск программ.
- **Контроль активности программ** (на стр. 288) регистрирует действия, совершаемые программами в операционной системе защищенной виртуальной машины, и регулирует деятельность программ, исходя из того, к какой группе Контроль активности программ относит эту программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к персональным данным пользователя и ресурсам операционной системы. К персональным данным пользователя относятся файлы пользователя (папка "Документы", файлы cookie, данные об активности пользователя), а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.
- **Веб-Контроль** (на стр. 306) позволяет установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.
- **Контроль целостности системы** (на стр. 326) позволяет отслеживать изменения в операционной системе защищенной виртуальной машины.

Работа компонентов контроля основана на *правилах*:

- Контроль запуска программ использует в своей работе правила контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. 277).
- Контроль активности программ использует в своей работе правила контроля программ (см. раздел "Работа с правилами контроля программ" на стр. 293).
- Веб-Контроль использует в своей работе правила доступа к веб-ресурсам (см. раздел "О правилах доступа к веб-ресурсам" на стр. 307).
- Контроль целостности системы использует в своей работе правила контроля целостности системы (см. раздел "Создание и изменение правила контроля целостности системы" на стр. 332).

Набор функциональных компонентов Легкого агента, которые вы можете использовать на виртуальной машине, зависит от гостевой операционной системы виртуальной машины:

- На виртуальную машину с операционной системой Microsoft Windows для рабочих станций вы можете установить следующие функциональные компоненты:

- все компоненты защиты;
- компоненты контроля, кроме Контроля целостности системы.

Для установки сертифицированной версии программы вам нужно исключить из установки на виртуальную машину с операционной системой Microsoft Windows для рабочих станций компоненты Сетевой экран, Защита от сетевых атак и Контроль устройств.

Не поддерживается установка и работа функционального компонента AMSI-защита (на стр. 221) на виртуальных машинах с гостевыми операционными системами ниже Windows 10.

- На виртуальную машину с операционной системой Microsoft Windows для серверов вы можете установить следующие функциональные компоненты:
  - компоненты защиты:
    - Файловый Антивирус;
    - Почтовый Антивирус;
    - Мониторинг системы;
    - AMSI-защита;
  - компоненты контроля:
    - Контроль запуска программ;
    - Контроль целостности системы.

Для установки сертифицированной версии программы вам нужно исключить из установки на виртуальную машину с операционной системой Microsoft Windows для серверов компоненты Сетевой экран и Защита от сетевых атак.

Не поддерживается установка и работа функционального компонента AMSI-защита (на стр. 221) на виртуальных машинах с гостевыми операционными системами ниже Windows Server 2016.
Функциональный компонент Контроль целостности системы (см. раздел "Контроль целостности системы" на стр. 326) работает только на виртуальных машинах с файловой системой NTFS или FAT32.

- На виртуальную машину с операционной системой Linux вы можете установить только компонент защиты Файловый Антивирус.

Дополнительные функции программы

Программа Kaspersky Security содержит ряд дополнительных функций. Дополнительные функции предусмотрены для поддержки программы в актуальном состоянии, расширения возможностей

использования программы, для оказания помощи в работе.

- **Лицензирование** (см. раздел "**О лицензии**" на стр. 79). Использование программы по коммерческой лицензии обеспечивает полнофункциональную работу программы, доступ к обновлению баз программы, получение подробной информации о программе, а также помощь специалистов Службы технической поддержки "Лаборатории Касперского".
- **Обновление баз программы** (на стр. 390). Программа Kaspersky Security загружает обновленные базы программы, которые обеспечивают актуальность защиты операционной системы защищенной виртуальной машины от вирусов и других вредоносных программ.
- **Kaspersky Security Network** (см. раздел "**Участие в Kaspersky Security Network**" на стр. 399). Участие в Kaspersky Security Network позволяет повысить эффективность защиты операционной системы виртуальной машины за счет использования информации о репутации файлов, веб-ресурсов и программного обеспечения, полученной от пользователей во всем мире.
- **Managed Detection and Response** (на стр. 388). Взаимодействие с решением Kaspersky Managed Detection and Response позволяет осуществлять непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.
- **Интеграция с Kaspersky Endpoint Agent**. Вы можете установить программу Kaspersky Endpoint Agent на виртуальной машине с установленным компонентом Легкий агент для Windows. Программа Kaspersky Endpoint Agent обеспечивает взаимодействие между программой Kaspersky Security и решениями "Лаборатории Касперского", предназначенными для обнаружения сложных угроз.
- **Резервное хранилище** (на стр. 417). Если в ходе антивирусной проверки операционной системы защищенной виртуальной машины программа обнаруживает зараженный файл, она блокирует этот файл и удаляет его из папки исходного размещения. Копии вылеченных и удаленных файлов программа помещает в *резервное хранилище*.
- **Отчеты** (см. раздел "**События, уведомления и отчеты**" на стр. 422). В процессе работы программы для каждого функционального компонента и задачи программы формируется отчет. Отчет содержит список событий, произошедших во время работы программы, и всех выполненных программой операций. В случае возникновения проблем отчеты можно отправлять в "Лабораторию Касперского", чтобы специалисты Службы технической поддержки могли подробнее изучить ситуацию.
- **Уведомления** (см. раздел "**События, уведомления и отчеты**" на стр. 422). С помощью уведомлений программа информирует о текущем состоянии защиты операционной системы защищенной виртуальной машины. Программа может отображать уведомления на экране или отправлять по электронной почте.
- **Поддержка** (см. раздел "**Обращение в Службу технической поддержки**" на стр. 503). Все зарегистрированные пользователи программы Kaspersky Security могут обращаться за помощью к специалистам Службы технической поддержки. Вы можете отправить запрос через портал Kaspersky CompanyAccount (см. раздел "Техническая поддержка через Kaspersky CompanyAccount" на стр. 504) на веб-сайте Службы технической поддержки или получить консультацию сотрудников по телефону (см. раздел "Техническая поддержка по телефону" на стр. 503).

kaspersky

Требования

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

В этом разделе

Требования к компонентам Kaspersky Security Center

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

- Kaspersky Security Center 15 Linux (взаимодействие с Сервером администрирования Kaspersky Security Center на базе Linux осуществляется с помощью Kaspersky Security Center Web Console);
- Kaspersky Security Center 14 Windows.
- Kaspersky Security Center 13 Windows;
- Kaspersky Security Center 12 Windows.

В этом документе описана работа с версией Kaspersky Security Center 13.

Для работы Kaspersky Security требуются следующие компоненты Kaspersky Security Center:

- Сервер администрирования.

  На Сервере администрирования должны быть настроены следующие службы:

  - Служба прокси-сервера активации – используется при активации программы Kaspersky Security. Настройка службы прокси-сервера активации выполняется в свойствах Сервера администрирования Kaspersky Security Center.
  - Служба прокси-сервера KSN – обеспечивает обмен данными между программой Kaspersky Security и Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 399). Настройка службы прокси-сервера KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center.

  Подробнее о службе прокси-сервера активации и службе прокси-сервера KSN см. в документации

Kaspersky Security Center.

- Консоль администрирования на основе MMC (далее также "Консоль администрирования") или Kaspersky Security Center Web Console.
- Агент администрирования. Агент администрирования осуществляет взаимодействие между Сервером администрирования и виртуальными машинами с установленной программой Kaspersky Security.

  Агент администрирования требуется установить на все виртуальные машины, которые вы хотите защищать (см. раздел "Установка Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 84).

  Агент администрирования не требуется устанавливать на SVM, так как Агент администрирования включен в состав образов SVM.

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 (см. раздел "Требования для установки Сервера интеграции" на стр. 20).

Требования для установки Сервера интеграции

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

- Windows Server 2022 Standard / Datacenter / Essentials;
- Windows Server 2019 Standard / Datacenter / Essentials.
- Windows Server 2016 Standard / Datacenter.
- Windows Server 2012 R2 Standard / Datacenter / Essentials.
- Windows Server 2012 Standard / Datacenter / Essentials.

На компьютере, на котором вы планируете установить Консоль Сервера интеграции, операционная система должна быть установлена в режиме Desktop experience.

Для работы Сервера интеграции, Консоли Сервера интеграции и плагинов управления Kaspersky Security требуется платформа Microsoft .NET Framework 4.6. Если платформа не установлена, при наличии доступа в интернет мастер установки компонентов Kaspersky Security предложит ее установить в ходе установки Сервера интеграции, Консоли Сервера интеграции и mmc-плагинов управления Kaspersky Security.

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

- четырехъядерный виртуальный процессор с частотой 2 ГГц;
- объем свободного места на диске:
  - для Консоли Сервера интеграции – 4 ГБ;
  - для Сервера интеграции – 4 ГБ;

- объем оперативной памяти:
  - для Консоли Сервера интеграции – 4 ГБ;
  - для Сервера интеграции – 4 ГБ.

В зависимости от размера виртуальной инфраструктуры может изменяться необходимый объем оперативной памяти и объем свободного места на диске. Для увеличения производительности работы Сервера интеграции рекомендуется 10 ГБ свободного места на диске.

Для работы командлетов PowerShell™ требуется Windows PowerShell 4.0. Командлет используется для замены самоподписанного SSL-сертификата Сервера интеграции. Замену рекомендуется выполнить после установки Сервера интеграции. (см. раздел "Установка mmc-плагинов управления Kaspersky Security и Сервера интеграции" на стр. 58) Для работы программы Kaspersky Security и защиты виртуальной инфраструктуры Windows PowerShell не требуется.

Требования к виртуальной инфраструктуре

Для работы программы Kaspersky Security в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров в зависимости от платформы виртуализации:

- **Платформа Microsoft Hyper-V**:
  - Гипервизор Microsoft Windows Server 2019 Hyper-V (Desktop experience / Core).
  - Гипервизор Microsoft Windows Server 2016 Hyper-V (Desktop experience / Core) со всеми доступными обновлениями.
  - Гипервизор Microsoft Windows Server 2012 R2 Hyper-V (Desktop experience / Core) со всеми доступными обновлениями.

  Поддерживается установка и работа программы на гипервизорах Microsoft Windows Server (Hyper-V), входящих в состав кластера гипервизоров под управлением службы Windows Failover Clustering. На узлах кластера должна быть включена технология Cluster Shared Volumes.
- **Платформа Citrix Hypervisor**: гипервизор Citrix Hypervisor 8.2 LTSR.
- **Платформа VMware vSphere™**:
  - Гипервизор VMware ESXi™ 7.0 с последними обновлениями.
  - Гипервизор VMware ESXi 6.7 с последними обновлениями.
  - Гипервизор VMware ESXi 6.5 с последними обновлениями.

  Для развертывания и работы Kaspersky Security в виртуальной инфраструктуре VMware должен быть установлен сервер управления виртуальной инфраструктурой VMware vCenter Server® 7.0, VMware vCenter Server 6.7 или VMware vCenter Server 6.5 со всеми доступными обновлениями. Поддерживается установка и работа программы в инфраструктуре под управлением как автономных серверов VMware vCenter Server, так и группы серверов VMware vCenter Server, работающих в режиме Linked mode.

  При защите виртуальных машин в инфраструктуре VMware программа Kaspersky Security может использовать в своей работе VMware NSX™ Manager™ одного из следующих типов:
  - VMware NSX-V Manager из пакета VMware NSX Data Center for vSphere 6.4.6.
  - VMware NSX-T Manager из пакета VMware NSX-T Data Center 3.0.0.
  - VMware NSX-T Manager из пакета VMware NSX-T Data Center 2.5.1.

Если используется VMware NSX Manager, то Kaspersky Security может назначать теги безопасности (Security Tags) (см. раздел "О тегах безопасности (Security Tags)" на стр. 163) защищенным виртуальным машинам.

Не поддерживается одновременное использование VMware NSX-V Manager и VMware NSX-T Manager для одного VMware vCenter Server.

- **Платформа KVM (Kernel-based Virtual Machine)**: гипервизор KVM на базе одной из следующих операционных систем:
  - Ubuntu Server 20.04 LTS.
  - Ubuntu Server 18.04 LTS.
  - Red Hat® Enterprise Linux® Server 7.9.
  - CentOS 7.9.

  Для развертывания SVM на гипервизорах KVM под управлением операционной системы CentOS требуется удалить или закомментировать строку Defaults requiretty в конфигурационном файле /etc/sudoers операционной системы гипервизора.

  При защите виртуальных машин в инфраструктуре KVM программа Kaspersky Security может использовать в своей работе VMware NSX-T Manager одной из следующих версий:
  - VMware NSX-T Manager из пакета VMware NSX-T Data Center 3.0.0.
  - VMware NSX-T Manager из пакета VMware NSX-T Data Center 2.5.1.

  Если используется VMware NSX-T Manager, то Kaspersky Security может назначать теги безопасности (Security Tags) (см. раздел "О тегах безопасности (Security Tags)" на стр. 163) защищенным виртуальным машинам.
- **Платформа Proxmox VE**:
  - Гипервизор Proxmox VE 6.4.
  - Гипервизор Proxmox VE 6.3.

  Поддерживается только Proxmox VE на базе KVM. Не поддерживается работа программы на гипервизоре Proxmox VE с использованием LXC (Linux Containers).
- **Платформа Скала-Р**: гипервизор Р-Виртуализация 7.0.13.

  Для развертывания и работы SVM (виртуальная машина защиты) на гипервизорах Р-Виртуализация в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой Скала-Р Управление 1.80.
- **Платформа HUAWEI FusionSphere**: гипервизор HUAWEI FusionCompute CNA 8.0.

  Для развертывания и работы SVM (виртуальная машина защиты) на гипервизорах HUAWEI FusionCompute CNA в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой HUAWEI FusionCompute VRM 8.0.
- **Платформа Nutanix Acropolis**: гипервизор Nutanix AHV 5.19.1.

  Для развертывания и работы SVM (виртуальная машина защиты) на гипервизорах Nutanix AHV в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой Nutanix Prism версии 5.19.1 и выше.

- **Платформа Enterprise Cloud Platform VeiL**: гипервизор VeiL Node 4.5.

  Имеются ограничения в установке и работе программы в виртуальной инфраструктуре Enterprise Cloud Platform VeiL. Подробнее см. в Базе знаний (https://support.kaspersky.ru/15719).

- **Платформа SharxBase**: гипервизор SharxBase 5.10.

  Имеются ограничения в установке и работе программы в виртуальной инфраструктуре SharxBase. Подробнее см. в Базе знаний (https://support.kaspersky.ru/15719).

Для развертывания SVM на гипервизорах Microsoft Windows Server (Hyper-V) и VMware ESXi вы можете использовать сервер управления виртуальной инфраструктурой Microsoft System Center Virtual Machine Manager (далее "Microsoft SCVMM") одной из следующих версий:

- Microsoft SCVMM 2019 с последними обновлениями.
- Microsoft SCVMM 2016 с последними обновлениями.
- Microsoft SCVMM 2012 R2 с последними обновлениями.
- **Платформа Альт Сервер Виртуализации.**

  Для установки и работы программного изделия требуется платформа Альт Сервер Виртуализации версии 10.0. В составе платформы должен быть установлен базовый гипервизор платформы Альт Сервер Виртуализации 10.0 (гипервизор на базе KVM).

- **Платформа Программный комплекс средств виртуализации Брест.**

  Для установки и работы программного изделия требуется платформа Программный комплекс средств виртуализации Брест версии 2.9 или 3.2. В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

- **Среда виртуализации zVirt.**

  Для установки и работы программного изделия в виртуальной инфраструктуре должен быть установлен гипервизор zVirt Node 3.1, 3.3 или 4.0.

- **Платформа Система управления средой виртуализации ROSA Virtualization.**

  Для установки и работы программного изделия требуется платформа Система управления средой виртуализации ROSA Virtualization версии 2.1. В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

- **Платформа РЕД Виртуализация.**

  Для установки и работы программного изделия требуется платформа РЕД Виртуализация версии 7.3. В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

- **Платформа Astra Linux.**

  Для установки и работы программного изделия требуется платформа Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) с установленным обновлением Бюллетень № 2022-1221SE17MD (оперативное обновление 1.7.3.UU.1). В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

  Имеются ограничения в установке и работе программного изделия в виртуальной инфраструктуре. Подробнее в Базе знаний (https://support.kaspersky.ru/15809).

Требования к ресурсам SVM с Сервером защиты Kaspersky Security

Для функционирования программы для SVM требуется выделить следующее минимальное количество системных ресурсов:

- двухъядерный виртуальный процессор;
- объем свободного места на диске – 30 ГБ;
- объем оперативной памяти – 2 ГБ;
- виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Требования к виртуальной машине для установки Легкого агента для Windows

Для установки и функционирования Легкого агента для Windows виртуальная машина должна удовлетворять следующим минимальным аппаратным требованиям:

- виртуальный процессор с частотой 1,5 ГГц;
- объем свободного места на диске – 2 ГБ;
- объем оперативной памяти – 2 ГБ;
- виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора Citrix Hypervisor должна быть установлена программа XenTools.

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора VMware ESXi должен быть установлен пакет VMware Tools™.

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора HUAWEI FusionCompute CNA должен быть установлен пакет HUAWEI Tools.

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора Microsoft Windows Server (Hyper-V) должен быть установлен пакет служб интеграции (Integration Services).

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора KVM должен быть установлен пакет qemu-guest-agent

Для установки и функционирования Легкого агента для Windows на виртуальной машине должна быть установлена одна из следующих гостевых операционных систем:

- Windows 11 21H2 Pro / Enterprise / Education.
- Windows 10 Desktop Pro / Enterprise / 2016 LTSC / 2019 LTSC / 19H1 / 19H2 / 20H1 / 20H2 (32 / 64-разрядная).
- Windows 8.1 Update 1 Professional / Enterprise (32 / 64-разрядная).
- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-разрядная).
- Windows Server 2022 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2019 Standard / Datacenter (Desktop experience / Core).

- Windows Server 2016 Standard / Datacenter (Desktop experience / Core).
- Windows Server 2012 R2 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2012 Standard / Datacenter / Essentials (Desktop experience / Core).
- Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (Desktop experience / Core).

Набор функциональных компонентов Легкого агента, которые вы можете использовать на виртуальной машине, зависит от гостевой операционной системы виртуальной машины.

Во избежание задержек процесса установки программы на операционных системах Windows 7 и Windows Server 2008 R2 убедитесь, что операционная система Windows автоматически обновляет списки доверенных и недоверенных (отозванных) сертификатов поставщиков программного обеспечения через интернет посредством Windows Update. Для систем, не имеющих доступа к Windows Update, или систем, на которых автоматическое обновление списков доверенных и недоверенных сертификатов отключено, требуется обеспечить актуальность этих списков вручную согласно рекомендациям Microsoft, описанным на сайте технической поддержки Microsoft: https://support.microsoft.com/en-us/kb/2677070 и https://support.microsoft.com/en-us/kb/2813430.

Легкий агент для Windows может защищать виртуальные машины в составе инфраструктуры, в которой используются следующие решения для виртуализации:

- Citrix Virtual Apps and Desktops 7 1912 LTSR с последними установленными обновлениями.
- Citrix XenApp and XenDesktop 7.15 LTSR с последними установленными обновлениями.
- Citrix Provisioning 7 1912 LTSR с последними установленными обновлениями.
- Citrix Provisioning Services 7.15 LTSR с последними установленными обновлениями.
- VMware Horizon™ 8.2 (2103).
- VMware App Volumes (2103).
- HUAWEI FusionAccess 8.0.

Если вы используете указанные решения для виртуализации, вам нужно настроить на золотом образе рекомендованные исключения, указанные на странице программы в Базе знаний (https://support.kaspersky.ru/14049#block2).

Требования к виртуальной машине для установки Легкого агента для Linux

Для установки и функционирования Легкого агента для Linux виртуальная машина должна удовлетворять следующим минимальным аппаратным требованиям:

- виртуальный процессор с частотой 1,5 ГГц;
- объем свободного места на диске – 2 ГБ;
- объем оперативной памяти – 2 ГБ;
- виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Программные требования для установки и функционирования Легкого агента для Linux:

- интерпретатор языка Perl версии 5.0 или выше (http://www.perl.org);
- утилита which;
- установленный пакет dmidecode;
- для выполнения процедуры удаленной установки Легкого агента для Linux требуется установленный пакет sudo.

Если операционная система не поддерживает технологию fanotify, для обработки операций над объектами файловой системы потребуется компиляция модуля ядра операционной системы Linux. Для этого на виртуальной машине должен находиться исходный код ядра операционной системы и установленные пакеты для компиляции (gcc, binutils, glibc, glibc-devel, make, ld).

Перед установкой Легкого агента для Linux на виртуальной машине под управлением гипервизора Citrix Hypervisor должна быть установлена программа XenTools.

Перед установкой Легкого агента для Linux на виртуальной машине под управлением гипервизора VMware ESXi должен быть установлен пакет VMware Tools.

Перед установкой Легкого агента для Linux на виртуальной машине под управлением гипервизора HUAWEI FusionCompute CNA должен быть установлен пакет HUAWEI Tools.

Перед установкой Легкого агента для Linux на виртуальной машине под управлением гипервизора Microsoft Windows Server (Hyper-V) должен быть установлен пакет служб интеграции (Integration Services).

Для установки и функционирования Легкого агента для Linux на виртуальной машине должна быть установлена одна из следующих гостевых операционных систем для серверов:

- Debian GNU / Linux 10.7 (32 / 64-разрядная).
- Debian GNU / Linux 9.13 (32 / 64-разрядная).
- Ubuntu Server 20.04 LTS (64-разрядная).
- Ubuntu Server 18.04 LTS (64-разрядная).
- CentOS 8.1 (64-разрядная).
- CentOS 8.3 (64-разрядная).
- CentOS 7.9 (64-разрядная).
- Red Hat Enterprise Linux Server 8.3 (64-разрядная).
- Red Hat Enterprise Linux Server 7.9 (64-разрядная)
- SUSE Linux Enterprise Server 15 SP2 (64-разрядная).
- Альт 8 СП (64-разрядная).
- РЕД ОС 7.3 (64-разрядная).
- Oracle® Linux 8.3 (64-разрядная).
- Oracle Linux 7.9 (64-разрядная).
- Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) (без поддержки режимов Мандатного разграничения доступа и

Замкнутой программной среды).

- Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды).

Перед установкой Легкого агента для Linux на виртуальной машине с операционной системой Oracle Linux требуется установить архиватор tar.

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с

последующей блокировкой попыток аутентификации при превышении установленного значения.

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

Подготовка к установке программы

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

Общие действия

- Проверить состав компонентов Kaspersky Security Center (см. раздел "Требования к компонентам Kaspersky Security Center" на стр. 19), а также соответствие компонентов Kaspersky Security Center и компонентов виртуальной инфраструктуры аппаратным и программным требованиям программы Kaspersky Security (см. раздел "Требования" на стр. 19).
- Убедиться в том, что на виртуальных машинах, которые вы планируете защищать с помощью Kaspersky Security, не установлено антивирусное программное обеспечение.
- Подготовить файлы, необходимые для установки программы:
  a. Загрузить с веб-сайта "Лаборатории Касперского" файл, необходимый для запуска мастера установки компонентов Kaspersky Security (см. раздел "Файлы, необходимые для установки программы" на стр. 31).
  b. Подготовить образы SVM с компонентом Сервер защиты (см. раздел "Подготовка образов SVM" на стр. 39) и разместить в одной папке на компьютере, где установлена Консоль администрирования Kaspersky Security Center, или в одной папке на сетевом ресурсе, к которому учетная запись пользователя, выполняющего установку, имеет доступ на чтение.
  c. Если для установки Легкого агента вы не планируете использовать автоматически созданные инсталляционные пакеты, с помощью мастера установки компонентов Kaspersky Security распаковать файлы, необходимые для установки Легкого агента для Windows и Легкого агента для Linux (см. раздел "Распаковка дистрибутивов Легкого агента" на стр. 34).
- Убедиться в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика между виртуальными машинами, разрешено прохождение сетевого трафика через порты, используемые при установке и работе программы (см. раздел "Настройка портов, используемых программой" на стр. 35).
- Если в сети используется динамическая IP-адресация, обеспечить возможность маршрутизации сетевого трафика от SVM до компьютера, на котором установлен Сервер администрирования Kaspersky Security Center.
- Установить последние обновления Windows перед началом установки Легкого агента для Windows, Сервера интеграции, Консоли Сервера интеграции и плагинов управления Kaspersky Security.
- Если вы хотите, чтобы виртуальные машины с установленными компонентами Kaspersky Security автоматически перемещались в группы администрирования после установки программы, создать группы администрирования в Консоли администрирования Kaspersky Security Center и настроить правила автоматического перемещения виртуальных машин в группы администрирования (см. раздел "Настройка правил перемещения виртуальных машин в группы администрирования" на стр. 55).

Для обеспечения безопасного соединения между программой и гипервизором рекомендуется использовать алгоритм шифрования AES256 для шифрования входящих соединений на гипервизоре по протоколам TLS, SSH и другим подобным.

Дополнительные действия для платформы Microsoft Hyper-V

В виртуальной инфраструктуре на платформе Microsoft Hyper-V вам нужно также выполнить следующие действия перед началом установки программы Kaspersky Security:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлен пакет служб интеграции (Integration Services).
- Убедиться в том, что на гипервизоре включен общий сетевой ресурс ADMIN$. На гипервизорах Microsoft Windows Server 2012 R2 Hyper-V для включения общего сетевого ресурса ADMIN$ требуется предварительно установить роль файлового сервера (File Server) с помощью мастера настройки сервера.
- Убедиться в том, что на диске, на котором находится общий сетевой ресурс ADMIN$, достаточно места для размещения образа SVM. В ходе установки компонента Сервер защиты образ SVM копируется на общий сетевой ресурс ADMIN$, затем оттуда переносится в папку, указанную в ходе развертывания SVM.
- Убедиться в том, что на гипервизорах, не входящих в домен Active Directory®, установлено программное обеспечение удаленного управления Windows Remote Management (WinRM) версии 3.0. Windows Remote Management (WinRM) версии 3.0 входит в состав инсталляционного пакета Windows Management Framework 3.0, доступного для загрузки с сайта Microsoft: http://www.microsoft.com/en-us/download/details.aspx?id=34595.
- Если вы хотите использовать доменную учетную запись для подключения Сервера интеграции к гипервизору, требуется убедиться, что выполняются следующие условия:
  - Сервер интеграции имеет возможность определять адрес гипервизора с помощью службы доменных имен (DNS) того домена, в котором находится гипервизор, на котором разворачивается SVM.
  - DNS-сервер имеет прямую и обратную записи для Сервера интеграции.
  - Зоны, содержащие записи о Сервере интеграции и гипервизоре, на котором развернута SVM, интегрированы с Active Directory.
  - Компьютер, с которого выполняется развертывание SVM, имеет возможность разрешать имена гипервизоров, на которых разворачивается SVM.
- Если вы хотите, чтобы имя пользователя и пароль учетной записи для подключения к гипервизору, указываемые во время развертывания SVM, передавались в зашифрованном виде, вы можете настроить защищенное соединение с использованием SSL-сертификата между гипервизором, на котором будет развернута SVM, и компьютером, где установлена Консоль администрирования Kaspersky Security Center.

Дополнительные действия для платформы VMware vSphere

В виртуальной инфраструктуре на платформе VMware vSphere вам нужно также выполнить следующие действия перед началом установки программы Kaspersky Security:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлен пакет VMware Tools.
- Если при подключении компьютера, на котором установлена Консоль администрирования Kaspersky Security Center, к серверу VMware vCenter Server используется прокси-сервер, требуется убедиться в том, что виртуальные машины доступны через прокси-сервер.

Дополнительные действия для платформы Citrix Hypervisor

В виртуальной инфраструктуре на платформе Citrix Hypervisor перед началом установки программы

Kaspersky Security вам нужно убедиться, что на виртуальных машинах, которые вы хотите защищать, установлена программа XenTools.

Дополнительные действия для платформы Proxmox VE

В виртуальной инфраструктуре на платформе Proxmox VE перед началом установки программы Kaspersky Security вам нужно убедиться, что в директории /var/tmp имеется не менее 30 Гб свободного места.

Дополнительные действия для платформы HUAWEI FusionSphere

В виртуальной инфраструктуре на платформе HUAWEI FusionSphere перед началом установки программы Kaspersky Security вам нужно убедиться, что на виртуальных машинах, которые вы хотите защищать, установлен пакет HUAWEI Tools.

Дополнительные действия для платформы Astra Linux

Перед началом установки программы в виртуальной инфраструктуре на платформе Astra Linux вам нужно настроить конфигурацию учетной записи, которая будет использоваться для развертывания, удаления и изменения конфигурации SVM., следующим образом:

- Выполните команду:

$ sudo usermod -a -G kvm,libvirt,libvirt-qemu,libvirt-admin <имя_пользователя>

- Откройте конфигурационный файл sudoers с помощью команды:

sudo visudo

- Укажите в файле:

<имя пользователя> ALL = (ALL) NOPASSWD: ALL

где <имя пользователя> – имя учетной записи, которая будет использоваться для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM.

- Сохраните и закройте файл sudoers.

В этом разделе

Файлы, необходимые для установки программы

Этот раздел содержит перечень файлов, которые необходимы для установки компонентов программы Kaspersky Security.

Мастер установки компонентов Kaspersky Security

Мастер установки компонентов Kaspersky Security требуется для решения следующих задач:

- установка mmc-плагинов управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции (см. раздел "Установка mmc-плагинов управления Kaspersky Security и Сервера интеграции" на стр. 58);
- распаковка в выбранную папку файлов (см. раздел "Распаковка дистрибутивов Легкого агента" на стр. 34), необходимых для установки Легкого агента для Windows и Легкого агента для Linux.

Для запуска мастера установки компонентов Kaspersky Security требуется файл ksvla-components_5.2.X.X_mlg.exe, где 5.2.X.X – номер версии программы.

Mmc-плагины управления Kaspersky Security и Сервер интеграции

Установка mmc-плагинов управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции выполняется с помощью мастера установки компонентов Kaspersky Security (см. раздел "Установка mmc-плагинов управления Kaspersky Security и Сервера интеграции" на стр. 58). Вам нужно разместить файл ksvla-components_5.2.X.X_mlg.exe на компьютере, где установлена программа Kaspersky Security Center.

Сервер защиты

Для установки Сервера защиты (см. раздел "Установка Сервера защиты" на стр. 66) требуется файл образа SVM и файл описания образов (файл в формате XML).

Образы SVM для развертывания на гипервизорах разных типов и файлы описания образов вам нужно создать в ходе подготовки к установке программы (см. раздел "Подготовка образов SVM" на стр. 39).

Файл образа SVM и файл описания образов (файл в формате XML) требуется разместить в одной папке на компьютере, где установлена Консоль администрирования Kaspersky Security Center, или в одной папке на сетевом ресурсе, к которому учетная запись пользователя, выполняющего установку, имеет доступ на чтение. Если вы хотите установить Сервер защиты на гипервизоры разных типов, в одной папке требуется разместить файлы образов SVM для каждого типа гипервизоров и файл описания образов.

Легкий агент для Windows

Файлы, необходимые для установки компонента Легкий агент для Windows, входят в состав мастера установки компонентов Kaspersky Security.

В ходе установки плагинов управления Kaspersky Security и Сервера интеграции на компьютере, где установлен Сервер администрирования Kaspersky Security Center, мастер установки компонентов Kaspersky Security автоматически создает в Kaspersky Security Center инсталляционный пакет для удаленной установки Легкого агента для Windows (см. раздел "Установка Легкого агента для Windows через Kaspersky Security Center" на стр. 85). Этот инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** -> **Удаленная установка** -> **Инсталляционные пакеты** под именем **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows (5.2.X.X)**, где 5.2.X.X – номер версии программы.

С помощью мастера вы также можете распаковать в выбранную папку дистрибутив Легкого агента для Windows (см. раздел "Распаковка дистрибутивов Легкого агента" на стр. 34). Для запуска мастера вам требуется файл ksvla-components_5.2.X.X_mlg.exe.

Дистрибутив Легкого агента для Windows содержит следующие файлы:

- incompatible.txt – файл содержит список программ, несовместимых с программой Kaspersky Security. Этот список используется при установке Легкого агента для Windows.
- ksvla.kud – файл описания программы. Вы можете использовать этот файл в качестве дистрибутива

при создании инсталляционного пакета Легкого агента для Windows вручную в Kaspersky Security Center (см. раздел "Создание инсталляционного пакета Легкого агента для Windows" на стр. 86).

- ksvla_x64.msi – инсталляционный пакет в формате MSI для установки Легкого агента для Windows на 64-разрядную операционную систему. Вы можете использовать этот файл при установке Легкого агента из командной строки или с помощью механизма групповых политик службы каталогов (Active Directory Group Policies).
- ksvla_x86.msi – инсталляционный пакет в формате MSI для установки Легкого агента для Windows на 32-разрядную операционную систему. Вы можете использовать этот файл при установке Легкого агента из командной строки или с помощью механизма групповых политик службы каталогов (Active Directory Group Policies).
- license.txt – файл содержит текст Лицензионного соглашения, в котором указано, на каких условиях вы можете пользоваться программой, и Политики конфиденциальности, которая описывает обработку и передачу данных. Этот файл используется при установке Легкого агента для Windows.
- setup.exe – вы можете использовать этот файл для запуска мастера установки Легкого агента для Windows.

Легкий агент для Linux

Файлы, необходимые для установки компонента Легкий агент для Linux, входят в состав мастера установки компонентов Kaspersky Security.

В ходе установки плагинов управления Kaspersky Security и Сервера интеграции на компьютере, где установлен Сервер администрирования Kaspersky Security Center, мастер установки компонентов Kaspersky Security автоматически создает в Kaspersky Security Center инсталляционный пакет для удаленной установки Легкого агента для Linux (см. раздел "Установка Легкого агента для Linux через Kaspersky Security Center" на стр. 98). Этот инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** -> **Удаленная установка** -> **Инсталляционные пакеты** под именем **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux (5.2.X.X)**, где 5.2.X.X – номер версии программы.

С помощью мастера вы также можете распаковать в выбранную папку дистрибутив Легкого агента для Linux (см. раздел "Распаковка дистрибутивов Легкого агента" на стр. 34). Дистрибутив содержит файлы, необходимые для всех способов установки Легкого агента для Linux. Для запуска мастера вам требуется файл ksvla-components_5.2.X.X_mlg.exe.

Дистрибутив Легкого агента для Linux содержит следующие файлы:

- license.txt – файл содержит текст Лицензионного соглашения, в котором указано, на каких условиях вы можете пользоваться программой, и Политики конфиденциальности, которая описывает обработку и передачу данных. Этот файл используется при установке Легкого агента для Linux.
- lightagent.ini – конфигурационный файл первоначальной настройки.
- lightagent.kud – файл описания программы. Вы можете использовать этот файл в качестве дистрибутива при создании инсталляционного пакета Легкого агента для Linux вручную в Kaspersky Security Center (см. раздел "Создание инсталляционного пакета Легкого агента для Linux" на стр. 100).
- lightagent-5.2.X-X-bundle.sh, где 5.2.X-X – номер версии программы. Вы можете использовать этот самораспаковывающийся shar-архив для установки Легкого агента для Linux из командной строки (см. раздел "Установка Легкого агента для Linux из командной строки" на стр. 93).

  Архив lightagent-5.2.X-X-bundle.sh содержит скрипт установки и пакеты, необходимые для установки Легкого агента для Linux и Агента администрирования Kaspersky Security Center.

Агент администрирования Kaspersky Security Center

Для взаимодействия компонентов Легкий агент, установленных на виртуальных машинах, с Kaspersky Security Center вам требуется установить Агент администрирования на виртуальные машины, где будет установлен Легкий агент (см. раздел "Установка Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 84). Агент администрирования не требуется устанавливать на SVM, так как этот компонент включается в состав образов SVM.

На виртуальной машине с операционной системой Windows вы можете установить Агент администрирования, который входит в комплект поставки программы Kaspersky Security Center версии 13 или 12.

На виртуальной машине с компонентом Легкий агент для Linux должен быть установлен Агент администрирования Kaspersky Security Center, который входит в комплект поставки программы Kaspersky Security для виртуальных сред 5.2 Легкий агент:

- Пакет для установки Агента администрирования входит в состав shar-архива, который используется для установки Легкого агента для Linux из командной строки (см. раздел "Установка Легкого агента для Linux из командной строки" на стр. 93).
- Агент администрирования входит в состав инсталляционного пакета для удаленной установки Легкого агента для Linux (см. раздел "Установка Легкого агента для Linux через Kaspersky Security Center" на стр. 98), автоматически созданного мастером установки компонентов Kaspersky Security. Если вы создаете инсталляционный пакет для Легкого агента для Linux вручную (см. раздел "Создание инсталляционного пакета Легкого агента для Linux" на стр. 100), Агент администрирования также будет включен в состав этого пакета.

Распаковка дистрибутивов Легкого агента

Мастер установки компонентов Kaspersky Security содержит дистрибутивы Легкого агента для Windows и Легкого агента для Linux. С помощью мастера вы можете распаковать в указанную папку файлы, необходимые для всех способов установки Легкого агента для Windows (см. раздел "Установка Легкого агента для Windows через Kaspersky Security Center" на стр. 85) и Легкого агента для Linux (см. раздел "Установка Легкого агента для Linux" на стр. 92).

Для удаленной установки Легкого агента для Windows и Легкого агента для Linux вы можете использовать инсталляционные пакеты, которые создаются автоматически в результате установки плагинов управления Kaspersky Security и Сервера интеграции (см. раздел "Установка mmc-плагинов управления Kaspersky Security и Сервера интеграции" на стр. 58) на компьютере, где установлен Сервер администрирования Kaspersky Security Center.

► *Чтобы распаковать дистрибутивы Легкого агента, выполните следующие действия:*

1. Запустите файл ksvla-components_5.2.X.X_mlg.exe, где 5.2.X.X – номер версии программы. Этот файл входит в комплект поставки (см. раздел "Файлы, необходимые для установки программы" на стр. 31).

   Запустится мастер установки компонентов Kaspersky Security.
2. На первом шаге в окне мастера отображается язык локализации мастера и компонентов Kaspersky Security – русский. Перейдите к следующему шагу мастера.
3. Выберите действие **Распаковать дистрибутивы Легкого агента** и перейдите к следующему шагу

мастера.

4. Выберите папку, в которую мастер поместит файлы, необходимые для установки Легкого агента для Windows и Легкого агента для Linux, и перейдите к следующему шагу мастера.

   Начнется распаковка дистрибутивов. Дождитесь завершения работы мастера.

   После окончания распаковки вы можете открыть папку распаковки по ссылке, расположенной в окне.

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

Информация о работе мастера записывается в файлы трассировки мастера установки компонентов Kaspersky Security (см. раздел "О файлах трассировки мастера установки компонентов Kaspersky Security" на стр. 509). Если работа мастера завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Настройка портов, используемых программой

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

Таблица 1. Порты, используемые программой

Порт и протокол	Направление	Назначение и описание
80 TCP 443 TCP	От мастера управления SVM к VMware vCenter Server.	Мастер, с помощью которого выполняется установка, обновление и удаление компонента Сервер защиты, а также изменение конфигурации SVM. Запускается из Консоли Сервера интеграции. Для развертывания SVM на гипервизоре VMware ESXi с помощью VMware vCenter Server.
Secure virtual machine, виртуальная машина защиты. Виртуальная машина на гипервизоре, на которой установлен Сервер защиты, компонент программы Kaspersky Security. 443 TCP	От мастера управления SVM к гипервизору ESXi.	Для развертывания SVM на гипервизоре VMware ESXi с помощью VMware vCenter Server.
135 TCP / UDP 445 TCP / UDP	От мастера управления SVM к гипервизору Microsoft Windows Server (Hyper-V).	Для развертывания SVM на гипервизоре Microsoft Windows Server (Hyper-V).

Порт и протокол	Направление	Назначение и описание
80 TCP 443 TCP	От мастера управления SVM к гипервизору Citrix Hypervisor.	Для развертывания SVM на гипервизоре Citrix Hypervisor.
22 TCP	От мастера управления SVM к гипервизору KVM.	Для развертывания SVM на гипервизоре KVM.
22 TCP 8006 TCP	От мастера управления SVM к гипервизору Proxmox VE.	Для развертывания SVM на гипервизоре Proxmox VE.
7443 TCP	От мастера управления SVM к HUAWEI FusionCompute VRM.	Для развертывания SVM на гипервизоре HUAWEI FusionCompute CNA с помощью HUAWEI FusionCompute VRM.
8779 TCP	От мастера управления SVM к гипервизору HUAWEI FusionCompute CNA.	Для развертывания SVM на гипервизоре HUAWEI FusionCompute CNA с помощью HUAWEI FusionCompute VRM.
9440 TCP	От мастера управления SVM к Nutanix Prism Central.	Для развертывания SVM на гипервизоре Nutanix AHV в инфраструктуре под управлением Nutanix Prism Central.
9440 TCP	От мастера управления SVM к Nutanix Prism Element.	Для развертывания SVM на гипервизоре Nutanix AHV в инфраструктуре под управлением Nutanix Prism Element.
22 TCP	От мастера управления SVM к SVM.	Для изменения конфигурации SVM.
7271 TCP	От мастера управления SVM к Серверу интеграции.	Компонент программы Kaspersky Security. Осуществляет взаимодействие между компонентами программы Kaspersky Security и виртуальной инфраструктурой. Для добавления параметров подключения к гипервизору на Сервер интеграции.
80 TCP 443 TCP	От Сервера интеграции к VMware vCenter Server.	Для взаимодействия Сервера интеграции с гипервизором VMware ESXi с помощью VMware vCenter Server.
135 TCP / UDP 445 TCP / UDP 5985 TCP 5986 TCP	От Сервера интеграции к гипервизору Microsoft Windows Server (Hyper-V).	Для взаимодействия Сервера интеграции с гипервизором Microsoft Windows Server (Hyper-V).
80 TCP 443 TCP	От Сервера интеграции к гипервизору Citrix Hypervisor.	Для взаимодействия Сервера интеграции с гипервизором Citrix Hypervisor.
22 TCP	От Сервера интеграции к гипервизору KVM.	Для взаимодействия Сервера интеграции с гипервизором KVM.

Порт и протокол	Направление	Назначение и описание
8006 TCP	От Сервера интеграции к гипервизору Proxmox VE.	Для взаимодействия Сервера интеграции с гипервизором Proxmox VE.
7443 TCP	От Сервера интеграции к HUAWEI FusionCompute VRM.	Для взаимодействия Сервера интеграции с гипервизором HUAWEI FusionCompute CNA с помощью HUAWEI FusionCompute VRM.
9440 TCP	От Сервера интеграции к Nutanix Prism Central.	Для взаимодействия Сервера интеграции с гипервизором Nutanix AHV в инфраструктуре под управлением Nutanix Prism Central.
9440 TCP	От Сервера интеграции к Nutanix Prism Element.	Для взаимодействия Сервера интеграции с гипервизором Nutanix AHV в инфраструктуре под управлением Nutanix Prism Element.
8000 UDP	От SVM к Легкому агенту.	Компонент программы Kaspersky Security. Устанавливается на каждую виртуальную машину, которую требуется защищать. Для передачи Легким агентам информации о доступных SVM с использованием списка адресов SVM.
7271 TCP	От мастера управления SVM к Серверу интеграции.	Для добавления параметров подключения к гипервизору на Сервер интеграции.
7271 TCP	От SVM к Серверу интеграции.	Для взаимодействия SVM и Сервера интеграции.
7271 TCP	От Легкого агента к Серверу интеграции.	Для взаимодействия Легкого агента и Сервера интеграции.
8000 UDP	От Легкого агента к SVM.	Для получения Легким агентом информации о состоянии SVM.
11111 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение сведений о лицензии) от Легкого агента на SVM при незащищенном соединении.
11112 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение сведений о лицензии) от Легкого агента на SVM при защищенном соединении.
9876 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента на SVM при незащищенном соединении.
9877 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента на SVM при защищенном соединении.
80 TCP	От Легкого агента к SVM.	Для обновления баз программы на Легком агенте.

Порт и протокол	Направление	Назначение и описание
15000 UDP	От Kaspersky Security Center к SVM.	Для управления программой на SVM через Kaspersky Security Center.
13000 TCP	От SVM к Kaspersky Security Center.	Для управления программой на SVM через Kaspersky Security Center при защищенном соединении.
14000 TCP	От SVM к Kaspersky Security Center.	Для управления программой на SVM через Kaspersky Security Center при незащищенном соединении.
15000 UDP	От Kaspersky Security Center к Легким агентам.	Для управления программой на защищенных виртуальных машинах через Kaspersky Security Center.
Виртуальная машина, на которой установлен компонент Легкий агент. 13000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления программой на защищенных виртуальных машинах через Kaspersky Security Center при защищенном соединении.
14000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления программой на защищенных виртуальных машинах через Kaspersky Security Center при незащищенном соединении.

Во время установки Легкий агент выполняет настройку брандмауэра Windows, чтобы разрешить входящий и исходящий трафик для процесса avp.exe. Если для брандмауэра Windows используется доменная политика, требуется настроить правила для входящих и исходящих подключений для процесса avp.exe в доменной политике. Если используется другой брандмауэр, требуется настроить правило для подключений для процесса avp.exe для этого брандмауэра.

Если вы используете гипервизор Citrix Hypervisor или VMware ESXi и на сетевом адаптере гостевой операционной системы виртуальной машины включен беспорядочный режим (promiscuous mode), гостевая операционная система получает все Ethernet-фреймы, проходящие через виртуальный коммутатор, если это разрешено политикой VLAN. Этот режим может использоваться для мониторинга и анализа трафика в сегменте сети, в котором работают SVM и защищенные виртуальные машины. Если вы не настроили защиту соединения между SVM и защищенными виртуальными машинами (см. раздел "Защита соединения между Легким агентом и SVM" на стр. 172), трафик между SVM и защищенными виртуальными машинами не зашифрован и передается в открытом виде. В целях безопасности не рекомендуется использовать беспорядочный режим в сетевых сегментах с работающей SVM. Если такой режим необходим вам, например, для мониторинга трафика сторонними виртуальными машинами с целью выявления попыток несанкционированного доступа к сети и устранения сетевых неполадок, вам нужно настроить соответствующие ограничения, чтобы защитить трафик между SVM и защищенными виртуальными машинами от несанкционированного доступа.

Подготовка образов SVM

Программа Kaspersky Security поставляется в виде бинарных компонентов. Перед началом установки программы вам нужно создать образы SVM с компонентом Сервер защиты, используя поставляемые пакеты.

В результате формируется набор архивов для установки Сервера защиты на гипервизоры разных типов. Каждый архив содержит образ SVM и файл описания образов.

Аппаратные и программные требования для создания образа

- Гипервизоры VMware ESXi 6.0, VMware ESXi 6.5 или VMware ESXi 6.7.
- Минимум 4 ГБ оперативной памяти под виртуальную машину.
- Минимум 80 ГБ дискового пространства на виртуальной машине.

► *Чтобы создать образ SVM с компонентом Сервер защиты, выполните следующие действия:*

1. Создайте виртуальную машину с установленной операционной системой CentOS 7.6.
2. На созданной виртуальной машине войдите в систему под учетной записью root.
3. Установите VMware ovftool 4.3.0 (дистрибутив доступен по адресу https://www.vmware.com/support/developer/ovf).
4. Установите пакеты cmake (версии не ниже 3.0), dosfstools, openssl-devel, util-linux, device-mapper, psmisc, kpartx, e2fsprogs, parted, xmlsec1, libguestfs-tools, libguestfs-tools-c, virt-v2v, libvirt-daemon, libvirt-daemon-config-network.
5. Скопируйте архивы ksvla-svmbuild-5.2.27.348-3rd-party.tar.bz2 и ksvla-svmbuild-5.2.27.348-kl.tar.bz2 в пустую директорию на виртуальной машине и распакуйте их. Результатом будет являться набор следующих директорий и файлов.
   - centos – репозиторий, содержащий пакеты дистрибутива CentOS 7 (см. *Список 1*);
   - guest_tools – репозиторий, содержащий пакеты гостевых утилит, необходимых для поддержки гипервизоров на платформах: Microsoft Hyper-V, Citrix Hypervisor, VMware vSphere (см. *Список 2*);
   - kl – репозиторий, содержащий пакеты Сервера защиты, Агента администрирования и утилит, необходимых для сборки образов SVM (см. *Список 3*);
   - master – директория, содержащая скрипты и конфигурационные файлы, необходимые для сборки SVM;
   - nginx – репозиторий, содержащий пакеты Nginx (см. *Список 4*);
   - vm-tools – дистрибутивы гостевых утилит, необходимых для поддержки гипервизоров на платформах: Huawei FusionSphere, Citrix Hypervisor, Virtuozzo (см. *Список 5*);
   - build_ksvla_svm_52.sh – скрипт сборки SVM.
6. Поместите файл сертификата с именем cert.pem в директорию, в которую вы распаковали файлы.
7. Перейдите в директорию, в которую вы распаковали файлы, далее все пути будут указаны относительно нее.
8. Выполните команду `bash ./build_ksvla_svm_52.sh`.
9. Дождитесь успешного завершения команды.

В результате сборки будут созданы архивы, содержащие файлы образов SVM и файлы описания образов SVM (файлы в формате XML) для развертывания Сервера защиты на гипервизоры разных типов:

- ./build/ksvla-svm_kvm_proxmox-ve_skala-r_huawei-fusionsphere_5.2.27.348_mlg.zip
- ./build/ksvla-svm_citrix-hypervisor_5.2.27.348_mlg.zip
- ./build/ksvla-svm_microsoft-hyper-v_5.2.27.348_mlg.zip
- ./build/ksvla-svm_vmware-vsphere_5.2.27.348_mlg.zip

Список 1

acl-2.2.51-15.el7.x86_64.rpm

at-3.1.13-24.el7.x86_64.rpm

attr-2.4.46-13.el7.x86_64.rpm

audit-libs-2.8.5-4.el7.x86_64.rpm

audit-libs-python-2.8.5-4.el7.x86_64.rpm

autogen-libopts-5.18-5.el7.x86_64.rpm

avahi-libs-0.6.31-20.el7.x86_64.rpm

basesystem-10.0-7.el7.centos.noarch.rpm

bash-4.2.46-34.el7.x86_64.rpm

bc-1.06.95-13.el7.x86_64.rpm

bind-export-libs-9.11.4-26.P2.el7_9.5.x86_64.rpm

bind-libs-9.11.4-26.P2.el7_9.5.x86_64.rpm

bind-libs-lite-9.11.4-26.P2.el7_9.5.x86_64.rpm

bind-license-9.11.4-26.P2.el7_9.5.noarch.rpm

bind-utils-9.11.4-26.P2.el7_9.5.x86_64.rpm

binutils-2.27-44.base.el7.x86_64.rpm

bpftool-3.10.0-1160.31.1.el7.x86_64.rpm

bzip2-1.0.6-13.el7.x86_64.rpm

bzip2-libs-1.0.6-13.el7.x86_64.rpm

ca-certificates-2020.2.41-70.0.el7_8.noarch.rpm

centos-release-7-9.2009.1.el7.centos.x86_64.rpm

checkpolicy-2.5-8.el7.x86_64.rpm

chkconfig-1.7.6-1.el7.x86_64.rpm

chrpath-0.16-0.el7.x86_64.rpm

cifs-utils-6.2-10.el7.x86_64.rpm

cloud-init-19.4-7.el7.centos.4.x86_64.rpm

coreutils-8.22-24.el7_9.2.x86_64.rpm

cpio-2.11-28.el7.x86_64.rpm

cracklib-2.9.0-11.el7.x86_64.rpm

cracklib-dicts-2.9.0-11.el7.x86_64.rpm

cronie-1.4.11-23.el7.x86_64.rpm

cronie-anacron-1.4.11-23.el7.x86_64.rpm

crontabs-1.11-6.20121102git.el7.noarch.rpm

cryptsetup-libs-2.0.3-6.el7.x86_64.rpm

cups-libs-1.6.3-51.el7.x86_64.rpm

curl-7.29.0-59.el7_9.1.x86_64.rpm

cyrus-sasl-lib-2.1.26-23.el7.x86_64.rpm

dbus-1.10.24-15.el7.x86_64.rpm

dbus-libs-1.10.24-15.el7.x86_64.rpm

device-mapper-1.02.170-6.el7_9.5.x86_64.rpm

device-mapper-event-1.02.170-6.el7_9.5.x86_64.rpm

device-mapper-event-libs-1.02.170-6.el7_9.5.x86_64.rpm

device-mapper-libs-1.02.170-6.el7_9.5.x86_64.rpm

device-mapper-multipath-0.4.9-134.el7_9.x86_64.rpm

device-mapper-multipath-libs-0.4.9-134.el7_9.x86_64.rpm

device-mapper-persistent-data-0.8.5-3.el7_9.2.x86_64.rpm

dhclient-4.2.5-83.el7.centos.1.x86_64.rpm

dhcp-4.2.5-83.el7.centos.1.x86_64.rpm

dhcp-common-4.2.5-83.el7.centos.1.x86_64.rpm

dhcp-libs-4.2.5-83.el7.centos.1.x86_64.rpm

dialog-1.2-5.20130523.el7.x86_64.rpm

diffutils-3.3-5.el7.x86_64.rpm

dmidecode-3.2-5.el7_9.1.x86_64.rpm

dosfstools-3.0.20-10.el7.x86_64.rpm

dracut-033-572.el7.x86_64.rpm

e2fsprogs-1.42.9-19.el7.x86_64.rpm

e2fsprogs-libs-1.42.9-19.el7.x86_64.rpm

elfutils-default-yama-scope-0.176-5.el7.noarch.rpm

elfutils-libelf-0.176-5.el7.x86_64.rpm

elfutils-libs-0.176-5.el7.x86_64.rpm

ethtool-4.8-10.el7.x86_64.rpm

expat-2.1.0-12.el7.x86_64.rpm

file-5.11-37.el7.x86_64.rpm

file-libs-5.11-37.el7.x86_64.rpm

filesystem-3.2-25.el7.x86_64.rpm

findutils-4.5.11-6.el7.x86_64.rpm

fipscheck-1.4.1-6.el7.x86_64.rpm

fipscheck-lib-1.4.1-6.el7.x86_64.rpm

freetype-2.8-14.el7_9.1.x86_64.rpm

ftp-0.17-67.el7.x86_64.rpm

fuse-2.9.2-11.el7.x86_64.rpm

fuse-libs-2.9.2-11.el7.x86_64.rpm

gawk-4.0.2-4.el7_3.1.x86_64.rpm

gdb-7.6.1-120.el7.x86_64.rpm

gdbm-1.10-8.el7.x86_64.rpm

GeoIP-1.5.0-14.el7.x86_64.rpm

geoipupdate-2.5.0-1.el7.x86_64.rpm

gettext-0.19.8.1-3.el7.x86_64.rpm

gettext-libs-0.19.8.1-3.el7.x86_64.rpm

glib2-2.56.1-9.el7_9.x86_64.rpm

glibc-2.17-324.el7_9.i686.rpm

glibc-2.17-324.el7_9.x86_64.rpm

glibc-common-2.17-324.el7_9.x86_64.rpm

gmp-6.0.0-15.el7.x86_64.rpm

gnupg2-2.0.22-5.el7_5.x86_64.rpm

gnutls-3.3.29-9.el7_6.x86_64.rpm

gpgme-1.3.2-5.el7.x86_64.rpm

gpm-libs-1.20.7-6.el7.x86_64.rpm

grep-2.20-3.el7.x86_64.rpm

groff-base-1.22.2-8.el7.x86_64.rpm

grub2-2.02-0.87.el7.centos.6.x86_64.rpm

grub2-common-2.02-0.87.el7.centos.6.noarch.rpm

grub2-efi-x64-2.02-0.87.el7.centos.6.x86_64.rpm

grub2-pc-2.02-0.87.el7.centos.6.x86_64.rpm

grub2-pc-modules-2.02-0.87.el7.centos.6.noarch.rpm

grub2-tools-2.02-0.87.el7.centos.6.x86_64.rpm

grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64.rpm

grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64.rpm

grubby-8.28-26.el7.x86_64.rpm

gssproxy-0.7.0-30.el7_9.x86_64.rpm

gzip-1.5-10.el7.x86_64.rpm

hardlink-1.0-19.el7.x86_64.rpm

hostname-3.13-3.el7_7.1.x86_64.rpm

hwdata-0.252-9.7.el7.x86_64.rpm

hyperv-daemons-0-0.34.20180415git.el7.x86_64.rpm

hyperv-daemons-license-0-0.34.20180415git.el7.noarch.rpm

hypervfcopyd-0-0.34.20180415git.el7.x86_64.rpm

hypervkvpd-0-0.34.20180415git.el7.x86_64.rpm

hyperv-tools-0-0.34.20180415git.el7.noarch.rpm

hypervvssd-0-0.34.20180415git.el7.x86_64.rpm

info-5.1-5.el7.x86_64.rpm

initscripts-9.49.53-1.el7_9.1.x86_64.rpm

iotop-0.6-4.el7.noarch.rpm

iproute-4.11.0-30.el7.x86_64.rpm

iptables-1.4.21-35.el7.x86_64.rpm

iptables-services-1.4.21-35.el7.x86_64.rpm

iputils-20160308-10.el7.x86_64.rpm

iscsi-initiator-utils-6.2.0.874-20.el7_9.x86_64.rpm

iscsi-initiator-utils-iscsiuio-6.2.0.874-20.el7_9.x86_64.rpm

jansson-2.10-1.el7.x86_64.rpm

json-c-0.11-4.el7_0.x86_64.rpm

kernel-3.10.0-1160.31.1.el7.x86_64.rpm

kernel-plus-3.10.0-1160.31.1.el7.centos.plus.x86_64.rpm

keyutils-1.5.8-3.el7.x86_64.rpm

keyutils-libs-1.5.8-3.el7.x86_64.rpm

keyutils-libs-devel-1.5.8-3.el7.x86_64.rpm

kmod-20-28.el7.x86_64.rpm

kmod-libs-20-28.el7.x86_64.rpm

kpartx-0.4.9-134.el7_9.x86_64.rpm

krb5-devel-1.15.1-50.el7.x86_64.rpm

krb5-libs-1.15.1-50.el7.x86_64.rpm

less-458-9.el7.x86_64.rpm

libacl-2.2.51-15.el7.x86_64.rpm

libaio-0.3.109-13.el7.x86_64.rpm

libassuan-2.1.0-3.el7.x86_64.rpm

libattr-2.4.46-13.el7.x86_64.rpm

libbasicobjects-0.1.1-32.el7.x86_64.rpm

libblkid-2.23.2-65.el7_9.1.x86_64.rpm

libcap-2.22-11.el7.x86_64.rpm

libcap-ng-0.7.5-4.el7.x86_64.rpm

libcgroup-0.41-21.el7.x86_64.rpm

libcollection-0.7.0-32.el7.x86_64.rpm

libcom_err-1.42.9-19.el7.x86_64.rpm

libcom_err-devel-1.42.9-19.el7.x86_64.rpm

libcroco-0.6.12-6.el7_9.x86_64.rpm

libcurl-7.29.0-59.el7_9.1.x86_64.rpm

libdb-5.3.21-25.el7.x86_64.rpm

libdb-utils-5.3.21-25.el7.x86_64.rpm

libdrm-2.4.97-2.el7.x86_64.rpm

libedit-3.0-12.20121213cvs.el7.x86_64.rpm

libestr-0.1.9-2.el7.x86_64.rpm

libevent-2.0.21-4.el7.x86_64.rpm

libfastjson-0.99.4-3.el7.x86_64.rpm

libffi-3.0.13-19.el7.x86_64.rpm

libgcc-4.8.5-44.el7.i686.rpm

libgcc-4.8.5-44.el7.x86_64.rpm

libgcrypt-1.5.3-14.el7.x86_64.rpm

libgomp-4.8.5-44.el7.x86_64.rpm

libgpg-error-1.12-3.el7.x86_64.rpm

libidn-1.28-4.el7.x86_64.rpm

libini_config-1.3.1-32.el7.x86_64.rpm

libkadm5-1.15.1-50.el7.x86_64.rpm

libldb-1.5.4-2.el7.x86_64.rpm

libmnl-1.0.3-7.el7.x86_64.rpm

libmount-2.23.2-65.el7_9.1.x86_64.rpm

libmspack-0.5-0.8.alpha.el7.x86_64.rpm

libnetfilter_conntrack-1.0.6-1.el7_3.x86_64.rpm

libnfnetlink-1.0.1-4.el7.x86_64.rpm

libnfsidmap-0.25-19.el7.x86_64.rpm

libpath_utils-0.2.1-32.el7.x86_64.rpm

libpcap-1.5.3-12.el7.x86_64.rpm

libpciaccess-0.14-1.el7.x86_64.rpm

libpng-1.5.13-8.el7.x86_64.rpm

libpwquality-1.2.3-5.el7.x86_64.rpm

libref_array-0.1.5-32.el7.x86_64.rpm

libselinux-2.5-15.el7.x86_64.rpm

libselinux-devel-2.5-15.el7.x86_64.rpm

libselinux-python-2.5-15.el7.x86_64.rpm

libselinux-utils-2.5-15.el7.x86_64.rpm

libsemanage-2.5-14.el7.x86_64.rpm

libsemanage-python-2.5-14.el7.x86_64.rpm

libsepol-2.5-10.el7.x86_64.rpm

libsepol-devel-2.5-10.el7.x86_64.rpm

libsmartcols-2.23.2-65.el7_9.1.x86_64.rpm

libss-1.42.9-19.el7.x86_64.rpm

libssh2-1.8.0-4.el7.x86_64.rpm

libstdc++-4.8.5-44.el7.i686.rpm

libstdc++-4.8.5-44.el7.x86_64.rpm

libtalloc-2.1.16-1.el7.x86_64.rpm

libtasn1-4.10-1.el7.x86_64.rpm

libtdb-1.3.18-1.el7.x86_64.rpm

libtevent-0.9.39-1.el7.x86_64.rpm

libtirpc-0.2.4-0.16.el7.x86_64.rpm

libtool-ltdl-2.4.2-22.el7_3.x86_64.rpm

libunistring-0.9.3-9.el7.x86_64.rpm

libusbx-1.0.21-1.el7.x86_64.rpm

libuser-0.60-9.el7.x86_64.rpm

libutempter-1.1.6-4.el7.x86_64.rpm

libuuid-2.23.2-65.el7_9.1.x86_64.rpm

libverto-0.2.5-4.el7.x86_64.rpm

libverto-devel-0.2.5-4.el7.x86_64.rpm

libverto-libevent-0.2.5-4.el7.x86_64.rpm

libwbclient-4.10.16-15.el7_9.x86_64.rpm

libxml2-2.9.1-6.el7.5.x86_64.rpm

libxml2-python-2.9.1-6.el7.5.x86_64.rpm

libxslt-1.1.28-6.el7.x86_64.rpm

libyaml-0.1.4-11.el7_0.x86_64.rpm

linux-firmware-20200421-80.git78c0348.el7_9.noarch.rpm

lm_sensors-libs-3.4.0-8.20160601gitf9185e5.el7.x86_64.rpm

logrotate-3.8.6-19.el7.x86_64.rpm

lsof-4.87-6.el7.x86_64.rpm

lua-5.1.4-15.el7.x86_64.rpm

lz4-1.8.3-1.el7.x86_64.rpm

make-3.82-24.el7.x86_64.rpm

mariadb-libs-5.5.68-1.el7.x86_64.rpm

mc-4.8.7-11.el7.x86_64.rpm

memcached-1.4.15-10.el7_3.1.x86_64.rpm

ncurses-5.9-14.20130511.el7_4.x86_64.rpm

ncurses-base-5.9-14.20130511.el7_4.noarch.rpm

ncurses-libs-5.9-14.20130511.el7_4.x86_64.rpm

net-snmp-5.7.2-49.el7_9.1.x86_64.rpm

net-snmp-agent-libs-5.7.2-49.el7_9.1.x86_64.rpm

net-snmp-libs-5.7.2-49.el7_9.1.x86_64.rpm

nettle-2.7.1-9.el7_9.x86_64.rpm

net-tools-2.0-0.25.20131004git.el7.x86_64.rpm

nfs-utils-1.3.0-0.68.el7.x86_64.rpm

nspr-4.25.0-2.el7_9.x86_64.rpm

nss-3.53.1-7.el7_9.x86_64.rpm

nss-pem-1.0.3-7.el7.x86_64.rpm

nss-softokn-3.53.1-6.el7_9.x86_64.rpm

nss-softokn-freebl-3.53.1-6.el7_9.i686.rpm

nss-softokn-freebl-3.53.1-6.el7_9.x86_64.rpm

nss-sysinit-3.53.1-7.el7_9.x86_64.rpm

nss-tools-3.53.1-7.el7_9.x86_64.rpm

nss-util-3.53.1-1.el7_9.x86_64.rpm

ntp-4.2.6p5-29.el7.centos.2.x86_64.rpm

ntpdate-4.2.6p5-29.el7.centos.2.x86_64.rpm

openldap-2.4.44-23.el7_9.x86_64.rpm

openssh-7.4p1-21.el7.x86_64.rpm

openssh-clients-7.4p1-21.el7.x86_64.rpm

openssh-server-7.4p1-21.el7.x86_64.rpm

openssl-1.0.2k-21.el7_9.x86_64.rpm

openssl-devel-1.0.2k-21.el7_9.x86_64.rpm

openssl-libs-1.0.2k-21.el7_9.x86_64.rpm

open-vm-tools-11.0.5-3.el7_9.3.x86_64.rpm

os-prober-1.58-9.el7.x86_64.rpm

p11-kit-0.23.5-3.el7.x86_64.rpm

p11-kit-trust-0.23.5-3.el7.x86_64.rpm

pam-1.1.8-23.el7.x86_64.rpm

parted-3.1-32.el7.x86_64.rpm

passwd-0.79-6.el7.x86_64.rpm

pciutils-3.5.1-3.el7.x86_64.rpm

pciutils-libs-3.5.1-3.el7.x86_64.rpm

pcre-8.32-17.el7.x86_64.rpm

pcre-devel-8.32-17.el7.x86_64.rpm

perl-5.16.3-299.el7_9.x86_64.rpm

perl-Business-ISBN-2.06-2.el7.noarch.rpm

perl-Business-ISBN-Data-20120719.001-2.el7.noarch.rpm

perl-Carp-1.26-244.el7.noarch.rpm

perl-constant-1.27-2.el7.noarch.rpm

perl-Data-Dumper-2.145-3.el7.x86_64.rpm

perl-Encode-2.51-7.el7.x86_64.rpm

perl-Exporter-5.68-3.el7.noarch.rpm

perl-File-Path-2.09-2.el7.noarch.rpm

perl-File-Temp-0.23.01-3.el7.noarch.rpm

perl-Filter-1.49-3.el7.x86_64.rpm

perl-Getopt-Long-2.40-3.el7.noarch.rpm

perl-HTTP-Tiny-0.033-3.el7.noarch.rpm

perl-libs-5.16.3-299.el7_9.x86_64.rpm

perl-macros-5.16.3-299.el7_9.x86_64.rpm

perl-parent-0.225-244.el7.noarch.rpm

perl-PathTools-3.40-5.el7.x86_64.rpm

perl-Pod-Escapes-1.04-299.el7_9.noarch.rpm

perl-podlators-2.5.1-3.el7.noarch.rpm

perl-Pod-Perldoc-3.20-4.el7.noarch.rpm

perl-Pod-Simple-3.28-4.el7.noarch.rpm

perl-Pod-Usage-1.63-3.el7.noarch.rpm

perl-Scalar-List-Utils-1.27-248.el7.x86_64.rpm

perl-Socket-2.010-5.el7.x86_64.rpm

perl-Storable-2.45-3.el7.x86_64.rpm

perl-Text-ParseWords-3.29-4.el7.noarch.rpm

perl-threads-1.87-4.el7.x86_64.rpm

perl-threads-shared-1.43-6.el7.x86_64.rpm

perl-Time-HiRes-1.9725-3.el7.x86_64.rpm

perl-Time-Local-1.2300-2.el7.noarch.rpm

perl-URI-1.60-9.el7.noarch.rpm

pinentry-0.8.1-17.el7.x86_64.rpm

pkgconfig-0.27.1-4.el7.x86_64.rpm

policycoreutils-2.5-34.el7.x86_64.rpm

policycoreutils-python-2.5-34.el7.x86_64.rpm

popt-1.13-16.el7.x86_64.rpm

procps-ng-3.3.10-28.el7.x86_64.rpm

psmisc-22.20-17.el7.x86_64.rpm

pth-2.0.7-23.el7.x86_64.rpm

pygpgme-0.3-9.el7.x86_64.rpm

pyliblzma-0.5.3-11.el7.x86_64.rpm

pyserial-2.6-6.el7.noarch.rpm

python-2.7.5-90.el7.x86_64.rpm

python-babel-0.9.6-8.el7.noarch.rpm

python-backports-1.0-8.el7.x86_64.rpm

python-backports-ssl_match_hostname-3.5.0.1-1.el7.noarch.rpm

python-chardet-2.2.1-3.el7.noarch.rpm

python-configobj-4.7.2-7.el7.noarch.rpm

python-iniparse-0.4-9.el7.noarch.rpm

python-ipaddress-1.0.16-2.el7.noarch.rpm

python-IPy-0.75-6.el7.noarch.rpm

python-jinja2-2.7.2-4.el7.noarch.rpm

python-jsonpatch-1.2-4.el7.noarch.rpm

python-jsonpointer-1.9-2.el7.noarch.rpm

python-kitchen-1.1.1-5.el7.noarch.rpm

python-libs-2.7.5-90.el7.x86_64.rpm

python-lxml-3.2.1-4.el7.x86_64.rpm

python-markupsafe-0.11-10.el7.x86_64.rpm

python-prettytable-0.7.2-3.el7.noarch.rpm

python-pycurl-7.19.0-19.el7.x86_64.rpm

python-requests-2.6.0-10.el7.noarch.rpm

python-setuptools-0.9.8-7.el7.noarch.rpm

python-six-1.9.0-2.el7.noarch.rpm

python-urlgrabber-3.10-10.el7.noarch.rpm

python-urllib3-1.10.2-7.el7.noarch.rpm

pyxattr-0.5.1-5.el7.x86_64.rpm

PyYAML-3.10-11.el7.x86_64.rpm

qemu-guest-agent-2.12.0-3.el7.x86_64.rpm

qrencode-libs-3.4.1-3.el7.x86_64.rpm

quota-4.01-19.el7.x86_64.rpm

quota-nls-4.01-19.el7.noarch.rpm

readline-6.2-11.el7.x86_64.rpm

rootfiles-8.1-11.el7.noarch.rpm

rpcbind-0.2.0-49.el7.x86_64.rpm

rpm-4.11.3-45.el7.x86_64.rpm

rpm-build-libs-4.11.3-45.el7.x86_64.rpm

rpm-libs-4.11.3-45.el7.x86_64.rpm

rpm-python-4.11.3-45.el7.x86_64.rpm

rsyslog-8.24.0-57.el7_9.1.x86_64.rpm

samba-client-libs-4.10.16-15.el7_9.x86_64.rpm

samba-common-4.10.16-15.el7_9.noarch.rpm

samba-common-libs-4.10.16-15.el7_9.x86_64.rpm

sed-4.2.2-7.el7.x86_64.rpm

setools-libs-3.3.8-4.el7.x86_64.rpm

setup-2.8.71-11.el7.noarch.rpm

shadow-utils-4.6-5.el7.x86_64.rpm

shared-mime-info-1.8-5.el7.x86_64.rpm

slang-2.2.4-11.el7.x86_64.rpm

sqlite-3.7.17-8.el7_7.1.x86_64.rpm

strace-4.24-6.el7.x86_64.rpm

sudo-1.8.23-10.el7_9.1.x86_64.rpm

sysstat-10.1.5-19.el7.x86_64.rpm

system-config-firewall-base-1.2.29-10.el7.noarch.rpm

systemd-219-78.el7_9.3.x86_64.rpm

systemd-libs-219-78.el7_9.3.x86_64.rpm

systemd-sysv-219-78.el7_9.3.x86_64.rpm

sysvinit-tools-2.88-14.dsf.el7.x86_64.rpm

tar-1.26-35.el7.x86_64.rpm

tcpdump-4.9.2-4.el7_7.1.x86_64.rpm

tcp_wrappers-7.6-77.el7.x86_64.rpm

tcp_wrappers-libs-7.6-77.el7.x86_64.rpm

traceroute-2.0.22-2.el7.x86_64.rpm

trousers-0.3.14-2.el7.x86_64.rpm

tzdata-2021a-1.el7.noarch.rpm

unzip-6.0-22.el7_9.x86_64.rpm

usbutils-007-5.el7.x86_64.rpm

ustr-1.0.4-16.el7.x86_64.rpm

util-linux-2.23.2-65.el7_9.1.x86_64.rpm

vim-common-7.4.629-8.el7_9.x86_64.rpm

vim-enhanced-7.4.629-8.el7_9.x86_64.rpm

vim-filesystem-7.4.629-8.el7_9.x86_64.rpm

vim-minimal-7.4.629-8.el7_9.x86_64.rpm

wget-1.14-18.el7_6.1.x86_64.rpm

which-2.20-7.el7.x86_64.rpm

xmlsec1-1.2.20-7.el7_4.x86_64.rpm

xmlsec1-openssl-1.2.20-7.el7_4.x86_64.rpm

xz-5.2.2-1.el7.x86_64.rpm

xz-libs-5.2.2-1.el7.x86_64.rpm

yum-3.4.3-168.el7.centos.noarch.rpm

yum-metadata-parser-1.1.4-10.el7.x86_64.rpm

yum-plugin-fastestmirror-1.1.31-54.el7_8.noarch.rpm

yum-utils-1.1.31-54.el7_8.noarch.rpm

zlib-1.2.7-19.el7_9.x86_64.rpm

zlib-devel-1.2.7-19.el7_9.x86_64.rpm

Список 2

open-vm-tools-deploypkg-9.4.10-3.x86_64.rpm

Список 3

kl-lightagent-qemu-img-2.11.1-21.x86_64.rpm

kl-lightagent-scanserver-5.2.27-1114.x86_64.rpm

kl-lightagent-toolchain-libgcc-7.3.0-0.x86_64.rpm

kl-lightagent-xva-img-1.0.0-21.x86_64.rpm

klnagent64-12.0.0-60.x86_64.rpm

Список 4

nginx-1.20.1-1.el7.ngx.x86_64.rpm

Список 5

huawei-compute

vz-guest-tools

xenserver65

Учетные записи для установки и работы программы

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

Для запуска Консоли Сервера интеграции вы можете использовать следующие учетные записи:

- Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен Microsoft Windows, для запуска Консоли Сервера интеграции вы можете использовать учетную запись, которая входит в локальную или доменную группу KLAdmins, или учетную запись, которая входит в группу локальных администраторов. Также вы можете использовать учетную запись администратора Сервера интеграции, созданную автоматически при установке Сервера интеграции.
- Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен Microsoft Windows или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, для запуска Консоли Сервера интеграции вы можете использовать только учетную запись администратора Сервера интеграции, созданную автоматически при установке Сервера интеграции.

Гипервизор VMware ESXi

Для установки и работы программы на гипервизоре VMware ESXi требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись администратора со следующими правами:

- Datastore.Allocate space
- Datastore.Low level file operations
- Datastore.Remove file
- Global.Cancel task
- Global.Licenses
- Host.Config.Virtual machine autostart configuration
- Host.Inventory.Modify cluster
- Network.Assign network
- Tasks.Create task
- vApp.Import
- Virtual machine.Configuration.Add new disk
- Virtual machine.Configuration.Add or remove device
- Virtual machine.Configuration.Memory
- Virtual machine.Interaction.Power Off
- Virtual machine.Interaction.Power On
- Virtual machine.Provisioning.Customize
- Virtual machine.Inventory.Create new (только для VMware vCenter Server 6.0 и VMware vCenter Server 6.5)
- Virtual machine.Inventory.Remove (только для VMware vCenter Server 6.0 и VMware vCenter Server 6.5)
- System.Anonymous (только для VMware vCenter Server 6.0)
- System.Read (только для VMware vCenter Server 6.0)
- System.View (только для VMware vCenter Server 6.0)

- Для подключения Сервера интеграции к VMware vCenter Server рекомендуется использовать учетную запись, которой назначена предустановленная системная роль ReadOnly.
- Для подключения Сервера интеграции к VMware NSX Manager требуется учетная запись VMware NSX Manager, которой назначена роль Enterprise Administrator.

Права должны быть назначены учетным записям на верхнем уровне иерархии объектов управления VMware – на уровне VMware vCenter Server.

Гипервизор Microsoft Windows Server (Hyper-V)

Для развертывания, удаления и изменения конфигурации SVM на гипервизоре Microsoft Windows Server (Hyper-V) требуется встроенная учетная запись локального администратора или доменная учетная запись, входящая в группу Администраторы Hyper-V. В случае доменной учетной записи вам также требуется выдать права на удаленное подключение и использование следующих пространств имен WMI:

- root\cimv2;

- root\MSCluster;
- root\virtualization;
- root\virtualization\v2 (для версий операционных систем Microsoft Windows для серверов, начиная с версии Windows Server 2012 R2).

Для подключения Сервера интеграции к гипервизору Microsoft Windows Server (Hyper-V) также используется встроенная учетная запись локального администратора или доменная учетная запись, входящая в группу Администраторы Hyper-V, которой предоставлены указанные выше права.

Гипервизор Citrix Hypervisor

Для установки и работы программы на гипервизоре Citrix Hypervisor требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с правами Pool Admin.
- Для подключения Сервера интеграции к гипервизору Citrix Hypervisor рекомендуется использовать учетную запись с ролью Read Only.

Гипервизор KVM

Для установки и работы программы на гипервизоре KVM требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись root или учетная запись, которая имеет право выполнять действия от имени учетной записи root.
- Для подключения Сервера интеграции к гипервизору KVM рекомендуется использовать учетную запись непривилегированного пользователя, которой разрешен доступ к Unix-сокету "только для чтения" (libvirt-sock-ro) службы libvirtd (libvirtd daemon).

Гипервизор Proxmox VE

Для установки и работы программы на гипервизоре Proxmox VE требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись root или учетная запись, которая имеет право выполнять действия от имени учетной записи root.
- Для подключения Сервера интеграции к гипервизору Proxmox VE рекомендуется использовать учетную запись, которой предоставлен доступ с ролью PVEAuditor к корневой директории (/) и всем дочерним директориям.

Гипервизор Р-Виртуализация

Для установки и работы программы на гипервизоре Р-Виртуализация требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с ролью "Главный администратор".
- Для подключения Сервера интеграции к серверу управления виртуальной инфраструктурой Скала-Р Управление рекомендуется использовать учетную запись с ролью "Мониторинг инфраструктуры".

Гипервизор HUAWEI FusionCompute CNA

Для установки и работы программы на гипервизоре HUAWEI FusionCompute CNA требуются следующие

учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с ролью VMManager.
- Для подключения Сервера интеграции к HUAWEI FusionCompute VRM рекомендуется использовать учетную запись с ролью Auditor.

Гипервизор Nutanix AHV

Для установки и работы программы на гипервизоре Nutanix AHV требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с ролью Cluster Admin.
- Для подключения Сервера интеграции к серверу управления виртуальной инфраструктурой Nutanix Prism рекомендуется использовать учетную запись с ролью Viewer. В инфраструктуре под управлением Nutanix Prism Central учетная запись с ролью Viewer требуется на сервере Nutanix Prism Central и на серверах Nutanix Prism Element.

Настройка правил перемещения виртуальных машин в группы администрирования

Чтобы управлять работой компонентов программы Kaspersky Security, установленных на виртуальных машинах, через Kaspersky Security Center, вам требуется поместить виртуальные машины в группы администрирования, настроив правила автоматического перемещения виртуальных машин в группы администрирования.

Группа администрирования – это набор виртуальных машин, объединенных по какому-либо признаку с целью управления виртуальными машинами группы как единым целым.

Перед началом установки программы Kaspersky Security вы можете создать в Kaspersky Security Center группы администрирования, в которые вы хотите поместить виртуальные машины с установленными компонентами программы, и настроить правила автоматического перемещения виртуальных машин в группы администрирования.

Если правила перемещения виртуальных машин в группы администрирования не настроены, после установки программы Kaspersky Security Center помещает виртуальные машины, обнаруженные в сети, в список **Нераспределенные устройства**. В этом случае вам требуется вручную переместить виртуальные машины в группы администрирования.

► *Чтобы настроить правила перемещения виртуальных машин в группы администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Нераспределенные устройства**.
3. Откройте контекстное меню и выберите пункт **Свойства**.

   Откроется окно **Свойства: Нераспределенные устройства**.
4. В разделе **Перемещение устройств** нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
5. Настройте правило перемещения виртуальных машин в группы администрирования.

Подробнее о настройке правил перемещения виртуальных машин в группы см. в документации Kaspersky Security Center.

6. Нажмите на кнопку **OK**, чтобы закрыть окно **Новое правило**.

   Новое правило отобразится в списке правил в разделе **Перемещение устройств**.

7. Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: Нераспределенные устройства**.

При создании правил перемещения виртуальных машин в группы администрирования вы можете использовать теги. SVM и защищенные виртуальные машины с установленным Агентом администрирования Kaspersky Security Center автоматически передают информацию о тегах в Kaspersky Security Center.

Установка программы

Установка программы Kaspersky Security для виртуальных сред 5.2 Легкий агент в виртуальной инфраструктуре состоит из следующих этапов:

1. Установка mmc-плагинов управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции (см. раздел "Установка mmc-плагинов управления Kaspersky Security и Сервера интеграции" на стр. 58).

   - Для управления программой с помощью Kaspersky Security Center используются следующие mmc-плагины управления:
     - Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows.
     - Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux.
     - Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты.

     Плагины управления Kaspersky Security 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.
   - Консоль Сервера интеграции должна быть установлена на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

   После установки плагинов управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции рекомендуется запустить в Консоли администрирования Kaspersky Security Center задачу загрузки обновлений в хранилище и убедиться, что задача выполнена успешно.

   При первом запуске Консоли администрирования Kaspersky Security Center после установки плагинов управления Kaspersky Security автоматически запускается мастер первоначальной настройки управляемой программы для каждого установленного плагина. В результате работы мастера создаются политика по умолчанию для Сервера защиты и задачи (см. раздел "Автоматическое создание задач и политики по умолчанию для Сервера защиты" на стр. 62).

2. Установка компонента Сервер защиты Kaspersky Security (см. раздел "Установка Сервера защиты" на стр. 66) путем развертывания SVM на гипервизорах.

   Если вы устанавливаете программу в инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager, после завершения развертывания SVM вам нужно настроить подключение Сервера интеграции к VMware NSX Manager (см. раздел "Изменение и удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 437) в Консоли Сервера интеграции.

3. Подготовка Сервера защиты к работе (на стр. 78).

4. Установка компонента Агент администрирования Kaspersky Security Center на виртуальные машины (см. раздел "Установка Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 84).

5. Установка на виртуальные машины компонента Легкий агент для Windows (см. раздел "Установка Легкого агента для Windows" на стр. 84) и / или Легкий агент для Linux (см. раздел "Установка Легкого агента для Linux" на стр. 92).

   Вы можете установить Легкий агент для Windows на виртуальные машины в составе

инфраструктуры, в которой используются следующие решения для виртуализации:

- Citrix Virtual Apps and Desktops (Citrix XenApp and XenDesktop).
- Citrix App Layering (см. раздел "Совместимость с технологией Citrix App Layering" на стр. 91).
- Citrix Provisioning (Citrix Provisioning Services) (см. раздел "Совместимость с технологией Citrix Provisioning Services" на стр. 92).
- VMware Horizon.

6. Подготовка Легких агентов к работе (на стр. 102).

В этом разделе

Установка mmc-плагинов управления Kaspersky Security и Сервера интеграции

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

Для установки требуется не менее 4 ГБ свободного места на диске, который содержит папку %ProgramData%.

Для установки mmc-плагинов управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции требуется платформа Microsoft .NET Framework 4.6. Вы можете установить платформу Microsoft .NET Framework предварительно, или мастер установки компонентов Kaspersky Security предложит ее установить в ходе установки компонентов программы Kaspersky Security. Для установки требуется доступ в

интернет. В случае проблем с установкой Microsoft .NET Framework убедитесь, что на компьютере установлены обновления Windows KB2919442 и KB2919355.

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

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 плагины управления Kaspersky Security и Консоль Сервера интеграции;
- Если на компьютере установлены Сервер администрирования Kaspersky Security Center и Консоль администрирования Kaspersky Security Center:
  - устанавливаются плагины управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции;
  - создаются инсталляционные пакеты для удаленной установки Легкого агента для Windows и Легкого агента для Linux. Созданные инсталляционные пакеты размещаются в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** -> **Удаленная установка** -> **Инсталляционные пакеты** под следующими именами:
    - **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows (5.2.X.X)**,
    - **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux (5.2.X.X)**,

      где 5.2.X.X – номер версии программы.

Для успешной установки Сервера интеграции нужно в настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика, разрешить соединения на порт, который SVM и Легкие агенты будут использовать для подключения к Серверу интеграции. По умолчанию используется порт 7271 по протоколу TCP.

Для взаимодействия Сервера интеграции с Консолью Сервера интеграции, с SVM, с Легкими агентами и с VMware vCenter Server используется защищенное SSL-соединение. Для устранения известных уязвимостей операционной системы для протокола SSL при установке Сервера интеграции в реестр операционной системы вносятся изменения, описанные в базе технической поддержки Microsoft (http://support.microsoft.com/kb/245030). В результате этих изменений отключаются следующие криптографические шифры и протоколы:

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

В ходе установки Сервера интеграции в реестре операционной системы устанавливается самоподписанный SSL-сертификат Сервера интеграции, который используется для установки защищенного соединения с Сервером интеграции и для шифрования канала связи между SVM и Легким агентом, установленным на виртуальных машинах. После установки Сервера интеграции рекомендуется заменить этот самоподписанный сертификат на более надежный сертификат. Процедура замены сертификата описана в Базе знаний (https://support.kaspersky.ru/14677).

► *Чтобы установить mmc-плагины управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции с помощью мастера, выполните следующие действия:*

1. На компьютере, где установлены Консоль администрирования и Сервер администрирования Kaspersky Security Center, запустите файл ksvla-components_5.2.X.X_mlg.exe, где 5.2.X.X – номер версии программы. Этот файл входит в комплект поставки (см. раздел "Файлы, необходимые для установки программы" на стр. 31).

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

   Запустится мастер установки компонентов Kaspersky Security.

2. На первом шаге в окне мастера отображается язык локализации мастера и компонентов Kaspersky Security – русский. Перейдите к следующему шагу мастера.

3. Убедитесь, что выбрано действие **Установить компоненты управления** и перейдите к следующему шагу мастера.

   Мастер проверяет объем свободного места на диске, который содержит папку %ProgramData%. Если на диске менее 4 ГБ свободного места, мастер выдает сообщение об ошибке, переход к следующему шагу невозможен. В этом случае завершите работу мастера, освободите место на диске и запустите мастер установки компонентов Kaspersky Security повторно.

4. На этом шаге 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.

5. Если на компьютере, на котором запущен мастер, установлен Сервер администрирования Kaspersky Security Center и этот компьютер не входит в домен Microsoft Windows, 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.

6. 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 1025–65535 и перейдите к следующему шагу мастера.

7. Просмотрите информацию о действиях, которые выполнит мастер над плагинами управления, Сервером интеграции и Консолью Сервера интеграции, и нажмите на кнопку **Далее**, чтобы начать выполнение перечисленных действий.

8. Дождитесь завершения работы мастера.

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

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

После установки mmc-плагины управления Kaspersky Security отображаются в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center (см. раздел "Результат установки mmc-плагинов и Сервера интеграции" на стр. 61).

Информация о работе мастера записывается в файлы трассировки мастера установки компонентов Kaspersky Security (см. раздел "О файлах трассировки мастера установки компонентов Kaspersky Security" на стр. 509). Если работа мастера завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Результат установки mmc-плагинов и Сервера интеграции

После завершения установки mmc-плагинов Kaspersky Security и Сервера интеграции в Консоли администрирования Kaspersky Security Center в рабочей области узла **Сервер администрирования <Имя сервера>** на закладке **Мониторинг** в блоке **Развертывание** отображается ссылка для запуска Консоли Сервера интеграции: **Управление Kaspersky Security для виртуальных сред <номер версии> Легкий агент**, где <номер версии> – номер установленной версии программы Kaspersky Security.

Установленные mmc-плагины отображаются в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел **Сервер администрирования <Имя сервера>** и выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню и выберите пункт **Свойства**.
- Откройте окно свойств Сервера администрирования по ссылке **Свойства сервера администрирования**. Ссылка находится в рабочей области узла **Сервер администрирования <Имя сервера>** в блоке **Сервер администрирования**.

Откроется окно **Свойства: Сервер администрирования <Имя сервера>**.

3. В списке слева в разделе **Дополнительно** выберите раздел **Информация об установленных плагинах управления программами**.

   В правой части окна в списке установленных плагинов управления отображаются mmc-плагины Kaspersky Security:

   - **Kaspersky Security для виртуальных сред <номер версии> Легкий агент – Сервер защиты**;
   - **Kaspersky Security для виртуальных сред <номер версии> Легкий агент для Linux**;
   - **Kaspersky Security для виртуальных сред <номер версии> Легкий агент для Windows**;

   где <номер версии> – номер установленной версии программы Kaspersky Security.

Автоматическое создание задач и политики по умолчанию для Сервера защиты

При первом запуске Консоли администрирования Kaspersky Security Center после установки mmc-плагинов Kaspersky Security автоматически запускается мастер первоначальной настройки управляемой программы. Мастер запускается три раза подряд и позволяет создать политику по умолчанию для Сервера защиты и следующие задачи:

- задачу поиска вирусов для Легкого агента для Windows;
- задачу поиска вирусов для Легкого агента для Linux;
- задачу обновления баз на Сервере защиты.

Если мастер первоначальной настройки управляемой программы не запустился автоматически, вы можете запустить его вручную.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел **Сервер администрирования**, откройте контекстное меню и выберите пункт **Все задачи** → **Мастер первоначальной настройки управляемых программ**.
3. Нажмите на кнопку **Далее** в окне приветствия и на следующем шаге выберите в качестве управляемой программы одно из следующих значений:
   - **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты**, если вы хотите создать политику по умолчанию для Сервера защиты и задачу обновления баз на Сервере защиты;
   - **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux**, если вы хотите создать задачу поиска вирусов для Легкого агента для Linux;
   - **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows**, если вы хотите

создать задачу поиска вирусов для Легкого агента для Windows.

Запустится мастер первоначальной настройки Kaspersky Security.

Чтобы создать политику по умолчанию для Сервера защиты и все перечисленные выше задачи, вам нужно запустить мастер первоначальной настройки управляемой программы три раза подряд.

Создание задач

Задачи создаются в автоматическом режиме. Ваше участие в работе мастера не требуется.

Задача поиска вирусов для Легкого агента для Windows создается для группы администрирования **Управляемые устройства** и может запускаться на всех виртуальных машинах с установленным компонентом Легкий агент для Windows, которые будут помещены в группу администрирования **Управляемые устройства** или в любую вложенную группу администрирования. Вы можете изменить параметры задачи, настроенные по умолчанию (см. раздел "Настройка параметров задачи поиска вирусов для Легкого агента для Windows" на стр. 358).

Задача поиска вирусов для Легкого агента для Linux создается для группы администрирования **Управляемые устройства** и может запускаться на всех виртуальных машинах с установленным компонентом Легкий агент для Linux, которые будут помещены в группу администрирования **Управляемые устройства** или в любую вложенную группу администрирования. Вы можете изменить параметры задачи, настроенные по умолчанию (см. раздел "Настройка параметров задачи поиска вирусов для Легкого агента для Linux" на стр. 365).

Задача обновления баз на Сервере защиты создается для группы администрирования **Управляемые устройства** и позволяет загружать пакет обновлений баз программы (см. раздел "Обновление баз программы" на стр. 390) на все SVM, которые будут помещены в группу администрирования **Управляемые устройства** или в любую вложенную группу администрирования. Эта задача запускается при каждой загрузке пакета обновлений в хранилище Сервера администрирования Kaspersky Security Center.

Создание политики по умолчанию для Сервера защиты

Политика по умолчанию для Сервера защиты создается для группы администрирования **Управляемые устройства** под именем **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты** и применяется на всех SVM, которые будут помещены в группу администрирования **Управляемые устройства** или в любую вложенную группу администрирования.

При создании политики по умолчанию для Сервера защиты мастер предлагает вам настроить следующие параметры:

1. Принять решение об участии в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 399).

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

   В зависимости от расположения инфраструктуры различают:

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

   Участие в KSN добровольное. Перед принятием решения об участии в KSN 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 к KSN, выберите вариант **Я не принимаю условия настоящего Положения о Kaspersky Security Network**.

При необходимости вы сможете изменить решение об участии в KSN позже (см. раздел "Настройка использования Kaspersky Security Network в политике Сервера защиты" на стр. 401).

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

2. Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в доменную или локальную группу KLAdmins или в группу локальных администраторов, указать параметры подключения SVM к Серверу интеграции:

   a. Проверьте адрес и порт для подключения к Серверу интеграции в окне **Параметры подключения SVM к Серверу интеграции**. В полях указан порт, используемый по умолчанию (7271), и доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Вы можете изменить порт и указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

   Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

   b. Нажмите на кнопку **OK** в окне **Параметры подключения SVM к Серверу интеграции**. В открывшемся окне **Подключение к Серверу интеграции** укажите пароль администратора Сервера интеграции (пароль учетной записи admin).

   Мастер создания политики проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно Проверка сертификата Сервера интеграции. С помощью кнопки в окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку Игнорировать. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

   После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи для подключения SVM к Серверу интеграции.

Остальные параметры политики принимают значения по умолчанию.

Значения параметров политики, установленные по умолчанию, соответствуют рекомендациям специалистов "Лаборатории Касперского" и достаточны для первоначальной настройки программы. Во время работы с программой вы можете выполнить более тонкую настройку параметров политики для Сервера защиты (см. раздел "Политика для Сервера защиты" на стр. 123).

Если вы не настроили параметры подключения SVM к Серверу интеграции или подключиться с указанными параметрами не удалось, политика создается в состоянии **Неактивная политика**. Позже вы можете настроить параметры этой политики и активировать ее.

Запуск Консоли Сервера интеграции

Из Консоли Сервера интеграции (см. раздел "О Консоли Сервера интеграции" на стр. 153) запускается мастер управления SVM, с помощью которого выполняется установка, обновление и удаление компонента Сервер защиты, а также изменение конфигурации SVM.

В Консоли Сервера интеграции вы также можете посмотреть и настроить параметры Сервера интеграции (см. раздел "Просмотр и изменение параметров Сервера интеграции" на стр. 435).

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

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел **Сервер администрирования <Имя сервера>**.
3. Запустите Консоль Сервера интеграции по ссылке **Управление Kaspersky Security для виртуальных сред <номер версии> Легкий агент**, где <номер версии> – номер установленной версии программы Kaspersky Security. Ссылка расположена в блоке **Развертывание**.
4. Если выполняется одно из следующих условий, откроется окно для ввода параметров подключения к Серверу интеграции:
   - если компьютер, на котором установлена Консоль Сервера интеграции, не входит в домен Microsoft Windows;
   - если компьютер, на котором установлена Консоль Сервера интеграции, входит в домен, но ваша доменная учетная запись не входит в доменную или локальную группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции;
   - если компьютер, на котором установлена Консоль Сервера интеграции, входит в домен, но не

удалось подключиться к Серверу интеграции, используя заданные в параметрах Сервера интеграции адрес и порт подключения.

Укажите следующие параметры подключения:

- Адрес и порт Сервера интеграции, к которому выполняется подключение.

  В качестве адреса вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

  Если Консоль Сервера интеграции установлена на том же компьютере, на котором установлен Сервер администрирования Kaspersky Security Center, то по умолчанию для подключения к Серверу интеграции используется адрес, заданный в параметрах Сервера администрирования Kaspersky Security Center. Вы можете изменить этот адрес в окне свойств папки **Инсталляционные пакеты** в дереве консоли (**Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**, окно открывается по пункту контекстного меню **Свойства**).

  > Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

- Учетную запись для подключения к Серверу интеграции:
  - Если компьютер, на котором установлена Консоль Сервера интеграции, входит в домен и ваша учетная запись входит в доменную или локальную группу KLAdmins или в группу локальных администраторов, вы можете использовать вашу учетную запись. Для этого установите флажок **Использовать доменную учетную запись**.

    Если вы хотите использовать учетную запись администратора Сервера интеграции, 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 доменную или локальную группу KLAdmins или в группу локальных администраторов, вы можете использовать только учетную запись администратора Сервера интеграции. Введите пароль администратора Сервера интеграции в поле **Пароль**.

Нажмите на кнопку **Подключить**.

5. Консоль проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат не является доверенным или не соответствует ранее установленному сертификату, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. 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.

Установка Сервера защиты

Установка Сервера защиты выполняется посредством развертывания SVM на гипервизоре. На одном

гипервизоре может быть развернуто несколько SVM. Рекомендации по развертыванию SVM на гипервизорах описаны на странице программы в Базе знаний (https://support.kaspersky.ru/14053).

► *Чтобы установить компонент Сервер защиты, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. В разделе **Управление SVM** нажмите на кнопку **Управление SVM**, чтобы запустить мастер управления SVM.
3. Следуйте указаниям мастера.

В этом разделе

Выбор действия

На этом шаге выберите вариант **Развертывание SVM**.

Перейдите к следующему шагу мастера.

Выбор гипервизоров для развертывания SVM

На этом шаге выберите гипервизоры, на которых вы хотите развернуть SVM.

Если ранее развертывание SVM на гипервизорах в вашей виртуальной инфраструктуре не выполнялось, список гипервизоров пуст. Если на гипервизорах в вашей виртуальной инфраструктуре уже развернуты SVM, в таблице отображается список этих гипервизоров и SVM, развернутых на гипервизорах. Вы можете добавить в список гипервизоры, на которых вы хотите развернуть SVM.

► *Чтобы добавить гипервизоры в список, выполните следующие действия:*

1. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры подключения к виртуальной инфраструктуре**.

2. Укажите следующие параметры подключения мастера управления SVM к гипервизорам, на которых вы хотите развернуть SVM, или к серверу управления виртуальной инфраструктурой, под управлением которого работают гипервизоры:

   - Тип гипервизора или сервера управления виртуальной инфраструктурой.
   - Адреса гипервизоров или адрес сервера управления виртуальной инфраструктурой, под управлением которого работают гипервизоры.

     Вы можете указать в качества адреса гипервизора или сервера управления виртуальной инфраструктурой его IP-адрес в формате IPv4 или полное доменное имя (FQDN). Вы можете указать IP-адреса или полные доменные имена гипервизоров через точку с запятой, через пробел или с новой строки. Количество правильно распознанных адресов отображается под списком адресов.

     Вы можете также указать порт для подключения к гипервизору или серверу управления виртуальной инфраструктурой в формате <IP-адрес>:<порт>.

     Если вы устанавливаете программу на гипервизорах Microsoft Windows Server (Hyper-V), входящих в состав кластера гипервизоров под управлением службы Windows Failover Clustering, вы можете указать адрес любого узла кластера. Все гипервизоры, входящие в состав кластера, будут добавлены в список.

     Если вы устанавливаете программу на гипервизорах VMware ESXi под управлением серверов VMware vCenter Server, которые работают в режиме Linked mode, вы можете указать адрес любого из этих серверов VMware vCenter Server. Все гипервизоры, которые работают под управлением серверов VMware vCenter Server в режиме Linked mode, будут добавлены в список.

     Если вы устанавливаете программу на гипервизорах, которые находятся под управлением Microsoft SCVMM, вы можете указать параметры подключения к Microsoft SCVMM. Все гипервизоры, которые находятся под управлением Microsoft SCVMM, будут добавлены в список.

     Если вы устанавливаете программу в инфраструктуре под управлением Nutanix Prism Element, вам нужно указать адрес Nutanix Prism Element. Если инфраструктура находится под управлением Nutanix Prism Central, вам нужно указать адрес Nutanix Prism Central. Все серверы Nutanix Prism Element, находящиеся под управлением Nutanix Prism Central, будут добавлены в список.

   - Имя и пароль учетной записи, которая используется для подключения мастера к гипервизору или к серверу управления виртуальной инфраструктурой. Эта учетная запись должна обладать правами администратора (см. раздел "Учетные записи для установки и работы программы" на стр. 52).

     > Если вы используете доменную учетную запись для подключения к гипервизору или к серверу управления виртуальной инфраструктурой, вы можете указывать имя учетной записи в формате <домен>\<имя пользователя> или <имя пользователя>@<домен>.

3. Если вы разворачиваете SVM на гипервизоре VMware ESXi, Citrix Hypervisor, KVM, Proxmox VE, P-Виртуализация, HUAWEI FusionCompute CNA или Nutanix AHV, для подключения Сервера интеграции к виртуальной инфраструктуре во время работы программы рекомендуется использовать учетную запись, которая обладает правами только на чтение (см. раздел "Учетные записи для установки и работы программы" на стр. 52). Установите флажок **Учетная запись с правами только на чтение** и укажите имя и пароль учетной записи, которую будет использовать Сервер интеграции для подключения к виртуальной инфраструктуре.

   Если флажок не установлен, Сервер интеграции использует для подключения к виртуальной инфраструктуре учетную запись с правами администратора.

Если вы разворачиваете SVM на гипервизоре Microsoft Windows Server (Hyper-V), для подключения Сервера интеграции к виртуальной инфраструктуре может использоваться только учетная запись с правами администратора.

4. Нажмите на кнопку **Подключиться**.

   Окно **Параметры подключения к виртуальной инфраструктуре** закроется. Мастер добавляет выбранные гипервизоры и / или серверы управления виртуальной инфраструктурой в список и пытается установить подключение.

   При этом мастер проверяет подлинность всех гипервизоров и серверов управления виртуальной инфраструктурой, к которым выполняется подключение, кроме гипервизора Microsoft Windows Server (Hyper-V). Для гипервизора Microsoft Windows Server (Hyper-V) проверка подлинности не выполняется.

   Для проверки подлинности мастер получает от каждого гипервизора или сервера управления виртуальной инфраструктурой SSL-сертификат или отпечаток открытого ключа и проверяет их.

   Если не удалось установить подлинность полученного сертификата, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. Если сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и продолжить подключение к гипервизору или к серверу управления виртуальной инфраструктурой. Для этого нажмите на кнопку **Считать сертификат подлинным**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center. Если вы не считаете этот сертификат подлинным, нажмите на кнопку **Отмена** в окне **Проверка сертификата**, чтобы прервать подключение, и замените сертификат на новый.

   Если не удалось установить подлинность открытого ключа, открывается окно **Проверка отпечатка открытого ключа** с сообщением об этом. Если вы хотите подтвердить подлинность открытого ключа и продолжить подключение к гипервизору, нажмите на кнопку **Считать открытый ключ подлинным**. Отпечаток открытого ключа будет сохранен на компьютере, где установлена Консоль администрирования Kaspersky Security Center. Если вы не считаете этот открытый ключ подлинным, нажмите на кнопку **Отмена** в окне **Проверка отпечатка открытого ключа**, чтобы прервать подключение.

   Если подключение к гипервизору или серверу управления виртуальной инфраструктурой не удалось установить, информация об ошибках подключения отображается в таблице.

В таблице отображается следующая информация о гипервизорах и SVM, ранее развернутых на гипервизорах:

- **Имя**

  Имя гипервизора, сервера управления виртуальной инфраструктурой или имя SVM, развернутой на гипервизоре.

  Если имеются ограничения для развертывания SVM на гипервизоре или не установлено соединение с гипервизором или сервером управления виртуальной инфраструктурой, в графе **Имя** отображается значок предупреждения. В таблице и во всплывающей подсказке к значку отображается описание ограничения или ошибки подключения.

- **Состояние**

  Состояние гипервизора или SVM.

  Для гипервизора указывается одно из следующих значений: `Включен`, `Выключен`.

Если не удалось установить подключение к гипервизору, в графе отображается `Соединение не установлено`.

Для SVM указывается одно из следующих значений: `Запущена`, `Остановлена`.

- **Защита**

  Номер версии программы, установленной на SVM.

- **Тип**

  Тип гипервизора или сервера управления виртуальной инфраструктурой.

Вы можете выполнить поиск гипервизора или сервера управления виртуальной инфраструктурой в списке. Поиск выполняется по значению графы **Имя**. Поиск инициируется во время ввода символов в поле **Найти**. В таблице отображаются только те гипервизоры и серверы управления виртуальной инфраструктурой, которые удовлетворяют условиям поиска. Чтобы сбросить результаты поиска, нужно удалить содержимое поля **Найти**.

Вы можете обновить список гипервизоров в таблице с помощью кнопки **Обновить**, расположенной над списком. При этом выполняется проверка SSL-сертификатов гипервизоров и серверов управления виртуальной инфраструктурой, как при добавлении гипервизора или сервера управления виртуальной инфраструктурой в список.

С помощью кнопок в графе **Имя** вы можете выполнить следующие действия:

- Удалить из списка выбранный гипервизор или все гипервизоры под управлением выбранного сервера управления виртуальной инфраструктурой.

  Сервер интеграции продолжает подключаться к удаленному из этого списка гипервизору или серверу управления виртуальной инфраструктурой и получать информацию о виртуальной инфраструктуре, необходимую для работы SVM.

- Если не удалось подключиться к гипервизору или серверу управления виртуальной инфраструктурой, открыть окно **Параметры подключения к виртуальной инфраструктуре** для изменения параметров учетной записи, под которой выполняется подключение.

  После изменения параметров выполняется проверка SSL-сертификата или отпечатка открытого ключа гипервизора или сервера управления виртуальной инфраструктурой, как при добавлении гипервизоров или серверов управления виртуальной инфраструктурой в список.

► *Чтобы выбрать гипервизоры для развертывания SVM, выполните следующие действия:*

1. Установите в таблице флажки слева от названий гипервизоров, на которых вы хотите развернуть SVM.

   Вы можете выбирать гипервизоры, для которых отсутствуют ограничения для развертывания SVM.

2. Если вы хотите разрешить параллельное развертывание SVM на нескольких гипервизорах, установите флажок **Разрешить параллельное развертывание одновременно на N гипервизорах**.

Перейдите к следующему шагу мастера.

Выбор образа SVM

На этом шаге укажите файл образа SVM для развертывания на гипервизоре. Файл образа SVM и файл

описания образов SVM (файл в формате XML), которые вы создали во время подготовки к установке программы (см. раздел "Подготовка образов SVM" на стр. 39), должны быть размещены в одной папке. Если вы устанавливаете Сервер защиты на гипервизоры разных типов, в одной папке должны быть размещены файлы образов SVM для каждого типа гипервизоров и файл описания образов SVM.

Чтобы указать образ SVM, нажмите на кнопку **Обзор** и в открывшемся окне выберите файл описания образов SVM (файл в формате XML).

После выбора файла в поле слева от кнопки отображается полный путь к файлу и его имя. Мастер автоматически выберет нужный файл образа SVM:

- файл в формате VHDX для развертывания на гипервизоре Microsoft Windows Server (Hyper-V);
- файл в формате XVA для развертывания на гипервизоре Citrix Hypervisor;
- файл в формате OVA для развертывания на гипервизоре VMware ESXi;
- файл в формате QCOW2 для развертывания на гипервизоре KVM, на гипервизоре Proxmox VE, на гипервизоре P-Виртуализация, на гипервизоре HUAWEI FusionCompute CNA или на гипервизоре Nutanix AHV.

В окне отображается следующая информация о выбранном образе:

- **Производитель**

  Производитель программы, которая установлена на SVM.

- **Издатель**

  Издатель, который опубликовал файл образа SVM. Для развертывания SVM используйте файлы образов, издателем которых является "Лаборатория Касперского".

- **Название программы**

  Название программы, которая установлена на SVM.

- **Версия SVM**

  Номер версии образа SVM.

- **Описание**

  Краткое описание образа SVM.

- **Размер виртуального диска**

  Объем дискового пространства, которое требуется для развертывания SVM в хранилище данных гипервизора.

Мастер выполняет проверку подлинности образа. Результаты проверки отображаются в окне следующим образом:

- Если образ является подлинным, в поле **Издатель** отображается значение **АО "Лаборатория Касперского"**.
- Если подлинность образа не подтверждена, в верхней части окна отображается сообщение об ошибке, в поле **Издатель** отображается значение **Неизвестно**.

Если подлинность образа не подтверждена, рекомендуется повторно создать образ SVM (см. раздел "Подготовка образов SVM" на стр. 39).

В блоке **Проверка целостности образа SVM** отображается информация о результатах проверки файла образа SVM для каждого типа гипервизоров. Если проверка файла образа не выполнялась, отображается сообщение **Проверка не проводилась**.

Рекомендуется выполнить проверку целостности файла образа SVM. Для этого нажмите на кнопку **Проверить** в блоке **Проверка целостности образа SVM**. Результаты проверки отображаются в окне следующим образом:

- Если проверка целостности файла образа прошла успешно, отображается сообщение **Целостность не нарушена**.
- Если файл образа изменен или поврежден или формат образа не поддерживается, в верхней части окна отображается сообщение об ошибке, в блоке **Проверка целостности образа SVM** отображается информация об обнаруженной проблеме.

Если проверка целостности файла образа SVM завершилась с ошибкой, рекомендуется повторно создать образ SVM (см. раздел "Подготовка образов SVM" на стр. 39) и убедиться, что во время копирования не произошло ошибок и что образ не был поврежден.

Если подлинность образа подтверждена и проверка целостности файла образа завершилась успешно, перейдите к следующему шагу мастера.

Если подлинность образа не подтверждена, проверка целостности файла образа не выполнялась или завершилась с ошибкой, но вы принимаете на себя риск и хотите использовать выбранный образ SVM, для перехода к следующему шагу мастера вам нужно установить флажок, расположенный в нижней части окна.

Ввод параметров SVM

На этом шаге в графе **Гипервизор** отображается IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором будет развернута SVM.

В графе **Имя SVM** введите полное доменное имя (FQDN) SVM, которая будет развернута на гипервизоре, и укажите следующие параметры SVM:

- **Хранилище**

  Хранилище данных гипервизора для образа SVM.

  В раскрывающемся списке отображаются хранилища, доступные для развертывания SVM.

  Если вы разворачиваете SVM на гипервизоре Microsoft Windows Server (Hyper-V), входящем в кластер, в списке доступны для выбора только общие хранилища.

  Если вы разворачиваете SVM на гипервизоре Microsoft Windows Server (Hyper-V), не входящем в кластер, вы можете ввести путь к хранилищу вручную.

- **Имя сети**

  Имя виртуальной сети, которую SVM должна использовать для связи с

виртуальными машинами и Сервером администрирования Kaspersky Security Center.

Вы можете указать одну или несколько виртуальных сетей, доступных на гипервизоре. Для добавления или удаления поля для выбора виртуальных сетей используйте кнопки, расположенные рядом с полем выбора сети.

Если в виртуальной инфраструктуре используется компонент VMware Distributed Virtual Switch, вы можете указать распределенную группу портов (Distributed Virtual Port Group), к которой будет подключена SVM.

Если вы планируете использовать динамическую IP-адресацию (DHCP) для всех SVM, сетевые параметры будут получены от сервера DHCP по первой виртуальной сети из списка указанных сетей для каждой из SVM. Убедитесь, что мастер сможет подключиться к SVM с сетевыми параметрами первой виртуальной сети, полученными от сервера DHCP.

- **Идентификатор VLAN**

  Идентификатор виртуальной локальной сети (VLAN), которая используется для связи SVM с виртуальными машинами и Сервером администрирования Kaspersky Security Center.

  Если виртуальная локальная сеть не используется, в графе отображается `Нет`.

Графа **Идентификатор VLAN** отображается, если для развертывания SVM выбран гипервизор Microsoft Windows Server (Hyper-V).

Перейдите к следующему шагу мастера.

Настройка сетевых параметров SVM

На этом шаге укажите сетевые параметры для SVM. Выполните одно из следующих действий:

- Выберите вариант **Динамическая IP-адресация (DHCP)**, если вы хотите использовать для всех SVM сетевые параметры, полученные по протоколу DHCP.

  По умолчанию для каждой SVM используются IP-адрес DNS-сервера и IP-адрес альтернативного DNS-сервера, полученные по протоколу DHCP. Если на предыдущем шаге вы указали несколько виртуальных сетей для SVM, по умолчанию сетевые параметры для SVM будут получены от сервера DHCP по первой виртуальной сети из списка указанных сетей.

  Если вы хотите указать IP-адрес DNS-сервера и альтернативного DNS-сервера вручную, снимите флажок **Использовать список DNS-серверов, полученных по DHCP**. Откроется таблица, содержащая следующую информацию:

  - **Гипервизор**

    IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором будет развернута SVM.

  - **Имя SVM**

    Полное доменное имя (FQDN) SVM.

  Укажите IP-адреса DNS-серверов в графах таблицы **DNS-сервер** и **Альтернативный DNS-сервер**.

- Выберите вариант **Статическая IP-адресация**, если вы хотите назначить все сетевые параметры SVM вручную. Откроется таблица, содержащая следующую информацию:

- **Гипервизор**

  IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором будет развернута SVM.

- **Имя SVM**

  Полное доменное имя (FQDN) SVM.

- **Имя сети**

  Имя виртуальной сети, которую SVM должна использовать для связи с виртуальными машинами и Сервером администрирования Kaspersky Security Center.

Укажите следующие сетевые параметры для каждой SVM:

- IP-адрес SVM;
- маска подсети;
- шлюз;
- DNS-сервер;
- альтернативный DNS-сервер.

Если на предыдущем шаге вы указали несколько виртуальных сетей для SVM, укажите сетевые параметры для каждой виртуальной сети.

Перейдите к следующему шагу мастера.

Ввод параметров подключения к Kaspersky Security Center

Этот шаг выполняется, если мастер не может автоматически определить параметры подключения к Kaspersky Security Center.

На этом шаге укажите следующие параметры подключения SVM к Серверу администрирования Kaspersky Security Center:

- **Адрес**

  Адрес компьютера, на котором установлен Сервер администрирования Kaspersky Security Center. Вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера.

- **Порт**

  Номер порта для подключения SVM к Серверу администрирования Kaspersky Security Center.

- **SSL-порт**

  Номер порта для подключения SVM к Серверу администрирования Kaspersky Security Center с использованием SSL-сертификата.

Перейдите к следующему шагу мастера.

Создание пароля конфигурирования и пароля учетной записи root

На этом шаге создайте пароль конфигурирования и пароль учетной записи root на SVM.

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.

Пароль конфигурирования требуется для изменения конфигурации SVM. Задайте пароль конфигурирования в полях **Пароль** и **Подтверждение пароля** в блоке **Пароль конфигурирования**.

Учетная запись root используется для доступа к операционной системе на SVM. Задайте пароль учетной записи root в полях **Пароль** и **Подтверждение пароля** в блоке **Пароль учетной записи root**.

Если вы хотите настроить доступ для учетной записи root к SVM через SSH, установите флажок **Разрешить удаленный доступ для учетной записи root через SSH**.

Перейдите к следующему шагу мастера.

Запуск развертывания SVM

На этом шаге в окне мастера отображаются все ранее введенные параметры, необходимые для развертывания SVM на гипервизоре:

- **Файл описания образов SVM** – полный путь и имя файла описания образов SVM (файла в формате XML), который вы указали на шаге выбора образа SVM.
- **Сетевые параметры SVM** – способ назначения сетевых параметров SVM. Возможные значения: Динамическая IP-адресация (DHCP), Статическая IP-адресация.
- **Удаленный доступ для учетной записи root через SSH** – возможность удаленного доступа для учетной записи root к SVM через SSH. Возможные значения: Разрешен, Запрещен.
- **Параметры подключения к Kaspersky Security Center** – IP-адрес (в формате IPv4) или полное доменное имя (FQDN) компьютера, на котором установлен Сервер администрирования Kaspersky Security Center, и номера портов для подключения SVM к Серверу администрирования Kaspersky Security Center.
- **Параллельное развертывание** – количество гипервизоров, на которых SVM будут разворачиваться параллельно.

Таблица **Индивидуальные параметры для каждого гипервизора** содержит параметры развертывания SVM на каждом гипервизоре:

- **Гипервизор** – IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором будет развернута SVM.
- **Имя SVM** – полное доменное имя (FQDN) SVM.
- **Хранилище** – хранилище данных гипервизора для образа SVM.
- **Имя сети** – имя виртуальной сети, которую SVM должна использовать для связи с виртуальными

машинами и Сервером администрирования Kaspersky Security Center.

- Все сетевые параметры, которые вы указали для SVM.

Чтобы запустить развертывание SVM, перейдите к следующему шагу мастера.

Развертывание SVM

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

В окне построчно отображаются этапы развертывания каждой SVM с указанием статуса выполнения каждого из этапов: **Выполняется N%**, **Ожидание**, **Пропущено**, **Завершено**, **Ошибка**.

На последнем этапе развертывания SVM выполняется проверка подключения SVM к Серверу интеграции. Если установить соединение между SVM и Сервером интеграции не удалось, в окне отображается предупреждение об этом. После завершения развертывания SVM рекомендуется проверить, что Сервер интеграции запущен и доступен по сети со стороны SVM.

Если в ходе развертывания SVM на гипервизоре возникает ошибка, мастер выполняет на этом гипервизоре откат внесенных изменений. На остальных гипервизорах развертывание продолжается.

После завершения развертывания SVM автоматически включается.

Перейдите к следующему шагу мастера.

Завершение развертывания SVM

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

По ссылкам вы можете открыть краткий отчет и журнал работы мастера управления SVM.

В кратком отчете вы можете посмотреть следующую информацию:

- Адреса гипервизоров, на которых были развернуты SVM.
- Адреса развернутых SVM.
- Краткое описание выполненных этапов развертывания каждой SVM с указанием времени начала и окончания каждого этапа. Если при выполнении этапа произошла ошибка, информация об этом отображается в отчете.

Краткий отчет сохраняется во временном файле. Чтобы использовать информацию отчета в дальнейшем, нужно сохранить файл в место постоянного хранения.

Журнал работы мастера управления SVM (см. раздел "О журнале работы мастера управления SVM" на стр. 511) содержит информацию, указанную вами на каждом шаге мастера. Если развертывание SVM завершилось с ошибкой, вы можете использовать журнал работы мастера при обращении в Службу технической поддержки.

Журнал работы мастера управления SVM сохраняется на том компьютере, на котором был запущен мастер, в файле %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\<номер версии программы>\KasperskyDeploymentWizard.log и не содержит информации об учетных записях. Информация в файле перезаписывается при каждом запуске мастера. Чтобы использовать информацию журнала работы мастера в дальнейшем, нужно сохранить файл в место постоянного хранения.

Завершите работу мастера.

Если в вашей виртуальной инфраструктуре используется гипервизор Microsoft Windows Server (Hyper-V), после развертывания SVM в журнале событий может появиться сообщение о том, что на SVM требуется обновить пакет служб интеграции (Integration Services). Вы можете игнорировать это сообщение, для работы SVM обновление пакета служб интеграции не требуется.

Подготовка Сервера защиты к работе

После установки Сервера защиты рекомендуется проверить системную дату на SVM средствами используемого гипервизора. Несоответствие системной даты на Сервере администрирования Kaspersky Security Center и системной даты на SVM может привести к ошибке соединения SVM с Kaspersky Security Center и неверной работе программы.

После развертывания SVM на гипервизоре вы можете изменить выделенные под SVM ресурсы гипервизора, например, в соответствии с рекомендациями специалистов "Лаборатории Касперского" (см. раздел "Требования к ресурсам SVM с Сервером защиты Kaspersky Security" на стр. 24). Производительность SVM вы можете регулировать с помощью ресурсов, выделенных для нее.

После установки Сервера защиты требуется выполнить следующие действия:

1. Убедиться в том, что новые SVM подключены к Серверу интеграции. Вы можете посмотреть список подключенных SVM (см. раздел "Просмотр списка SVM, подключенных к Серверу интеграции" на стр. 105) в Консоли Сервера интеграции.
2. Активировать программу на всех новых SVM (см. раздел "Об активации программы" на стр. 78).

   Чтобы активировать программу на SVM, требуется добавить лицензионный ключ на SVM с помощью задачи активации программы (см. раздел "Процедура активации программы" на стр. 82). После установки компонента Легкий агент на виртуальных машинах компонент Сервер защиты передаст сведения о лицензии компоненту Легкий агент.
3. Обновить базы программы на всех новых SVM (см. раздел "Процедура обновления баз программы" на стр. 83).

В этом разделе

Об активации программы

Активация программы – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии (см. раздел "О лицензии" на стр. 79).

Для активации программы требуется добавить лицензионный ключ на все SVM. *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" и отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Для добавления лицензионного ключа на SVM используется *задача активации программы* (см. раздел "*Процедура активации программы*" на стр. 82). При создании задачи активации программы используется

ключ из хранилища ключей Kaspersky Security Center.

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

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

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

После активации программы на SVM компонент Сервер защиты передает сведения о лицензии компоненту Легкий агент, установленному на защищенных виртуальных машинах. Если статус лицензионного ключа изменяется, SVM передает информацию об этом Легкому агенту.

Информацию о лицензии, по которой активирована программа, вы можете посмотреть на защищенной виртуальной машине:

- для Легкого агента для Windows – в локальном интерфейсе Легкого агента для Windows в окне **Лицензирование**;
- для Легкого агента для Linux – с помощью команды `license`.

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

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

Если на защищенную виртуальную машину с компонентом Легкий агент для Windows не переданы сведения о лицензии, Легкий агент для Windows функционирует в режиме ограниченной функциональности:

- работает только компонент Легкого агента Файловый Антивирус;
- выполняются только задачи полной проверки, выборочной проверки и проверки важных областей;
- обновление баз и модулей программы, необходимых для работы Легкого агента, выполняется только один раз.

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

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

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

Предусмотрены следующие типы лицензий:

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

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

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

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Security). Чтобы продолжить использование Kaspersky Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

Функциональность программы, доступная по лицензии, зависит от *вида лицензии*. Для программы Kaspersky Security предусмотрены следующие виды лицензии:

- стандартная лицензия;
- расширенная лицензия.

> На всех SVM, подключенных к одному Серверу интеграции, программа должна быть активирована по лицензии одного вида.

Следующая функциональность программы доступна, только если вы используете программу по расширенной лицензии:

- Компонент Контроль целостности системы.
- Компонент Контроль запуска программ, установленный на виртуальной машине с операционной системой для серверов.
- Расширенные возможности выбора SVM: использование тегов для подключения Легких агентов к SVM и настройка алгоритма выбора SVM для подключения.

> Рекомендуется учитывать, что функциональность программы, доступная по расширенной лицензии, доступна на Легком агенте, только если Легкий агент подключен к SVM, на которую добавлен ключ для расширенной лицензии.

Для программы 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, на которых установлен компонент Легкий агент.

Для программы Kaspersky Security для виртуальных сред 5.2 Легкий агент вы также можете использовать ключ, предназначенный для программы Kaspersky Endpoint Security для бизнеса – Универсальный. Этот ключ позволяет защищать определенное количество виртуальных машин независимо от установленной на них операционной системы.

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

Особенности добавления ключей

При добавлении ключей следует учитывать следующие особенности:

- Не поддерживается одновременное использование на SVM нескольких лицензионных ключей одного типа. Если вы добавляете ключ на SVM, на которую ранее был добавлен ключ того же типа, новый ключ заменяет ранее добавленный ключ.
- 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 системам 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 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 удаляется с SVM. 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) резервный 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 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 / расширенная лицензия).

  Например, если вы добавляете ключ, соответствующий расширенной лицензии, а ранее программа использовалась по стандартной лицензии, то все активные и (при наличии) резервные ключи, соответствующие стандартной лицензии, удаляются с SVM. Вместо них добавляется ключ, соответствующий расширенной лицензии.

Процедура активации программы

Для активации программы требуется создать и выполнить задачу активации на всех SVM.

Активация программы должна быть выполнена на SVM с актуальными системными датой и временем. Если вы изменили системные дату и время после активации программы, ключ становится неработоспособным. Программа переходит к режиму работы без обновления баз, и Kaspersky Security Network недоступен. Восстановить работоспособность ключа можно только переустановкой операционной системы.

Если вы используете схему лицензирования по количеству защищаемых виртуальных машин, для защиты виртуальных машин с операционными системами для серверов и с операционными системами для рабочих станций вам нужно создать две задачи активации: для добавления на SVM ключа для серверов и для добавления на SVM ключа для рабочих станций.

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

1. Добавьте ключ в хранилище ключей Kaspersky Security Center:
   a. Откройте Консоль администрирования Kaspersky Security Center.
   b. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
   c. В рабочей области нажмите на кнопку **Добавить код активации или файл ключа**. Запустится мастер добавления ключа в хранилище.
   d. В окне мастера **Выбор способа активации программы** нажмите на кнопку **Активировать программу с помощью файла ключа**.
   e. На этом шаге мастера укажите путь к файлу ключа. Для этого нажмите на кнопку **Обзор** и в открывшемся окне выберите файл с расширением key. Перейдите к следующему шагу мастера.

f. Завершите работу мастера добавления ключа в хранилище.

Добавленный ключ отобразится в списке ключей в папке **Лицензии Лаборатории Касперского**.

2. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите папку с названием группы администрирования, в которую входят SVM.
3. В рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**. Запустится мастер создания задачи.
4. На первом шаге мастера укажите программу, для которой создается задача, и тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты** выберите **Активация программы**. Перейдите к следующему шагу мастера.
5. На этом шаге мастера выберите ключ из хранилища ключей Kaspersky Security Center. Для этого нажмите на кнопку **Добавить**. Откроется окно **Хранилище ключей Kaspersky Security Center**. Выберите ключ и нажмите на кнопку **OK**. Перейдите к следующему шагу мастера.
6. На этом шаге мастера вы можете настроить параметры расписания запуска задачи. Задача активации может запускать по расписанию, также вы можете в любой момент запустить задачу вручную. Перейдите к следующему шагу мастера.
7. На этом шаге мастера в поле **Имя** введите название задачи. Перейдите к следующему шагу мастера.
8. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**. Завершите работу мастера.

   Созданная задача активации программы отобразится в списке задач.
9. Дождитесь запуска задачи по расписанию, если вы настроили расписание запуска задачи, или запустите задачу вручную.

Вы можете запускать задачу (см. раздел "Запуск и остановка задач" на стр. 147) и просматривать информацию о результатах выполнения задачи в Консоли администрирования Kaspersky Security Center (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 148).

Процедура обновления баз программы

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

1. Убедитесь в том, что в Kaspersky Security Center создана задача загрузки обновлений в хранилище. Если задача загрузки обновлений в хранилище отсутствует, создайте ее (см. в документации Kaspersky Security Center).
2. Дождитесь запуска по расписанию задачи загрузки обновлений в хранилище или запустите задачу вручную.
3. Убедитесь в том, что задача загрузки обновлений в хранилище выполнена успешно (см. подробнее в документации Kaspersky Security Center).
4. Убедитесь в том, что в Kaspersky Security Center создана задача обновления баз на Сервере защиты. Если задача обновления баз на Сервере защиты отсутствует, запустите вручную мастер первоначальной настройки, чтобы создать ее (см. раздел "Автоматическое создание задач и политики по умолчанию для Сервера защиты" на стр. 62).
5. Дождитесь запуска задачи обновления баз на Сервере защиты по расписанию или запустите задачу вручную.

6. Убедитесь в том, что задача выполнена успешно. Вы можете просматривать информацию о результатах выполнения задачи в Консоли администрирования Kaspersky Security Center (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 148).

В результате выполнения задачи компонент Сервер защиты загружает пакет обновлений из хранилища Сервера администрирования в папку на SVM и автоматически устанавливает на SVM обновления баз, необходимых для работы Сервера защиты.

Установка Агента администрирования Kaspersky Security Center на виртуальные машины

Агент администрирования Kaspersky Security Center, установленный на защищенных виртуальных машинах, обеспечивает взаимодействие между Сервером администрирования Kaspersky Security Center и защищенными виртуальными машинами и позволяет управлять работой Легкого агента с помощью Kaspersky Security Center.

Вы можете установить Агент администрирования следующим способом:

- На виртуальные машины с операционной системой Windows – в ходе удаленной установки Легкого агента для Windows (см. раздел "Установка Легкого агента для Windows через Kaspersky Security Center" на стр. 85) с помощью мастера удаленной установки или задачи удаленной установки программы.

  Если вы используете мастер удаленной установки, Агент администрирования будет установлен автоматически.

  Если вы используете задачу удаленной установки программы, в параметрах задачи вы можете установить флажок **Установить Агент администрирования совместно с данной программой**.

- На виртуальные машины с операционной системой Linux – в результате установки Легкого агента для Linux из командной строки (см. раздел "Установка Легкого агента для Linux из командной строки" на стр. 93) или в результате удаленной установки Легкого агента для Linux через Kaspersky Security Center (см. раздел "Установка Легкого агента для Linux через Kaspersky Security Center" на стр. 98). Агент администрирования входит в состав shar-архива для установки Легкого агента для Linux и в состав инсталляционного пакета для Легкого агента для Linux, автоматически созданного мастером установки компонентов Kaspersky Security. Если вы создаете инсталляционный пакет для Легкого агента для Linux вручную (см. раздел "Создание инсталляционного пакета Легкого агента для Linux" на стр. 100), Агент администрирования будет включен в состав этого пакета.

  Вы также можете установить на виртуальную машину с операционной системой Linux только Агент администрирования, не устанавливая Легкий агент для Linux. Для этого вам нужно запустить установку Легкого агента для Linux из командной строки с параметром `--skip-product`.

Установка Легкого агента для Windows

Вы можете установить компонент Легкий агент для Windows удаленно с рабочего места администратора с помощью программы Kaspersky Security Center (см. раздел "Установка Легкого агента для Windows через Kaspersky Security Center" на стр. 85).

Перед началом установки Легкого агента для Windows рекомендуется закрыть все программы, работающие в операционной системе виртуальной машины.

Во время установки Легкий агент выполняет настройку брандмауэра Windows, чтобы разрешить входящий и исходящий трафик для процесса avp.exe. Если для брандмауэра Windows используется доменная политика, требуется настроить правила для входящих и исходящих подключений для процесса avp.exe в доменной политике. Если используется другой брандмауэр, требуется настроить правило для подключений для процесса avp.exe для этого брандмауэра. При первом запуске после установки компонент Сетевой экран будет включен, что приведет к отключению брандмауэра Windows.

На виртуальных машинах с гостевыми операционными системами ниже Windows 10 и Windows Server 2016 не поддерживается установка и работа компонента AMSI-защита (на стр. 221).

В этом разделе

Установка Легкого агента для Windows через Kaspersky Security Center

Вы можете установить Легкий агент для Windows удаленно с рабочего места администратора с помощью программы Kaspersky Security Center.

Установка выполняется с помощью мастера удаленной установки или задачи удаленной установки программы (см. подробнее в документации Kaspersky Security Center). Для установки используется инсталляционный пакет, который содержит набор параметров, необходимых для установки программы.

Вы можете использовать инсталляционный пакет, автоматически созданный мастером установки компонентов Kaspersky Security в ходе установки mmc-плагинов управления Kaspersky Security и Сервера интеграции, или создать инсталляционный пакет вручную (см. раздел "Создание инсталляционного пакета Легкого агента для Windows" на стр. 86).

Автоматически созданный инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** -> **Удаленная установка** -> **Инсталляционные пакеты** под именем **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows (5.2.X.X)**, где 5.2.X.X – номер версии программы.

Если вы хотите использовать автоматически созданный инсталляционный пакет, для установки программы в сертифицированном состоянии вам нужно изменить параметры установки Легкого агента для Windows в свойствах этого инсталляционного пакета перед началом установки (см. раздел "Настройка параметров инсталляционного пакета Легкого агента для Windows" на стр. 88).

Перед началом установки на виртуальной машине выполняется поиск и удаление программ, одновременная работа которых с Легким агентом может привести к конфликтам. Если автоматически удалить такие программы не удалось, установка завершается с ошибкой.

Если инсталляционный пакет предназначен для установки Легкого агента для Windows на виртуальные машины, на которых используется технология Citrix Provisioning (Citrix Provisioning Services), вам нужно выполнить одно из следующих действий:

- Перед созданием инсталляционного пакета вручную внести в файл ksvla.kud из состава дистрибутива Легкого агента для Windows следующее изменение:

  добавить параметр `/pINSTALLONPVS=1` в секции `[Setup]` в конце строки `Params=/s /pAKINSTALL=1 /pEULAANDPRIVACYPOLICY=1`.

- В параметрах созданного инсталляционного пакета установить флажок **Обеспечить совместимость с Citrix Provisioning (Citrix Provisioning Services)**.

В ходе удаленной установки Легкого агента для Windows через Kaspersky Security Center может быть автоматически установлен Агент администрирования Kaspersky Security Center (см. раздел "Установка Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 84).

В этом разделе

Создание инсталляционного пакета Легкого агента для Windows

Перед созданием инсталляционного пакета вам нужно распаковать дистрибутив (см. раздел "Распаковка дистрибутивов Легкого агента" на стр. 34) Легкого агента для Windows в папку, доступную для Сервера администрирования Kaspersky Security Center.

► *Чтобы создать инсталляционный пакет Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите **Дополнительно** -> **Удаленная установка** -> **Инсталляционные пакеты**.

3. Нажмите на кнопку **Создать инсталляционный пакет**, чтобы запустить мастер создания инсталляционного пакета.
4. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
5. В открывшемся окне введите название нового инсталляционного пакета и перейдите к следующему шагу мастера.
6. Выберите дистрибутив программы Kaspersky Security. Для этого откройте стандартное окно Windows с помощью кнопки **Обзор** и укажите путь к файлу ksvla.kud из состава дистрибутива Легкого агента для Windows.

   После выбора файла в окне мастера отобразится название программы.

   По умолчанию в окне мастера **Выбор дистрибутива программы для установки** установлен флажок **Скопировать обновления из хранилища в инсталляционный пакет**. Kaspersky Security Center включает в инсталляционный пакет все обновления баз Легкого агента для Windows, загруженные в хранилище Kaspersky Security Center. После установки компонента Легкий агент для Windows на виртуальной машине автоматически обновляются базы Легкого агента для Windows.

   Перейдите к следующему шагу мастера.
7. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Для продолжения создания инсталляционного пакета 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.
8. Мастер загружает файлы, необходимые для установки программы, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.
9. Выполните следующие действия:
   - Укажите компоненты, которые должны быть установлены на защищенной виртуальной машине в результате установки Легкого агента для Windows с использованием этого инсталляционного пакета.
     - Для установки программы в сертифицированном состоянии на виртуальные машины с операционными системами Microsoft Windows для серверов настройте список **Компоненты для установки на ОС для серверов** следующим образом:
       - установите флажки: **Почтовый Антивирус**, **Контроль запуска программ**, **Мониторинг системы**, **Контроль целостности системы**, **Интеграция с Kaspersky Endpoint Agent**, **AMSI-защита**;
       - снимите флажки: **Сетевой экран**, **Защита от сетевых атак**.
     - Для установки программы в сертифицированном состоянии на виртуальные машины с операционными системами Microsoft Windows для рабочих станций настройте список **Компоненты для установки на ОС для рабочих станций** следующим образом:
       - установите флажки: **Почтовый Антивирус**, **Веб-Антивирус**, **Контроль активности программ**, **Контроль запуска программ**, **Веб-Контроль**, **Мониторинг системы**, **Интеграция с Kaspersky Endpoint Agent**, **AMSI-защита**;
       - снимите флажки: **Сетевой экран**, **Защита от сетевых атак**, **Контроль устройств**.

Установка компонентов Сетевой экран, Защита от сетевых атак, Контроль устройств приводит к выходу программы из сертифицированного состояния.

- При необходимости укажите путь к папке установки. По умолчанию Легкий агент устанавливается в следующую папку в зависимости от операционной системы:
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\ – для 64-разрядных операционных систем.
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\ – для 32-разрядных операционных систем.

  Перейдите к следующему шагу мастера.

10. Мастер создает инсталляционный пакет и выводит сообщение об окончании процедуры. Завершите работу мастера.

Созданный инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** -> **Удаленная установка** -> **Инсталляционные пакеты**. Вы можете использовать один и тот же инсталляционный пакет многократно.

После создания инсталляционного пакета вы можете изменить параметры установки Легкого агента для Windows или выполнить более детальную настройку параметров установки (см. раздел "Настройка параметров инсталляционного пакета Легкого агента для Windows" на стр. 88).

Настройка параметров инсталляционного пакета Легкого агента для Windows

► *Чтобы настроить параметры инсталляционного пакета Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите **Дополнительно** -> **Удаленная установка** -> **Инсталляционные пакеты**.
3. В списке инсталляционных пакетов выберите инсталляционный пакет Легкого агента и откройте окно **Свойства: <имя инсталляционного пакета>** одним из следующих способов:
   - двойным щелчком мыши;
   - по правой клавише мыши вызовите контекстное меню и выберите пункт **Свойства**;
   - по ссылке **Настроить параметры инсталляционного пакета**, расположенной справа от списка задач в блоке с параметрами инсталляционного пакета.

   Все разделы окна **Свойства: <имя инсталляционного пакета>**, кроме раздела **Параметры**, стандартны для программы Kaspersky Security Center. Описание стандартных разделов см. в документации Kaspersky Security Center.
4. В списке слева выберите раздел **Параметры** и укажите компоненты, которые должны быть установлены на защищенной виртуальной машине в результате установки Легкого агента для Windows с использованием этого инсталляционного пакета.
   - Для установки программы в сертифицированном состоянии на виртуальные машины с операционными системами Microsoft Windows для серверов настройте список **Компоненты для установки на ОС для серверов** следующим образом:
     - установите флажки: **Почтовый Антивирус**, **Контроль запуска программ**, **Мониторинг**

системы, **Контроль целостности системы**, **Интеграция с Kaspersky Endpoint Agent**, **AMSI-защита**;

- снимите флажки: **Сетевой экран**, **Защита от сетевых атак**.

- Для установки программы в сертифицированном состоянии на виртуальные машины с операционными системами Microsoft Windows для рабочих станций настройте список **Компоненты для установки на ОС для рабочих станций** следующим образом:
  - установите флажки: **Почтовый Антивирус**, **Веб-Антивирус**, **Контроль активности программ**, **Контроль запуска программ**, **Веб-Контроль**, **Мониторинг системы**, **Интеграция с Kaspersky Endpoint Agent**, **AMSI-защита**;
  - снимите флажки: **Сетевой экран**, **Защита от сетевых атак**, **Контроль устройств**.

Установка компонентов Сетевой экран, Защита от сетевых атак, Контроль устройств приводит к выходу программы из сертифицированного состояния.

Также вы можете выполнить следующие действия:

- Включить или выключить защиту процесса установки программы Kaspersky Security, чтобы во время установки программы ни один процесс не мог изменить содержимое папки установки программы, внедриться в процесс установки или остановить его. По умолчанию защита включена.
- Включить или выключить добавление в системную переменную окружения %PATH% пути к папке установки программы. По умолчанию путь к папке установки добавляется в переменную. В результате для запуска из командной строки исполняемого файла, расположенного в папке установки программы, не требуется вводить путь к исполняемому файлу. Достаточно ввести имя исполняемого файла.
- Включить или выключить добавление в доверенную зону программ, рекомендованных компанией Microsoft для исключения из проверки. По умолчанию программы, рекомендованные компанией Microsoft для исключения из проверки, добавляются в доверенную зону.
- Установить флажок **Установка на шаблон для временных пулов VDI**, если инсталляционный пакет предназначен для установки Легкого агента на шаблон временных виртуальных машин, из которого будет создана инфраструктура VDI одного из следующих типов:
  - каталог Citrix XenDesktop random;
  - каталог Citrix XenDesktop static без сохранения изменений пользователя;
  - automated-пул VMware Horizon типа instant clone;
  - группа виртуальных машин типа Linked Clone для HUAWEI FusionAccess.

  Если флажок установлен, обновления, требующие перезагрузки защищенной виртуальной машины, не будут устанавливаться на виртуальных машинах, созданных из этого шаблона. При получении обновлений, требующих перезагрузки защищенной виртуальной машины, Легкий агент будет отправлять в Kaspersky Security Center сообщение о необходимости обновления баз программы на шаблоне защищенных виртуальных машин.

  Не рекомендуется устанавливать флажок **Установка на шаблон для временных пулов VDI**, если инсталляционный пакет будет использоваться для установки Легкого агента на шаблон временных виртуальных машин, из которого будет создана инфраструктура VDI одного из следующих типов:

  - каталог Citrix XenDesktop static dedicated с использованием локальных дисков;

- automated-пул VMware Horizon типа full clone;
- группа виртуальных машин типа Full Copy для HUAWEI FusionAccess.

- Установить флажок **Обеспечить совместимость с Citrix Provisioning (Citrix Provisioning Services)**, если инсталляционный пакет предназначен для установки Легкого агента на виртуальную машину, на которой используется технология Citrix Provisioning (Citrix Provisioning Services).
- Указать путь к папке, в которую вы хотите установить Легкий агент. По умолчанию Легкий агент устанавливается в следующую папку в зависимости от операционной системы:
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\ – для 64-разрядных операционных систем.
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\ – для 32-разрядных операционных систем.

Все разделы окна **Свойства: <имя инсталляционного пакета>**, кроме раздела **Параметры**, стандартны для программы Kaspersky Security Center. Описание стандартных разделов см. в документации Kaspersky Security Center.

5. Нажмите на кнопку **OK** в окне **Свойства: <имя инсталляционного пакета>**.

Установка Легкого агента для Windows на шаблон виртуальных машин

► *Чтобы установить компонент Легкий агент для Windows на шаблон виртуальных машин, выполните следующие действия:*

1. Включите на гипервизоре виртуальную машину, являющуюся шаблоном виртуальных машин.
2. В параметрах инсталляционного пакета (см. раздел "Настройка параметров инсталляционного пакета Легкого агента для Windows" на стр. 88) установите флажок **Установка на шаблон для временных пулов VDI**, если вы устанавливаете Легкий агент на шаблон временных виртуальных машин, из которого будет создана инфраструктура VDI одного из следующих типов:
   - каталог Citrix XenDesktop random;
   - каталог Citrix XenDesktop static без сохранения изменений пользователя;
   - automated-пул VMware Horizon типа instant clone;
   - группа виртуальных машин типа Linked Clone для HUAWEI FusionAccess.

   Если флажок установлен, обновления, требующие перезагрузки защищенной виртуальной машины, не будут устанавливаться на виртуальных машинах, созданных из этого шаблона. При получении обновлений, требующих перезагрузки защищенной виртуальной машины, Легкий агент будет отправлять в Kaspersky Security Center сообщение о необходимости обновления баз программы на шаблоне защищенных виртуальных машин.

   Не рекомендуется устанавливать флажок **Установка на шаблон для временных пулов VDI**, если вы устанавливаете Легкий агент на шаблон временных виртуальных машин, из которого будет создана инфраструктура VDI одного из следующих типов:
   - каталог Citrix XenDesktop static dedicated с использованием локальных дисков;
   - automated-пул VMware Horizon типа full clone;

- группа виртуальных машин типа Full Copy для HUAWEI FusionAccess.

3. Установите компонент Легкий агент для Windows (см. раздел "Установка Легкого агента для Windows через Kaspersky Security Center" на стр. 85) на шаблон виртуальных машин.
4. После завершения установки настройте параметры подключения Легкого агента к SVM в локальном интерфейсе Легкого агента для Windows (см. раздел "Настройка параметров обнаружения SVM" на стр. 168). После подключения Сервер защиты передает Легкому агенту сведения о лицензии. Вам требуется дождаться получения Легким агентом сведений о лицензии.
5. Легкий агент проверяет наличие пакета обновлений в папке на той SVM, к которой он подключен. При наличии пакета обновлений Легкий агент для Windows устанавливает на защищенной виртуальной машине обновления баз программы, необходимые для своей работы.

   Вы можете дождаться получения Легким агентом обновлений баз или запустить задачу обновления вручную в локальном интерфейсе Легкого агента для Windows, а затем выполнить проверку шаблона виртуальных машин на наличие вредоносных программ.

   Рекомендуется перезагрузить шаблон виртуальных машин для оптимизации процесса загрузки операционной системы.

После завершения установки Легкого агента на шаблон виртуальных машин вы можете создавать виртуальные машины из этого шаблона. Подробнее см. в документации к виртуальной инфраструктуре.

Об установке Легкого агента на шаблоны виртуальных машин см. также в Базе знаний (https://support.kaspersky.ru/14049).

Совместимость с технологией Citrix App Layering

Вы можете использовать программу Kaspersky Security для защиты виртуальных машин в инфраструктуре, в которой используется технология Citrix App Layering (ранее UniDesk).

Если для сохранения состояния временных виртуальных машин вы планируете использовать полный пользовательский слой (Full User Layer), перед установкой программы на шаблоне виртуальных машин вам нужно выполнить следующие действия:

1. Внести в реестр операционной системы на слое приложений (Application Layer) следующие изменения:
   a. В разделе реестра HKLM\SYSTEM\CurrentControlSet\Services\uniflt\ создать новый ключ типа мультистроковый параметр с именем AlwaysOnBoot:
      - `C:\ProgramData\KasperskyLab\`
      - `C:\ProgramData\Kaspersky Lab\`
      - `C:\Program Files(x86)\Kaspersky Lab\`
   b. В разделе реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr создать новый ключ типа DWORD с именем MiniFilterBypass и значением 1.
2. Перезагрузить виртуальную машину.

Для установки программы на виртуальных машинах в инфраструктуре, в которой используется технология Citrix App Layering, вам нужно выполнить следующие действия:

1. Установить Агент администрирования Kaspersky Security Center и Легкий агент для Windows на шаблоне виртуальных машин на слой приложений (Application Layer).
2. Создать образ виртуальной машины, состоящий из нескольких слоев.

3. Развернуть созданный образ на гипервизорах, которые поддерживают решение Citrix App Layering.
4. Настроить создание временных виртуальных машин из созданного образа.

Подробнее об установке антивирусного ПО совместно с Citrix App Layering см. в документации Citrix App Layering (https://docs.citrix.com/en-us/citrix-app-layering/4.html).

Совместимость с технологией Citrix Provisioning Services

Вы можете установить Легкий агент на виртуальную машину, на которой используется технология Citrix Provisioning (Citrix Provisioning Services).

Если на виртуальной машине установлено программное обеспечение Citrix Provisioning Services Target Device, требуется удалить его перед началом установки компонента Легкий агент. После установки Легкого агента требуется установить Citrix Provisioning Services Target Device.

Чтобы обеспечить совместимость программы с технологией Citrix Provisioning (Citrix Provisioning Services), требуется во время установки Легкого агента (см. раздел "Установка Легкого агента для Windows через Kaspersky Security Center" на стр. 85) установить флажок **Обеспечить совместимость с Citrix Provisioning (Citrix Provisioning Services)**.

В локальном интерфейсе Легкого агента вы можете посмотреть информацию о совместимости с технологией Citrix Provisioning (Citrix Provisioning Services) в окне **Поддержка**, которое открывается из главного окна программы (см. раздел "Главное окно программы" на стр. 120).

Установка Легкого агента для Linux

Легкий агент для Linux может быть установлен на виртуальную машину одним из следующих способов:

- из командной строки;
- удаленно с рабочего места администратора с помощью программы Kaspersky Security Center (см. раздел "Установка Легкого агента для Linux через Kaspersky Security Center" на стр. 98).

Если операционная система виртуальной машины, на которую вы планируете установить Легкий агент для Linux, не поддерживает технологию fanotify, для обработки операций над объектами файловой системы требуется компиляция модуля ядра операционной системы Linux. Компиляция будет выполнена автоматически после установки Легкого агента для Linux. Чтобы компиляция завершилась успешно, перед установкой Легкого агента для Linux вам нужно загрузить исходные коды ядра операционной системы на виртуальную машину и установить на виртуальной машине пакеты для компиляции (gcc, binutils, glibc, glibc-devel, make, ld). Если вы планируете установить Легкий агент удаленно через Kaspersky Security Center или из командной строки в тихом режиме, исходные коды ядра операционной системы требуется разместить в директории по умолчанию.

kaspersky

В этом разделе

Установка Легкого агента для Linux из командной строки

Перед началом установки вам нужно распаковать дистрибутив Легкого агента для Linux (см. раздел "Распаковка дистрибутивов Легкого агента" на стр. 34).

Вы можете установить Легкий агента для Linux из командной строки одним из следующих способов:

- в тихом режиме (см. раздел "Установка Легкого агента для Linux в тихом режиме" на стр. 94);
- в интерактивном режиме (см. раздел "Установка Легкого агента для Linux в интерактивном режиме" на стр. 96).

Установка компонента Легкий агент для Linux из командной строки выполняется с помощью скрипта установки, который содержится в самораспаковывающемся shar-архиве lightagent-5.2.X-X-bundle.sh, где 5.2.X-X – номер версии программы.

В состав архива lightagent-5.2.X-X-bundle.sh входят пакеты, необходимые для установки Легкого агента для Linux и Агента администрирования Kaspersky Security Center поддерживаемой версии.

Вы можете запускать установку Легкого агента для Linux со следующими параметрами:

- `--skip-product` – установка только Агента администрирования Kaspersky Security Center.
- `--skip-klnagent` – установка только Легкого агента для Linux с предварительной проверкой, что установлена поддерживаемая версия Агента администрирования (версия, которая входит в состав shar-архива). Если поддерживаемая версия Агента администрирования не установлена, то Легкий агент для Linux не будет установлен, установка завершается с ошибкой.
- `--skip-klnagent --skip-klnagent-version-check` – установка только Легкого агента для Linux с предварительной проверкой, что на виртуальной машине установлен Агент администрирования любой версии. Если Агент администрирования не установлен, то Легкий агент для Linux не будет установлен, установка завершается с ошибкой.

  Для работы Легкого агента для Linux требуется Агент администрирования одной из следующих версий: 12.0.1.60 (для 32-разрядных операционных систем) или 12.0.0.60 (для 64-разрядных операционных систем).

- `--auto-install=<путь к конфигурационному файлу>` – установка Легкого агента для Linux и Агента администрирования в тихом режиме, где <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, содержащему параметры для первоначальной настройки Легкого агента для Linux и Агента администрирования.
- `-x` – распаковка содержимого shar-архива в директорию, где расположен shar-архив.

- `--force-install` – установка Легкого агента для Linux и Агента администрирования с предварительным удалением ранее установленного Легкого агента.
- `--clean` – установка Легкого агента для Linux и Агента администрирования с предварительным удалением ранее установленных Легкого агента для Linux и Агента администрирования, включая их директории, конфигурационные файлы, измененные пользователем, базы и файлы трассировки.

Установка Легкого агента для Linux в тихом режиме

Если операционная система виртуальной машины, на которую вы планируете установить Легкий агент для Linux, не поддерживает технологию fanotify, перед началом установки убедитесь, что на виртуальной машине исходные коды ядра операционной системы находятся в директории по умолчанию и установлены пакеты для компиляции (gcc, binutils, glibc, glibc-devel, make, ld).

► *Чтобы установить Легкий агент для Linux из командной строки в тихом режиме, выполните следующие действия:*

1. В конфигурационном файле lightagent.ini укажите параметры, которые должен использовать скрипт установки во время первоначальной настройки Легкого агента для Linux. Файл lightagent.ini входит в состав дистрибутива Легкого агента для Linux (см. раздел "Файлы, необходимые для установки программы" на стр. 31). Вы можете указать следующие параметры:

   - `ACCEPT_EULA_AND_PRIVACYPOLICY` – согласие с условиями Лицензионного соглашения программы Kaspersky Security, которое заключается между вами и "Лабораторией Касперского", и Политики конфиденциальности, которая описывает обработку и передачу данных. Возможные значения: `yes`, `no`.

     Согласие с условиями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки программы.

     Установив значение `yes`, вы подтверждаете следующее:

     - вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения программы Kaspersky Security;
     - 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.

     Текст Лицензионного соглашения и Политики конфиденциальности входит в комплект поставки программы.

   - `CONNECTOR_LOCALE` – идентификатор языка Легкого агента для Linux. Возможные значения: `ru`, `en`, `fr`, `de`, `zh-Hans`, `zh-Hant`, `ja`.
   - `DEFAULT_KERNEL_SOURCES` – использовать путь по умолчанию к исходным кодам ядра операционной системы. Возможные значения: `yes`, `no`.

> Если операционная система не поддерживает технологию fanotify, требуется разместить исходные коды ядра операционной системы в директории по умолчанию и указать значение параметра `DEFAULT_KERNEL_SOURCES=yes`. Иначе установка Легкого агента завершится с ошибкой.

2. В конфигурационном файле klnagent.ini укажите параметры, которые должен использовать скрипт установки во время первоначальной настройки Агента администрирования. Файл klnagent.ini входит в состав дистрибутива Легкого агента для Linux (см. раздел "Файлы, необходимые для установки программы" на стр. 31). Вы можете указать следующие параметры:
   - `KLNAGENT_SERVER` – IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер администрирования Kaspersky Security Center.
   - `KLNAGENT_PORT` – номер порта для подключения Агента администрирования к Серверу администрирования. По умолчанию Сервер администрирования Kaspersky Security Center использует порт 14000.
   - `KLNAGENT_SSLPORT` – номер порта для подключения Агента администрирования к Серверу администрирования с использованием SSL-сертификата. По умолчанию Сервер администрирования использует порт 13000.
   - `KLNAGENT_USESSL` – использовать SSL-соединение для подключения к Серверу администрирования. Возможные значения: `1` (использовать SSL-соединение) или `0` (не использовать SSL-соединение).
   - `KLNAGENT_GW_MODE` – подключаться к Серверу администрирования через шлюз соединений. Возможные значения: `1` или `0`.

   > Требуется вводить значения параметров в формате <имя параметра>=<значение>. Пробелы между именем параметра и его значением не обрабатываются.

3. Выполните одно из следующих действий:
   - Запустите скрипт установки, выполнив следующую команду:

     ```
     # sh lightagent-5.2.X-X-bundle.sh --auto-install=<путь к конфигурационному файлу Легкого агента для Linux> --klnagent-auto-install=<путь к конфигурационному файлу Агента администрирования>
     ```

     где:
     - `5.2.X-X` – номер версии программы;
     - `<путь к конфигурационному файлу Легкого агента для Linux>` – полный путь к конфигурационному файлу первоначальной настройки lightagent.ini (см. пункт 1 этой инструкции). Скрипт установки будет использовать параметры, указанные в этом файле, при выполнении первоначальной настройки Легкого агента для Linux;
     - `<путь к конфигурационному файлу Агента администрирования>` – полный путь к конфигурационному файлу первоначальной настройки klnagent.ini (см. пункт 2 этой инструкции). Скрипт установки будет использовать параметры, указанные в этом файле, при выполнении первоначальной настройки Агента администрирования.
   - Объявите переменную окружения `KLAUTOANSWERS` и запустите скрипт установки, выполнив

следующие команды:

```
# export KLAUTOANSWERS=<путь к конфигурационному файлу Агента администрирования>
```

```
# export KLLIGHTAGENTAUTOANSWERS=<путь к конфигурационному файлу Легкого агента для Linux>
```

```
# sh lightagent-5.2.X-X-bundle.sh
```

где:

- `5.2.X-X` – номер версии программы;
- `<путь к конфигурационному файлу Легкого агента для Linux>` – полный путь к конфигурационному файлу первоначальной настройки lightagent.ini (см. пункт 1 этой инструкции). Скрипт установки будет использовать параметры, указанные в этом файле, при выполнении первоначальной настройки Легкого агента для Linux;
- `<путь к конфигурационному файлу Агента администрирования>` – полный путь к конфигурационному файлу первоначальной настройки klnagent.ini (см. пункт 2 этой инструкции). Скрипт установки будет использовать параметры, указанные в этом файле, при выполнении первоначальной настройки Агента администрирования.

Пути к конфигурационным файлам, содержащем параметры для первоначальной настройки Легкого агента для Linux и Агента администрирования могут совпадать, то есть это может быть один конфигурационный файл.

Параметр командной строки `--auto-install` имеет более высокий приоритет, чем переменная окружения.

В результате скрипт установки выполнит следующие действия:

1. Установка и первоначальная настройка Агента администрирования Kaspersky Security Center.

   Если требуемая версия Агента администрирования уже установлена, этот пункт будет пропущен.

2. Установка и первоначальная настройка Легкого агента для Linux.

Установка Легкого агента для Linux в интерактивном режиме

Если операционная система виртуальной машины, на которую вы планируете установить Легкий агент для Linux, не поддерживает технологию fanotify, перед началом установки убедитесь, что на виртуальную машину загружены исходные коды ядра операционной системы и на виртуальной машине установлены пакеты для компиляции (gcc, binutils, glibc, glibc-devel, make, ld).

► *Чтобы установить Легкий агент для Linux из командной строки в интерактивном режиме, запустите скрипт установки, выполнив следующую команду:*

```
# sh lightagent-5.2.X-X-bundle.sh
```

где `5.2.X-X` – номер версии программы.

В результате скрипт установки выполнит следующие действия:

1. Установка Агента администрирования Kaspersky Security Center.

   Если требуемая версия Агента администрирования уже установлена, этот пункт будет пропущен.

   После установки Агента администрирования требуется выполнить его первоначальную настройку.

2. Установка Легкого агента для Linux.

   После установки Легкого агента для Linux требуется выполнить его первоначальную настройку.

► *Чтобы выполнить первоначальную настройку Агента администрирования, выполните следующие действия:*

1. В командной строке запустите скрипт postinstall.pl, расположенный в директории:
   - /opt/kaspersky/klnagent64/lib/bin/setup/ – .для 64-разрядных операционных систем;
   - /opt/kaspersky/klnagent/lib/bin/setup/ – .для 32-разрядных операционных систем.
2. Укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер администрирования Kaspersky Security Center.
3. Если требуется, измените настроенные по умолчанию значения следующих параметров:
   - номер порта для подключения Агента администрирования к Серверу администрирования и номер порта для подключения с использованием SSL-сертификата;
   - возможность использования SSL-соединения для подключения к Серверу администрирования;
   - возможность подключения к Серверу администрирования через шлюз соединений.

Подробнее об установке и настройке Агента администрирования Kaspersky Security Center см. в документации Kaspersky Security Center.

► *Чтобы выполнить первоначальную настройку Легкого агента для Linux, выполните следующие действия:*

1. В командной строке запустите скрипт lightagent-setup.pl, расположенный в директории /opt/kaspersky/lightagent/bin/.
2. Ознакомьтесь с текстом Лицензионного соглашения программы Kaspersky Security, которое заключается между вами и "Лабораторией Касперского", и Политики конфиденциальности, которая описывает обработку и передачу данных. Для этого нажмите на клавишу **ENTER**. Для завершения просмотра используйте клавишу **Q**.

   После выхода из режима просмотра введите `yes` (или `y`), если вы согласны с условиями Лицензионного соглашения и Политики конфиденциальности. Установив значение `yes`, вы подтверждаете следующее:

   - вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения программы Kaspersky Security;
   - 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.

   Текст Лицензионного соглашения и Политики конфиденциальности входит в комплект поставки

программы.

> Согласие с условиями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки программы.

3. Укажите идентификатор языка событий Легкого агента для Linux, отправляемых в Kaspersky Security Center: `ru`, `en`, `fr`, `de`, `zh-Hans`, `zh-Hant`, `ja`.

   По умолчанию скрипт первоначальной настройки программы предлагает использовать идентификатор языка `en`. Нажмите на клавишу **ENTER**, чтобы подтвердить использование английского языка для событий или укажите другой идентификатор языка.

4. Скрипт первоначальной настройки программы проверяет наличие поддержки технологии fanotify операционной системой.

   - Если операционная система поддерживает технологию fanotify, скрипт первоначальной настройки программы переходит к настройке Легкого агента для Linux.
   - Если операционная система не поддерживает технологию fanotify, то для обработки операций над объектами файловой системы требуется компиляция модуля ядра операционной системы Linux. Для запуска компиляции модуля ядра вам нужно подтвердить, что исходные коды ядра операционной системы находятся в директории по умолчанию, или указать другой путь к исходным кодам ядра.

     Если скрипт первоначальной настройки программы обнаружит исходные коды ядра операционной системы в директории по умолчанию, на экране отобразится найденный путь. Нажмите на клавишу **ENTER**, чтобы подтвердить путь, или укажите другой путь. Скрипт первоначальной настройки программы запустит компиляцию модуля ядра операционной системы Linux на виртуальной машине.

Скрипт первоначальной настройки программы выполняет настройку Легкого агента для Linux. Если во время настройки возникают ошибки, информация о них отображается на экране.

Установка Легкого агента для Linux через Kaspersky Security Center

Вы можете установить Легкий агент для Linux удаленно с рабочего места администратора с помощью программы Kaspersky Security Center.

Установка выполняется с помощью мастера удаленной установки или с помощью задачи удаленной установки программы (см. подробнее в документации Kaspersky Security Center).

> Если операционная система виртуальной машины, на которую вы планируете установить Легкий агент для Linux, не поддерживает технологию fanotify, перед началом установки убедитесь, что на виртуальной машине исходные коды ядра операционной системы находятся в директории по умолчанию и установлены пакеты для компиляции (gcc, binutils, glibc, glibc-devel, make, ld).

Перед началом удаленной установки Легкого агента для Linux и Агента администрирования требуется выполнить следующие действия на виртуальной машине:

1. Проверить возможность подключения клиентской программы (например, программы PuTTY) к виртуальной машине по протоколу SSH.

   Если вы не можете подключиться к устройству, откройте файл /etc/ssh/sshd_config и убедитесь, что

параметры имеют следующие значения:

`PasswordAuthentication no`

`ChallengeResponseAuthentication yes`

Если требуется, измените значения параметров, сохраните файл /etc/ssh/sshd_config и перезапустите службу SSH, используя команду `sudo service ssh restart`.

2. Выключить запрос пароля sudo для учетной записи пользователя, которая используется для подключения к виртуальной машине. Для этого выполните следующие действия:

   a. Откройте конфигурационный файл sudoers с помощью команды `sudo visudo`.

   b. В файле укажите: `<имя пользователя> ALL = (ALL) NOPASSWD: ALL`

      где <имя пользователя> – учетная запись пользователя, которая будет использоваться для подключения к виртуальной машине по протоколу SSH.

   c. Сохраните и закройте файл sudoers.

   d. Повторно подключитесь к виртуальной машине через SSH и выполните команду `sudo whoami`, чтобы убедиться, что служба sudo не требует ввода пароля.

Для удаленной установки используется инсталляционный пакет, который содержит набор параметров, необходимых для установки Легкого агента для Linux и Агента администрирования Kaspersky Security Center. Мастер установки компонентов Kaspersky Security автоматически создает такой инсталляционный пакет в ходе установки mmc-плагинов Kaspersky Security и Сервера интеграции. Этот инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты** под именем **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux (5.2.X.X)**, где 5.2.X.X – номер версии программы.

Вы можете использовать инсталляционный пакет, автоматически созданный мастером установки компонентов Kaspersky Security, или создать инсталляционный пакет вручную (см. раздел "Создание инсталляционного пакета Легкого агента для Linux" на стр. 100).

Не поддерживается совместная установка Легкого агента для Linux и Агента администрирования, который входит в комплект поставки Kaspersky Security Center. Если вы используете задачу удаленной установки программ для установки Легкого агента для Linux, убедитесь, что в параметрах задачи не установлен флажок **Установить Агент администрирования совместно с данной программой**. Агент администрирования поддерживаемой версии входит в инсталляционный пакет для Легкого агента для Linux и будет установлен автоматически в результате удаленной установки Легкого агента для Linux.

Перед началом установки выполняется проверка наличия Агента администрирования на виртуальной машине. Если обнаружена установленная версия Агента администрирования, не совместимая с компонентом Легкий агент для Linux, установка завершается с ошибкой. Вам требуется удалить Агент администрирования на виртуальной машине и запустить удаленную установку Легкого агента для Linux повторно.

kaspersky

В этом разделе

Создание инсталляционного пакета Легкого агента для Linux

Перед созданием инсталляционного пакета вам нужно распаковать дистрибутив Легкого агента для Linux в папку, доступную для Сервера администрирования Kaspersky Security Center.

► *Чтобы создать вручную инсталляционный пакет Легкого агента для Linux, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
3. Нажмите на кнопку **Создать инсталляционный пакет**.

   Запустится мастер создания инсталляционного пакета.
4. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
5. Введите имя нового инсталляционного пакета и перейдите к следующему шагу мастера.
6. Выберите дистрибутив программы Kaspersky Security. Для этого откройте стандартное окно Windows с помощью кнопки **Обзор** и укажите путь к файлу lightagent.kud.

   В окне мастера отобразится название программы.

   Перейдите к следующему шагу мастера.
7. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Для продолжения создания инсталляционного пакета требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения программы Kaspersky Security и Политики конфиденциальности. Для подтверждения установите оба флажка в окне мастера.

   Перейдите к следующему шагу мастера.
8. Мастер загружает файлы, необходимые для установки программы, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.
9. Завершите работу мастера.

Созданный инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**. Вы можете использовать один и тот же инсталляционный пакет многократно.

После создания инсталляционного пакета Легкого агента для Linux вам нужно настроить параметры инсталляционного пакета (см. раздел "Настройка параметров Агента администрирования в свойствах инсталляционного пакета Легкого агента для Linux" на стр. 101). В окне свойств инсталляционного пакета вы можете указать параметры подключения Агента администрирования, который будет установлен на виртуальную машину вместе с Легким агентом для Linux, к Серверу администрирования Kaspersky Security Center.

Настройка параметров Агента администрирования в свойствах инсталляционного пакета Легкого агента для Linux

В свойствах инсталляционного пакета Легкого агента для Linux вы можете настроить параметры подключения Агента администрирования, который будет установлен на виртуальную машину вместе с Легким агентом для Linux, к Серверу администрирования Kaspersky Security Center.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
3. В списке инсталляционных пакетов выберите инсталляционный пакет Легкого агента для Linux и откройте окно **Свойства: <имя инсталляционного пакета>** одним из следующих способов:
   - двойным щелчком мыши;
   - по правой клавише мыши вызовите контекстное меню и выберите пункт **Свойства**;
   - по ссылке **Настроить параметры инсталляционного пакета**, расположенной справа от списка задач в блоке с параметрами инсталляционного пакета.
4. В списке слева выберите раздел **Параметры** и настройте следующие параметры подключения Агента администрирования к Серверу администрирования Kaspersky Security Center:
   - **Адрес Сервера администрирования**
   - **Номер порта**.
   - **Номер SSL-порта**
   - **Использовать сертификат Сервера администрирования**
   - **Использовать SSL-соединение**

   Все разделы окна **Свойства: <имя инсталляционного пакета>**, кроме раздела **Параметры**, стандартны для программы Kaspersky Security Center. Описание стандартных разделов см. в документации Kaspersky Security Center.
5. Нажмите на кнопку **OK** в окне **Свойства: <имя инсталляционного пакета>**.

Подготовка Легких агентов к работе

Для подготовки Легких агентов к работе требуется выполнить следующие действия:

1. Создать политику для Легкого агента для Windows. В политике для Легкого агента для Windows требуется настроить подключение защищенной виртуальной машины к SVM и включить защиту доступа к функциям и параметрам Легкого агента для Windows.
2. Создать политику для Легкого агента для Linux. В политике для Легкого агента для Linux требуется настроить подключение защищенной виртуальной машины к SVM.
3. Убедиться в том, что на защищенных виртуальных машинах установлены обновления баз, необходимых для работы Легкого агента. Если требуется, запустить задачу обновления вручную.

Создание политики для Легкого агента для Windows

► *Чтобы создать политику для Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, в которую входят виртуальные машины с компонентом Легкий агент для Windows.
3. В рабочей области выберите закладку **Политики** и нажмите на кнопку **Новая политика**. Откроется мастер создания политики.
4. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows**. Перейдите к следующему шагу мастера.
5. В поле **Имя** введите название политики. Перейдите к следующему шагу мастера.
6. С помощью кнопки **Далее** перейдите к шагу "Параметры обнаружения SVM" и выберите способ, который Легкие агенты будут использовать для обнаружения SVM, работающих в сети, и получения информации о них (см. раздел "Настройка параметров обнаружения SVM" на стр. 168).
7. С помощью кнопки **Далее** перейдите к шагу "Защита паролем" и настройте следующие параметры:
   a. Установите флажок **Включить защиту паролем**.
   b. Введите имя и пароль учетной записи, которой разрешен доступ к параметрам программы в локальном интерфейсе Легкого агента.
   c. Введите пароль в полях **Пароль** и **Подтверждение пароля**.
   d. Нажмите на кнопку **Настройка** и выберите в открывшемся окне вариант **Все операции (кроме уведомлений об опасности)**.
8. Перейдите к следующему шагу и завершите работу мастера создания политики.

> Для первоначальной настройки программы не требуется настраивать другие параметры политики для Легкого агента для Windows, вы можете использовать значения, установленные по умолчанию. Во время работы с программой вы можете выполнить более тонкую настройку параметров политики для Легкого агента для Windows (см. раздел "Политика для Легкого агента для Windows" на стр. 128).

Создание политики для Легкого агента для Linux

► *Чтобы создать политику для Легкого агента для Linux, выполните следующие действия:*

1. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, в которую входят виртуальные машины с компонентом Легкий агент для Linux.
2. В рабочей области выберите закладку **Политики** и нажмите на кнопку **Новая политика**. Откроется мастер создания политики.
3. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux**. Перейдите к следующему шагу мастера.
4. В поле **Имя** введите имя политики. Перейдите к следующему шагу мастера.
5. С помощью кнопки **Далее** перейдите к шагу "Параметры обнаружения SVM" и выберите способ, который Легкие агенты будут использовать для обнаружения SVM, работающих в сети, и получения информации о них (см. раздел "Настройка параметров обнаружения SVM" на стр. 168).
6. Перейдите к следующему шагу и завершите работу мастера создания политики.

Для первоначальной настройки программы не требуется настраивать другие параметры политики для Легкого агента для Linux, вы можете использовать значения, установленные по умолчанию. Во время работы с программой вы можете выполнить более тонкую настройку параметров политики для Легкого агента для Linux (см. раздел "Политика для Легкого агента для Linux" на стр. 136).

Обновление баз программы на защищенной виртуальной машине

Обновление баз выполняется с помощью задачи обновления. Задача обновления запускается автоматически.

Информация о запуске задачи обновления на виртуальной машине с компонентом Легкий агент для Windows отобразится в окне **Отчеты и хранилища** в разделе **Обновление** после первого запуска задачи. При необходимости вы можете запустить задачу обновления вручную (см. раздел "Запуск и остановка задачи обновления в локальном интерфейсе" на стр. 395).

Чтобы проверить актуальность баз программы на виртуальной машине с компонентом Легкий агент для Linux, выполните команду для Легкого агента для Linux `lightagent productinfo` (см. раздел "`Просмотр информации о программе`" на стр. 481). Убедитесь, что команда вывела информацию о базах программы, базы актуальны. При необходимости вы можете запустить задачу обновления с помощью команды `lightagent update` (см. раздел "`Обновление баз`" на стр. 490).

Изменения в Консоли администрирования Kaspersky Security Center после установки программы Kaspersky Security

Отображение виртуальных машин и SVM в дереве консоли

После установки Kaspersky Security в виртуальной инфраструктуре SVM и защищенные виртуальные машины с установленным Агентом администрирования передают информацию о себе в Kaspersky Security Center. По умолчанию Kaspersky Security Center добавляет виртуальные машины с установленной программой Kaspersky Security в папку **Нераспределенные устройства**.

В Консоли администрирования Kaspersky Security Center SVM отображается под именем, которое вы указали во время развертывания этой SVM. Имя защищенной виртуальной машины совпадает с сетевым именем виртуальной машины (hostname). Если на Сервере администрирования Kaspersky Security Center уже зарегистрирована виртуальная машина с таким именем, то к имени новой виртуальной машины добавляется окончание с порядковым номером, например: <Имя>~1, <Имя>~2.

Если перед установкой программы вы настроили правила перемещения виртуальных машин в группы администрирования, Kaspersky Security Center перемещает виртуальные машины с установленной программой Kaspersky Security в указанные группы администрирования в соответствии с настроенными правилами перемещения виртуальных машин.

После развертывания на гипервизоре SVM передает в Kaspersky Security Center следующий тег:

%VmType%=SVM – признак, определяющий, что виртуальная машина является SVM.

Защищенная виртуальная машина с установленным Агентом администрирования Kaspersky Security Center передает в Kaspersky Security Center следующий тег:

%VmType%=<Persistent / Nonpersistent> – признак, определяющий, является ли виртуальная машина временной виртуальной машиной.

Вы можете использовать указанные теги при создании правил перемещения SVM и защищенных виртуальных машин в группы администрирования.

Вы можете вручную переместить виртуальные машины в группу администрирования **Управляемые устройства** или во вложенные группы администрирования (подробнее о перемещении виртуальных машин в группы администрирования см. в документации Kaspersky Security Center).

Политика и задачи по умолчанию

После установки mmc-плагинов Kaspersky Security для группы администрирования **Управляемые устройства** автоматически создается политика по умолчанию для Сервера защиты и следующие задачи:

- задача поиска вирусов для Легкого агента для Windows;
- задача поиска вирусов для Легкого агента для Linux;
- задача обновления баз на Сервере защиты.

Инсталляционные пакеты

В результате установки mmc-плагинов Kaspersky Security и Сервера интеграции на Сервере администрирования Kaspersky Security Center создаются инсталляционные пакеты:

- **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows (5.2.X.X)**;
- **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux (5.2.X.X)**;

  где 5.2.X.X – номер версии программы.

Инсталляционные пакеты размещаются в Консоли администрирования в папке **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**. Вы можете использовать эти инсталляционные пакеты для удаленной установки Легкого агента для Windows и Легкого агента для Linux (см. раздел "Установка Легкого агента для Linux через Kaspersky Security Center" на стр. 98).

Просмотр списка SVM, подключенных к Серверу интеграции

Программа Kaspersky Security позволяет просмотреть список всех SVM, которые подключены к Серверу интеграции.

► *Чтобы получить информацию об SVM, подключенных к Серверу интеграции, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Список подключенных SVM**.

   В таблице справа отображается следующая информация обо всех SVM, подключенных к Серверу интеграции:

   - IP-адрес SVM.
   - IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором развернута SVM.
3. Чтобы посмотреть подробную информацию, выберите SVM в таблице и откройте окно **Информация об SVM** двойным щелчком мыши или по ссылке **Детальная информация**, расположенной над таблицей.

   В окне отображается следующая информация о выбранной SVM:

   - Уникальный идентификатор SVM на гипервизоре.
   - IP-адрес SVM.
   - IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором развернута SVM.
   - Порт на SVM для передачи запросов на проверку от Легких агентов при защищенном соединении.
   - Порт на SVM для передачи запросов на проверку от Легких агентов при незащищенном соединении.
   - Порт на SVM для передачи служебных запросов от Легких агентов при защищенном соединении.
   - Порт на SVM для передачи служебных запросов от Легких агентов при незащищенном соединении.
   - Информация о том, шифруется ли канал передачи данных от Легких агентов.
4. Нажмите на кнопку **Закрыть** в окне **Информация об SVM**, чтобы закрыть окно.

Просмотр списка Легких агентов, подключенных к SVM

В свойствах программы Kaspersky Security, установленной на SVM, отображается список Легких агентов, подключенных к этой SVM.

► *Чтобы просмотреть список Легких агентов, подключенных к SVM, с помощью Консоли*

администрирования, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, в которой находится SVM.
3. В рабочей области выберите закладку **Устройства**.
4. В списке выберите SVM, для которой вы хотите посмотреть список подключенных Легких агентов, и откройте окно **Свойства: <Имя SVM>** двойным щелчком мыши.
5. В окне свойств SVM в списке слева выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на этой SVM.
6. Выберите программу **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты** и откройте окно параметров программы двойным щелчком мыши.
7. В окне параметров программы в списке слева выберите раздел **Подключенные Легкие агенты**.

   В правой части окна отобразится таблица, содержащая список Легких агентов, подключенных к SVM. В поле над таблицей отображается время последнего запроса к SVM.

   В таблице отображается следующая информация:

   - Имя виртуальной машины с установленным Легким агентом.
   - IP-адрес и порт, которые использует Легкий агент для подключения к SVM.
   - Версия операционной системы, установленной на защищенной виртуальной машине.
   - Тип операционной системы, установленной на защищенной виртуальной машине: операционная система для серверов или операционная система для рабочих станций.
   - Идентификатор защищенной виртуальной машины.
   - Путь к защищенной виртуальной машине в виртуальной инфраструктуре.
8. Если вы хотите обновить информацию о Легких агентах, подключенных к SVM, нажмите на кнопку **Обновить**.

Процедура приемки

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

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

1. Убедитесь, что на компьютере, где установлена Консоль администрирования Kaspersky Security Center, в списке установленных программ операционной системы отображается **Kaspersky Security для виртуальных сред 5.2 Легкий агент – компоненты управления**.
2. Убедитесь, что на компьютере, где установлена Консоль администрирования Kaspersky Security Center, в списке служб операционной системы присутствует служба **Сервер интеграции для Kaspersky Security для виртуальных сред** и эта служба запущена.
3. Убедитесь, что в Консоли администрирования Kaspersky Security Center в блоке **Развертывание** отображается ссылка для запуска Консоли Сервера интеграции. При переходе по ссылке запускается Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65). После ввода параметров подключения происходит подключение к Серверу интеграции.
4. Убедитесь, что в Консоли администрирования Kaspersky Security Center в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center присутствуют mmc-плагины управления Kaspersky Security (см. раздел "Результат установки mmc-плагинов и Сервера интеграции" на стр. 61).
5. Убедитесь, что в Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** дерева консоли присутствуют группы администрирования, которые вы настроили (см. раздел "Настройка правил перемещения виртуальных машин в группы администрирования" на стр. 55). Проверьте, что все виртуальные машины с компонентами программы помещены в эти группы администрирования.
6. Убедитесь, что в Консоли администрирования Kaspersky Security Center задача активации и задача обновления баз программы на SVM завершены успешно на всех развернутых SVM. Список задач отображается на закладке **Задачи** в рабочей области группы администрирования, в которую входят SVM. Вы можете посмотреть результаты выполнения задачи по ссылке **Просмотреть результаты**, расположенной справа от списка задач.
7. В Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в которую входят SVM, и убедитесь, что на закладке **Устройства** все SVM имеют статус **OK** (зеленый).
8. Для каждой SVM убедитесь, что отображается информация о лицензии. Для этого откройте окно свойств SVM, выберите раздел **Программы**, затем выберите в списке программу Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты, откройте окно свойств программы и перейдите в раздел **Лицензионные ключи**.
9. Для каждой SVM убедитесь, что отображается информация о базах программы. Для этого откройте окно свойств SVM, выберите раздел **Программы**, затем выберите в списке программу Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты, откройте окно свойств программы и перейдите в раздел **Общие**.
10. Убедитесь, что в Консоли администрирования Kaspersky Security Center создана активная политика для Сервера защиты.
11. В Консоли администрирования Kaspersky Security Center откройте группу администрирования, в

которую входят виртуальные машины с компонентом Легкий агент для Windows, и убедитесь, что на закладке **Устройства** все виртуальные машины имеют статус **ОК** (зеленый) и состояние защиты **Выполняется**.

12. Убедитесь, что в Консоли администрирования Kaspersky Security Center создана активная политика для Легкого агента для Windows. Откройте свойства политики и убедитесь, что в разделе **Параметры обнаружения SVM** указан адрес SVM, к которой могут подключаться Легкие агенты для Windows.
13. На виртуальной машине с компонентом Легкий агент для Windows откройте главное окно программы и убедитесь, что следующие компоненты запущены (отображаются значки статуса работы компонента):
    - Файловый Антивирус.
    - Почтовый Антивирус.
    - Веб-Антивирус.
    - Мониторинг системы.
    - AMSI-защита.
    - Контроль запуска программ.
    - Контроль активности программ.
    - Веб-Контроль.
    - Контроль целостности системы.
14. На виртуальной машине с компонентом Легкий агент для Windows откройте окно **Поддержка** (по ссылке из главного окна программы) и убедитесь, что отображается IP-адрес SVM, к которой подключен Легкий агент, а также информация о лицензии.
15. На виртуальной машине с компонентом Легкий агент для Windows на закладке **Центр управления** в блоке **Управление задачами** проверьте статус задачи **Обновление**: базы должны быть актуальными.
16. В Консоли администрирования Kaspersky Security Center откройте группу администрирования, в которую входят виртуальные машины с компонентом Легкий агент для Linux, и убедитесь, что на закладке **Устройства** все виртуальные машины имеют статус **ОК** (зеленый) и состояние защиты **Выполняется**.
17. Убедитесь, что в Консоли администрирования Kaspersky Security Center создана активная политика для Легкого агента для Linux. Откройте свойства политики и убедитесь, что в разделе **Параметры обнаружения SVM** указан адрес SVM, к которой могут подключаться Легкие агенты для Linux.
18. На виртуальной машине с компонентом Легкий агент для Linux выполните следующие команды:
    - `lightagent svminfo`. Убедитесь, что команда вывела способ обнаружения SVM (не пустой) и IP-адрес SVM, к которой подключен Легкий агент.
    - `lightagent status File_Monitoring`. Убедитесь, что команда вывела состояние задачи постоянной защиты `Running` (выполняется).
    - `lightagent license`. Убедитесь, что команда вывела информацию о лицензии.
    - `lightagent productinfo`. Убедитесь, что команда вывела информацию о базах программы, базы актуальны.

kaspersky

В этом разделе

Сертифицированное состояние программы

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

- Программа активирована на всех SVM (см. раздел "Подготовка Сервера защиты к работе" на стр. 78), сведения о лицензии переданы на защищенные виртуальные машины (см. раздел "Об активации программы" на стр. 78).
- Базы программы обновлены на всех SVM (см. раздел "Подготовка Сервера защиты к работе" на стр. 78) и на всех защищенных виртуальных машинах (см. раздел "Подготовка Легких агентов к работе" на стр. 102).
- Настроена активная политика для Сервера защиты с параметрами по умолчанию (см. раздел "Подготовка Легких агентов к работе" на стр. 102).
- Настроена активная политика для Легкого агента для Windows (см. раздел "Подготовка Легких агентов к работе" на стр. 102).
- Настроена активная политика для Легкого агента для Linux (см. раздел "Подготовка Легких агентов к работе" на стр. 102).
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

Проверка работоспособности программы

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе (см. раздел "Процедура приемки" на стр. 107).
- Программа находится в сертифицированном состоянии (см. раздел "Сертифицированное состояние программы" на стр. 109).

В процедурах проверки работоспособности компонентов программы используется тестовый образец зараженного файла. В качестве тестового образца используется EICAR-файл, который можно получить на сайте http://www.eicar.org в разделе **Download**. Если вы скачали архив, его потребуется предварительно распаковать.

Проверка работоспособности функции защиты виртуальной машины с гостевой операционной системой Windows

1. Отключите защиту виртуальной машины:
   a. Откройте свойства политики, под управлением которой находится виртуальная машина с установленным компонентом Легкий агент для Windows.

b. Перейдите в раздел **Файловый Антивирус** и снимите флажок **Файловый Антивирус**.

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

2. Поместите зараженный EICAR-файл в новую папку на системном диске на виртуальной машине.
3. Очистите список событий на Сервере администрирования Kaspersky Security Center:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Выделите любое событие в списке и в контекстном меню выберите команду **Удалить все**.

> Эта операция требуется для обнуления данных в отчетах.

4. Включите защиту виртуальной машины:
   a. Откройте свойства политики, под управлением которой находится виртуальная машина с установленным компонентом Легкий агент для Windows.
   b. Перейдите в раздел **Файловый Антивирус** и установите флажок **Файловый Антивирус**.
5. Проверьте доступ к зараженному файлу: попробуйте открыть подготовленный на виртуальной машине тестовый зараженный файл с помощью текстового редактора, например Блокнота. Программа выдает ошибку о том, что указанный файл отсутствует или доступ к нему запрещен.
6. Убедитесь, что зараженный файл был удален с виртуальной машины.
7. Проверьте наличие событий об обнаружении и удалении зараженного файла:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Убедитесь, что в списке отображаются события об обнаружении зараженного файла и его успешном удалении.
8. Проверьте информацию в отчете об обнаруженных вирусах:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **Отчеты**.
   c. Выберите **Отчет о вирусах**. Сформированный отчет откроется в новом окне.
   d. Убедитесь, что в сводной и детальной таблицах отчета отображается корректная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности функции защиты виртуальной машины с гостевой операционной системой Linux

1. Отключите защиту виртуальной машины:
   a. Откройте свойства политики, под управлением которой находится виртуальная машина с установленным компонентом Легкий агент для Linux.
   b. Перейдите в раздел **Файловый Антивирус** и снимите флажок **Файловый Антивирус**.

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

2. Поместите зараженный EICAR-файл в новую папку на системном диске на виртуальной машине.
3. Очистите список событий на Сервере администрирования Kaspersky Security Center:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Выделите любое событие в списке и в контекстном меню выберите команду **Удалить все**.

> Эта операция требуется для обнуления данных в отчетах.

4. Включите защиту виртуальной машины:
   a. Откройте свойства политики, под управлением которой находится виртуальная машина с установленным компонентом Легкий агент для Linux.
   b. Перейдите в раздел **Файловый Антивирус** и установите флажок **Файловый Антивирус**.
5. Проверьте доступ к зараженному файлу: попробуйте открыть подготовленный на виртуальной машине тестовый зараженный файл на чтение, например командой `cat eicar.com`. Программа выдает ошибку о том, что указанный файл отсутствует или доступ к нему запрещен.
6. Убедитесь, что зараженный файл был удален с виртуальной машины.
7. Проверьте наличие событий об обнаружении и удалении зараженного файла:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Убедитесь, что в списке отображаются события об обнаружении зараженного файла и его успешном удалении.
8. Проверьте информацию в отчете об обнаруженных вирусах:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **Отчеты**.
   c. Выберите **Отчет о вирусах**. Сформированный отчет откроется в новом окне.
   d. Убедитесь, что в сводной и детальной таблицах отчета отображается корректная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности функции проверки файлов виртуальной машины с гостевой операционной системой Windows

1. Отключите защиту виртуальной машины:
   a. Откройте свойства политики, под управлением которой находится виртуальная машина с установленным компонентом Легкий агент для Windows.
   b. Перейдите в раздел **Файловый Антивирус** и снимите флажок **Файловый Антивирус**.

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

2. Поместите зараженный EICAR-файл в новую папку на системном диске на виртуальной машине.
3. Очистите список событий на Сервере администрирования Kaspersky Security Center:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Выделите любое событие в списке и в контекстном меню выберите команду **Удалить все**.

> Эта операция требуется для обнуления данных в отчетах.

4. Создайте задачу проверки для виртуальной машины:
   a. В Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** дерева консоли выберите группу администрирования, в которую входит защищенная виртуальная машина с зараженным образцом.
   b. В рабочей области перейдите на закладку **Задачи**.
   c. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
   d. На первом шаге в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows** выберите **Поиск вирусов**. Перейдите к следующему шагу мастера.
   e. На этом шаге мастера выберите область действия задачи: укажите папку на виртуальной машине с ранее подготовленным зараженным файлом.
   f. Для всех остальных параметров задачи оставьте значения, заданные по умолчанию.
   g. Завершите работу мастера создания задачи.
5. Запустите задачу: выберите задачу в списке задач и в контекстном меню выберите команду **Запустить**. Задача переходит в состояние **Выполняется**.
6. Дождитесь успешного завершения задачи.
7. Убедитесь, что зараженный файл был удален с виртуальной машины.
8. Проверьте наличие событий об обнаружении и удалении зараженного файла:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Убедитесь, что в списке отображаются события об обнаружении зараженного файла и его успешном удалении.
9. Проверьте информацию в отчете об обнаруженных вирусах:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **Отчеты**.
   c. Выберите **Отчет о вирусах**. Сформированный отчет откроется в новом окне.
   d. Убедитесь, что в сводной и детальной таблицах отчета отображается корректная информация

об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности функции проверки файлов виртуальной машины с гостевой операционной системой Linux

1. Отключите защиту виртуальной машины:
   a. Откройте свойства политики, под управлением которой находится виртуальная машина с установленным компонентом Легкий агент для Linux.
   b. Перейдите в раздел **Файловый Антивирус** и снимите флажок **Файловый Антивирус**.

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

2. Поместите зараженный EICAR-файл в новую папку на системном диске на виртуальной машине.
3. Очистите список событий на Сервере администрирования Kaspersky Security Center:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Выделите любое событие в списке и в контекстном меню выберите команду **Удалить все**.

   Эта операция требуется для обнуления данных в отчетах.

4. Создайте задачу проверки для виртуальной машины:
   a. В Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** дерева консоли выберите группу администрирования, в которую входит защищенная виртуальная машина с зараженным образцом.
   b. В рабочей области перейдите на закладку **Задачи**.
   c. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
   d. На первом шаге в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux** выберите **Поиск вирусов**. Перейдите к следующему шагу мастера.
   e. На этом шаге мастера выберите область действия задачи: укажите папку на виртуальной машине с ранее подготовленным зараженным файлом.
   f. Для всех остальных параметров задачи оставьте значения, заданные по умолчанию.
   g. Завершите работу мастера создания задачи.
5. Запустите задачу: выберите задачу в списке задач и в контекстном меню выберите команду **Запустить**. Задача переходит в состояние **Выполняется**.
6. Дождитесь успешного завершения задачи.
7. Убедитесь, что зараженный файл был удален с виртуальной машины.
8. Проверьте наличие событий об обнаружении и удалении зараженного файла:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **События**.
   c. Убедитесь, что в списке отображаются события об обнаружении зараженного файла и его

успешном удалении.

9. Проверьте информацию в отчете об обнаруженных вирусах:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
   b. В рабочей области перейдите на закладку **Отчеты**.
   c. Выберите **Отчет о вирусах**. Сформированный отчет откроется в новом окне.
   d. Убедитесь, что в сводной и детальной таблицах отчета отображается корректная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности компонента Почтовый Антивирус

Для выполнения процедуры проверки требуются две виртуальные машины:

- виртуальная машина с компонентом Легкий агент для Windows и настроенным почтовым клиентом Microsoft Outlook®;
- виртуальная машина, на которой не установлен компонент Легкий агент для Windows, с настроенным почтовым клиентом Microsoft Outlook.

1. С виртуальной машины, на которой не установлен компонент Легкий агент для Windows, отправьте сообщение электронной почты с зараженным EICAR-файлом во вложении на адрес электронной почты, доступ к которому настроен в почтовом клиенте Microsoft Outlook на защищенной виртуальной машине.
2. На защищенной виртуальной машине получите сообщение с помощью почтового клиента Microsoft Outlook.
3. Убедитесь, что EICAR-файл удален из вложения, а тема сообщения заменена на "Message has been disinfected: <исходная тема сообщения>".
4. Проверьте информацию в отчете о работе Почтового Антивируса в локальном интерфейсе:
   a. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
   b. В левой части окна в списке компонентов и задач выберите компонент **Почтовый Антивирус**. Отчет отобразится в правой части окна.
   c. Убедитесь, что в отчете отображается информация об обнаружении угрозы.

Проверка работоспособности компонента Веб-Антивирус

1. На виртуальной машине с установленным компонентом Легкий агент для Windows в браузере откройте веб-страницу http://www.eicar.org/download/eicar.com.
2. Убедитесь, что вместо запрашиваемой страницы отображается сообщение "Доступ запрещен", сформированное Легким агентом для Windows.
3. Проверьте информацию в отчете о работе Веб-Антивируса в локальном интерфейсе:
   a. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
   b. В левой части окна в списке компонентов и задач выберите компонент **Веб-Антивирус**. Отчет отобразится в правой части окна.
   c. Убедитесь, что в отчете отображается событие об обнаружении угрозы.

Проверка работоспособности компонента Мониторинг системы

1. На виртуальной машине с установленным компонентом Легкий агент для Windows отключите все компоненты Легкого агента.
2. Отключите в параметрах операционной системы компонент User Account Control. Перезагрузите виртуальную машину.
3. Создайте файл test.bat, содержащий следующую строку:

   ```
   echo test > C:\TestBSSDetectAction.tst
   ```

4. Включите компонент Мониторинг системы.
5. Запустите созданный файл test.bat от имени администратора.
6. Убедитесь, что файл test.bat удален.
7. Проверьте информацию в отчете о работе Мониторинга системы в локальном интерфейсе:
   a. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
   b. В левой части окна в списке компонентов и задач выберите компонент **Мониторинг системы**. Отчет отобразится в правой части окна.
   c. Убедитесь, что в отчете отображается информация об обнаруженной угрозе в файле test.bat.

О правах доступа к функциям программы

Программа поддерживает следующие роли безопасности:

- Администратор безопасности (локальный и удаленный).
- Администратор сервера (только в случае установки компонента Легкий агент на серверах).
- Пользователь ИС (только в случае установки компонента Легкий агент для Windows на рабочих станциях).

Удаленный администратор безопасности

Удаленный администратор безопасности – это администратор, который управляет программой через Kaspersky Security Center.

Доступ к функциям программы Kaspersky Security через Kaspersky Security Center предоставляется пользователю в соответствии с его правами доступа к Серверу администрирования Kaspersky Security Center и его объектам. Для полноценной работы с программой Kaspersky Security через Kaspersky Security Center пользователь должен обладать правами роли "Главный администратор" Kaspersky Security Center.

По умолчанию роль "Главный администратор" назначается следующим группам пользователей Kaspersky Security Center:

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

Если программа используется в режиме multitenancy, роль "Главный администратор" также назначается учетной записи, под которой администратор клиента подключается к виртуальному Серверу администрирования, настроенному для этого клиента. Учетная запись администратора клиента создается автоматически в результате выполнения процедуры создания клиента и обладает правами главного администратора на виртуальном Сервере администрирования.

Для пользователей, которые не обладают правами роли "Главный администратор", доступ к функциям программы Kaspersky Security через Kaspersky Security Center ограничен или запрещен.

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

Локальный администратор безопасности

Локальный администратор безопасности – это администратор, который управляет компонентом Легкий агент для Windows через локальный интерфейс или с помощью командной строки или управляет компонентом Легкий агент для Linux с помощью командной строки.

Доступ к функциям Легкого агента для Windows для локального администратора безопасности может быть ограничен или запрещен удаленным администратором безопасности в политике для Легкого агента для Windows. Если доступ к функциям и параметрам программы защищен паролем, локальный администратор безопасности должен знать имя пользователя и пароль учетной записи, которой разрешен доступ к программе.

Для управления работой Легкого агента для Linux с помощью командной строки локальный администратор безопасности должен работать под учетной записью root. Пользователю, который не обладает

привилегиями учетной записи root, доступ к функциям программы запрещен.

Администратор сервера

Администратор сервера – это администратор, который управляет компонентом Легкий агент для Windows или Легкий агент для Linux, установленным на серверах.

В случае Легкого агента для Linux администратор сервера работает под учетной записью root и имеет доступ к функциям и параметрам программы.

В случае Легкого агента для Windows доступ к функциям Легкого агента для Windows для администратора сервера может быть ограничен или запрещен удаленным администратором безопасности в политике для Легкого агента для Windows. Если доступ к функциям и параметрам программы защищен паролем, то для администратора сервера доступ к функциям и параметрам программы ограничен в соответствии с настроенными параметрами защиты доступа.

Пользователь ИС

Пользователь ИС – это пользователь рабочей станции, на которой установлен компонент Легкий агент для Windows или Легкий агент для Linux.

Пользователь ИС может запускать проверку выбранного объекта на вирусы через контекстное меню или по команде SCAN. Доступ к остальным функциям и параметрам программы для пользователя ИС запрещен.

Концепция управления программой

Вы можете управлять работой программы и настраивать ее параметры следующими способами:

- Через систему удаленного централизованного управления программами "Лаборатории Касперского" – Kaspersky Security Center (см. раздел "Об управлении программой через Kaspersky Security Center" на стр. 118).
- В локальном интерфейсе для Легкого агента для Windows (см. раздел "Об управлении программой через локальный интерфейс Легкого агента для Windows" на стр. 119).
- С помощью командной строки для Легкого агента для Linux (см. раздел "Управление Легким агентом для Linux из командной строки" на стр. 479).
- С помощью командной строки для Легкого агента для Windows (см. раздел "Управление Легким агентом для Windows из командной строки" на стр. 493).

В этом разделе

Об управлении программой через Kaspersky Security Center

Kaspersky Security Center позволяет вам удаленно управлять работой программы Kaspersky Security. Используя возможности Kaspersky Security Center, вы можете:

- устанавливать программу в виртуальную инфраструктуру;
- запускать и останавливать программу Kaspersky Security на защищенных виртуальных машинах;
- централизованно управлять работой программы:
  - управлять защитой виртуальных машин;
  - управлять задачами программы;
  - управлять лицензионными ключами для программы;
- обновлять базы и модули программы;
- формировать отчеты о событиях, которые произошли во время работы программы;
- удалять программу из виртуальной инфраструктуры.

Для управления компонентами программы Kaspersky Security с помощью Kaspersky Security Center

используются следующие mmc-плагины управления:

- Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows.
- Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux.
- Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты.

Управление работой программы Kaspersky Security через Kaspersky Security Center, независимо от используемой консоли управления, осуществляется с помощью политик и задач:

- *Политики* определяют параметры защиты виртуальных машин и параметры работы Легких агентов и Сервера защиты (см. раздел "Управление программой с помощью политик Kaspersky Security Center" на стр. 122).
- *Задачи* реализуют такие функции программы, как активация программы, проверка виртуальных машин, обновление баз программы (см. раздел "Управление программой с помощью задач" на стр. 140).

С помощью политик и задач вы можете установить одинаковые значения параметров работы программы Kaspersky Security для всех защищенных виртуальных машин или SVM, входящих в состав группы администрирования.

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

Об управлении программой через локальный интерфейс Легкого агента для Windows

Этот раздел содержит информацию об основных элементах локального интерфейса программы для Легкого агента для Windows.

В этом разделе

Значок программы в области уведомлений

Сразу после запуска программы Kaspersky Security на защищенной виртуальной машине в области уведомлений панели задач Microsoft Windows появляется значок программы.

Значок программы выполняет следующие функции:

- служит индикатором работы программы;
- обеспечивает доступ к контекстному меню значка программы и главному окну программы.

Значок программы отражает состояние защиты виртуальной машины, а также показывает действия, которые программа выполняет в текущий момент:

- Значок означает, что работа всех компонентов защиты программы включена.
- Значок означает, что Kaspersky Security проверяет сообщение электронной почты.
- Значок означает, что Kaspersky Security проверяет входящий или исходящий сетевой трафик.
- Значок означает, что Kaspersky Security обновляет базы и модули программы.
- Значок означает, что в работе Kaspersky Security произошли важные события, на которые нужно обратить внимание. Например, выключен Файловый Антивирус, базы и модули программы устарели.
- Значок означает, что в работе Kaspersky Security произошли события критической важности. Например, сбой в работе компонента(ов), повреждение баз и модулей программы.

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Security для виртуальных сред 5.2 Легкий агент**. Открывает закладку **Центр управления** главного окна программы. С помощью закладки **Центр управления** вы можете регулировать работу компонентов и задач программы, просматривать статистику об обработанных файлах и обнаруженных угрозах.
- **Настройка**. Открывает закладку **Настройка** главного окна программы. С помощью закладки **Настройка** вы можете изменить параметры программы, установленные по умолчанию.
- **Приостановка защиты и контроля / Возобновление защиты и контроля**. Временно выключает / включает работу компонентов защиты и компонентов контроля. Этот пункт контекстного меню не влияет на выполнение задачи обновления и задач проверки и доступен только при выключенной политике Kaspersky Security Center.
- **Выключение политики / Включение политики**. Выключает / включает политику Kaspersky Security Center. Этот пункт доступен, если Kaspersky Security работает под политикой Kaspersky Security Center и в параметрах политики установлен пароль на выключение политики.
- **О программе**. Открывает информационное окно со сведениями о программе.
- **Выход**. Завершает работу Kaspersky Security. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти виртуальной машины.

Вы можете открыть контекстное меню значка программы наведением курсора мыши на значок программы в области уведомлений панели задач Microsoft Windows и нажатием на правую клавишу мыши.

Главное окно программы

В главном окне программы находятся элементы интерфейса, предоставляющие вам доступ к основным функциям программы.

► *Чтобы открыть главное окно программы, выполните одно из следующих действий:*

- Наведите курсор на значок программы в области уведомлений панели задач Microsoft Windows и нажмите на левую клавишу мыши.
- В контекстном меню значка программы выберите пункт **Kaspersky Security для виртуальных сред 5.2 Легкий агент**.

- В меню **Пуск** выберите пункт **Программы** / **Kaspersky Security для виртуальных сред 5.2 Легкий агент**.

Главное окно программы можно условно разделить на три части:

- В верхней части окна расположены элементы интерфейса, с помощью которых вы можете просмотреть следующую информацию:
  - сведения о программе;
  - статистику репутационных баз;
  - список необработанных объектов;
  - хранилище резервных копий зараженных файлов, которые были удалены или изменены в ходе работы программы;
  - отчеты о событиях, произошедших в ходе работы программы в целом, работы отдельных компонентов и выполнения задач.
- В центральной части окна находятся закладки **Центр управления** и **Настройка**:
  - Закладка **Центр управления** позволяет регулировать работу компонентов и задач программы. Когда вы открываете главное окно программы, в нем отображается закладка **Центр управления**.
  - Закладка **Настройка** позволяет изменять параметры программы, установленные по умолчанию.
- В нижней части окна расположены ссылки:
  - **Справка**. По ссылке осуществляется переход к справочной системе программы Kaspersky Security.
  - **Поддержка**. По ссылке открывается окно **Поддержка** с информацией об операционной системе, текущей версии программы, информацией о подключении защищенной виртуальной машины к SVM и Серверу интеграции и ссылками на информационные ресурсы "Лаборатории Касперского".
  - **Лицензия**. По ссылке открывается окно **Лицензирование** с информацией о действующей лицензии.

Окно настройки параметров программы

Окно настройки параметров Kaspersky Security предназначено для настройки параметров работы программы в целом, отдельных ее компонентов, отчетов и хранилищ, задач проверки и задачи обновления.

► *Чтобы открыть окно настройки параметров программы, выполните одно из следующих действий:*

- выберите закладку **Настройка** в главном окне программы (см. раздел "Главное окно программы" на стр. 120);
- выберите пункт **Настройка** в контекстном меню значка программы.

Окно настройки параметров программы состоит из двух частей:

- В левой части окна содержатся компоненты программы, задачи и другие составляющие, предназначенные для настройки.
- В правой части окна содержатся элементы управления, с помощью которых вы можете настроить

работу составляющей, выбранной в левой части окна.

Управление программой с помощью политик Kaspersky Security Center

Для управления параметрами программы Kaspersky Security для виртуальных сред 5.2 Легкий агент используются следующие политики Kaspersky Security Center:

- **Политика для Сервера защиты** (на стр. 123). Политика определяет параметры работы Сервера защиты и применяется на всех SVM, входящих в группу администрирования, для которой настроена политика.

  После установки mmc-плагинов управления Kaspersky Security в Kaspersky Security Center автоматически создается политика по умолчанию для Сервера защиты (см. раздел "Автоматическое создание задач и политики по умолчанию для Сервера защиты" на стр. 62). Политика создается для группы администрирования **Управляемые устройства** под именем **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты** и применяется на всех SVM, которые помещаются в папку **Управляемые устройства** или в любую вложенную группу администрирования.

  Вы можете изменить значения параметров этой политики, настроенные по умолчанию.

- **Политика для Легкого агента для Windows** (на стр. 128). Политика определяет параметры работы Легких агентов, установленных на защищенных виртуальных машинах с гостевыми операционными системами Windows. Политика применяется на всех защищенных виртуальных машинах, входящих в группу администрирования, для которой настроена политика.

- **Политика для Легкого агента для Linux** (на стр. 136). Политика определяет параметры работы Легких агентов, установленных на защищенных виртуальных машинах с гостевыми операционными системами Linux. Политика применяется на всех защищенных виртуальных машинах, входящих в группу администрирования, для которой настроена политика.

Вы можете выполнять следующие действия над политиками:

- создавать политику;
- изменять параметры политики;
- удалять политику;
- изменять состояние политики.

Параметры и блоки параметров политик имеют *атрибут "замок"*, который показывает, наложен ли запрет на изменение параметра или блока параметров в локальных параметрах программы, в параметрах задач и в политиках вложенного уровня иерархии (для вложенных групп администрирования, виртуальных и подчиненных Серверов администрирования).

В политике для Легкого агента для Windows и в политике для Легкого агента для Linux вы можете создавать *профили политик*. Использование профилей политик позволяет более гибко настроить параметры работы Легких агентов на разных виртуальных машинах. Профиль политики может содержать параметры, которые отличаются от параметров "базовой" политики и применяются на защищенных виртуальных машинах при выполнении настроенных вами условий (правил активации).

Вы можете создавать и настраивать профили политики в свойствах политик для Легкого агента в разделе **Профили политик**.

Подробнее о работе с политиками и профилями политик см. в документации Kaspersky Security Center.

В этом разделе

Политика для Сервера защиты

С помощью политики для Сервера защиты вы можете настраивать следующие параметры работы программы:

- Параметры использования Kaspersky Security Network (KSN) в работе программы (см. раздел "Участие в Kaspersky Security Network" на стр. 399).
- Параметры обновления модулей программы в ходе обновления баз программы.
- Параметры SNMP-мониторинга состояния SVM.
- Параметры подключения SVM к Серверу интеграции (см. раздел "Настройка параметров подключения SVM к Серверу интеграции" на стр. 164).
- Параметры подключения Легких агентов к SVM:
  - теги для подключения Легких агентов (см. раздел "Настройка использования тегов для подключения" на стр. 170);
  - параметры защиты соединения между Легкими агентами и SVM (см. раздел "Защита соединения между Легким агентом и SVM" на стр. 172).
- Дополнительные параметры работы SVM.

> Если вы хотите настраивать дополнительные параметры работы SVM, вам нужно включить их отображение в политике (см. раздел "Настройка отображения дополнительных параметров политики для Сервера защиты" на стр. 124).

В свойствах политики для Сервера защиты вы можете включить или выключить использование функциональности Managed Detection and Response в работе программы Kaspersky Security (см. раздел "Managed Detection and Response" на стр. 388).

> Изменение некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

kaspersky

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

О настройке общих параметров политики и параметрах событий см. в документации Kaspersky Security Center.

В этом разделе

Настройка отображения дополнительных параметров политики для Сервера защиты

По умолчанию в мастере создания политики для Сервера защиты и в свойствах политики для Сервера защиты не отображаются дополнительные параметры работы SVM (см. раздел "Создание политики для Сервера защиты" на стр. 124).

Если вы хотите настраивать дополнительные параметры работы SVM, вам нужно предварительно создать ключ `AdvancedUI` типа REG_DWORD и установить значение `1` для этого ключа в следующей ветке реестра операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center:

- HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Products\SVM\<номер версии>\Settings\ – для 32-разрядных операционных систем;
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\Components\34\Products\SVM\<номер версии>\Settings\ – для 64-разрядных операционных систем;

  где <номер версии> – номер установленной версии программы Kaspersky Security в формате X.X.X.X.

Создание политики для Сервера защиты

► *Чтобы создать политику для Сервера защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите создать политику.

   На закладке **Устройства** папки с названием группы администрирования вы можете просмотреть список SVM, которые входят в состав этой группы администрирования.
3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.
5. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты**.

Перейдите к следующему шагу мастера.

6. Введите название новой политики.

   Перейдите к следующему шагу мастера.

7. На этом шаге вам предлагается принять участие в программе Kaspersky Security Network (KSN) (см. раздел "Участие в Kaspersky Security Network" на стр. 399). Для этого 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 решение об участии в KSN позже (см. раздел "Настройка использования Kaspersky Security Network в политике Сервера защиты" на стр. 401).

   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.

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

   Перейдите к следующему шагу мастера.

8. На этом шаге вам предлагается настроить автоматическое получение обновлений модулей программы вместе с пакетом обновлений баз программы.

   Допускается устанавливать только обновления модулей программы, прошедшие инспекционный контроль. Включение автоматического обновления модулей приводит к выходу программы из сертифицированного состояния.

   По умолчанию программа Kaspersky Security не включает обновления модулей программы в пакет обновлений.

   Перейдите к следующему шагу мастера.

9. На этом шаге вам предлагается включить SNMP-мониторинг состояния SVM с помощью системы сетевого управления, использующей протокол SNMP.

Включение SNMP-мониторинга состояния SVM приводит к выходу программы из сертифицированного состояния.

По умолчанию SNMP-мониторинг состояния SVM выключен.

Перейдите к следующему шагу мастера.

10. Если вы включили отображение дополнительных параметров политики для Сервера защиты (см. раздел "Настройка отображения дополнительных параметров политики для Сервера защиты" на стр. 124), настройте дополнительные параметры работы SVM:

- **Максимальное количество одновременных запросов на проверку**

  Максимальное количество запросов на проверку от Легких агентов, которые одновременно обрабатывает SVM. Легкие агенты формируют запросы на проверку в ходе защиты виртуальных машин и в ходе выполнения задач проверки.

  По умолчанию SVM одновременно обрабатывает 75 запросов на проверку.

- **Максимальное количество задач проверки, запущенных по расписанию**

  Максимальное количество одновременно выполняемых на SVM задач проверки, которые запущены по расписанию на Легком агенте. Для SVM такие задачи проверки являются низкоприоритетными.

  По умолчанию одновременно выполняется пять низкоприоритетных задач проверки.

- **Максимальное количество задач проверки, запущенных вручную**

  Максимальное количество одновременно выполняемых на SVM задач проверки, которые вы запустили вручную. Для SVM такие задачи проверки являются высокоприоритетными.

  По умолчанию одновременно выполняется пять высокоприоритетных задач проверки.

Перейдите к следующему шагу мастера.

11. Проверьте адрес и порт для подключения SVM к Серверу интеграции. В полях указан порт, используемый по умолчанию (7271), и доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Вы можете изменить порт и указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

Перейдите к следующему шагу мастера.

Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, в открывшемся окне **Подключение к Серверу интеграции** укажите пароль администратора Сервера интеграции (пароль учетной записи admin).

Мастер создания политики проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью кнопки в окне вы можете посмотреть информацию о полученном

сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

12. Если вы хотите защищать соединение между Легкими агентами и SVM с помощью шифрования, настройте параметры защиты соединения между Легкими агентами и SVM (см. раздел "Защита соединения между Легким агентом и SVM" на стр. 172).

    Перейдите к следующему шагу мастера.

13. Если вы используете программу по расширенной лицензии, вы можете настроить параметры использования тегов для подключения Легких агентов к SVM (см. раздел "Настройка использования тегов для подключения" на стр. 170).

    Перейдите к следующему шагу мастера.

14. Завершите работу мастера создания политики.

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

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 на гипервизоре в соответствии с параметрами политики.

Если на SVM не запущен Агент администрирования, созданная политика не применяется на этой SVM.

Если на последнем шаге мастера создания политики вы выбрали вариант **Неактивная политика**, созданная политика не применяется на SVM.

Изменение параметров политики для Сервера защиты в Консоли администрирования

► *Чтобы изменить параметры политики для Сервера защиты в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - По ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
   - Двойным щелчком мыши.

- По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.

5. Измените параметры политики.

   Если вы хотите настроить дополнительные параметры работы SVM, вам нужно включить отображение дополнительных параметров политики для Сервера защиты в реестре операционной системы.

   Разделы **Общие** и **Оповещение о событиях** окна **Свойства: <Название политики>** стандартны для программы Kaspersky Security Center. Описание стандартных разделов см. в документации Kaspersky Security Center.

6. Нажмите на кнопку **OK** в окне **Свойства: <Название политики>**.

Политика для Легкого агента для Windows

С помощью политики для Легкого агента для Windows вы можете настраивать следующие параметры работы программы:

- Автоматический запуск программы на виртуальной машине (см. раздел "Включение и выключение автоматического запуска компонента Легкий агент для Windows" на стр. 156).
- Параметры работы следующих компонентов контроля:
  - Контроль запуска программ (на стр. 275).
  - Контроль активности программ (на стр. 288).
  - Веб-Контроль (на стр. 306).
  - Контроль целостности системы (на стр. 326).
- Общие параметры антивирусной защиты (см. раздел "Настройка общих параметров антивирусной защиты" на стр. 177).
- Параметры работы следующих компонентов защиты:
  - Файловый Антивирус (см. раздел "Защита файловой системы виртуальной машины. Файловый Антивирус" на стр. 197).
  - AMSI-защита (на стр. 221).
  - Почтовый Антивирус (см. раздел "Защита почты. Почтовый Антивирус" на стр. 224).
  - Веб-Антивирус (см. раздел "Защита веб-трафика виртуальной машины. Веб-Антивирус" на стр. 237).
  - Мониторинг системы (на стр. 262).
- Параметры подключения Легких агентов к SVM и Серверу интеграции:
  - Параметры обнаружения SVM, работающих в сети, и получения информации о них (см. раздел "Настройка параметров обнаружения SVM" на стр. 168).
  - Параметры подключения Легких агентов к Серверу интеграции (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 165). Подключение требуется настроить, если вы используете Сервер интеграции для получения информации об SVM, работающих в сети, и если вы используете теги для подключения Легких агентов к SVM.
  - Использование тегов для подключения к SVM (см. раздел "Настройка использования тегов для подключения" на стр. 170).

- Параметры защиты соединения между Легкими агентами и SVM (см. раздел "Защита соединения между Легким агентом и SVM" на стр. 172).
- Алгоритм, который используют Легкие агенты при выборе SVM (см. раздел "Настройка алгоритма выбора SVM" на стр. 174).

Все параметры подключения Легких агентов к SVM и Серверу интеграции, кроме параметров обнаружения SVM, недоступны для настройки при создании политики для Легкого агента для Windows. Вы можете настроить эти параметры в окне свойств политики (см. раздел "Изменение параметров политики для Легкого агента для Windows в Консоли администрирования" на стр. 135).

- Другие параметры работы программы:
  - Параметры контроля сетевого трафика (см. раздел "Контроль сетевого трафика" на стр. 247).
  - Параметры самозащиты программы (см. раздел "Самозащита программы" на стр. 405).
  - Параметры управления через локальный интерфейс локальными и групповыми задачами (за исключением задачи выборочной проверки).
  - Режим проверки виртуальной машины во время простоя.
  - Параметры проверки съемных дисков на виртуальной машине (см. раздел "Проверка съемных дисков при подключении к виртуальной машине" на стр. 382).
  - Параметры отчетов (см. раздел "Настройка параметров отчетов" на стр. 429) и резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 418).
  - Параметры взаимодействия локального интерфейса Легкого агента с пользователем (см. раздел "Настройка взаимодействия пользователя с локальным интерфейсом" на стр. 412).
  - Параметры защиты доступа к функциям и параметрам программы в локальном интерфейсе (см. раздел "Защита паролем доступа к параметрам программы в локальном интерфейсе" на стр. 408).
  - Параметры уведомлений в локальном интерфейсе о событиях, возникающих во время работы Легкого агента (см. раздел "Настройка событий и уведомлений Легкого агента для Windows" на стр. 425).

Изменение некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

О настройке общих параметров политики и параметрах событий см. в документации Kaspersky Security

Center.

Параметры, настроенные в политике для Легкого агента для Windows, пользователь защищенной виртуальной машины может также настраивать в локальном интерфейсе программы, если это не запрещено политикой.

Возможность изменять параметр программы локально на защищенной виртуальной машине определяется статусом «замка»:

- Если параметр закрыт "замком" (), это означает, что пользователь не может изменить значение параметра локально и для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" (), это означает, что пользователь может изменить значение параметра локально на каждой защищенной виртуальной машине группы администрирования.

В этом разделе

Создание политики для Легкого агента для Windows

► *Чтобы создать политику для Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите создать политику.

   На закладке **Устройства** папки с названием группы администрирования вы можете просмотреть список защищенных виртуальных машин, которые входят в состав этой группы администрирования.
3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.
5. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows**.

   Перейдите к следующему шагу мастера.
6. Введите название новой политики.

   Перейдите к следующему шагу мастера.
7. На этом шаге вы можете перенести в создаваемую политику параметры Легкого агента для Windows, ранее сохраненные на защищенной виртуальной машине. Для переноса параметров используется конфигурационный файл (см. раздел "Экспорт и импорт параметров Легкого агента для Windows в локальном интерфейсе" на стр. 416) в формате CFG, который вы можете создать в локальном интерфейсе Легкого агента.

   Для переноса параметров нажмите на кнопку **Выбрать** и в открывшемся окне **Выбор конфигурационного файла** выберите файл с расширением cfg. Путь к конфигурационному файлу отображается в поле **Конфигурационный файл**.

Вы можете использовать только конфигурационный файл, созданный в программе версии Kaspersky Security для виртуальных сред 5.2 Легкий агент.

На следующих шагах мастера создания политики вы можете изменить значения параметров, перенесенных из конфигурационного файла.

Перейдите к следующему шагу мастера.

8. Настройте параметры контроля виртуальных машин. В окне мастера отображается список компонентов контроля.

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия:

- Включить или выключить компонент контроля.

  По умолчанию компонент Контроль запуска программ выключен. Для приведения конфигурации программы в соответствие с сертифицированной конфигурацией требуется включить этот компоненты, установив флажок слева от названия компонента в списке.

  Выключение компонентов контроля приводит к выходу программы из сертифицированного состояния.

- Настроить параметры каждого компонента контроля. Для этого выберите компонент контроля в списке и нажмите на кнопку **Изменить**, расположенную над списком компонентов контроля. В открывшемся окне настройте параметры работы выбранного компонента и нажмите на кнопку **OK**.

- Запретить или разрешить изменение параметров каждого компонента контроля через локальный интерфейс Легкого агента для Windows. По умолчанию изменение всех параметров контроля через локальный интерфейс запрещено.

  Если вы хотите разрешить изменение параметров компонента контроля через локальный интерфейс, выберите этот компонент в списке и нажмите на кнопку **Открыть**, расположенную над списком компонентов, или нажмите на значок "замок" слева от названия компонента.

  Если изменение параметров компонента через локальный интерфейс запрещено, Kaspersky Security использует на всех защищенных виртуальных машинах параметры работы компонента, заданные политикой. Если изменение параметров компонента через локальный интерфейс разрешено, Kaspersky Security использует локальные значения параметров работы компонента, а не те, которые настроены в политике.

Перейдите к следующему шагу мастера.

9. Настройте параметры защиты виртуальных машин. В окне мастера отображается список компонентов защиты.

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия:

- Включить или выключить автоматический запуск программы на виртуальной машине (см. раздел "Включение и выключение автоматического запуска компонента Легкий агент для Windows" на стр. 156) и настроить общие параметры антивирусной защиты (см. раздел "Настройка общих параметров антивирусной защиты" на стр. 177). Для этого выберите в списке пункт **Основные параметры защиты** и нажмите на кнопку **Изменить**, расположенную над списком компонентов защиты. В открывшемся окне настройте параметры и нажмите на кнопку **OK**.
- Включить или выключить компонент защиты с помощью флажка слева от названия компонента в списке. По умолчанию все компоненты защиты включены.

  Выключение компонентов защиты приводит к выходу программы из сертифицированного состояния.

- Настроить параметры каждого компонента защиты. Для этого выберите компонент защиты в списке и нажмите на кнопку **Изменить**, расположенную над списком компонентов защиты. В открывшемся окне настройте параметры работы выбранного компонента и нажмите на кнопку **OK**.
- Запретить или разрешить изменение параметров каждого компонента защиты через локальный интерфейс Легкого агента для Windows. По умолчанию изменение всех параметров защиты через локальный интерфейс запрещено.

  Если вы хотите разрешить изменение параметров компонента защиты через локальный интерфейс, выберите этот компонент в списке и нажмите на кнопку **Открыть**, расположенную над списком компонентов, или нажмите на значок "замок" слева от названия компонента.

  Если изменение параметров компонента через локальный интерфейс запрещено, Kaspersky Security использует на всех защищенных виртуальных машинах параметры работы компонента, заданные политикой. Если изменение параметров компонента через локальный интерфейс разрешено, Kaspersky Security использует локальные значения параметров работы компонента, а не те, которые настроены в политике.

Перейдите к следующему шагу мастера.

10. Настройте параметры обнаружения SVM Легкими агентами:

- Если вы хотите использовать Сервер интеграции, проверьте адрес и порт для подключения SVM к Серверу интеграции. В полях указан порт, используемый по умолчанию (7271), и доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Вы можете изменить порт и указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

  Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

  Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, при переходе к следующему шагу мастера в открывшемся окне укажите пароль администратора Сервера интеграции (пароль учетной записи admin).

  Мастер создания политики проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью кнопки в окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

- Если вы хотите использовать список адресов SVM, введите один или несколько адресов с помощью кнопки **Добавить**.

  В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе программы.

  Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и применяется расширенный алгоритм выбора SVM, в разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкие агенты не смогут подключиться к SVM.

Перейдите к следующему шагу мастера.

11. Если требуется, измените настроенные по умолчанию исключения из проверки и защиты.

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

Список **Исключения** содержит названия программ или названия компаний-производителей программ, которые вы можете включить в доверенную зону или исключить из доверенной зоны (см. раздел "Настройка доверенной зоны" на стр. 179). Для настройки исключений выполните одно из следующих действий:

- Установите флажок слева от названия программы или компании-производителя, если вы хотите включить программу или программы компании-производителя в доверенную зону.

  Если флажок установлен, то файлы, папки и процессы, рекомендованные для этих программ, включаются в доверенную зону, а исполняемые файлы этих программ автоматически добавляются в список доверенных программ.

- Снимите флажок слева от названия программы или компании-производителя, если вы хотите исключить программу или программы компании-производителя из доверенной зоны.

Перейдите к следующему шагу мастера.

12. Настройте параметры взаимодействия пользователя с локальным интерфейсом Легкого агента (см. раздел "Настройка взаимодействия пользователя с локальным интерфейсом" на стр. 412) и параметры уведомлений о событиях, происходящих во время работы Легкого агента (см. раздел "Настройка событий и уведомлений Легкого агента для Windows" на стр. 425).

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Чтобы обеспечить возможность работы программы Kaspersky Security на виртуальной машине, на которой используется технология Windows Terminal Services, требуется снять флажок **Запускать локальный интерфейс программы**.

Если вы используете Легкий агент в инфраструктуре виртуальных рабочих столов (VDI) с операционной системой Microsoft Windows для рабочих станций, то для повышения производительности виртуальной инфраструктуры рекомендуется снять флажок **Запускать локальный интерфейс программы**.

Перейдите к следующему шагу мастера.

13. Настройте параметры защиты доступа к функциям и параметрам Легкого агента (см. раздел "Защита паролем доступа к параметрам программы в локальном интерфейсе" на стр. 408). Для этого выполните следующие действия:

    a. Установите флажок **Включить защиту паролем**.

    b. Укажите имя и пароль учетной записи, которой разрешен доступ к параметрам программы в

локальном интерфейсе Легкого агента.

c. Нажмите на кнопку **Настройка** и выберите в открывшемся окне операции с Легким агентом, которые будут защищены паролем.

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

Перейдите к следующему шагу мастера.

14. Завершите работу мастера создания политики.

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

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

Если на защищенной виртуальной машине не запущен Агент администрирования, созданная политика не применяется на этой виртуальной машине.

Если на последнем шаге мастера создания политики вы выбрали вариант **Неактивная политика**, созданная политика не применяется на защищенных виртуальных машинах.

Изменение параметров политики для Легкого агента для Windows в Консоли администрирования

► *Чтобы изменить параметры политики для Легкого агента для Windows в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - По ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

- Двойным щелчком мыши.
- По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.

5. Измените параметры политики.

   Разделы **Общие** и **Оповещение о событиях** окна **Свойства: <Название политики>** стандартны для программы Kaspersky Security Center. Описание стандартных разделов см. в документации Kaspersky Security Center.

6. Нажмите на кнопку **OK** в окне **Свойства: <Название политики>**.

Политика для Легкого агента для Linux

С помощью политики для Легкого агента для Linux вы можете настраивать следующие параметры работы программы:

- Общие параметры антивирусной защиты: список объектов для обнаружения (см. раздел "Выбор типов обнаруживаемых объектов" на стр. 177) и доверенная зона (см. раздел "Настройка доверенной зоны" на стр. 179).
- Параметры работы компонента Файловый Антивирус (см. раздел "Защита файловой системы виртуальной машины. Файловый Антивирус" на стр. 197).
- Параметры подключения Легких агентов к SVM и Серверу интеграции:
  - Параметры обнаружения SVM, работающих в сети, и получения информации о них (см. раздел "Настройка параметров обнаружения SVM" на стр. 168).
  - Параметры подключения Легких агентов к Серверу интеграции (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 165). Подключение требуется настроить, если вы используете Сервер интеграции для получения информации об SVM, работающих в сети, и если вы используете теги для подключения Легких агентов к SVM.
  - Использование тегов для подключения (см. раздел "Настройка использования тегов для подключения" на стр. 170) к SVM.
  - Параметры защиты соединения между Легкими агентами и SVM (см. раздел "Защита соединения между Легким агентом и SVM" на стр. 172).
  - Алгоритм, который используют Легкие агенты при выборе SVM (см. раздел "Настройка алгоритма выбора SVM" на стр. 174).

  Все параметры подключения Легких агентов к SVM и Серверу интеграции, кроме параметров обнаружения SVM, недоступны для настройки при создании политики для Легкого агента для Linux. Вы можете настроить эти параметры в окне свойств политики (см. раздел "Изменение параметров политики для Легкого агента для Linux в Консоли администрирования" на стр. 140).

- Параметры резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 418).

Изменение некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

О настройке общих параметров политики и параметрах событий см. в документации Kaspersky Security Center.

Создание политики для Легкого агента для Linux

► *Чтобы создать политику для Легкого агента для Linux, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите создать политику.

   На закладке **Устройства** папки с названием группы администрирования вы можете просмотреть список защищенных виртуальных машин, которые входят в состав этой группы администрирования.
3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.
5. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux**.

   Перейдите к следующему шагу мастера создания политики.
6. Введите название новой политики.

   Перейдите к следующему шагу мастера.
7. На этом шаге вы можете перенести в создаваемую политику параметры Легкого агента для Linux, ранее сохраненные на защищенной виртуальной машине. Для переноса параметров используется конфигурационный файл в формате CFG (см. раздел "Экспорт и импорт параметров Легкого агента для Windows в локальном интерфейсе" на стр. 416), который вы можете создать с помощью команд из командной строки Легкого агента для Linux.

   Для переноса параметров нажмите на кнопку **Выбрать** и в открывшемся окне **Выбор конфигурационного файла** выберите файл с расширением cfg. Путь к конфигурационному файлу отображается в поле **Конфигурационный файл**.

   Вы можете использовать только конфигурационный файл, созданный в программе версии Kaspersky Security для виртуальных сред 5.2 Легкий агент.

   На следующих шагах мастера создания политики вы можете изменить значения параметров,

перенесенных из конфигурационного файла.

Перейдите к следующему шагу мастера создания политики.

8. Настройте параметры защиты виртуальных машин.

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия:

- Настроить общие параметры защиты: выбрать типы объектов, которые должна обнаруживать программа Kaspersky Security (см. раздел "Выбор типов обнаруживаемых объектов" на стр. 177), и настроить доверенную зону (см. раздел "Настройка доверенной зоны" на стр. 179). Для этого выберите в списке пункт **Основные параметры защиты** и нажмите на кнопку **Изменить**, расположенную над списком компонентов защиты. В открывшемся окне настройте параметры и нажмите на кнопку **OK**.
- Включить или выключить Файловый Антивирус с помощью флажка слева от названия компонента в списке. По умолчанию Файловый Антивирус включен.

  Выключение компонента Файловый Антивирус приводит к выходу программы из сертифицированного состояния.

- Настроить параметры работы Файлового Антивируса. Для этого выберите Файловый Антивирус в списке и нажмите на кнопку **Изменить**, расположенную над списком. В открывшемся окне настройте параметры работы Файлового Антивируса (см. раздел "Настройка Файлового Антивируса Легкого агента для Linux" на стр. 212) и нажмите на кнопку **OK**.

Перейдите к следующему шагу мастера создания политики.

9. Настройте параметры обнаружения Легкими агентами SVM:

- Если вы хотите использовать Сервер интеграции, проверьте адрес и порт для подключения SVM к Серверу интеграции. В полях указан порт, используемый по умолчанию (7271), и доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Вы можете изменить порт и указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

  Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

  Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, при переходе к следующему шагу мастера

в открывшемся окне укажите пароль администратора Сервера интеграции (пароль учетной записи admin).

Мастер создания политики проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью кнопки в окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

- Если вы хотите использовать список адресов SVM, введите один или несколько адресов с помощью кнопки **Добавить**.

  В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе программы.

  Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и применяется расширенный алгоритм выбора SVM, в разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкие агенты не смогут подключиться к SVM.

Перейдите к следующему шагу мастера.

10. Завершите работу мастера создания политики.

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

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

Если на защищенной виртуальной машине не запущен Агент администрирования, созданная политика не применяется на этой виртуальной машине.

Если на последнем шаге мастера создания политики вы выбрали вариант **Неактивная политика**, созданная политика не применяется на защищенных виртуальных машинах.

Изменение параметров политики для Легкого агента для Linux в Консоли администрирования

► *Чтобы изменить параметры политики для Легкого агента для Linux в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - По ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
5. Измените параметры политики.

   Разделы **Общие** и **Оповещение о событиях** окна **Свойства: <Название политики>** стандартны для программы Kaspersky Security Center. Описание стандартных разделов см. в документации Kaspersky Security Center.
6. Нажмите на кнопку **OK** в окне **Свойства: <Название политики>**.

Управление программой с помощью задач

Вы можете управлять работой программы Kaspersky Security для виртуальных сред 5.2 Легкий агент с помощью задач как централизованно через Kaspersky Security Center, так и локально на защищенных виртуальных машинах (через локальный интерфейс Легкого агента для Windows или с помощью командной строки в случае Легкого агента для Linux).

Если на виртуальной машине применяется политика Kaspersky Security Center, по умолчанию управление локальными задачами через локальный интерфейс Легкого агента для Windows и из командной строки выключено.

Вы можете разрешить управление локальными задачами в политике Легкого агента для Windows (подраздел **Дополнительные параметры** в разделе **Другие параметры**).

В этом разделе

Управление задачами через Kaspersky Security Center

Для управления программой Kaspersky Security через Kaspersky Security Center вы можете использовать следующие задачи:

- Задачи, которые выполняются на SVM:
  - **Активация программы** (см. раздел "**Процедура активации программы**" на стр. 82). Kaspersky Security Center добавляет на SVM лицензионный ключ для активации программы или для продления срока действия лицензии.
  - **Обновление баз** (см. раздел "**Создание задачи обновления баз на Сервере защиты**" на стр. 393). Компонент Сервер защиты автоматически загружает пакет обновлений баз программы и устанавливает обновления баз на SVM.
  - **Откат обновления баз** (см. раздел "**Создание задачи отката обновления баз на Сервере защиты**" на стр. 397). Компонент Сервер защиты откатывает последнее обновление баз программы на SVM.
- Задачи, которые выполняются на защищенных виртуальных машинах с установленным компонентом Легкий агент для Windows:
  - **Инвентаризация** (см. раздел "**Создание задачи инвентаризации**" на стр. 281). Kaspersky Security выполняет поиск информации обо всех исполняемых файлах программ на защищенных виртуальных машинах. Получение информации о программах, установленных на защищенных виртуальных машинах, может быть полезно, например, для создания оптимальных правил контроля запуска программ.
  - **Поиск вирусов** (см. раздел "**Создание задачи поиска вирусов**" на стр. 355). Kaspersky Security выполняет антивирусную проверку областей защищенной виртуальной машины, указанных в параметрах задачи.
  - **Изменение состава компонентов программы**. Kaspersky Security устанавливает или удаляет функциональные компоненты Легкого агента на защищенных виртуальных машинах.
  - **Обновление снимка состояния системы** (см. раздел "**Создание и обновление снимка состояния системы**" на стр. 338). Kaspersky Security создает или обновляет ранее созданный снимок состояния системы, который используется при проверке целостности системы.
  - **Проверка целостности системы** (см. раздел "**Проверка целостности системы по расписанию или по требованию**" на стр. 340). Kaspersky Security сравнивает текущее состояние системы на выбранных виртуальных машинах с ранее созданным снимком состояния системы, чтобы обнаружить возможные изменения в выбранных объектах контроля.
  - **Сброс статуса целостности системы** (см. раздел "**Создание задачи сброса статуса целостности системы**" на стр. 351). Kaspersky Security отменяет для виртуальных машин статусы *Критический* и *Предупреждение*, полученные от компонента Контроль целостности системы.
- Задачу **Поиск вирусов** (см. раздел "**Создание задачи поиска вирусов**" на стр. 355), которая выполняется на защищенных виртуальных машинах с установленным компонентом Легкий агент для Linux. Kaspersky Security выполняет антивирусную проверку областей защищенной виртуальной машины, указанных в параметрах задачи.

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

- *Групповая задача* – задача, которая выполняется на клиентских устройствах выбранной группы администрирования. Применительно к программе Kaspersky Security групповые задачи

выполняются на SVM или защищенных виртуальных машинах, входящих в группы администрирования.

- *Задача для наборов устройств* – задача для одной или нескольких SVM или защищенных виртуальных машин, как входящих, так и не входящих в группы администрирования.

Вы можете выполнять следующие действия над задачами в Kaspersky Security Center:

- создавать (см. раздел "Создание задач" на стр. 144) и удалять задачи;
- изменять параметры задач (см. раздел "Изменение параметров задач" на стр. 146);
- запускать и останавливать задачи (см. раздел "Запуск и остановка задач" на стр. 147);
- просматривать результаты выполнения задач (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 148).

Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию обо всех событиях, произошедших во время выполнения задач.

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

Управление задачами через локальный интерфейс Легкого агента для Windows

Кроме задач, которые вы можете настраивать через Kaspersky Security Center, для управления программой Kaspersky Security для виртуальных сред 5.2 Легкий агент используются задачи, которые вы можете настраивать через локальный интерфейс Легкого агента для Windows на защищенной виртуальной машине, если отображение локальных задач и управление ими не запрещены политикой Легкого агента для Windows.

Для управления программой через локальный интерфейс Легкого агента для Windows вы можете использовать следующие задачи:

- **Полная проверка** (см. раздел "**Проверка виртуальной машины**" на стр. 354). Kaspersky Security выполняет тщательную проверку операционной системы защищенной виртуальной машины, включая память ядра, запущенные процессы и объекты автозапуска, загрузочные секторы, резервное хранилище операционной системы, а также все жесткие и съемные диски.
- **Выборочная проверка** (см. раздел "**Проверка виртуальной машины**" на стр. 354). Kaspersky Security проверяет на защищенной виртуальной машине объекты, выбранные пользователем.
- **Проверка важных областей** (см. раздел "**Проверка виртуальной машины**" на стр. 354). Kaspersky Security проверяет память ядра защищенной виртуальной машины, запущенные процессы и объекты автозапуска, загрузочные секторы и объекты заражения руткитами.
- **Обновление**. Легкий агент загружает с SVM пакет обновлений баз и модулей программы и устанавливает обновления на защищенную виртуальную машину.
- **Обновление снимка состояния системы**. Kaspersky Security создает или обновляет ранее созданный снимок состояния системы, который используется при проверке целостности системы.
- **Проверка целостности системы**. Kaspersky Security сравнивает текущее состояние системы на защищенной виртуальной машине с ранее созданным снимком состояния системы, чтобы обнаружить возможные изменения в выбранных объектах контроля.

Вы можете выполнять следующие действия над задачами в локальном интерфейсе:

- изменять параметры задач (см. раздел "Изменение параметров задач" на стр. 146);

- запускать и останавливать задачи (см. раздел "Запуск и остановка задач" на стр. 147);
- просматривать результаты выполнения задач (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 148).

Информация о результатах выполнения задач и обо всех событиях, произошедших во время выполнения задач, записывается в отчеты Kaspersky Security (см. раздел "Работа с отчетами в локальном интерфейсе" на стр. 431).

Управление задачами Легкого агента для Linux с помощью командной строки

Для управления Легким агентом для Linux с помощью командной строки доступны задачи следующих типов:

- *Полная проверка* (см. раздел "*Проверка виртуальной машины*" на стр. 486). Kaspersky Security выполняет тщательную проверку операционной системы защищенной виртуальной машины, включая системную память, объекты автозапуска, загрузочные секторы, а также все жесткие, съемные и сетевые диски.
- *Выборочная проверка* (см. раздел "*Проверка виртуальной машины*" на стр. 486). Kaspersky Security проверяет на защищенной виртуальной машине объекты, выбранные пользователем.
- *Обновление* (см. раздел "*Обновление баз*" на стр. 490). Легкий агент загружает с SVM пакет обновлений баз и модулей программы и устанавливает обновления на защищенную виртуальную машину.

Вы можете выполнять следующие действия над задачами (см. раздел «Управление Легким агентом для Linux из командной строки» на стр. 479):

- изменять параметры задач;
- запускать и останавливать задачи;
- просматривать результаты выполнения задач.

Создание задач

В Kaspersky Security Center вы можете создавать задачи, которые позволяют централизовано управлять программой Kaspersky Security. Задачи, которые позволяют управлять программой локально на защищенных виртуальных машинах, создавать не требуется, они создаются автоматически. Вы можете настаивать параметры локальных задач в локальном интерфейсе Легкого агента для Windows и в командной строке.

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

► *Чтобы создать задачу в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать групповую задачу для SVM или виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать групповую задачу для SVM или виртуальных машин, входящих в состав этой группы. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких SVM или виртуальных машин (задачу для набора устройств).
3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите mmc-плагин управления Kaspersky Security, для которого вы хотите создать задачу, и тип задачи.

   Перейдите к следующему шагу мастера создания задачи.
5. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора SVM или виртуальных машин, для которых вы создаете задачу. Вы можете выбрать SVM или виртуальные машины из списка устройств, обнаруженных Сервером администрирования, задать адреса SVM или виртуальных машин вручную, импортировать список SVM или виртуальных машин из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора SVM или виртуальных машин в открывшемся окне выполните одно из следующих действий:
   - В списке обнаруженных устройств укажите SVM или виртуальные машины, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия устройства.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM или виртуальных машин вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM или виртуальных машин.
   - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM или виртуальные машины, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.
6. Настройте доступные параметры задачи, следуя указаниям мастера создания задачи.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера, на последнем шаге установите флажок **Запустить задачу после завершения работы мастера**.
7. Завершите работу мастера.

Изменение параметров задач

Изменение параметров задач в Консоли администрирования Kaspersky Security Center

► *Чтобы изменить параметры задачи в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите изменить параметры задачи, созданной для SVM или виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите изменить параметры задачи, созданной для SVM или виртуальных машин, входящих в состав этой группы. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите изменить параметры задачи, созданной для одной или нескольких SVM или виртуальных машин.
3. В списке задач выберите нужную задачу и откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню задачи и выберите пункт **Свойства**.
4. Измените параметры задачи.
5. Нажмите на кнопку **Применить** или на кнопку **OK** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Изменение параметров задач в локальном интерфейсе Легкого агента для Windows

► *Чтобы изменить параметры задачи в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи.

   В правой части окна отобразятся параметры выбранной задачи.

   > Если в блоке отсутствуют какие-то задачи, это означает, что отображение локальных задач и управление ими запрещены политикой для всех защищенных виртуальных машин группы администрирования. Вы можете включить и выключить отображение локальных задач и управление ими в политике Легкого агента для Windows (подраздел **Дополнительные параметры** в разделе **Другие параметры**).

3. Настройте параметры задачи.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка задач

Запуск и остановка задач в Консоли администрирования Kaspersky Security Center

В Kaspersky Security Center вы можете запускать или останавливать задачу в любой момент независимо от выбранного режима запуска задачи.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите запустить или остановить выполнение задачи, созданной для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите запустить или остановить выполнение задачи, созданной для виртуальных машин, входящих в состав этой группы. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите запустить или остановить выполнение задачи, созданной для одной или нескольких виртуальных машин.
3. В списке задач выберите задачу, которую вы хотите запустить или остановить.
4. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу, по правой клавише мыши откройте контекстное меню и выберите пункт **Запустить**.
   - Если вы хотите остановить выполнение задачи, по правой клавише мыши откройте контекстное меню и выберите пункт **Остановить**.

Для задачи **Поиск вирусов** кроме запуска и остановки доступны действия **Приостановить** и **Возобновить**. На виртуальных машинах с компонентом Легкий агент для Windows также доступна автоматическая приостановка выполнения задачи в указанное время.

Запуск и остановка задач в локальном интерфейсе Легкого агента для Windows

В локальном интерфейсе вы можете запускать или останавливать задачу в любой момент независимо от выбранного режима запуска задачи, если отображение локальных задач и управление ими не запрещены политикой Легкого агента для Windows.

Запуск и остановка задачи **Поиск вирусов** выполняется через Kaspersky Security Center.

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

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление задачами**.

> Если в блоке отсутствуют какие-то задачи, это означает, что отображение локальных задач и управление ими запрещены политикой для всех защищенных виртуальных машин группы администрирования. Вы можете включить и выключить отображение локальных задач и управление ими в политике Легкого агента для Windows (подраздел **Дополнительные параметры** в разделе **Другие параметры**).

4. По правой клавише мыши на строке с названием задачи откройте контекстное меню действий с задачей.
5. Запустите или остановите задачу, выбрав нужный пункт меню.

   Если вы запустили задачу, статус выполнения задачи, отображающийся справа от названия задачи, изменится на `Выполняется`.

   Если вы остановили задачу, статус выполнения задачи изменится на `Остановлено`.

Вы можете настроить автоматическую приостановку выполнения задачи в указанное время.

Вы также можете запускать выборочную проверку любого файла, выбрав пункт **Проверить на вирусы** в контекстном меню Windows.

Просмотр информации о ходе и результатах выполнения задач

Просмотр информации о ходе и результатах выполнения задач в Консоли администрирования

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

- В окне **Результаты выполнения задачи**. Окно открывается с помощью пункта **Результаты** контекстного меню задачи.
- В списке событий, которые программа Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center. Списки событий вы можете просматривать на закладке **События** в рабочей области узла **Сервер администрирования <Имя сервера>**. Информация на закладке **События** представлена в виде выборок событий. Каждая выборка включает в себя только события определенного типа. В списке отображаются события из выборки, которая в настоящий момент указана в раскрывающемся списке **Выборки событий**. Чтобы отобразить список событий выборки, используйте кнопку **Запустить выборку**. Чтобы обновить список, используйте ссылку **Обновить**.

Просмотр информации о ходе и результатах выполнения задач в локальном интерфейсе Легкого агента для Windows

Процесс выполнения задачи отображается в поле напротив названия задачи в блоке **Управление задачами** на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120).

Информация о результатах выполнения задач и обо всех событиях, произошедших во время выполнения задач, записывается в отчеты Kaspersky Security (см. раздел "Работа с отчетами в локальном интерфейсе" на стр. 431).

О правах доступа к параметрам политик и задач в Kaspersky Security Center

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.

Для компонента Сервер защиты выделена одна функциональная область: **Базовая функциональность**. В эту функциональную область входят следующие параметры и функции:

- Параметры подключения SVM к Серверу интеграции.
- Параметры подключения Легких агентов к SVM.
- Параметры использования KSN.
- Дополнительные параметры работы SVM.
- Задача активации программы.
- Задача обновления баз программы и задача отката последнего обновления баз программы.

Для компонента Легкий агент для Windows выделены следующие функциональные области:

- **Компоненты защиты**. В эту функциональную область входят следующие параметры и функции:
  - Включение и выключение Файлового Антивируса для Windows.
  - Параметры работы Файлового Антивируса для Windows:
    - уровень безопасности файлов;
    - действие, которое программа выполняет при обнаружении зараженного файла;
    - область защиты Файлового Антивируса;
    - параметры проверки составных файлов, оптимизация и режим проверки;
    - автоматическая приостановка работы Файлового Антивируса;
    - использование эвристического анализа и технологии проверки iSwift.
  - Включение и выключение AMSI-защиты.
  - Параметры проверки составных файлов во время проверки объектов по AMSI-запросам.
  - Включение и выключение Почтового Антивируса.
  - Параметры работы Почтового Антивируса:
    - уровень безопасности почты;
    - действие, которое программа выполняет при обнаружении зараженного сообщения электронной почты;
    - область защиты Почтового Антивируса;
    - параметры проверки вложенных в сообщения составных файлов, фильтрация по типу вложений;
    - использование эвристического анализа и расширения Почтового Антивируса для программы Microsoft Office Outlook.

- Включение и выключение Веб-Антивируса.
- Параметры работы Веб-Антивируса:
  - уровень безопасности веб-трафика;
  - действие, которое программа выполняет при обнаружении вредоносного объекта веб-трафика;
  - включение и выключение проверки веб-адресов по базам фишинговых и вредоносных веб-адресов;
  - использование эвристического анализа и продолжительность кеширования Веб-Антивирусом веб-трафика;
  - список доверенных веб-адресов.
- Задача поиска вирусов для Легкого агента для Windows.

- **Базовая функциональность**. В эту функциональную область входят следующие параметры и функции:
  - Параметры подключения Легких агентов к SVM.
  - Параметры контроля сетевого трафика.
  - Список доменов, исключаемых из проверки защищенных соединений.
  - Параметры отчетов и резервного хранилища.
  - Параметры использования механизма самозащиты программы.
  - Параметры локального интерфейса Легкого агента для Windows.
  - Защита паролем доступа к параметрам программы в локальном интерфейсе.
  - Параметры управления задачами из локального интерфейса.
  - Параметры проверки съемных дисков при подключении.
  - Параметры автоматического запуска программы.
  - Параметры лечения активного заражения.
  - Задача изменения состава компонентов программы.
  - Параметры взаимодействия с Kaspersky Managed Detection and Response.
- **Контроль программ**. В эту функциональную область входят следующие параметры и функции:
  - Включение и выключение Контроля запуска программ.
  - Параметры работы Контроля запуска программ:
    - действие, которое выполняет Kaspersky Security при обнаружении попытки запуска программы, не разрешенной правилом контроля запуска программ;
    - настройка и использование категорий программ и правил контроля запуска программ;
    - контроль запуска исполняемых модулей и драйверов;
    - настройка шаблонов сообщений Контроля запуска программ.
  - Включение и выключение Контроля активности программ.
  - Параметры работы Контроля активности программ:

        - настройка и использование правил контроля программ;
        - защита ресурсов операционной системы.
    - Задача инвентаризации и получение информации о программах, которые установлены на защищенных виртуальных машинах.
- **Веб-Контроль**. В эту функциональную область входят следующие параметры и функции:
    - Включение и выключение Веб-Контроля.
    - Параметры работы Веб-Контроля:
        - настройка и использование правил доступа к веб-ресурсам;
        - настройка шаблонов сообщений Веб-Контроля.
- **Предотвращение вторжений**. В эту функциональную область входят следующие параметры и функции:
    - Проактивная защита виртуальной машины.
    - Защита папок общего доступа от внешнего шифрования.
    - Откат действий вредоносных программ.
- **Контроль целостности системы**. В эту функциональную область входят следующие параметры и функции:
    - Включение и выключение Контроля целостности системы.
    - Область действия контроля и область действия проверки целостности системы.
    - Задача обновления снимка состояния системы.
    - Задача проверки целостности системы.
    - Отчеты компонента Контроль целостности системы.
- **Доверенная зона.** В эту функциональную область входят следующие параметры и функции:
    - Список объектов и программ, исключаемых из проверки.
    - Включение и выключение использования исключений.
    - Список доверенных программ.

Для компонента Легкий агент для Linux выделены следующие функциональные области:

- **Компоненты защиты**. В эту функциональную область входят следующие параметры и функции:
    - Включение и выключение Файлового Антивируса для Linux.
    - Параметры работы Файлового Антивируса для Linux:
        - уровень безопасности файлов;
        - действие, которое программа выполняет при обнаружении зараженного файла;
        - область защиты Файлового Антивируса;
        - параметры проверки составных файлов и режим проверки;
        - использование эвристического анализа и технологии проверки iChecker.
    - Задача поиска вирусов для Легкого агента для Linux.
- **Базовая функциональность**. В эту функциональную область входят следующие параметры и

функции:

- Параметры подключения Легких агентов к SVM.
- Параметры резервного хранилища.

- **Доверенная зона.** В эту функциональную область входят следующие параметры и функции:
  - Список объектов и программ, исключаемых из проверки.
  - Включение и выключение использования исключений.

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

- Просмотр параметров политик.
- Создание политики.

> При создании политики пользователь может настроить только параметры, относящиеся к функциональным областям, в которых учетная запись пользователя обладает правами на изменение.

Для выполнения следующих действий с политиками и задачами учетная запись пользователя должна обладать правами в функциональных областях программы Kaspersky Security:

- Для изменения параметров ранее сохраненной политики требуются права на чтение и на изменение в функциональных областях, к которым относятся эти параметры.
- Для изменения состояния политики (активная/неактивная) и удаления политики требуются права на чтение и на изменение в функциональных областях, к которым относятся параметры политики, закрытые "замком". Если в политике есть параметры, закрытые "замком" (то есть, параметры, для которых установлен запрет на изменение параметра в дочерних политиках и локальном интерфейсе программы), и у пользователя нет прав на чтение и на изменение в функциональных областях, к которым относятся эти параметры, то удалить или изменить состояние политики невозможно. Если в политике нет параметров, для которых установлен запрет на изменение параметра в дочерних политиках и локальном интерфейсе программы, то удаление или изменение состояния политики доступны пользователю независимо от прав учетной записи в функциональных областях программы.
- Для создания, удаления и настройки параметров задач требуются права на чтение и на изменение в функциональной области, к которой относится задача.
- Для просмотра параметров задачи требуются права на чтение в функциональной области, к которой относится задача.
- Для запуска задачи требуются права на выполнение в функциональной области, к которой относится задача.

Настройка прав 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.

О Консоли Сервера интеграции

Консоль Сервера интеграции содержит следующие разделы:

Раздел Параметры Сервера интеграции

В этом разделе вы можете посмотреть информацию о Сервере интеграции (см. раздел "Просмотр параметров Сервера интеграции" на стр. 435).

Раздел Учетные записи Сервера интеграции

В этом разделе вы можете изменить пароли учетных записей (см. раздел "Изменение паролей учетных записей Сервера интеграции" на стр. 436), которые используются для подключения к Серверу интеграции.

Раздел Список подключенных SVM

В этом разделе вы можете посмотреть информацию об SVM, которые подключены к Серверу интеграции (см. раздел "Просмотр списка SVM, подключенных к Серверу интеграции" на стр. 105).

Раздел Управление SVM

Этот раздел открывается по умолчанию после запуска Консоли Сервера интеграции. В этом разделе вы можете запустить мастер управления SVM, который позволяет выполнить следующие действия:

- развернуть в виртуальной инфраструктуре SVM с компонентом Сервер защиты;
- изменить конфигурацию SVM;
- удалить SVM.

Раздел Параметры подключения к инфраструктуре

В этом разделе вы можете выполнить следующие действия:

- посмотреть статус подключения (см. раздел "Изменение и удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 437) Сервера интеграции к виртуальной инфраструктуре;
- изменить параметры подключения (см. раздел "Изменение параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 438) Сервера интеграции к виртуальной инфраструктуре;
- если программа Kaspersky Security установлена в инфраструктуре VMware, настроить использование VMware NSX Manager (см. раздел "Изменение параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 438) в работе программы;
- удалить гипервизор или сервер управления виртуальной инфраструктурой (см. раздел "Удаление

параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 440) из списка.

Раздел Список клиентов

Если вы используете программу в режиме multitenancy (см. раздел "Использование программы в режиме multitenancy" на стр. 446), в этом разделе вы можете посмотреть список всех клиентов (см. раздел "Получение информации о клиентах" на стр. 458), зарегистрированных в базе данных Сервера интеграции.

Раздел Параметры подключения к Kaspersky Security Center

Если вы используете программу в режиме multitenancy (см. раздел "Использование программы в режиме multitenancy" на стр. 446) и вы развернули структуру защиты клиентов средствами REST API Сервера интеграции, в этом разделе вы можете настроить параметры подключения (см. раздел "Настройка параметров подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 449), необходимые для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center.

Запуск и остановка программы

Запуск компонентов программы Kaspersky Security

Компонент Сервер защиты запускается автоматически при запуске операционной системы на SVM. Сервер защиты управляет рабочими процессами, в ходе которых выполняются защита виртуальных машин, задачи проверки, задачи обновления баз программы и отката обновлений.

> SVM, развернутая на гипервизоре VMware ESXi, автоматически запускается после включения гипервизора. Автоматическое включение SVM может не работать, если эта функция не активирована на уровне гипервизора или этот гипервизор находится в кластере VMware HA. См. подробнее в базе знаний VMware (https://kb.vmware.com/s/article/850).

Компонент Легкий агент по умолчанию запускается автоматически при запуске операционной системы на защищенной виртуальной машине.

Для Легкого агента для Windows вы можете включать и выключать автоматический запуск программы в политике для Легкого агента для Windows или в локальном интерфейсе (см. раздел "Включение и выключение автоматического запуска компонента Легкий агент для Windows" на стр. 156).

Компонент Сервер интеграции запускается автоматически при запуске операционной системы на компьютере, где установлен Сервер интеграции.

Включение защиты и запуск задач

Защита виртуальных машин включается автоматически при запуске компонентов Легкий агент и Сервер защиты.

> Если сведения о лицензии не переданы на защищенную виртуальную машину, Легкий агент работает в режиме ограниченной функциональности (см. раздел "Об активации программы" на стр. 78).

Задачи программы запускаются в соответствии со своим расписанием.

Остановка работы компонентов программы

Компоненты Сервер защиты и Легкий агент останавливаются автоматически при завершении работы операционной системы на SVM и защищенной виртуальной машине.

Средствами Kaspersky Security Center вы можете вручную завершать работу компонентов Сервер защиты и Легкий агент, запускать программу, а также приостанавливать и возобновлять защиту и контроль защищенных виртуальных машин (см. в документации Kaspersky Security Center).

Останавливать и запускать Легкий агент для Windows вручную (см. раздел "Запуск и остановка работы программы в локальном интерфейсе вручную" на стр. 157), а также приостанавливать и возобновлять защиту и контроль защищенных виртуальных машин (см. раздел "Приостановка и возобновление защиты и контроля виртуальной машины в локальном интерфейсе" на стр. 158) вы можете также через локальный интерфейс Легкого агента.

Останавливать и запускать Легкий агент для Linux вы можете стандартными средствами операционной системы Linux. Если вы остановите Легкий агент для Linux, все выполняющиеся задачи будут прерваны. После повторного запуска Легкого агента для Linux прерванные задачи автоматически не возобновляются.

Вы можете запускать задачи вручную (см. раздел "Запуск и остановка задачи" на стр. 482).

Компонент Сервер интеграции останавливается автоматически при завершении работы операционной системы на компьютере, где установлен Сервер интеграции.

В этом разделе

Включение и выключение автоматического запуска компонента Легкий агент для Windows

Вы можете включать и выключать автоматический запуск компонента Легкий агент для Windows в политике для Легкого агента для Windows и в локальном интерфейсе.

Под автоматическим запуском компонента Легкий агент подразумевается запуск программы на виртуальной машине, который выполняется без вашего участия после старта операционной системы. Этот вариант запуска программы установлен по умолчанию.

В первый раз компонент Легкий агент запускается автоматически после своей установки. В дальнейшем Легкий агент запускается автоматически после старта операционной системы.

► *Чтобы включить или выключить автоматический запуск Легкого агента в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Основные параметры защиты**.
6. Выполните одно из следующих действий:
   - Установите флажок **Запускать Kaspersky Security для виртуальных сред 5.2 Легкий агент при включении виртуальной машины**, если вы хотите включить автоматический запуск Легкого агента.
   - Снимите флажок **Запускать Kaspersky Security для виртуальных сред 5.2 Легкий агент при включении виртуальной машины**, если вы хотите выключить автоматический запуск Легкого агента.
7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить автоматический запуск Легкого агента в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. Выполните одно из следующих действий:
   - Установите флажок **Запускать Kaspersky Security для виртуальных сред 5.2 Легкий агент при включении виртуальной машины**, если вы хотите включить автоматический запуск программы.
   - Снимите флажок **Запускать Kaspersky Security для виртуальных сред 5.2 Легкий агент при включении виртуальной машины**, если вы хотите выключить автоматический запуск программы.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка работы программы в локальном интерфейсе вручную

Вы можете останавливать и запускать Легкий агент для Windows в локальном интерфейсе вручную.

Специалисты "Лаборатории Касперского" рекомендуют не завершать работу программы, поскольку в этом случае защита виртуальной машины и ваших персональных данных окажется под угрозой. Если требуется, вы можете приостановить защиту (см. раздел "Приостановка и возобновление защиты и контроля виртуальной машины в локальном интерфейсе" на стр. 158) виртуальной машины на необходимый срок, не завершая работу программы.

► *Чтобы остановить работу программы вручную, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Выход**.

Запускать программу вручную требуется в том случае, если вы выключили автоматический запуск программы.

► *Чтобы запустить программу вручную,*

в меню **Пуск** выберите пункт **Программы** → **Kaspersky Security для виртуальных сред 5.2 Легкий агент**.

Приостановка и возобновление защиты и контроля виртуальной машины в локальном интерфейсе

Вы можете приостанавливать и возобновлять защиту и контроль защищенных виртуальных машин в локальном интерфейсе Легкого агента для Windows.

Приостановка защиты и контроля виртуальной машины означает выключение на некоторое время всех компонентов защиты и компонентов контроля программы.

Индикатором работы программы служит значок программы в области уведомлений панели задач:

- Значок свидетельствует о приостановке защиты и контроля виртуальной машины.
- Значок свидетельствует о возобновлении защиты и контроля виртуальной машины.

Приостановка и возобновление защиты и контроля виртуальной машины не оказывает влияния на выполнение задач.

Если в момент приостановки и возобновления защиты и контроля виртуальной машины были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

► *Чтобы приостановить или возобновить защиту и контроль виртуальной машины, выполните следующие действия:*

1. Если вы хотите приостановить защиту и контроль виртуальной машины, выполните следующие действия:
   a. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
   b. В контекстном меню выберите пункт **Приостановка защиты и контроля**.

      Откроется окно **Приостановка защиты**.
   c. Выберите один из следующих вариантов:
      - **Приостановить на указанное время** – защита и контроль виртуальной машины включатся через интервал времени, указанный в раскрывающемся списке ниже. Вы можете выбрать нужный интервал в раскрывающемся списке.
      - **Приостановить до перезагрузки** – защита и контроль виртуальной машины включатся после перезапуска программы или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск программы.
      - **Приостановить** – защита и контроль виртуальной машины включатся тогда, когда вы решите возобновить ее.
2. Если вы хотите возобновить защиту и контроль виртуальной машины, то вы можете это сделать в любой момент, независимо от того, какой вариант приостановки защиты и контроля виртуальной машины вы выбрали ранее. Чтобы возобновить защиту и контроль виртуальной машины, выполните следующие действия:
   a. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
   b. В контекстном меню выберите пункт **Возобновление защиты и контроля**.

Состояние защиты виртуальной машины

Вы можете получать информацию о состоянии защиты виртуальных машин следующими способами:

- В Kaspersky Security Center с помощью статусов клиентских устройств (см. раздел "Статус клиентского устройства в Kaspersky Security Center" на стр. 159).
- В Kaspersky Security Center с помощью статусов функциональных компонентов Легкого агента на виртуальных машинах (см. раздел "Статусы функциональных компонентов Легкого агента на виртуальных машинах" на стр. 160).
- В локальном интерфейсе Легкого агента для Windows (см. раздел "Состояние защиты виртуальной машины в локальном интерфейсе Легкого агента для Windows" на стр. 161) (для виртуальных машин с установленным компонентом Легкий агент для Windows).
- С помощью команд из командной строки Легкого агента для Linux (см. раздел "Управление Легким агентом для Linux из командной строки" на стр. 479) (для виртуальных машин с установленным компонентом Легкий агент для Linux).
- С помощью тегов безопасности (Security Tags) (см. раздел "О тегах безопасности (Security Tags)" на стр. 163), которые программа Kaspersky Security может назначать защищенной виртуальной машине в инфраструктуре на платформе VMware ESXi или KVM.

На виртуальных машинах с операционной системой Windows 10 информация о работе программы Kaspersky Security и о состоянии защиты виртуальной машины также отображается в Центре безопасности Защитника Windows (Windows Defender Security Center) и в Центре безопасности и обслуживания (Security and Maintenance). При этом информация о работе программы и состоянии защиты виртуальной машины в Kaspersky Security Center и в локальном интерфейсе Легкого агента для Windows является более актуальной.

В этом разделе

Статус клиентского устройства в Kaspersky Security Center

Защищенная виртуальная машина (виртуальная машина, на которой установлен компонент программы Легкий агент) и SVM в Kaspersky Security Center являются клиентскими устройствами. Информация о состоянии клиентского устройства в Kaspersky Security Center отображается с помощью статуса клиентского устройства (*ОК*, *Критический*, *Предупреждение*).

Статус клиентского устройства изменяется 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.

  Получение статуса устройства от управляемой программы должно быть включено в Kaspersky Security Center в списках условий назначения статусов *Критический* и *Предупреждение*. Условия назначения статусов устройства настраиваются в окне свойств группы администрирования.

  Статус SVM изменяется, если нет подключения к Серверу интеграции.

  Статус защищенной виртуальной машины изменяется в следующих случаях:

  - нет подключения к Серверу интеграции;
  - нет подключения к SVM;
  - обнаружено отключение или подключение устройства;
  - обнаружено изменение в файлах или реестре на виртуальной машине.

Подробнее о статусах клиентского устройства см. в документации Kaspersky Security Center.

Статусы функциональных компонентов Легкого агента на виртуальных машинах

В Консоли администрирования Kaspersky Security Center вы можете получать следующую информацию о функциональных компонентах Легкого агента:

- В свойствах программы Kaspersky Security, установленной на виртуальной машине, отображается список функциональных компонентов Легкого агента для Windows или Легкого агента для Linux, в зависимости от виртуальной машины, которую вы выбрали. Для каждого компонента отображается статус, для установленных компонентов отображается номер версии Легкого агента, в составе которого установлен компонент.
- В отчете Kaspersky Security Center о статусе компонентов программы отображается информация о функциональных компонентах Легкого агента, установленных и не установленных на виртуальных машинах. Для каждого из установленных компонентов в отчете отображается количество виртуальных машин, на которых установлен этот компонент, и количество групп администрирования, к которым относятся эти виртуальные машины.

  Отчет о статусе компонентов программы доступен в списке шаблонов отчета в Консоли администрирования Kaspersky Security Center (на закладке **Отчеты** в рабочей области узла **Сервер администрирования**).
- В Консоли администрирования Kaspersky Security Center вы можете строить выборки виртуальных машин, задавая в качестве условия выборки статус компонентов и / или номер версии Легкого агента, в составе которого установлен компонент. Подробнее о настройке выборки устройств см. в

документации Kaspersky Security Center.

► *Чтобы посмотреть информацию о функциональных компонентах Легкого агента в свойствах программы Kaspersky Security на виртуальной машине с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, в которую входит нужная виртуальная машина.
3. В рабочей области выберите закладку **Устройства**.
4. В списке выберите виртуальную машину, для которой вы хотите посмотреть информацию о функциональных компонентах Легкого агента.
5. Откройте окно свойств виртуальной машины двойным щелчком мыши.

   Откроется окно **Свойства: <Имя виртуальной машины>**.
6. В списке слева выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на этой виртуальной машине.
7. Выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент** и откройте окно параметров программы двойным щелчком мыши.

   Откроется окно **Параметры программы Kaspersky Security для виртуальных сред 5.2 Легкий агент**.
8. В списке слева выберите раздел **Компоненты**.

В правой части окна отобразится список всех функциональных компонентов Легкого агента для Windows или компонент Файловый Антивирус Легкого агента для Linux, в зависимости от виртуальной машины, которую вы выбрали.

Состояние защиты виртуальной машины в локальном интерфейсе Легкого агента для Windows

Сведения о состоянии защиты каждой виртуальной машины с установленным компонентом Легкий агент для Windows вы можете посмотреть в локальном интерфейсе Легкого агента для Windows.

Программа Kaspersky Security использует следующие способы индикации о состоянии защиты виртуальной машины в главном окне программы (см. раздел «Главное окно программы» на стр. 120):

- Индикация с помощью значков статуса работы компонентов и состояний работы компонентов программы. Предусмотрены следующие варианты индикации:
  - В строке включенного компонента отображается зеленый значок статуса работы компонента . Справа отображается статистика о количестве проверенных этим компонентом объектов, найденных угроз и действиях компонента по устранению угроз.
  - В строке выключенного компонента отображается желтый значок статуса работы компонента . Статистика о работе компонента в этом случае не отображается.
  - Если все компоненты контроля или компоненты защиты выключены, в заголовке блока **Контроль рабочего места** или **Управление защитой** отображается состояние `выключен(о)`.

- Если один или несколько компонентов контроля или компонентов защиты выключены, в заголовке блока **Контроль рабочего места** или **Управление защитой** отображается состояние `частично включен(о) (работающих компонентов: <количество включенных компонентов блока> из <общее количество компонентов в блоке>)`.

- Индикация наличия угроз, обнаруженных компонентами программы (например, `разрешено запусков программ`, `запрещено запусков программ`, `проверено объектов`, `найдено угроз`):
  - Если блок **Контроль рабочего места** или **Управление защитой** свернут, индикация наличия угроз отображается в строке с общей статистикой о работе компонентов под заголовком блока.
  - Если блок **Контроль рабочего места** или **Управление защитой** развернут, индикация наличия угроз отображается в строке со статистикой о работе каждого компонента.

  В зависимости от угрозы информация об угрозе и ее уровне важности фиксируется в виде события и отображается на одной из закладок окна **Отчеты и Хранилища**:
  - **Отчеты** (см. раздел "**Работа с отчетами в локальном интерфейсе**" на стр. 431).
  - **Резервное хранилище**.
  - **Необработанные объекты**.

- Индикация с помощью сообщений о событиях в работе компонентов защиты, связанных с состоянием защищенной виртуальной машины (например, `Требуется перезагрузка виртуальной машины`, `Нет подключения к SVM` или `Ожидается обновление баз`). Сообщения отображаются следующим образом:
  - Если блок **Управление защитой** свернут, то сообщение отображается вместо строки со статистикой под заголовком блока.
  - Если блок **Управление защитой** развернут, то сообщение отображается вместо строки со статистикой компонента Файловый Антивирус.

  > Сообщение `Ожидается обновление баз` отображается после локальной установки программы или после установки через Kaspersky Security Center, если в мастере создания инсталляционного пакета снят флажок **Скопировать обновления из хранилища в инсталляционный пакет**. Базы будут обновлены после подключения Легкого агента для Windows к SVM. Для подключения Легкого агента к SVM требуется указать способ обнаружения SVM.

- Индикация с помощью сообщений о событиях, связанных с выполнением задач или отклонениями от оптимальной работы программы (например, `Базы сильно устарели` или `Ожидается обновление баз`). Сообщения отображаются следующим образом:
  - Если блок **Управление задачами** свернут, то сообщения отображаются в информационной области под заголовком блока.
  - Если блок **Управление задачами** развернут, то сообщения отображаются вместо строки со статистикой и расписанием задачи.

- Индикация с помощью сообщений о проблемах с лицензией.

  Информация о проблемах с лицензией (например, срок действия лицензии истек), отображается в виде сообщений, выделенных красным цветом, в окне **Лицензирование**, которое открывается по ссылке **Лицензия**, расположенной внизу главного окна программы.

Кроме того, программа может сообщать о событиях в работе программы с помощью уведомлений. Также информация о работе каждого компонента программы, о выполнении задач и о работе программы в целом фиксируется в отчетах (см. раздел "Работа с отчетами в локальном интерфейсе" на стр. 431).

На виртуальных машинах с операционной системой Windows 10 в Центре безопасности Защитника Windows (Windows Defender Security Center) и в Центре безопасности и обслуживания (Security and Maintenance) может отображаться неактуальная информация о работе программы Kaspersky Security и о состоянии защиты виртуальной машины. Вы можете получить актуальную информацию о работе программы и состоянии защиты виртуальной машины в Kaspersky Security Center или в локальном интерфейсе Легкого агента для Windows.

О тегах безопасности (Security Tags)

Если программа Kaspersky Security работает в виртуальной инфраструктуре на платформе VMware vSphere или KVM и использует в своей работе VMware NSX Manager, программа Kaspersky Security может назначать защищенной 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, во входящем трафике которой обнаружена активность, характерная для сетевых атак.

Kaspersky Security может назначать теги безопасности, только если вы включили использование VMware NSX Manager и настроили параметры подключения Сервера интеграции к VMware NSX Manager (см. раздел "Изменение параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 438).

Вы можете посматривать теги безопасности, назначенные виртуальной машине, в свойствах виртуальной машины:

- в консоли VMware vSphere Client в разделе **Hosts and Clusters** на закладке **Summary**;
- в веб-консоли VMware NSX Manager в разделе **Inventory** → **Virtual Machines**.

Тег безопасности *ANTI_VIRUS.VirusFound.threat=high*, назначенный виртуальной машине программой Kaspersky Security, снимается автоматически, если в результате выполнения задачи **Полная проверка** на виртуальной машине не обнаружены вирусы или другие вредоносные программы. Если тег безопасности *ANTI_VIRUS.VirusFound.threat=high* назначен виртуальной машине вручную средствами виртуальной инфраструктуры, его можно снять только вручную.

Тег безопасности *IDS_IPS.threat=high*, назначенный виртуальной машине программой Kaspersky Security или вручную средствами виртуальной инфраструктуры, можно снять только вручную.

После снятия тега вручную требуется перезапустить Легкий агент.

Подробнее о снятии и назначении тегов безопасности вручную см. в Базе знаний (https://support.kaspersky.ru/14752).

Настройка параметров подключения к Серверу интеграции

Для работы SVM требуется подключение SVM к Серверу интеграции.

В этом разделе описана настройка параметров подключения SVM к Серверу интеграции в свойствах политики с помощью Консоли администрирования (см. раздел "Настройка параметров подключения SVM к Серверу интеграции" на стр. 164). Вы также можете настраивать параметры подключения SVM к Серверу интеграции в Консоли администрирования во время создания политики для Сервера защиты (см. раздел "Создание политики для Сервера защиты" на стр. 124), в том числе во время создания политики по умолчанию для Сервера защиты (см. раздел "Автоматическое создание задач и политики по умолчанию для Сервера защиты" на стр. 62)).

Если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между SVM и Легкими агентами, вам также требуется настроить подключение Легких агентов к Серверу интеграции.

В этом разделе описана настройка параметров подключения Легких агентов к Серверу интеграции в свойствах политики с помощью Консоли администрирования, а также в локальном интерфейсе Легкого агента для Windows (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 165). Вы также можете настраивать параметры подключения Легких агентов к Серверу интеграции в Консоли администрирования во время создания политики для Легкого агента для Windows (см. раздел "Создание политики для Легкого агента для Windows" на стр. 130) и политики для Легкого агента для Linux (см. раздел "Создание политики для Легкого агента для Linux" на стр. 137).

В этом разделе

Настройка параметров подключения SVM к Серверу интеграции

► *Чтобы настроить параметры подключения SVM к Серверу интеграции в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите настроить параметры подключения к Серверу интеграции.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В списке слева выберите раздел **Параметры подключения SVM к Серверу интеграции**.

6. Укажите адрес и порт для подключения:
   a. По умолчанию в поле **Адрес** указывается доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Если этот компьютер не входит в домен или Сервер интеграции установлен на другом компьютере и в поле указан неверный адрес, укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

      Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

   b. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.
7. Нажмите на кнопку **Применить** в окне свойств политики.
8. Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, откроется окно **Подключение к Серверу интеграции**. Укажите пароль администратора Сервера интеграции (пароль учетной записи admin). После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи для подключения SVM к Серверу интеграции.

   Нажмите на кнопку **OK** в окне **Подключение к Серверу интеграции**.

   Mmc-плагин Kaspersky Security проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью кнопки в окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

   Выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, в окне свойств политики отображается ошибка. Проверьте введенные параметры подключения. Информация об ошибках подключения к Серверу интеграции может записываться в файл трассировки Сервера интеграции (см. раздел "О файлах трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 510) (если вы включили запись информации в файл трассировки).

Настройка параметров подключения Легких агентов к Серверу интеграции

► *Чтобы настроить подключение Легких агентов к Серверу интеграции в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите изменить параметры подключения к Серверу интеграции.

3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows, если вы хотите изменить параметры подключения для Легкого агента для Windows, или политику для Легкого агента для Linux, если вы хотите изменить параметры подключения для Легкого агента для Linux.
5. Откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
6. В списке слева выберите раздел **Параметры подключения к Серверу интеграции**.
7. Укажите адрес и порт для подключения:
   a. По умолчанию в поле **Адрес** указывается доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Если этот компьютер не входит в домен или Сервер интеграции установлен на другом компьютере и в поле указан неверный адрес, укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

   > Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

   b. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.
8. Нажмите на кнопку **Применить** в окне свойств политики.
9. Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, откроется окно **Подключение к Серверу интеграции**. Укажите пароль администратора Сервера интеграции (пароль учетной записи admin). После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи для подключения Легких агентов к Серверу интеграции.

   Нажмите на кнопку **OK** в окне **Подключение к Серверу интеграции**.

   Mmc-плагин Kaspersky Security проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью кнопки в окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

   Выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, в окне свойств политики отображается ошибка. Проверьте введенные параметры подключения. Информация об ошибках подключения к Серверу интеграции может записываться в файл трассировки Сервера интеграции (см. раздел "О файлах трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 510) (если вы включили запись информации в файл трассировки).

► *Чтобы настроить подключение Легкого агента для Windows к Серверу интеграции в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Подключение к SVM** выберите раздел **Параметры подключения к**

Серверу интеграции.

> Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Укажите адрес и порт для подключения:
   a. По умолчанию в поле **Адрес** указывается доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Если этот компьютер не входит в домен или Сервер интеграции установлен на другом компьютере и в поле указан неверный адрес, укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции.

   > Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

   b. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.
4. Нажмите на кнопку **Сохранить**.
5. Если защищенная виртуальная машина не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов на компьютере, на котором установлен Сервер интеграции, откроется окно **Подключение к Серверу интеграции**. Укажите пароль администратора Сервера интеграции (пароль учетной записи admin).

   Нажмите на кнопку **OK** в окне **Подключение к Серверу интеграции**.

   Выполняется проверка SSL-сертификата, полученного от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью кнопки в окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на защищенной виртуальной машине.

   Выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, открывается окно с сообщением об ошибке. Проверьте введенные параметры подключения. Информация об ошибках подключения к Серверу интеграции может записываться в файл трассировки Сервера интеграции (см. раздел "О файлах трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 510) (если вы включили запись информации в файл трассировки).

Настройка параметров подключения Легких агентов к SVM

Для настройки подключения Легкого агента к SVM предусмотрены следующие параметры программы:

- Способ обнаружения SVM. Вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM.
- Теги для подключения. Если вы используете теги для подключения, Легкий агент может подключаться только к тем SVM, для которых разрешено подключение Легких агентов с указанным тегом.
- Параметры защиты соединения между Легким агентом и SVM. Вы можете защищать соединение между Легкими агентами и SVM с помощью шифрования.
- Алгоритм выбора SVM для подключения. Вы можете указать, какой алгоритм должны использовать Легкие агенты при выборе SVM для подключения.

Использование тегов для подключения и применение расширенного алгоритма выбора SVM доступны, только если вы используете программу по расширенной лицензии.

В этом разделе

Настройка параметров обнаружения SVM

Вы можете настраивать параметры обнаружения SVM Легкими агентами в свойствах политики для Легкого агента с помощью Консоли администрирования, в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить параметры обнаружения SVM Легкими агентами в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите настроить параметры обнаружения SVM.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows, если вы хотите настроить параметры для Легкого агента для Windows, или политику для Легкого агента для Linux, если вы

хотите настроить параметры для Легкого агента для Linux.

5. Откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
6. В списке слева выберите раздел **Параметры обнаружения SVM**.
7. Выберите способ, который Легкие агенты используют для обнаружения SVM:
   - **Использовать Сервер интеграции**

     Если выбран этот вариант, компонент Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

     Если вы хотите использовать Сервер интеграции, вам нужно настроить параметры подключения Легких агентов к Серверу интеграции (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 165).

   - **Использовать список адресов SVM, заданный вручную**

     Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

     Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и применяется расширенный алгоритм выбора SVM, в разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкие агенты не смогут подключиться к SVM.

8. Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную**, сформируйте список SVM. Для этого выполните следующие действия:
   a. Нажмите на кнопку **Добавить**, расположенную над списком адресов SVM.

      Откроется окно **Адреса SVM**.

   b. Введите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM, к которой могут подключаться Легкие агенты, находящиеся под управлением политики. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

      В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе программы.

   c. Нажмите на кнопку **OK** в окне **Адреса SVM**.

      Выполняется проверка введенных адресов и полных доменных имен SVM. Если некоторые адреса или имена не распознаны, сообщение об этом и количество нераспознанных адресов или имен отображается в отдельном окне. Распознанные адреса и полные доменные имена отображаются в списке адресов SVM.

   d. Если вы хотите удалить IP-адрес или полное доменное имя SVM из списка, выберите его в списке и нажмите на кнопку **Удалить**, расположенную над списком.

9. Нажмите на кнопку **Применить**.

► *Чтобы настроить в локальном интерфейсе параметры обнаружения SVM Легким агентом, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Подключение к SVM** выберите раздел **Параметры обнаружения SVM**.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 7–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка использования тегов для подключения

Эта функциональность доступна, только если вы используете программу по расширенной лицензии.

Вы можете регулировать подключение Легких агентов к SVM с помощью тегов для подключения. Для этого вам требуется выполнить следующие действия:

1. Назначить теги для подключения Легким агентам.
2. Настроить использование тегов для подключения на SVM и указать теги для подключения, с которыми разрешено подключаться к этой SVM. Если Легкому агенту назначен тег, не указанный в параметрах SVM, Легкий агент не сможет подключиться к SVM.

В этом разделе

Назначение Легким агентам тегов для подключения

Эта функциональность доступна, только если вы используете программу по расширенной лицензии.

Вы можете назначать теги для подключения Легким агентам в свойствах политики для Легкого агента с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы назначить тег для подключения Легким агентам в Консоли администрирования,*

выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите настроить использование тегов для подключения.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows, если вы хотите настроить параметры для Легкого агента для Windows, или политику для Легкого агента для Linux, если вы хотите настроить параметры для Легкого агента для Linux.
5. Откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
6. В списке слева выберите раздел **Тег для подключения**.
7. Установите флажок **Использовать теги для подключения Легких агентов** и введите тег для подключения в поле **Тег**.

   В качестве тега для подключения вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`.

   > Легкие агенты, которым назначен тег, могут подключаться только к SVM, для которых разрешено подключение Легких агентов с этим тегом (см. раздел "Настройка использования тегов для подключения на SVM" на стр. 171).

8. Нажмите на кнопку **Применить**.

► *Чтобы назначить тег для подключения Легкому агенту для Windows в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Подключение к SVM** выберите раздел **Тег для подключения**.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункт 7 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка использования тегов для подключения на SVM

> Эта функциональность доступна, только если вы используете программу по расширенной лицензии.

► *Чтобы настроить в Консоли администрирования использование тегов для подключения на SVM, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите настроить параметры использования тегов для подключения.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В списке слева выберите раздел **Теги для подключения**.
6. Установите флажок **Разрешить подключение Легких агентов с указанными тегами** и укажите в поле ниже один или несколько тегов, назначенных Легким агентам, через точку с запятой.

   К SVM, находящимся под управлением этой политики, будут подключаться только Легкие агенты, которым назначены указанные теги.
7. Нажмите на кнопку **Применить**.

Защита соединения между Легким агентом и SVM

Вы можете настроить защиту соединения между Легкими агентами и SVM с помощью шифрования. Для этого вам требуется выполнить следующие действия:

- Включить и настроить защиту соединения на SVM.
- Включить защиту соединения на Легком агенте.

Легкий агент, для которого включена защита соединения, может подключаться только к тем SVM, на которых соединение защищено. По умолчанию защита соединения на Легких агентах и SVM выключена.

Защита соединения с помощью шифрования может снижать производительность работы программы Kaspersky Security.

В этом разделе

Включение и выключение защиты соединения на SVM

► *Чтобы включить или выключить защиту соединения на SVM с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите настроить параметры защиты соединения.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В списке слева выберите раздел **Защита соединения**.
6. Выполните одно из следующих действий:
   - Если вы хотите включить защиту соединения между Легкими агентами и SVM, установите флажок **Шифровать канал передачи данных между Легким агентом и SVM**.

     К SVM, находящимся под управлением этой политики, будут подключаться только Легкие агенты, для которых настроено защищенное соединение (см. раздел "Включение и выключение защиты соединения на Легком агенте" на стр. 173).
   - Если вы хотите выключить защиту соединения между Легкими агентами и SVM, снимите флажок **Шифровать канал передачи данных между Легким агентом и SVM**.
7. Если вы включили защиту соединения, вы можете разрешить подключение Легким агентам, для которых не удалось установить защищенное соединение или для которых не включена защита соединения. Для этого установите флажок **Разрешить незащищенное соединение, если не удалось установить защищенное соединение**.
8. Нажмите на кнопку **Применить**.

Включение и выключение защиты соединения на Легком агенте

Для защиты соединения требуется настроить подключение Легких агентов к Серверу интеграции.

Вы можете включать и выключать защиту соединения на Легких агентах в свойствах политики для Легкого агента с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы включить или выключить защиту соединения на Легких агентах с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите настроить защиту соединения между Легким агентом и SVM.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows, если вы хотите настроить параметры для Легкого агента для Windows, или политику для Легкого агента для Linux, если вы

хотите настроить параметры для Легкого агента для Linux.

5. Откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
6. В списке слева выберите раздел **Защита соединения**.
7. Выполните одно из следующих действий:
   - Если вы хотите включить защиту соединения между Легкими агентами и SVM, установите флажок **Шифровать канал передачи данных между Легким агентом и SVM**. Легкий агент, для которого включена защита соединения, может подключаться только к тем SVM, на которых соединение защищено (см. раздел "Включение и выключение защиты соединения на SVM" на стр. 173). По умолчанию защита соединения на Легких агентах и SVM выключена.
   - Если вы хотите выключить защиту соединения между Легкими агентами и SVM, снимите флажок **Шифровать канал передачи данных между Легким агентом и SVM**. Легкий агент, для которого выключена защита соединения, может подключаться к SVM, на которых соединение не защищается или разрешено незащищенное соединение (см. раздел "Включение и выключение защиты соединения на SVM" на стр. 173).
8. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить защиту соединения на Легком агенте для Windows в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Подключение к SVM** выберите раздел **Защита соединения**.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункт 7 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка алгоритма выбора SVM

Легкие агенты могут применять расширенный алгоритм выбора SVM, только если вы используете программу по расширенной лицензии.

Вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты, в свойствах политики для Легкого агента с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы указать с помощью Консоли администрирования, какой алгоритм выбора SVM должны использовать Легкие агенты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите настроить защиту

соединения между Легким агентом и SVM.

3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows, если вы хотите настроить параметры для Легкого агента для Windows, или политику для Легкого агента для Linux, если вы хотите настроить параметры для Легкого агента для Linux.

   Откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В списке слева выберите раздел **Алгоритм выбора SVM**.
6. Выберите один из следующих вариантов:
   - **Использовать стандартный алгоритм выбора SVM**

     Если выбран этот вариант и вы используете программу по стандартной лицензии, после установки и запуска на виртуальной машине Легкий агент пытается подключиться к SVM, развернутой на том же гипервизоре, на котором работает Легкий агент. Если на том гипервизоре, на котором работает Легкий агент, нет доступных для подключения SVM, Легкий агент выбирает из числа развернутых на других гипервизорах ту SVM, к которой подключено наименьшее количество Легких агентов.

     Если выбран этот вариант и вы используете программу по расширенной лицензии, после установки и запуска на виртуальной машине Легкий агент выбирает ту SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре.

     Этот вариант выбран по умолчанию.
   - **Использовать расширенный алгоритм выбора SVM**

     Если выбран этот вариант, вы можете указать с помощью ползунка **Расположение SVM**, каким образом Легкие агенты должны учитывать расположение SVM при выборе SVM для подключения. Например, Легкий агент может подключаться к SVM, развернутой на том же кластере гипервизоров или в том же Datacenter, что и Легкий агент. Также Легкий агент может не учитывать при выборе SVM ее расположение. По умолчанию Легкий агент подключается к SVM, развернутой на том же гипервизоре, на котором работает Легкий агент.

     Если в качестве способа обнаружения SVM Легкими агентами вы выбрали заданный вручную список адресов SVM, то подключение Легких агентов к SVM возможно, только если расположение SVM не учитывается. Вам нужно установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**.

     При выборе SVM Легкие агенты учитывают количество Легких агентов, подключенных к этой SVM, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.
7. Если вы выбрали вариант **Использовать расширенный алгоритм выбора SVM** и в качестве способа обнаружения SVM Легкими агентами используется Сервер интеграции, с помощью ползунка **Расположение SVM** укажите, каким образом Легкий агент должен учитывать расположение SVM в виртуальной инфраструктуре при выборе SVM для подключения. Вы можете установить ползунок в одну из следующих позиций:
   - **Гипервизор**. Легкий агент выбирает для подключения SVM, развернутую на том же гипервизоре, на котором работает Легкий агент. Если на том гипервизоре, на котором работает Легкий агент, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
   - **Кластер**. Легкий агент выбирает для подключения SVM, развернутую в том же кластере, в котором работает Легкий агент. Если в том же кластере, в котором работает Легкий агент, нет

доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Datacenter**. Легкий агент выбирает для подключения SVM, развернутую в том же Datacenter, в котором работает Легкий агент. Если в том же Datacenter, в котором работает Легкий агент, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
- **Не учитывать расположение SVM**. Легкий агент не учитывает при выборе SVM ее расположение.

По умолчанию ползунок установлен в позицию **Гипервизор**.

Если в качестве способа обнаружения SVM Легкими агентами вы выбрали заданный вручную список адресов SVM, требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкие агенты не смогут подключиться к SVM.

8. Нажмите на кнопку **Применить**.

► *Чтобы указать в локальном интерфейсе, какой алгоритм выбора SVM должен использовать Легкий агент, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Подключение к SVM** выберите раздел **Алгоритм выбора SVM**.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–7 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка общих параметров антивирусной защиты

Вы можете настроить следующие общие параметры защиты для работы различных компонентов программы Kaspersky Security:

- Список объектов, которые должна обнаруживать программа Kaspersky Security (см. раздел "Выбор типов обнаруживаемых объектов" на стр. 177).
- Список исключений из защиты Kaspersky Security (см. раздел "Настройка доверенной зоны" на стр. 179).
- Использование технологии лечения активного заражения для виртуальных машин с операционными системами Windows для серверов (см. раздел "Настройка лечения активного заражения через Kaspersky Security Center" на стр. 195).

В этом разделе

Выбор типов обнаруживаемых объектов

Программа Kaspersky Security позволяет гибко настраивать защиту виртуальной машины и выбирать типы объектов, которые программа обнаруживает в ходе работы. Программа всегда проверяет операционную систему на наличие вирусов, червей и троянских программ. Вы не можете выключить проверку этих типов объектов, так как такие объекты могут нанести значительный вред защищенной виртуальной машине. Чтобы обеспечить большую безопасность виртуальной машины, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных программ, которые могут быть использованы злоумышленником для нанесения вреда защищенной виртуальной машине или вашим данным.

► *Чтобы выбрать типы обнаруживаемых объектов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows, если вы хотите настроить параметры для Легкого агента для Windows, или политику для Легкого агента для Linux, если вы хотите настроить параметры для Легкого агента для Linux.
5. Откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

6. В окне свойств политики в списке слева выберите раздел **Основные параметры защиты**.
7. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка**.

   Откроется окно **Объекты для обнаружения**.
8. Установите флажки для типов объектов, которые должна обнаруживать программа Kaspersky Security.

   Обратите внимание, что обнаруженные объекты могут быть удалены программой.
9. Нажмите на кнопку **OK** в окне **Объекты для обнаружения**.

   Окно **Объекты для обнаружения** закроется. В блоке **Объекты для обнаружения** под надписью **Включено обнаружение объектов следующих типов** отобразятся выбранные вами типы объектов.
10. Нажмите на кнопку **Применить**.

► *Чтобы выбрать типы обнаруживаемых объектов в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 7–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка доверенной зоны

Доверенная зона – это сформированный вами список объектов и программ, которые программа Kaspersky Security не контролирует в процессе работы. Иначе говоря, это набор исключений из защиты и проверки.

Доверенную зону вы формируете в зависимости от особенностей объектов, с которыми требуется работать, а также от программ, установленных в гостевой операционной системе защищенной виртуальной машины. Включение объектов и программ в доверенную зону может потребоваться, например, если программа Kaspersky Security блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа безвредны.

Исключения из защиты и проверки

Исключение – это совокупность условий, описывающих объект или программу. Если объект удовлетворяет этим условиям, программа Kaspersky Security не проверяет этот объект на вирусы и другие вредоносные программы.

Некоторые легальные программы могут быть использованы злоумышленниками для нанесения вреда вашей виртуальной машине или вашим данным. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы в качестве вспомогательного компонента вредоносной программы. К таким программам относятся, например, программы удаленного администрирования, IRC-клиенты, FTP-серверы, различные утилиты для остановки процессов или сокрытия их работы, клавиатурные перехватчики, программы вскрытия паролей, программы автоматического дозвона. Это программное обеспечение не классифицируется как вирусы. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского" по ссылке https://securelist.ru/threats/riskware/.

В результате работы программы Kaspersky Security такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ вы можете настроить исключения из защиты и проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе программу Remote Administrator. Это система удаленного доступа, позволяющая работать на удаленном компьютере. Чтобы исключить блокировку этой программы, нужно создать исключение (см. раздел "Создание исключения" на стр. 182), где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Вы можете исключать из проверки объекты следующих типов:

- файлы определенного формата;
- файлы по маске;
- папки;
- программы;
- процессы программ;
- объекты по классификации Вирусной энциклопедии "Лаборатории Касперского".

Помимо добавленных вами исключений, из защиты и проверки Легкого агента для Linux по умолчанию исключены объекты файловой системы /dev, /sys и /proc.

Исключения могут использоваться в ходе работы следующих компонентов и задач программы:

- Файловый Антивирус.
- Почтовый Антивирус.
- Веб-Антивирус.
- AMSI-защита.
- Мониторинг системы.
- Контроль активности программ.
- Задачи проверки.

Кроме того, вы можете создать категорию исключений, содержащую исключения для Легкого агента для Windows, при использовании которой программа Kaspersky Security не проверяет входящие в категорию файлы или папки и/или объекты с указанным именем

Список доверенных программ

Список доверенных программ – это список программ, для которых программа Kaspersky Security не контролирует файловую и сетевую активность (в том числе и подозрительную), а также обращения этих программ к системному реестру. По умолчанию программа Kaspersky Security проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Программа Kaspersky Security исключает из проверки программы, добавленные в список доверенных программ (см. раздел "Добавление программы в список доверенных программ" на стр. 186).

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вы можете добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые программа Kaspersky Security классифицирует как опасные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости программы Kaspersky Security с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера программой Kaspersky Security и другой антивирусной программой), а также увеличить производительность виртуальной машины, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других вредоносных программ. Чтобы полностью исключить программу из проверки и защиты, требуется создать исключение для этой программы.

Если на вашей виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, программа Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, добавив ее в исключения.

kaspersky

В этом разделе

Настройка доверенной зоны Легкого агента для Windows

Вы можете выполнить следующие действия для настройки доверенной зоны Легкого агента для Windows:

- Создать исключение или категорию исключений (см. раздел "Создание исключения" на стр. 182), содержащую исключения для Легкого агента для Windows, при использовании которых программа Kaspersky Security не проверяет входящие в категорию файлы или папки и / или объекты с указанным именем.
- Изменить параметры исключения, используя кнопку **Изменить**.
- Приостановить использование исключения или категории исключений (см. раздел "Включение и выключение использования исключения или категории исключений" на стр. 184).
- Удалить исключение или категорию исключений (см. раздел "Удаление исключения или категории исключений" на стр. 185).
- Добавить программу в список доверенных программ (см. раздел "Добавление программы в список доверенных программ" на стр. 186).
- Приостановить исключение доверенной программы или категории программ из проверки программой Kaspersky Security (см. раздел "Включение и исключение доверенной программы или категории доверенных программ из проверки" на стр. 189).
- Удалить доверенную программу или категорию доверенных программ (см. раздел "Удаление доверенной программы или категории доверенных программ" на стр. 190).

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

kaspersky

В этом разделе

Создание исключения

Вы можете создать новое исключение или категорию исключений, содержащую исключения для Легкого агента для Windows, при использовании которых программа Kaspersky Security не проверяет указанные файлы или папки и / или объекты с указанным именем.

Программа Kaspersky Security не проверяет исключенный объект, если при запуске одной из задач проверки указан жесткий диск или папка, в которой находится объект. Но если вы запустили задачу выборочной проверки для объекта, программа Kaspersky Security проверяет объект, даже если для этого объекта создано исключение.

► *Чтобы создать исключение через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**. На закладке отображается список добавленных исключений, сгруппированных по категориям.
7. Если вы хотите добавить новое исключение, не входящее ни в одну из предустановленных категорий исключений, выполните следующие действия:
   a. Нажмите на кнопку **Добавить** и в контекстном меню выберите пункт **Категорию**.
   b. В открывшемся окне **Категория** в поле **Имя категории** введите имя новой категории исключений и нажмите на кнопку **OK**.
8. Если вы хотите добавить новое исключение в добавленную категорию или в одну из

предустановленных категорий исключений, выберите категорию, в которую вы хотите добавить исключение.

9. Нажмите на кнопку **Добавить** и в контекстном меню выберите пункт **Исключение**.

   Откроется окно **Исключение**.

10. В открывшемся окне **Исключение** выполните следующие действия:

    - Если вы хотите исключить из защиты и проверки файл или папку, выполните следующие действия:

      a. В блоке **Свойства** установите флажок **Файл или папка**.

      b. По ссылке **выберите файл или папку**, расположенной в блоке **Описание исключения**, откройте окно **Название файла или папки**. Введите путь к файлу или папке, маску пути к файлу или папке или выберите файл или папку в дереве папок.

      c. После выбора объекта нажмите на кнопку **ОК** в окне **Название файла или папки**.

      Путь к добавленному объекту появится в блоке **Описание исключения** окна **Исключения**.

    - Если вы хотите исключить из защиты и проверки объекты с определенным названием на основании классификации вредоносных и других программ, представленных в Вирусной энциклопедии "Лаборатории Касперского", выполните следующие действия:

      a. В блоке **Свойства** установите флажок **Название объекта**.

      b. По ссылке **введите название объекта**, расположенной в блоке **Описание исключения**, откройте окно **Название объекта**. Введите название или маску названия объекта согласно классификации Вирусной энциклопедии «Лаборатории Касперского» (https://threats.kaspersky.com/ru/threat/).

      c. Нажмите на кнопку **ОК** в окне **Название объекта**.

      Название добавленного объекта появится в блоке **Описание исключения** окна **Исключения**.

    - Если вы хотите исключить из защиты и проверки файл по его хешу, выполните следующие действия:

      a. В блоке **Свойства** установите флажок **Хеш файла**.

      b. По ссылке **введите хеш файла**, расположенной в блоке **Описание исключения**, откройте окно **Хеш файла**. Введите хеш файла, вычисляемый по алгоритму SHA-256, или нажмите на кнопку **Обзор** и выберите файл в открывшемся окне.

      c. Нажмите на кнопку **ОК** в окне **Хеш файла**.

      Хеш добавленного файла появится в блоке **Описание исключения** окна **Исключения**.

11. Определите компоненты программы Kaspersky Security, в работе которых должно быть использовано исключение:

    a. По ссылке **любые**, расположенной в блоке **Описание исключения**, откройте ссылку **выберите компоненты**.

    b. По ссылке **выберите компоненты** откройте окно **Компоненты защиты**.

    c. Выберите нужные компоненты.

    d. Нажмите на кнопку **ОК** в окне **Компоненты защиты**.

    Если компоненты указаны в параметрах исключения, то объект не проверяется только этими компонентами программы Kaspersky Security.

    Если компоненты не указаны в параметрах исключения, то объект не проверяется всеми

компонентами программы Kaspersky Security.

12. Нажмите на кнопку **OK** в окне **Исключение**.

    Добавленное исключение появится в списке исключений закладки **Исключения** окна **Доверенная зона**. В блоке **Описание исключения** отобразятся заданные параметры этого исключения.

13. Нажмите на кнопку **OK** в окне **Доверенная зона**.
14. Нажмите на кнопку **Применить**.

► *Чтобы создать исключение в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–13 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение использования исключения или категории исключений

Вы можете временно приостановить использование исключения или категории исключений, не удаляя их из списка исключений.

► *Чтобы включить или выключить использование исключения или категории исключений через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.

7. В списке исключений выберите нужное исключение или нужную категорию исключений и выполните одно из следующих действий:
   - Установите флажок рядом с названием исключения или категории исключений, если вы хотите использовать это исключение или категорию исключений.
   - Снимите флажок рядом с названием исключения или категории исключений, если вы хотите

временно приостановить использование этого исключения или категории исключений.

8. Нажмите на кнопку **OK** в окне **Доверенная зона**.
9. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить использование исключения или категории исключений в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Удаление исключения или категории исключений

Вы можете удалить исключение или категорию исключений, если вы не хотите, чтобы программа Kaspersky Security использовала это исключение или категорию исключений во время защиты и проверки виртуальной машины. Также вы можете временно приостановить использование исключения или категории исключений (см. раздел "Включение и выключение использования исключения или категории исключений" на стр. 184), не удаляя их из списка исключений.

► *Чтобы удалить исключение или категорию исключений через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.

7. В списке исключений выберите нужное исключение или нужную категорию исключений и нажмите на кнопку **Удалить**.

   Выбранные исключение или категория исключений исчезнут из списка исключений закладки **Исключения** окна **Доверенная зона**.

8. Нажмите на кнопку **OK** в окне **Доверенная зона**.

9. Нажмите на кнопку **Применить**.

► *Чтобы удалить исключение или категорию исключений в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Добавление программы в список доверенных программ

Вы можете сформировать список доверенных программ, для которых программа Kaspersky Security не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру.

► *Чтобы сформировать список доверенных программ через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.
7. Выберите закладку **Доверенные программы**.

   На закладке отображается список добавленных доверенных программ, сгруппированных по категориям.
8. Если вы хотите добавить в список доверенных программ новую программу, не входящую ни в одну из предустановленных категорий, выполните следующие действия:
   a. Нажмите на кнопку **Добавить** и в контекстном меню выберите пункт **Категорию**.
   b. В открывшемся окне **Категория** в поле **Имя категории** введите имя новой категории доверенных программ и нажмите на кнопку **OK**.
9. Если вы хотите добавить доверенную программу в добавленную категорию или в одну из

предустановленных категорий доверенных программ, в списке доверенных программ выберите категорию, в которую вы хотите добавить доверенную программу.

10. На закладке **Доверенные программы** нажмите на кнопку **Добавить** и в контекстном меню выберите пункт **Доверенную программу** –> **Обзор**.

    Откроется стандартное окно Microsoft Windows **Открыть файл**.

11. В окне Microsoft Windows **Открыть файл** выберите исполняемый файл программы, которую вы хотите добавить в список доверенных программ, и нажмите на кнопку **Открыть**.

    Откроется окно **Исключения для программы**.

12. В открывшемся окне **Исключения для программы** выполните следующие действия:

    a. В поле **Путь** введите путь к исполняемому файлу программы, которую вы хотите добавить в список доверенных программ.

    b. С помощью флажков настройте параметры контроля активности программы.

    Если вы установили флажок **Не проверять сетевой трафик**, то с помощью ссылок в нижней части окна вы можете настроить следующие параметры проверки трафика, передаваемого для этой программы:

    - исключать из проверки весь трафик или только зашифрованный трафик (см. раздел "Проверка защищенных соединений" на стр. 252);
    - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных IP-адресов;
    - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных портов.

    Вы можете изменять эти параметры щелчком мыши по ссылке.

    > Если в окне **Исключения для программы** не выбран ни один из видов активности программы, то происходит включение доверенной программы в проверку (см. раздел "Включение и исключение доверенной программы или категории доверенных программ из проверки" на стр. 189). Доверенная программа не удаляется из списка доверенных программ, но флажок для нее снят.

    c. Нажмите на кнопку **OK** в окне **Исключения для программы**.

    Добавленная доверенная программа появится в списке доверенных программ.

13. Нажмите на кнопку **OK** в окне **Доверенная зона**.

14. Нажмите на кнопку **Применить**.

► *Чтобы сформировать список доверенных программ в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).

2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.

4. Выберите закладку **Доверенные программы**.

   На закладке отображается список добавленных доверенных программ, сгруппированных по категориям.

5. Если вы хотите добавить в список доверенных программ новую программу, не входящую ни в одну из предустановленных категорий, выполните следующие действия:

   a. Нажмите на кнопку **Добавить** и в контекстном меню выберите пункт **Категорию**.

   b. В открывшемся окне **Категория** в поле **Имя категории** введите имя новой категории доверенных программ и нажмите на кнопку **ОК**.

6. Если вы хотите добавить доверенную программу в добавленную категорию или в одну из предустановленных категорий доверенных программ, выберите категорию, в которую вы хотите добавить доверенную программу.

7. На закладке **Доверенные программы** нажмите на кнопку **Добавить** и в контекстном меню выполните одно из следующих действий:

   - Выберите пункт **Программы**, если хотите найти программу в списке программ, установленных на виртуальной машине.

     Откроется окно **Выбор программы**.

   - Выберите пункт **Обзор**, если хотите указать путь к исполняемому файлу нужной программы.

     Откроется окно **Выбор файла**.

8. Выберите программу, которую вы хотите добавить в список доверенных программ.

   Откроется окно **Исключения для программы**.

9. С помощью флажков настройте параметры контроля активности программы.

   Если вы установили флажок **Не проверять сетевой трафик**, то с помощью ссылок в нижней части окна вы можете настроить следующие параметры проверки трафика, передаваемого для этой программы:

   - исключать из проверки весь трафик или только зашифрованный трафик;
   - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных IP-адресов;
   - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных портов.

   Вы можете изменять эти параметры щелчком мыши по ссылке.

Если в окне **Исключения для программы** не выбран ни один из видов активности программы, то происходит включение доверенной программы в проверку (см. раздел "Включение и исключение доверенной программы или категории доверенных программ из проверки" на стр. 189). Доверенная программа не удаляется из списка доверенных программ, но флажок для нее снят.

10. Нажмите на кнопку **OK** в окне **Исключения для программы**.

    Добавленная доверенная программа появится в списке доверенных программ.

11. Нажмите на кнопку **OK** в окне **Доверенная зона**.
12. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и исключение доверенной программы или категории доверенных программ из проверки

Вы можете временно приостановить исключение доверенной программы или категории доверенных программ из проверки программой Kaspersky Security, не удаляя доверенную программу или категорию программ из списка доверенных программ.

► *Чтобы включить доверенную программу или категорию программ в проверку или исключить доверенную программу или категорию программ из проверки через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.

7. Выберите закладку **Доверенные программы**.
8. В списке доверенных программ выберите нужную доверенную программу или категорию программ и выполните одно из следующих действий:
   - Установите флажок рядом с названием доверенной программы или категории программ, если хотите исключить ее из проверки программой Kaspersky Security.
   - Снимите флажок рядом с названием доверенной программы или категории программ, если хотите включить ее в проверку программой Kaspersky Security.
9. Нажмите на кнопку **OK** в окне **Доверенная зона**.
10. Нажмите на кнопку **Применить**.

► *Чтобы включить доверенную программу или категорию программ в проверку или исключить доверенную программу или категорию программ из проверки в локальном*

интерфейсе, выполните следующие действия:

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Удаление доверенной программы или категории доверенных программ

Вы можете удалить доверенную программу или категорию доверенных программ, если вы хотите, чтобы программа Kaspersky Security проверяла эту доверенную программу или категорию программ во время защиты и проверки виртуальной машины. Также вы можете временно включить доверенную программу или категорию программ в проверку (см. раздел "Включение и исключение доверенной программы или категории доверенных программ из проверки" на стр. 189), не удаляя их из списка доверенных программ.

► *Чтобы удалить доверенную программу или категорию программ через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.
7. Выберите закладку **Доверенные программы**.
8. В списке доверенных программ выберите нужную программу или нужную категорию программ и нажмите на кнопку **Удалить**.

   Выбранные программа или категория программ исчезнут из списка доверенных программ закладки **Доверенные программы** окна **Доверенная зона**.
9. Нажмите на кнопку **OK** в окне **Доверенная зона**.
10. Нажмите на кнопку **Применить**.

► *Чтобы удалить доверенную программу или категорию программ в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка исключений для Легкого агента для Linux

Вы можете выполнить следующие действия для настройки исключений для Легкого агента для Linux:

- Создать исключение или категорию исключений (см. раздел "Создание исключения" на стр. 192), содержащую исключения для Легкого агента для Linux, при использовании которых программа Kaspersky Security не проверяет входящие в категорию файлы или папки и / или объекты с указанным именем.
- Изменить параметры исключения, используя кнопку **Изменить**.
- Приостановить использование исключения или категории исключений (см. раздел "Включение и выключение использования исключения или категории исключений" на стр. 193).
- Удалить исключение или категорию исключений (см. раздел "Удаление исключения или категории исключений" на стр. 194).

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

kaspersky

В этом разделе

Создание исключения

Вы можете создать новое исключение или категорию исключений, содержащую исключения для Легкого агента для Linux, при использовании которых программа Kaspersky Security не проверяет указанные файлы или папки и / или объекты с указанным именем.

► *Чтобы создать исключение, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**. На закладке отображается список добавленных исключений, сгруппированных по категориям.
7. Если вы хотите добавить новое исключение, не входящее в предустановленную категорию исключений, выполните следующие действия:
   a. Нажмите на кнопку **Добавить** и в контекстном меню выберите пункт **Категорию**.
   b. В открывшемся окне **Категория** в поле **Имя категории** введите имя новой категории исключений и нажмите на кнопку **OK**.
8. Если вы хотите добавить новое исключение в добавленную категорию или в одну из предустановленных категорий исключений, выберите категорию, в которую вы хотите добавить исключение.
9. Нажмите на кнопку **Добавить** и в контекстном меню выберите пункт **Исключение**.

   Откроется окно **Исключение**.
10. В открывшемся окне **Исключение** выполните следующие действия:
    - Если вы хотите исключить из защиты и проверки файл или папку, выполните следующие действия:
      a. В блоке **Свойства** установите флажок **Файл или папка**.
      b. По ссылке **выберите файл или папку**, расположенной в блоке **Описание исключения**, откройте окно **Название файла или папки**. В этом окне вы можете ввести путь к файлу или

папке или маску пути к файлу или папке.

c. После выбора объекта нажмите на кнопку **OK** в окне **Название файла или папки**.

Путь к добавленному объекту появится в блоке **Описание исключения** окна **Исключения**.

- Если вы хотите исключить из защиты и проверки объекты с определенным названием на основании классификации вредоносных и других программ, представленных в Вирусной энциклопедии "Лаборатории Касперского", выполните следующие действия:

  a. В блоке **Свойства** установите флажок **Название объекта**.

  b. По ссылке **введите название объекта**, расположенной в блоке **Описание исключения**, откройте окно **Название объекта**. В этом окне вы можете ввести название или маску названия объекта согласно классификации Вирусной энциклопедии «Лаборатории Касперского» (https://threats.kaspersky.com/ru/threat/).

  c. Нажмите на кнопку **OK** в окне **Название объекта**.

  Название добавленного объекта появится в блоке **Описание исключения** окна **Исключения**.

11. Нажмите на кнопку **OK** в окне **Исключение**.

    Добавленное исключение появится в списке исключений закладки **Исключения** окна **Доверенная зона**. В блоке **Описание исключения** отобразятся заданные параметры этого исключения.

12. Нажмите на кнопку **OK** в окне **Доверенная зона**.

13. Нажмите на кнопку **Применить**.

Включение и выключение использования исключения или категории исключений

Вы можете временно приостановить использование исключения или категории исключений, не удаляя их из списка исключений.

► *Чтобы включить или выключить использование исключения или категории исключений, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.

7. В списке исключений выберите нужное исключение или нужную категорию исключений и выполните одно из следующих действий:

   - Установите флажок рядом с названием исключения или категории исключений, если вы хотите использовать это исключение или категорию исключений.
   - Снимите флажок рядом с названием исключения или категории исключений, если вы хотите

временно приостановить использование этого исключения или категории исключений.

8. Нажмите на кнопку **OK** в окне **Доверенная зона**.
9. Нажмите на кнопку **Применить**.

Удаление исключения или категории исключений

Вы можете удалить исключение или категорию исключений, если вы не хотите, чтобы программа Kaspersky Security использовала это исключение или категорию исключений во время защиты и проверки виртуальной машины. Также вы можете временно приостановить использование исключения или категории исключений (см. раздел "Включение и выключение использования исключения или категории исключений" на стр. 193), не удаляя их из списка исключений.

► *Чтобы удалить исключение или категорию исключений, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Основные параметры защиты**.
6. В правой части окна в блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.
7. В списке исключений выберите нужное исключение или нужную категорию исключений и нажмите на кнопку **Удалить**.

   Выбранные исключение или категория исключений исчезнут из списка исключений закладки **Исключения** окна **Доверенная зона**.
8. Нажмите на кнопку **OK** в окне **Доверенная зона**.
9. Нажмите на кнопку **Применить**.

Технология лечения активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность на защищенной виртуальной машине с операционной системой Windows для рабочих станций, программа Kaspersky Security выполняет расширенную процедуру лечения, применяя специальную технологию лечения активного заражения.

Технология лечения активного заражения направлена на лечение операционной системы Windows от вредоносных программ, которые уже запустили свои процессы в оперативной памяти и мешают программе Kaspersky Security удалить их с помощью других методов. В результате применения технологии лечения активного заражения угроза нейтрализуется. В процессе лечения активного заражения не рекомендуется запускать новые процессы или изменять реестр операционной системы Windows.

В локальном интерфейсе Легкого агента для Windows технология лечения активного заражения по

умолчанию включена, при необходимости вы можете ее выключить (см. раздел "Настройка технологии лечения активного заражения в локальном интерфейсе" на стр. 196). В политике для Легкого агента для Windows технология лечения активного заражения по умолчанию выключена, при необходимости вы можете ее включить (см. раздел "Настройка лечения активного заражения через Kaspersky Security Center" на стр. 195).

Технология лечения активного заражения требует значительных ресурсов операционной системы Windows, что может замедлить работу других программ.

После окончания процедуры лечения активного заражения программа выполняет перезагрузку защищенной виртуальной машины. После перезагрузки программа удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку защищенной виртуальной машины.

Незапланированная перезагрузка операционной системы для серверов может повлечь за собой проблемы, связанные с временным отказом доступа к данным операционной системы или потерей несохраненных данных. Поэтому на защищенных виртуальных машинах с операционными системами Windows для серверов технология лечения активного заражения не используется.

Если Легкий агент работает на временной виртуальной машине, технология лечения активного заражения не используется. В случае активного заражения этой временной виртуальной машины требуется убедиться в отсутствии вирусов и других вредоносных программ на шаблоне виртуальной машины, из которого она была создана, и выполнить пересоздание временной виртуальной машины.

В этом разделе

Настройка лечения активного заражения через Kaspersky Security Center

В политике для Легкого агента для Windows технология лечения активного заражения по умолчанию выключена. При необходимости вы можете настроить немедленное выполнение процедуры лечения активного заражения сразу после обнаружения заражения, с последующей перезагрузкой защищенной виртуальной машины без запроса подтверждения у пользователя.

► *Чтобы настроить выполнение лечения активного заражения без запроса подтверждения у пользователя, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел

Основные параметры защиты.

6. Установите флажок **Применять технологию лечения активного заражения**.
7. Нажмите на кнопку **OK** в окне **Свойства: <Название политики>**.
8. В рабочей области выберите закладку **Задачи**.
9. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
10. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

    В правой части окна отобразятся параметры задачи.
11. В блоке параметров **Действие при обнаружении угрозы** установите флажок **Выполнять лечение активного заражения немедленно.**
12. Нажмите на кнопку **Применить** в окне **Свойства: <Название задачи>**.

Настройка технологии лечения активного заражения в локальном интерфейсе

В локальном интерфейсе Легкого агента для Windows технология лечения активного заражения по умолчанию включена, при необходимости вы можете ее выключить.

► *Чтобы настроить технологию лечения активного заражения в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В правой части окна выполните одно из следующих действий:
   - Установите флажок **Применять технологию лечения активного заражения**, если хотите включить технологию лечения активного заражения.
   - Снимите флажок **Применять технологию лечения активного заражения**, если хотите выключить технологию лечения активного заражения.

   По умолчанию флажок **Применять технологию лечения активного заражения** установлен.

   > Если флажок недоступен, это означает, что вы не можете включить или выключить технологию лечения активного заражения, так как это запрещено политикой для всех защищенных виртуальных машин группы администрирования.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита файловой системы виртуальной машины. Файловый Антивирус

Файловый Антивирус позволяет избежать заражения файловой системы защищенной виртуальной машины. По умолчанию Файловый Антивирус запускается при старте программы, постоянно находится в оперативной памяти виртуальной машины и проверяет все открываемые, сохраняемые и запускаемые файлы на защищенной виртуальной машине на наличие в них вирусов и других вредоносных программ.

Файловый Антивирус использует методы сигнатурного и эвристического анализа, а также технологии iSwift (для Легкого агента для Windows) (см. раздел "Использование технологии iSwift в работе Файлового Антивируса" на стр. 211) и iChecker (для Легкого агента для Linux) (см. раздел "Использование технологии iChecker в работе Файлового Антивируса" на стр. 219).

Если при проверке в файле не обнаружены вирусы или другие вредоносные программы, программа Kaspersky Security разрешает доступ к этому файлу. Если в результате проверки Файловый Антивирус обнаруживает угрозу в файле, программа Kaspersky Security присваивает файлу статус, обозначающий тип обнаруженного объекта (например, *вирус*, *троянская программа*).

После этого программа выполняет над файлом действие, заданное в параметрах Файлового Антивируса.

В этом разделе

Настройка Файлового Антивируса Легкого агента для Windows

Выключение компонента приводит к выходу программы из сертифицированного состояния. Настройка некоторых параметров работы компонента может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия для настройки работы Файлового Антивируса Легкого агента

для Windows:

- Настроить автоматическую приостановку работы Файлового Антивируса (см. раздел "Включение и выключение Файлового Антивируса для Windows" на стр. 198) по расписанию или при запуске программ.
- Изменить уровень безопасности файлов (см. раздел "Изменение уровня безопасности файлов" на стр. 201).
- Изменить действие (см. раздел "Изменение действия Файлового Антивируса над зараженными файлами" на стр. 203), которое Файловый Антивирус выполняет при обнаружении зараженного файла.
- Сформировать область защиты Файлового Антивируса (см. раздел "Формирование области защиты Файлового Антивируса" на стр. 204).
- Настроить проверку составных файлов (см. раздел "Проверка составных файлов Файловым Антивирусом" на стр. 206).
- Оптимизировать проверку файлов (см. раздел "Оптимизация проверки файлов Файловым Антивирусом" на стр. 208).
- Изменить режим проверки файлов (см. раздел "Изменение режима проверки файлов" на стр. 209).
- Настроить использование эвристического анализа (см. раздел "Использование эвристического анализа в работе Файлового Антивируса" на стр. 210).
- Настроить использование технологии проверки iSwift (см. раздел "Использование технологии iSwift в работе Файлового Антивируса" на стр. 211).

В этом разделе

Включение и выключение Файлового Антивируса для Windows

По умолчанию Файловый Антивирус для Windows включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Файловый Антивирус для Windows при необходимости.

► *Чтобы включить или выключить Файловый Антивирус для Windows через Kaspersky Security*

Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. Выполните одно из следующих действий:
   - Установите флажок **Файловый Антивирус**, если вы хотите включить компонент Файловый Антивирус.
   - Снимите флажок **Файловый Антивирус**, если вы хотите выключить компонент Файловый Антивирус.
7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

► *Чтобы включить или выключить Файловый Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления** и раскройте блок **Управление защитой**.
3. По правой клавише мыши откройте контекстное меню строки **Файловый Антивирус** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Файловый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Файловый Антивирус**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Файловый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Файловый Антивирус**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

► *Чтобы включить или выключить Файловый Антивирус из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить Файловый Антивирус**, если вы хотите включить компонент Файловый Антивирус.
   - Снимите флажок **Включить Файловый Антивирус**, если вы хотите выключить компонент Файловый Антивирус.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Автоматическая приостановка работы Файлового Антивируса

Вы можете настроить автоматическую приостановку работы компонента Файловый Антивирус в указанное время или во время работы с определенными программами.

Приостановка работы Файлового Антивируса при конфликте с определенными программами является экстренной мерой. Если во время работы компонента возникают какие-либо конфликты, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. 503). Специалисты помогут вам наладить совместную работу Файлового Антивируса с другими программами на вашей виртуальной машине.

► *Чтобы настроить автоматическую приостановку работы Файлового Антивируса через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

Откроется окно **Файловый Антивирус**.

7. В окне **Файловый Антивирус** на закладке **Дополнительно** в блоке **Приостановка работы** выполните следующие действия:
   - Установите флажок **По расписанию** и нажмите на кнопку **Расписание**, если вы хотите настроить автоматическую приостановку работы Файлового Антивируса в указанное время.

     Откроется окно **Приостановка работы**.
   - Установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**, если вы хотите настроить автоматическую приостановку работы Файлового Антивируса при запуске указанных программ.

     Откроется окно **Программы**.
8. Выполните следующие действия:
   - Если вы настраиваете автоматическую приостановку работы Файлового Антивируса в указанное время, то в окне **Приостановка работы** в полях **Приостановить в** и **Возобновить в** укажите время (в формате ЧЧ:ММ), в течение которого работу Файлового Антивируса следует приостанавливать. Далее нажмите на кнопку **ОК**.
   - Если вы настраиваете автоматическую приостановку работы Файлового Антивируса при запуске указанных программ, то в окне **Программы** с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список программ, во время работы которых работу Файлового Антивируса следует приостанавливать. Далее нажмите на кнопку **ОК**.
9. Нажмите на кнопку **ОК** в окне **Файловый Антивирус**.
10. Нажмите на кнопку **Применить**.

► *Чтобы настроить автоматическую приостановку работы Файлового Антивируса в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение уровня безопасности файлов

Для защиты файловой системы виртуальной машины Файловый Антивирус применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности файлов*. Вы можете выбрать один из предустановленных уровней безопасности файлов или настроить параметры уровня безопасности файлов самостоятельно. Предусмотрено три уровня безопасности файлов: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности файлов **Рекомендуемый** считаются оптимальными и рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности файлов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности файлов (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите настроить уровень безопасности файлов самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Файловый Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности файлов, название уровня безопасности файлов в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности файлов на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

► *Чтобы изменить уровень безопасности файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности файлов (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите настроить уровень безопасности файлов самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Файловый Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности файлов, название уровня безопасности файлов в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности файлов на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия Файлового Антивируса над зараженными файлами

► *Чтобы изменить через Kaspersky Security Center действие Файлового Антивируса над зараженными файлами, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Выбирать действие автоматически**.
   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.
   - **Выполнять действие: Лечить**.
   - **Выполнять действие: Удалять**.
   - **Выполнять действие: Блокировать**.

   По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Лечить. Удалять, если лечение невозможно**.

   > В отношении файлов, являющихся частью приложения Windows Store®, программа Kaspersky Security выполняет действие **Удалять** вне зависимости от выбранного варианта.

   > При удалении или лечении копии файлов сохраняются в резервном хранилище.
7. Нажмите на кнопку **Применить**.

► *Чтобы изменить действие Файлового Антивируса над зараженными файлами в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Выбирать действие автоматически**.

- **Выполнять действие: Лечить. Удалять, если лечение невозможно**.
- **Выполнять действие: Лечить**.
- **Выполнять действие: Удалять**.
- **Выполнять действие: Блокировать**.

По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Лечить. Удалять, если лечение невозможно**.

В отношении файлов, являющихся частью приложения Windows Store, программа Kaspersky Security выполняет действие **Удалять** вне зависимости от выбранного варианта.

При удалении или лечении копии файлов сохраняются в резервном хранилище.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование области защиты Файлового Антивируса

Областью защиты называются объекты, которые компонент проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты Файлового Антивируса являются местоположение и тип проверяемых файлов. По умолчанию Файловый Антивирус проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков виртуальной машины. Вы можете расширить или сузить область защиты, добавив или удалив проверяемые объекты или изменив тип проверяемых файлов.

► *Чтобы сформировать область защиты Файлового Антивируса с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Общие** в блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять Файловым Антивирусом:
   - Выберите **Все файлы**, если вы хотите проверять все файлы.
   - Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов,

которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее подвержены заражению.

- Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее подвержены заражению.

Выбирая тип проверяемых файлов, нужно помнить следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.
- Злоумышленник может отправить вирус или другую вредоносную программу на вашу виртуальную машину в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Файловый Антивирус проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие вредоносные программы.
- Список проверяемых расширений и список проверяемых форматов меняются динамически и соответствуют текущей необходимости поддержания безопасности вашей виртуальной машины.

8. В блоке **Область защиты** выполните одно из следующих действий:

   - Если вы хотите добавить новый объект в список проверяемых объектов, нажмите на кнопку **Добавить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите изменить путь к объекту, выберите объект в списке объектов и нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите удалить объект из области защиты, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

     Откроется окно подтверждения удаления.

9. Выполните одно из следующих действий:

   - Если вы хотите добавить новый объект, в окне **Выбор объекта** выберите объект и нажмите на кнопку **Добавить**.

     Все объекты, выбранные в окне **Выбор объекта**, отобразятся в списке **Область защиты** в окне **Файловый Антивирус**.

     Нажмите на кнопку **ОК**.

   - Если вы хотите изменить путь к объекту из списка проверяемых объектов, в окне **Выбор объекта** укажите другой путь к объекту в поле **Объект** и нажмите на кнопку **ОК**.

   - Если вы хотите удалить объект, в окне подтверждения удаления нажмите на кнопку **Да**.

10. Если требуется, повторите пункты 8 и 9 для добавления объектов, изменения пути к ним или удаления объектов из области защиты.

11. Если вы хотите исключить объект из области защиты, в списке **Область защиты** снимите флажок рядом с ним. Объект остается в списке проверяемых объектов, но исключается из проверки Файловым Антивирусом.

12. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
13. Нажмите на кнопку **Применить**.

► *Чтобы сформировать область защиты Файлового Антивируса в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–12 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка составных файлов Файловым Антивирусом

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить через Kaspersky Security Center проверку составных файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Производительность** в блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, самораспаковывающиеся архивы или вложенные OLE-объекты, установив соответствующие флажки.
8. Если вы хотите, чтобы Файловый Антивирус проверял только новые и измененные составные файлы всех типов, в блоке **Оптимизация проверки** установите флажок **Проверять только новые**

и измененные файлы.

Если флажок **Проверять только новые и измененные файлы** не установлен, в блоке **Проверка составных файлов** для каждого типа составного файла вы можете выбрать, нужно ли проверять все файлы этого типа или только новые. Для выбора нажмите на ссылку **все / новые**, расположенную рядом с названием типа составного файла. Ссылка меняет свое значение после нажатия на нее левой клавишей мыши.

9. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.

10. В блоке **Фоновая проверка** выполните одно из следующих действий:

    - Если вы хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера в фоновом режиме, установите флажок **Распаковывать составные файлы в фоновом режиме** и в поле **Минимальный размер файла** укажите нужное значение.
    - Если вы не хотите, чтобы Файловый Антивирус распаковывал составные файлы в фоновом режиме, снимите флажок **Распаковывать составные файлы в фоновом режиме**.

11. В блоке **Ограничение по размеру** выполните одно из следующих действий:

    - Если вы хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.
    - Если вы не хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.

    Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

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

12. Нажмите на кнопку **OK** в окне **Составные файлы**.
13. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
14. Нажмите на кнопку **Применить**.

► *Чтобы настроить проверку составных файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–13 предыдущей инструкции.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Оптимизация проверки файлов Файловым Антивирусом

Вы можете оптимизировать проверку файлов Файловым Антивирусом: сократить время проверки и увеличить скорость работы программы. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

► *Чтобы оптимизировать проверку файлов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Производительность** в блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.
8. Нажмите на кнопку **ОК** в окне **Файловый Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы оптимизировать проверку файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором Файловый Антивирус начинает проверять файлы. По умолчанию Файловый Антивирус использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, Файловый Антивирус принимает решение о проверке файлов на основании анализа операций, которые вы, программа от вашего имени или имени другого пользователя (на основании учетных данных, с которыми был осуществлен вход в операционную систему) или операционная система выполняют над файлами. Например, работая с документом Microsoft Office Word, Файловый Антивирус проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

► *Чтобы изменить режим проверки файлов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Дополнительно** в блоке **Режим проверки** выберите нужный режим:
   - **Интеллектуальный**.
   - **При доступе и изменении**.
   - **При доступе**.
   - **При выполнении**.
8. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы изменить режим проверки файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе Файлового Антивируса

Во время своей работы Файловый Антивирус использует сигнатурный анализ. В процессе сигнатурного анализа Файловый Антивирус сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" сигнатурный анализ всегда включен.

Для повышения эффективности защиты вы можете использовать эвристический анализ. В процессе эвристического анализа Файловый Антивирус анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

► *Чтобы настроить использование эвристического анализа в работе Файлового Антивируса через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Производительность** в блоке **Методы проверки** выполните одно из следующих действий:
   - Если вы хотите, чтобы Файловый Антивирус использовал эвристический анализ, установите флажок **Эвристический анализ** и с помощью ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы Файловый Антивирус не использовал эвристический анализ, снимите флажок **Эвристический анализ**.
8. Нажмите на кнопку **ОК** в окне **Файловый Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы настроить использование эвристического анализа в работе Файлового Антивируса в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование технологии iSwift в работе Файлового Антивируса

Вы можете включить использование технологии iSwift, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы настроить использование технологии iSwift в работе Файлового Антивируса через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Дополнительно** в блоке **Технология проверки** выполните одно из следующих действий:
   - Установите флажок **Технология iSwift**, если вы хотите использовать эту технологию в работе Файлового Антивируса.
   - Снимите флажок **Технология iSwift**, если вы не хотите использовать эту технологию в работе Файлового Антивируса.
8. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы настроить использование технологии iSwift в работе Файлового Антивируса в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Файлового Антивируса Легкого агента для Linux

Выключение компонента приводит к выходу программы из сертифицированного состояния. Настройка некоторых параметров работы компонента может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия для настройки работы Файлового Антивируса Легкого агента для Linux через Kaspersky Security Center:

- Изменить уровень безопасности файлов (см. раздел "Изменение уровня безопасности файлов" на стр. 214).
- Изменить действие (см. раздел "Изменение действия Файлового Антивируса над зараженными файлами" на стр. 214), которое Файловый Антивирус выполняет при обнаружении зараженного файла.
- Сформировать область защиты Файлового Антивируса (см. раздел "Формирование области защиты Файлового Антивируса" на стр. 215).
- Настроить проверку составных файлов (см. раздел "Проверка составных файлов Файловым Антивирусом" на стр. 216).
- Изменить режим проверки файлов (см. раздел "Изменение режима проверки файлов" на стр. 217).

- Настроить использование эвристического анализа (см. раздел "Использование эвристического анализа в работе Файлового Антивируса" на стр. 218).
- Настроить использование технологии проверки iChecker (см. раздел "Использование технологии iChecker в работе Файлового Антивируса" на стр. 219).

В этом разделе

Включение и выключение Файлового Антивируса для Linux

По умолчанию Файловый Антивирус для Linux включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Файловый Антивирус для Linux при необходимости.

► *Чтобы включить или выключить Файловый Антивирус для Linux, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. Выполните одно из следующих действий:
   - Установите флажок **Файловый Антивирус**, если вы хотите включить компонент Файловый Антивирус.
   - Снимите флажок **Файловый Антивирус**, если вы хотите выключить компонент Файловый Антивирус.
7. Нажмите на кнопку **Применить**.

Изменение уровня безопасности файлов

Для защиты файловой системы защищенной виртуальной машины Файловый Антивирус применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности файлов*. Вы можете выбрать один из предустановленных уровней безопасности файлов или настроить параметры уровня безопасности файлов самостоятельно. Предусмотрено три уровня безопасности файлов: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности файлов **Рекомендуемый** считаются оптимальными и рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности файлов (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите настроить уровень безопасности файлов самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Файловый Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности файлов, название уровня безопасности файлов в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности файлов на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

Изменение действия Файлового Антивируса над зараженными файлами

► *Чтобы изменить действие Файлового Антивируса над зараженными файлами, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый**

Антивирус.

В правой части окна отобразятся параметры компонента Файловый Антивирус.

6. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Лечить. Удалять, если лечение невозможно**.
   - **Лечить**.
   - **Удалять**.
   - **Блокировать**.

   По умолчанию выбран вариант **Лечить. Удалять, если лечение невозможно**.

   При удалении или лечении копии файлов сохраняются в резервном хранилище.

7. Нажмите на кнопку **Применить**.

Формирование области защиты Файлового Антивируса

Областью защиты называются объекты, которые компонент Файловый Антивирус проверяет во время своей работы. По умолчанию Файловый Антивирус проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков защищенной виртуальной машины. Вы можете расширить или сузить область проверки, добавив или удалив объекты, которые проверяет Файловый Антивирус.

► *Чтобы сформировать область защиты Файлового Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.

7. В окне **Файловый Антивирус** выберите закладку **Общие**.
8. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять Файловым Антивирусом:
   - Выберите **Все файлы**, если вы хотите проверять все файлы.
   - Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее подвержены заражению.

- Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее подвержены заражению.

Список проверяемых расширений и список проверяемых форматов меняются динамически и соответствуют текущей необходимости поддержания безопасности вашей виртуальной машины.

9. В блоке **Область защиты** выполните одно из следующих действий:
   - Если вы хотите добавить новый объект в список проверяемых объектов, нажмите на кнопку **Добавить**.

     Откроется окно **Выбор объекта**.
   - Если вы хотите изменить путь к объекту, выберите объект в списке объектов и нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.
   - Если вы хотите удалить объект из области защиты, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

     Откроется окно подтверждения удаления.
10. Выполните одно из следующих действий:
    - Если вы хотите добавить новый объект, в окне **Выбор объекта** укажите путь к объекту в поле **Объект** и нажмите на кнопку **Добавить**.

      Объект, добавленный в окне **Выбор объекта**, отобразится в списке **Область защиты** в окне **Файловый Антивирус**.

      Нажмите на кнопку **ОК**.
    - Если вы хотите изменить путь к объекту из списка проверяемых объектов, в окне **Выбор объекта** укажите другой путь к объекту в поле **Объект** и нажмите на кнопку **ОК**.
    - Если вы хотите удалить объект, в окне подтверждения удаления нажмите на кнопку **Да**.
11. Если требуется, повторите пункты 9 и 10 для добавления объектов, изменения пути к ним или удаления объектов из области защиты.
12. Если вы хотите исключить объект из области защиты, в списке **Область защиты** снимите флажок рядом с ним. Объект остается в списке проверяемых объектов, но исключается из проверки Файловым Антивирусом.
13. Нажмите на кнопку **ОК** в окне **Файловый Антивирус**.
14. Нажмите на кнопку **Применить**.

Проверка составных файлов Файловым Антивирусом

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Производительность** в блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: упакованные файлы, архивы, самораспаковывающиеся архивы, почтовые базы или файлы почтовых форматов, установив соответствующие флажки.
8. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.
9. В блоке **Ограничение по времени** выполните одно из следующих действий:
   - Если вы хотите, чтобы Файловый Антивирус пропускал файлы по истечении заданного времени, установите флажок **Пропускать файлы, если их проверка длится более** и в поле **Максимальное время проверки** укажите нужное значение.
   - Если вы не хотите, чтобы Файловый Антивирус пропускал файлы по истечении заданного времени, снимите флажок **Пропускать файлы, если их проверка длится более**.
10. В блоке **Ограничение по размеру** выполните одно из следующих действий:
    - Если вы хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.
    - Если вы не хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.

    Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

    > Файловый Антивирус проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
11. Нажмите на кнопку **OK** в окне **Составные файлы**.
12. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
13. Нажмите на кнопку **Применить**.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором Файловый Антивирус начинает проверять

файлы. По умолчанию Файловый Антивирус использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, Файловый Антивирус принимает решение о проверке файлов на основании анализа операций, которые вы, программа от вашего имени или имени другого пользователя (на основании учетных данных, с которыми был осуществлен вход в операционную систему) или операционная система выполняют над файлами. Например, работая с документом Microsoft Office Word, Файловый Антивирус проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

► *Чтобы изменить режим проверки файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Дополнительно** в блоке **Режим проверки** выберите нужный режим:
   - **Интеллектуальный**.
   - **При доступе и изменении**.
   - **При доступе**.
8. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
9. Нажмите на кнопку **Применить**.

Использование эвристического анализа в работе Файлового Антивируса

Во время своей работы Файловый Антивирус использует сигнатурный анализ. В процессе сигнатурного анализа Файловый Антивирус сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" сигнатурный анализ всегда включен.

Для повышения эффективности защиты вы можете использовать эвристический анализ. В процессе эвристического анализа Файловый Антивирус анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

► *Чтобы настроить использование эвристического анализа в работе Файлового Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
7. В окне **Файловый Антивирус** на закладке **Производительность** в блоке **Методы проверки** выполните одно из следующих действий:
   - Если вы хотите, чтобы Файловый Антивирус использовал эвристический анализ, установите флажок **Эвристический анализ** и с помощью ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы Файловый Антивирус не использовал эвристический анализ, снимите флажок **Эвристический анализ**.
8. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
9. Нажмите на кнопку **Применить**.

Использование технологии iChecker в работе Файлового Антивируса

Вы можете включить использование технологии iChecker, которая позволяет увеличить скорость проверки за счет исключения из проверки некоторых файлов по специальному алгоритму, учитывающему дату выпуска баз программы, дату предыдущей проверки файла, а также изменение параметров проверки.

► *Чтобы настроить использование технологии iChecker в работе Файлового Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Linux и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Linux в списке слева выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.

7. В окне **Файловый Антивирус** на закладке **Дополнительно** в блоке **Технология проверки** выполните одно из следующих действий:

   - Установите флажок **Технология iChecker**, если вы хотите использовать эту технологию в работе Файлового Антивируса.
   - Снимите флажок **Технология iChecker**, если вы не хотите использовать эту технологию в работе Файлового Антивируса.

8. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.
9. Нажмите на кнопку **Применить**.

AMSI-защита

Компонент AMSI-защита позволяет программам Microsoft Office и другим сторонним программам запрашивать проверку объектов на вирусы и другие угрозы, используя интерфейс Windows Antimalware Scan Interface от Microsoft (AMSI). Подробнее об интерфейсе AMSI см. в документации Microsoft.

Если AMSI-защита включена, Kaspersky Security может выполнять проверку объекта по AMSI-запросу и сообщать результат проверки той программе, от которой был получен запрос. Сторонняя программа после получения уведомления об угрозе может предотвращать вредоносные действия (например, завершить работу).

Для работы компонента AMSI-защита на защищенной виртуальной машине требуется подключение Легкого агента, установленного на виртуальной машине, к SVM. В случае разрыва соединения работа компонента AMSI-защита приостанавливается, запросы на проверку объектов не выполняются, информация о непроверенных объектах сохраняется в отчете, доступном в локальном интерфейсе Легкого агента для Windows.

Вы можете настроить параметры (см. раздел "Настройка параметров проверки объектов по AMSI-запросам" на стр. 223) проверки объектов по AMSI-запросам. В ходе проверки Kaspersky Security может применять настроенные исключения из защиты и проверки.

Kaspersky Security может блокировать взаимодействие сторонней программы с компонентом AMSI-защита и отклонять AMSI-запросы от сторонней программы, например, если превышено максимальное количество запросов от этой программы за промежуток времени. При этом Kaspersky Security отправляет информацию об отклонении AMSI-запроса на Сервер администрирования Kaspersky Security Center. Если вы хотите, чтобы Kaspersky Security не отклонял запросы от программы, даже если превышено максимальное количество запросов, вам нужно добавить эту программу в список доверенных программ (см. раздел "Добавление программы в список доверенных программ" на стр. 186) и настроить для этой программы исключение **Не блокировать взаимодействие с AMSI-защитой**.

Не поддерживается установка и работа компонента AMSI-защита на виртуальных машинах с гостевыми операционными системами ниже Windows 10 и Windows Server 2016.

В этом разделе

Включение и выключение AMSI-защиты

По умолчанию AMSI-защита включена и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить AMSI-защиту при необходимости.

► *Чтобы включить или выключить AMSI-защиту через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **AMSI-защита**.

   В правой части окна отобразятся параметры компонента AMSI-защита.
6. Выполните одно из следующих действий:
   - Установите флажок **AMSI-защита**, если вы хотите включить компонент AMSI-защита.
   - Снимите флажок **AMSI-защита**, если вы хотите выключить компонент AMSI-защита.
7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить AMSI-защиту в локальном интерфейсе Легкого агента для Windows , выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления** и раскройте блок **Управление защитой**.
3. По правой клавише мыши откройте контекстное меню строки **AMSI-защита** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить компонент AMSI-защита.

     Значок статуса работы компонента , отображающийся слева в строке **AMSI-защита**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить компонент AMSI-защита.

     Значок статуса работы компонента , отображающийся слева в строке **AMSI-защита**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

Настройка параметров проверки объектов по AMSI-запросам

► *Чтобы настроить параметры проверки объектов по AMSI-запросам от сторонних программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **AMSI-защита**.

   В правой части окна отобразятся параметры компонента AMSI-защита.
6. В блоке **Проверка составных файлов** укажите, какие составные файлы будет проверять Kaspersky Security по запросу от сторонних программ: архивы, самораспаковывающиеся архивы, вложенные OLE-объекты.
7. В блоке **Ограничение по размеру** выполните одно из следующих действий:
   - Если вы хотите разрешить программе Kaspersky Security распаковывать составные файлы большого размера при проверке объектов по запросу от сторонних программ, снимите флажок **Не распаковывать составные файлы большого размера**.
   - Если вы хотите запретить распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение. Kaspersky Security не будет распаковывать составные файлы больше указанного размера.

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

Защита почты. Почтовый Антивирус

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с операционной системой Windows для серверов или с операционной системой Windows для рабочих станций.

Выключение компонента приводит к выходу программы из сертифицированного состояния. Настройка некоторых параметров работы компонента может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Почтовый Антивирус проверяет входящие и исходящие сообщения электронной почты (далее также "сообщения" и "почта") на вирусы и другие вредоносные программы. Почтовый Антивирус запускается при старте программы, постоянно находится в оперативной памяти виртуальной машины и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP и NNTP.

Почтовый Антивирус может проверять сообщения, получаемые или отправляемые по протоколам, которые обеспечивают защищенную передачу данных (см. раздел "Проверка защищенных соединений" на стр. 252).

Индикатором работы Почтового Антивируса в локальном интерфейсе Легкого агента для Windows служит значок программы в области уведомлений панели задач. Значок программы принимает вид  каждый раз при проверке сообщения, если включена анимация значка программы.

Почтовый Антивирус перехватывает и проверяет каждое сообщение электронной почты, которое вы принимаете или отправляете. Если угрозы в сообщении не обнаружены, сообщение становится для вас доступным.

Если в результате проверки Почтовый Антивирус обнаруживает угрозу в сообщении, Kaspersky Security присваивает сообщению статус, обозначающий тип обнаруженного объекта (например, *вирус*, *троянская программа*).

После этого программа блокирует зараженное сообщение и выполняет действие (см. раздел "Изменение действия над зараженными сообщениями электронной почты" на стр. 228), заданное в параметрах

Почтового Антивируса.

Почтовый Антивирус взаимодействует с почтовыми клиентами, установленными на защищенной виртуальной машине. Для почтового клиента Microsoft Office Outlook предусмотрено встраиваемое расширение, позволяющее производить более тонкую настройку параметров проверки сообщений. Расширение Почтового Антивируса встраивается в почтовый клиент Microsoft Office Outlook во время установки программы Kaspersky Security.

Вы можете выполнить следующие действия для настройки работы Почтового Антивируса:

- Изменить уровень безопасности почты (см. раздел "Изменение уровня безопасности почты" на стр. 227).
- Изменить действие (см. раздел "Изменение действия над зараженными сообщениями электронной почты" на стр. 228), которое программа выполняет над зараженными сообщениями электронной почты.
- Сформировать область защиты Почтового Антивируса (см. раздел "Формирование области защиты Почтового Антивируса" на стр. 229).
- Настроить проверку вложенных в сообщения составных файлов (см. раздел "Проверка вложенных в сообщения составных файлов" на стр. 231).
- Настроить фильтрацию по типу вложений (см. раздел "Фильтрация вложений в сообщениях" на стр. 232) в сообщениях электронной почты.
- Настроить использование эвристического анализа (см. раздел "Использование эвристического анализа в работе Почтового Антивируса" на стр. 233).
- Настроить параметры проверки почты в программе Microsoft Office Outlook (см. раздел "Проверка почты в Microsoft Office Outlook" на стр. 235).

В этом разделе

Включение и выключение Почтового Антивируса

По умолчанию Почтовый Антивирус включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Почтовый Антивирус при необходимости.

► *Чтобы включить или выключить Почтовый Антивирус через Kaspersky Security Center,*

выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
6. Выполните одно из следующих действий:
   - Установите флажок **Почтовый Антивирус**, если вы хотите включить компонент Почтовый Антивирус.
   - Снимите флажок **Почтовый Антивирус**, если вы хотите выключить компонент Почтовый Антивирус.
7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

► *Чтобы включить или выключить Почтовый Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления** и раскройте блок **Управление защитой**.
3. По правой клавише мыши откройте контекстное меню строки **Почтовый Антивирус** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Почтовый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Почтовый Антивирус**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Почтовый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Почтовый Антивирус**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

► *Чтобы включить или выключить Почтовый Антивирус из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить Почтовый Антивирус**, если вы хотите включить компонент Почтовый Антивирус.
   - Снимите флажок **Включить Почтовый Антивирус**, если вы хотите выключить компонент Почтовый Антивирус.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение уровня безопасности почты

Для защиты почты Почтовый Антивирус применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности почты*. Вы можете выбрать один из предустановленных уровней безопасности почты или настроить уровень безопасности почты самостоятельно. Предусмотрено три уровня безопасности почты: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности почты **Рекомендуемый** считаются оптимальными и рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности почты через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
6. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности почты (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите настроить уровень безопасности почты самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Почтовый Антивирус**.

После того как вы самостоятельно настроили уровень безопасности почты, название уровня безопасности почты в блоке **Уровень безопасности** изменится на **Другой**.

- Если вы хотите изменить самостоятельно настроенный уровень безопасности почты на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.

7. Нажмите на кнопку **Применить**.

► *Чтобы изменить уровень безопасности почты в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности почты (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите настроить уровень безопасности почты самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Почтовый Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности почты, название уровня безопасности почты в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить самостоятельно настроенный уровень безопасности почты на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия над зараженными сообщениями электронной почты

► *Чтобы изменить через Kaspersky Security Center действие над зараженными сообщениями электронной почты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
6. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое программа выполняет при обнаружении зараженного сообщения электронной почты:
   - **Выбирать действие автоматически**.

- **Выполнять действие: Лечить. Удалять, если лечение невозможно**.
- **Выполнять действие: Лечить**.
- **Выполнять действие: Удалять**.
- **Выполнять действие: Блокировать**.

По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Лечить. Удалять, если лечение невозможно**.

При удалении или лечении сообщений копии сообщений сохраняются в резервном хранилище.

7. Нажмите на кнопку **Применить**.

► *Чтобы изменить действие над зараженными сообщениями электронной почты в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое программа выполняет при обнаружении зараженного сообщения электронной почты:
   - **Выбирать действие автоматически**.
   - **Выполнять действие: Лечить. Удалять, если лечение невозможно.**
   - **Выполнять действие: Лечить.**
   - **Выполнять действие: Удалять.**
   - **Выполнять действие: Блокировать.**

   По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Лечить. Удалять, если лечение невозможно**.

   При удалении или лечении сообщений копии сообщений сохраняются в резервном хранилище.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование области защиты Почтового Антивируса

Под областью защиты подразумеваются объекты, которые компонент проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты Почтового Антивируса являются параметры интеграции Почтового Антивируса в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет Почтовый Антивирус. По умолчанию Почтовый Антивирус проверяет входящие и исходящие сообщения, трафик почтовых протоколов POP3, SMTP, IMAP и NNTP, а также интегрируется в программу Microsoft Office Outlook. Расширение Почтового Антивируса встраивается в почтовый клиент Microsoft Office Outlook во время установки программы

Kaspersky Security.

► *Чтобы сформировать область защиты Почтового Антивируса через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
7. В окне **Почтовый Антивирус** на закладке **Общие** в блоке **Область защиты** выполните одно из следующих действий:
   - Выберите вариант **Входящие и исходящие сообщения**, если вы хотите, чтобы Почтовый Антивирус проверял все входящие и исходящие сообщения на защищенной виртуальной машине.
   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы Почтовый Антивирус проверял только входящие сообщения на защищенной виртуальной машине.

     Если вы выбираете проверку только входящих сообщений, рекомендуется однократно проверить все исходящие сообщения, поскольку существует вероятность того, что на защищенной виртуальной машине есть почтовые черви, которые используют электронную почту в качестве канала распространения. Это позволит избежать неконтролируемой рассылки зараженных сообщений с защищенной виртуальной машины.
8. В блоке **Встраивание в систему** выполните следующие действия:
   - Установите флажок **Трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы Почтовый Антивирус проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на защищенной виртуальной машине.
   - Снимите флажок **Трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы Почтовый Антивирус не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на защищенной виртуальной машине. В этом случае сообщения проверяет расширение Почтового Антивируса, встроенное в почтовый клиент Microsoft Office Outlook, после их получения на защищенной виртуальной машине.
   - Установите флажок **Дополнительно: расширение в Microsoft Office Outlook**, если вы хотите открыть доступ к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook и включить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP и IMAP, после их получения на защищенной виртуальной машине с помощью расширения, интегрированного в программу Microsoft Office Outlook.
   - Снимите флажок **Дополнительно: расширение в Microsoft Office Outlook**, если вы хотите

закрыть доступ к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook и выключить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP и IMAP, после их получения на защищенной виртуальной машине с помощью расширения, интегрированного в программу Microsoft Office Outlook.

> Если вы используете почтовый клиент, отличный от Microsoft Office Outlook, то при снятом флажке **Трафик POP3 / SMTP / NNTP / IMAP** Почтовый Антивирус не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

9. Нажмите на кнопку **OK** в окне **Почтовый Антивирус**.
10. Нажмите на кнопку **Применить**.

► *Чтобы сформировать область защиты Почтового Антивируса в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка вложенных в сообщения составных файлов

Вы можете включить или выключить проверку вложенных в сообщения составных файлов, ограничить максимальный размер проверяемых файлов, вложенных в сообщения, и максимальную длительность проверки файлов, вложенных в сообщения.

► *Чтобы настроить через Kaspersky Security Center проверку вложенных в сообщения составных файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.

7. В окне **Почтовый Антивирус** на закладке **Общие** в блоке **Проверка составных файлов** выполните следующие действия:

   - Снимите флажок **Проверять вложенные архивы**, если вы хотите, чтобы Почтовый Антивирус не выполнял проверку вложенных в сообщения архивов.
   - Установите флажок **Не проверять архивы размером более N МБ**, если вы хотите, чтобы Почтовый Антивирус не проверял вложенные в сообщения архивы размером более указанного количества мегабайт. Если вы установили этот флажок, укажите максимальный размер архивов в поле рядом с названием флажка.
   - Установите флажок **Не проверять архивы более N с**, если вы хотите, чтобы Почтовый Антивирус не проверял вложенные в сообщения архивы, если на их проверку затрачивается более указанного количества секунд. Если вы установили этот флажок, укажите максимальное время проверки архивов в поле рядом с названием флажка.

8. Нажмите на кнопку **ОК** в окне **Почтовый Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы настроить проверку вложенных в сообщения составных файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Фильтрация вложений в сообщениях

Вредоносные программы могут распространяться через почту в виде вложений в сообщениях. Вы можете настроить фильтрацию по типу вложений в сообщениях электронной почты, которая позволяет автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, программа Kaspersky Security может защитить вашу виртуальную машину от автоматического запуска вредоносной программы.

► *Чтобы настроить через Kaspersky Security Center фильтрацию вложений, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы

администрирования, в состав которой входят нужные защищенные виртуальные машины.

3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
7. В окне **Почтовый Антивирус** на закладке **Фильтр вложений** выполните одно из следующих действий:
   - Выберите вариант **Не применять фильтр**, если вы хотите, чтобы Почтовый Антивирус не фильтровал вложения в сообщениях.
   - Выберите вариант **Переименовывать вложения указанных типов**, если вы хотите, чтобы Почтовый Антивирус изменял названия вложенных в сообщения файлов указанных типов.
   - Выберите вариант **Удалять вложения указанных типов**, если вы хотите, чтобы Почтовый Антивирус удалял вложенные в сообщения файлы указанных типов.
8. Если на шаге 7 инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, становится активным список типов файлов. Установите флажки напротив нужных типов файлов. Вы можете изменить список типов файлов с помощью кнопок **Добавить**, **Изменить**, **Удалить**.
9. Нажмите на кнопку **OK** в окне **Почтовый Антивирус**.
10. Нажмите на кнопку **Применить**.

► *Чтобы настроить фильтрацию вложений в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе Почтового Антивируса

Для повышения эффективности защиты вы можете использовать эвристический анализ в работе Почтового

Антивируса. В процессе эвристического анализа программа Kaspersky Security анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать в сообщениях новые вредоносные объекты, записей о которых еще нет в базах программы.

► *Чтобы настроить через Kaspersky Security Center использование эвристического анализа в работе Почтового Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
7. В окне **Почтовый Антивирус** на закладке **Дополнительно** в блоке **Метод проверки** выполните следующие действия:
   - Если вы хотите, чтобы Почтовый Антивирус использовал эвристический анализ, установите флажок **Эвристический анализ** и с помощью ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы Почтовый Антивирус не использовал эвристический анализ, снимите флажок **Эвристический анализ**.
8. Нажмите на кнопку **OK** в окне **Почтовый Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы настроить использование эвристического анализа в работе Почтового Антивируса в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка почты в Microsoft Office Outlook

Во время установки программы Kaspersky Security в программу Microsoft Office Outlook встраивается расширение Почтового Антивируса. Оно позволяет перейти к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook, а также указать, в какой момент проверять сообщения электронной почты на вирусы и другие вредоносные программы. Расширение Почтового Антивируса для программы Microsoft Office Outlook может проверять входящие и исходящие сообщения, переданные по протоколам POP3, SMTP, NNTP и IMAP.

Вы можете настроить параметры расширения Почтового Антивируса в политике для Легкого агента для Windows с помощью Kaspersky Security Center (см. раздел "Настройка режима проверки почты с помощью Kaspersky Security Center" на стр. 235) или в программе Microsoft Office Outlook (см. раздел "Настройка проверки почты в Microsoft Office Outlook" на стр. 236).

Настройка параметров Почтового Антивируса из программы Microsoft Office Outlook доступна в том случае, если в свойствах политики Легкого агента для Windows или локальном интерфейсе Легкого агента установлен флажок **Дополнительно: расширение в Microsoft Office Outlook** (см. раздел "**Формирование области защиты Почтового Антивируса**" на стр. 229).

В программе Microsoft Office Outlook входящие сообщения сначала проверяет Почтовый Антивирус (если в свойствах политики Легкого агента или локальном интерфейсе Легкого агента установлен флажок **Трафик POP3 / SMTP / NNTP / IMAP**), а затем проверяет расширение Почтового Антивируса для программы Microsoft Office Outlook. Исходящие сообщения сначала проверяет расширение Почтового Антивируса для программы Microsoft Office Outlook, а затем проверяет Почтовый Антивирус.

В этом разделе

Настройка режима проверки почты с помощью Kaspersky Security Center

► *Чтобы настроить режим работы расширения компонента Почтовый Антивирус для программы Microsoft Office Outlook с помощью Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Почтовый Антивирус**.
6. В правой части окна отобразятся параметры компонента Почтовый Антивирус.

7. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.

8. В окне **Почтовый Антивирус** на закладке **Общие** в блоке **Встраивание в систему** нажмите на кнопку **Настройка**.

   Откроется окно **Защита почты**.

9. В окне **Защита почты** выполните следующие действия:

   - Установите флажок **Проверять при получении**, если вы хотите, чтобы расширение компонента Почтовый Антивирус для программы Microsoft Office Outlook проверяло входящие сообщения в момент их поступления в почтовый ящик.
   - Установите флажок **Проверять при прочтении**, если вы хотите, чтобы расширение компонента Почтовый Антивирус для программы Microsoft Office Outlook проверяло входящие сообщения в тот момент, когда пользователь открывает их для чтения.
   - Установите флажок **Проверять при отправке**, если вы хотите, чтобы расширение компонента Почтовый Антивирус для программы Microsoft Office Outlook проверяло исходящие сообщения в момент их отправки.

10. Нажмите на кнопку **ОК** в окне **Защита почты**.
11. Нажмите на кнопку **ОК** в окне **Почтовый Антивирус**.
12. Нажмите на кнопку **Применить**.

Настройка проверки почты в Microsoft Office Outlook

Настройка параметров Почтового Антивируса из программы Microsoft Office Outlook доступна в том случае, если в свойствах политики Легкого агента для Windows или локальном интерфейсе Легкого агента установлен флажок **Дополнительно: расширение в Microsoft Office Outlook** (см. раздел "**Формирование области защиты Почтового Антивируса**" на стр. 229).

► *Чтобы перейти к настройке проверки почты в программе Microsoft Office Outlook, выполните следующие действия:*

1. Откройте главное окно программы Microsoft Office Outlook.

   В верхнем левом углу выберите закладку **Файл**.

2. Нажмите на кнопку **Параметры**.

   Откроется окно **Параметры Outlook**.

3. Выберите раздел **Надстройки**.

   В правой части окна отобразятся параметры плагинов, встроенных в программу Microsoft Office Outlook.

4. Нажмите на кнопку **Параметры надстроек**.

   Откроется окно **Параметры надстроек**.

Защита веб-трафика виртуальной машины. Веб-Антивирус

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с операционной системой Windows для рабочих станций.

Выключение компонента приводит к выходу программы из сертифицированного состояния. Настройка некоторых параметров работы компонента может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Каждый раз при работе в интернете вы подвергаете информацию, хранящуюся на виртуальной машине, риску заражения вирусами и другими вредоносными программами. Они могут проникать на виртуальную машину, когда вы скачиваете бесплатные программы или просматриваете информацию на веб-сайтах, которые до вашего посещения подверглись атаке хакеров. Сетевые черви могут проникнуть на вашу виртуальную машину до открытия веб-страницы или скачивания файла, то есть непосредственно в момент установки соединения с интернетом.

Веб-Антивирус проверяет веб-адреса по базам вредоносных и фишинговых веб-адресов и защищает веб-трафик, поступающий на виртуальную машину и отправляемый с нее.

Веб-Антивирус может проверять веб-трафик, передаваемый по защищенным соединениям (см. раздел "Проверка защищенных соединений" на стр. 252).

Веб-Антивирус перехватывает и анализирует на присутствие вирусов и других вредоносных программ каждую веб-страницу или файл, к которому вы или некоторая программа обращаетесь по протоколам HTTP, FTP, а также HTTPS, FTPS, WS и WSS, если включена проверка защищенных соединений (на стр. 252). Далее происходит следующее:

- если на веб-странице или в файле не обнаружен вредоносный код, они сразу же становятся доступными для вас;
- если веб-страница или файл содержат вредоносный код, программа выполняет действие (см. раздел "Изменение действия над вредоносными объектами веб-трафика" на стр. 241), заданное в параметрах Веб-Антивируса.

Вы можете выполнить следующие действия для настройки работы Веб-Антивируса:

- Изменить уровень безопасности веб-трафика (см. раздел "Изменение уровня безопасности веб-трафика" на стр. 240).
- Изменить действие (см. раздел "Изменение действия над вредоносными объектами веб-трафика" на стр. 241), которое программа выполняет над вредоносными объектами веб-трафика.
- Настроить проверку Веб-Антивирусом веб-адресов по базам фишинговых и вредоносных веб-адресов (см. раздел "Проверка веб-адресов по базам фишинговых и вредоносных веб-адресов" на стр. 242).
- Настроить использование эвристического анализа (см. раздел "Использование эвристического анализа в работе Веб-Антивируса" на стр. 243) при антивирусной проверке веб-трафика, а также для обнаружения фишинговых веб-адресов.
- Сформировать список доверенных веб-адресов (см. раздел "Формирование списка доверенных веб-адресов" на стр. 244).

Под веб-адресом подразумевается адрес как отдельной веб-страницы, так и веб-сайта.

В этом разделе

Включение и выключение Веб-Антивируса

По умолчанию Веб-Антивирус включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Веб-Антивирус при необходимости.

► *Чтобы включить или выключить Веб-Антивирус через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел

Веб-Антивирус.

В правой части окна отобразятся параметры компонента Веб-Антивирус.

6. Выполните одно из следующих действий:
   - Установите флажок **Веб-Антивирус**, если вы хотите включить компонент Веб-Антивирус.
   - Снимите флажок **Веб-Антивирус**, если вы хотите выключить компонент Веб-Антивирус.
7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

► *Чтобы включить или выключить Веб-Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.
4. По правой клавише мыши откройте контекстное меню строки **Веб-Антивирус** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Веб-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Веб-Антивирус**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Веб-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Веб-Антивирус**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

► *Чтобы включить или выключить Веб-Антивирус из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить Веб-Антивирус**, если вы хотите включить компонент Веб-Антивирус.
   - Снимите флажок **Включить Веб-Антивирус**, если вы хотите выключить компонент Веб-Антивирус.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение уровня безопасности веб-трафика

Для защиты веб-трафика Веб-Антивирус применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности веб-трафика*. Предусмотрено три уровня безопасности веб-трафика: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности веб-трафика **Рекомендуемый** считаются оптимальными и рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности веб-трафика через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
6. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности веб-трафика (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите настроить уровень безопасности веб-трафика самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Веб-Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности веб-трафика, название уровня безопасности веб-трафика в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности веб-трафика на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

► *Чтобы изменить уровень безопасности веб-трафика в локальном интерфейсе, выполните*

следующие действия:

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности веб-трафика (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите настроить уровень безопасности веб-трафика самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Веб-Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности веб-трафика, название уровня безопасности веб-трафика в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности веб-трафика на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия над вредоносными объектами веб-трафика

► *Чтобы изменить через Kaspersky Security Center действие над вредоносными объектами веб-трафика, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
6. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое программа выполняет над вредоносными объектами веб-трафика:
   - **Выбирать действие автоматически**.
   - **Запрещать загрузку**.
   - **Разрешать загрузку**.

   По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Запрещать загрузку**.
7. Нажмите на кнопку **Применить**.

► *Чтобы изменить действие над вредоносными объектами веб-трафика в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Security выполняет над вредоносными объектами веб-трафика:
   - **Выбирать действие автоматически**.
   - **Запрещать загрузку**.
   - **Разрешать загрузку**.

   По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Запрещать загрузку**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка веб-адресов по базам фишинговых и вредоносных веб-адресов

База вредоносных веб-адресов содержит список веб-ресурсов, содержимое которых может быть расценено как опасное.

Проверка веб-адресов по базе фишинговых веб-адресов позволяет избежать *фишинг-атак*. Частным примером фишинг-атаки может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадете на точную копию веб-сайта банка, адрес которого, на первый взгляд, не отличается от адреса оригинального веб-сайта. Однако вы находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия будут отслеживаться и могут быть использованы для кражи ваших денежных средств.

Веб-Антивирус отслеживает попытки перейти на фишинговый веб-сайт во время проверки веб-трафика и блокирует доступ к таким веб-сайтам.

Списки фишинговых и вредоносных веб-адресов включены в комплект поставки программы Kaspersky Security и обновляются в процессе обновления баз программы.

► *Чтобы настроить проверку веб-адресов по базам фишинговых и вредоносных веб-адресов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел

Веб-Антивирус.

В правой части окна отобразятся параметры компонента Веб-Антивирус.

6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.

7. В окне **Веб-Антивирус** на закладке **Общие** выполните следующие действия:

   - В блоке **Методы проверки** установите флажок **Проверять веб-адреса по базе вредоносных веб-адресов**, если вы хотите, чтобы Веб-Антивирус проверял веб-адреса по базам вредоносных веб-адресов.
   - В блоке **Параметры антифишинга** установите флажок **Проверять веб-адреса по базе фишинговых веб-адресов**, если вы хотите, чтобы Веб-Антивирус проверял веб-адреса по базам фишинговых веб-адресов.

   Для проверки веб-адресов по базам фишинговых и вредоносных веб-адресов вы также можете использовать репутационные базы Kaspersky Security Network.

8. Нажмите на кнопку **OK** в окне **Веб-Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы настроить проверку веб-адресов по базам фишинговых и вредоносных веб-адресов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе Веб-Антивируса

Для повышения эффективности защиты вы можете использовать эвристический анализ в работе Веб-Антивируса. В процессе эвристического анализа Kaspersky Security анализирует активность программ в операционной системе защищенной виртуальной машины. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

► *Чтобы настроить через Kaspersky Security Center использование эвристического анализа в работе Веб-Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
7. В окне **Веб-Антивирус** на закладке **Общие** выполните следующие действия:
   - Если вы хотите, чтобы Веб-Антивирус использовал эвристический анализ при проверке веб-трафика на вирусы и другие вредоносные программы, в блоке **Методы проверки** установите флажок **Эвристический анализ для обнаружения вирусов** и с помощью ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы Веб-Антивирус использовал эвристический анализ при проверке веб-адресов, в блоке **Параметры антифишинга** установите флажок **Эвристический анализ для обнаружения фишинговых веб-адресов**.
8. Нажмите на кнопку **OK** в окне **Веб-Антивирус**.
9. Нажмите на кнопку **Применить**.

► *Чтобы настроить использование эвристического анализа в работе Веб-Антивируса в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–8 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка доверенных веб-адресов

Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Веб-Антивирус не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других

вредоносных программ. Такая возможность может быть использована, например, в том случае, если Веб-Антивирус препятствует загрузке файла с известного вам веб-сайта.

► *Чтобы сформировать список доверенных веб-адресов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
7. В окне **Веб-Антивирус** на закладке **Доверенные веб-адреса** установите флажок **Не проверять веб-трафик с доверенных веб-адресов**.
8. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете. Для этого выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Адрес / Маска адреса**.
   b. Введите адрес веб-сайта / веб-страницы или маску адреса веб-сайта / веб-страницы.
   c. Нажмите на кнопку **ОК**.

      В списке доверенных веб-адресов появится новая запись.
   d. Если требуется, повторите пункты a–c этой инструкции.
9. Нажмите на кнопку **ОК** в окне **Веб-Антивирус**.
10. Нажмите на кнопку **Применить**.

► *Чтобы сформировать список доверенных веб-адресов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–9 предыдущей инструкции.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль сетевого трафика

Во время работы программы Kaspersky Security компоненты Почтовый Антивирус, Веб-Антивирус и Веб-Контроль контролируют сетевой трафик защищенных виртуальных машин.

Вы можете настроить следующие общие параметры контроля сетевого трафика:

- параметры контроля открытых TCP- и UDP-портов (см. раздел "Контроль сетевых портов" на стр. 247) защищенной виртуальной машины;
- параметры проверки трафика, передаваемого по защищенным соединениям (см. раздел "Проверка защищенных соединений" на стр. 252).

В этом разделе

Контроль сетевых портов

Во время работы программы Kaspersky Security компоненты Почтовый Антивирус, Веб-Антивирус и Веб-Контроль могут контролировать потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты защищенной виртуальной машины. Например, Почтовый Антивирус анализирует информацию, передаваемую по SMTP-протоколу, а Веб-Антивирус анализирует информацию, передаваемую по протоколам HTTP и FTP.

Kaspersky Security подразделяет TCP- и UDP-порты операционной системы на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для уязвимых служб, рекомендуется контролировать более тщательно, так как эти сетевые порты с большей вероятностью могут являться целью сетевой атаки. Если вы используете нестандартные службы, которым отведены нестандартные сетевые порты, эти сетевые порты также могут являться целью для атакующего компьютера. Вы можете задать список сетевых портов и список программ, запрашивающих сетевой доступ, на которые компоненты Почтовый Антивирус и Веб-Антивирус должны обращать особое внимание во время слежения за сетевым трафиком.

Вы можете выполнить следующие действия для настройки параметров контроля сетевых портов:

- Выбрать режим контроля сетевых портов (см. раздел "Выбор режима контроля сетевых портов" на стр. 248).
- Сформировать список контролируемых сетевых портов (см. раздел "Формирование списка контролируемых сетевых портов" на стр. 249).
- Сформировать список программ, для которых контролируются все сетевые порты (см. раздел "Формирование списка программ, для которых контролируются все сетевые порты" на стр. 250).

kaspersky

В этом разделе

Выбор режима контроля сетевых портов

► *Чтобы выбрать через Kaspersky Security Center режим контроля сетевых портов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.
6. В блоке **Контролируемые порты** выберите режим контроля сетевых портов:
   - Есть вы хотите, чтобы компоненты Kaspersky Security контролировали потоки данных, передаваемые через любые открытые TCP- и UDP-порты виртуальной машины, выберите вариант **Контролировать все сетевые порты**.
   - Есть вы хотите, чтобы компоненты Kaspersky Security контролировали потоки данных, передаваемые через выбранные по умолчанию и указанные вами сетевые порты виртуальной машины, выберите вариант **Контролировать только выбранные порты**. Вы можете настроить список контролируемых портов (см. раздел "Формирование списка контролируемых сетевых портов" на стр. 249) и / или список программ, для которых контролируются порты (см. раздел "Формирование списка программ, для которых контролируются все сетевые порты" на стр. 250), в окне **Сетевые порты**. Окно **Сетевые порты** открывается по кнопке **Настройка**.

     Этот режим контроля сетевых портов используется по умолчанию.
7. Нажмите на кнопку **Применить**.

► *Чтобы выбрать в локальном интерфейсе режим контроля сетевых портов, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункт 6 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка контролируемых сетевых портов

Если используется режим контроля сетевых портов (см. раздел "Выбор режима контроля сетевых портов" на стр. 248) "Контролировать только выбранные порты", то вы можете настроить список контролируемых портов. По умолчанию список настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского".

► *Чтобы сформировать через Kaspersky Security Center список контролируемых сетевых портов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.
6. В правой части окна в блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты**.
7. Нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые порты**. Окно **Сетевые порты** содержит список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика.
8. В списке сетевых портов выполните следующие действия:
   - Установите флажки напротив названий тех сетевых портов, которые вы хотите включить в список контролируемых сетевых портов.

     По умолчанию флажки установлены для всех сетевых портов, представленных в окне **Сетевые порты**.
   - Снимите флажки напротив названий тех сетевых портов, которые вы хотите исключить из списка контролируемых сетевых портов.
9. Если нужный сетевой порт отсутствует в списке сетевых портов, вы можете добавить его. Для этого выполните следующие действия:

   a. По ссылке **Добавить**, расположенной под списком сетевых портов, откройте окно **Сетевой порт**.

b. В поле **Порт** введите номер сетевого порта.

c. В поле **Описание** введите название сетевого порта.

d. Нажмите на кнопку **OK** в окне **Сетевой порт**.

Добавленный сетевой порт отобразится в конце списка сетевых портов.

10. Нажмите на кнопку **OK** в окне **Сетевые порты**.
11. Нажмите на кнопку **Применить**.

► *Чтобы сформировать в локальном интерфейсе список контролируемых сетевых портов, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–10 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Во время работы протокола FTP в пассивном режиме соединение может устанавливаться через случайный сетевой порт, который не добавлен в список контролируемых сетевых портов. Чтобы защищать такие соединения, нужно включить контроль для всех сетевых портов (см. раздел "Выбор режима контроля сетевых портов" на стр. 248) или настроить контроль всех сетевых портов для программ (см. раздел "Формирование списка программ, для которых контролируются все сетевые порты" на стр. 250), с помощью которых устанавливается FTP-соединение.

Формирование списка программ, для которых контролируются все сетевые порты

Если используется режим контроля сетевых портов (см. раздел "Выбор режима контроля сетевых портов" на стр. 248) "Контролировать только выбранные порты", то вы можете сформировать список программ, для которых программа Kaspersky Security контролирует все сетевые порты.

В список программ, для которых программа Kaspersky Security контролирует все сетевые порты, рекомендуется включить программы, которые принимают или передают данные по протоколу FTP.

► *Чтобы сформировать через Kaspersky Security Center список программ, для которых*

контролируются все сетевые порты, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.
6. В правой части окна в блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты**.
7. Нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые порты**.
8. Установите флажок **Контролировать все порты для указанных программ**.
9. В списке программ, расположенном под флажком **Контролировать все порты для указанных программ**, выполните следующие действия:
   - Установите флажки напротив названий программ, для которых нужно контролировать все сетевые порты.

     По умолчанию флажки установлены для всех программ, представленных в окне **Сетевые порты**.
   - Снимите флажки напротив названий программ, для которых не нужно контролировать сетевые порты.
10. Если нужная программа отсутствует в списке программ, вы можете добавить ее. Для этого выполните следующие действия:
    a. По ссылке **Добавить**, расположенной под списком программ, откройте окно **Программа**.
    b. В поле **Путь** введите путь к исполняемому файлу программы.
    c. В поле **Название** введите название программы.
    d. Нажмите на кнопку **OK** в окне **Программа**.

       Добавленная программа отобразится в конце списка программ в окне **Сетевые порты**.
11. Нажмите на кнопку **OK** в окне **Сетевые порты**.
12. Нажмите на кнопку **Применить**.

► *Чтобы сформировать в локальном интерфейсе список программ, для которых контролируются все сетевые порты, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных

соединений.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты**.
4. Выполните пункты 6–9 предыдущей инструкции.
5. Если нужная программа отсутствует в списке программ, вы можете добавить ее. Для этого выполните следующие действия:
   a. По ссылке **Добавить**, расположенной под списком программ, откройте контекстное меню.
   b. Выберите способ добавления программы в список программ:
      - Выберите пункт **Программы**, если вы хотите выбрать программу из списка программ, установленных на защищенной виртуальной машине.

        Откроется окно, в котором вы можете выбрать название программы.
      - Выберите пункт **Обзор**, если вы хотите указать местонахождение исполняемого файла программы.

        Откроется окно, в котором вы можете указать путь к исполняемому файлу программы.
   c. После выбора программы откроется окно **Программа**.
   d. В поле **Название** введите название для выбранной программы.
   e. Нажмите на кнопку **OK**.

      Добавленная программа отобразится в конце списка программ в окне **Сетевые порты**.
6. Нажмите на кнопку **OK** в окне **Сетевые порты**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка защищенных соединений

Программа Kaspersky Security позволяет проверять трафик, передаваемый по защищенным соединениям, которые установлены с использованием следующих протоколов: TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0 и SSL 3.0.

Программа не контролирует трафик, передаваемый по защищенным соединениям с использованием протокола TLS 1.3, если в TLS 1.3 используется технология Encrypted Server Name Indication.

Программа не контролирует трафик, передаваемый по защищенным соединениям с использованием протокола SSL 2.0.

По умолчанию Kaspersky Security перехватывает трафик, передаваемый по защищенным соединениям,

расшифровывает его и передает на проверку компонентам Почтовый Антивирус, Веб-Антивирус и Веб-Контроль. Компоненты Kaspersky Security обрабатывают трафик в соответствии с настроенными для них параметрами.

Если проверка защищенных соединений выключена, в работе компонентов программы имеются следующие ограничения:

- Почтовый Антивирус не проверяет сообщения, получаемые или отправляемые по протоколам, которые обеспечивают защищенную передачу данных.
- Веб-Антивирус не проверяет веб-страницы и файлы, доступ к которым выполняется по защищенным соединениям.
- Веб-Контроль во время контроля доступа к веб-ресурсам по защищенным соединениям не применяет правила доступа, в которых используются фильтры по содержанию.

Если при проверке защищенного соединения возникает ошибка, соединение с веб-ресурсом разрывается. При этом по умолчанию Kaspersky Security добавляет доменное имя веб-ресурса в список доменов, проверка защищенных соединений с которыми завершается с ошибкой. Все веб-ресурсы доменов, находящихся в этом списке, исключаются из проверки защищенных соединений. При повторном обращении к веб-ресурсам этого домена Kaspersky Security разрешает установить соединение, но не выполняет расшифровку и проверку трафика. Вы можете настроить действие (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 256), которое выполняет Kaspersky Security при возникновении ошибки проверки защищенного соединения.

При расшифровке трафика Kaspersky Security проверяет сертификат веб-ресурса, с которым устанавливается защищенное соединение. По умолчанию при обнаружении ошибки сертификата Kaspersky Security разрешает установить соединение. При этом, если соединение устанавливается через браузер, на экран выводится предупреждение об ошибке сертификата. Вы можете настроить действие (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 256), которое выполняет Kaspersky Security при обнаружении ошибки сертификата веб-ресурса.

Kaspersky Security не проверяет защищенные соединения, которые входят в список предустановленных исключений (см. раздел "Просмотр списка предустановленных исключений" на стр. 255) из проверки защищенных соединений. Список предустановленных исключений сформирован специалистами "Лаборатории Касперского", входит в комплект поставки программы Kaspersky Security и обновляется автоматически при обновлении баз программы. Вы можете посмотреть список предустановленных исключений в локальном интерфейсе Легкого агента для Windows.

Вы можете настроить также следующие исключения из проверки защищенных соединений:

- Исключение веб-ресурсов доверенных доменов (см. раздел "Исключение веб-ресурсов из проверки защищенных соединений" на стр. 258). Kaspersky Security не расшифровывает трафик и не проверяет сертификаты веб-ресурсов, если защищенное соединение установлено с веб-ресурсом домена, добавленного в список доверенных доменов.
- Исключение доверенных программ (см. раздел "Исключение программ из проверки защищенных соединений" на стр. 259). Kaspersky Security не расшифровывает трафик и не проверяет сертификаты веб-ресурсов, если защищенное соединение инициировано программой, для которой настроено исключение из проверки зашифрованного трафика.

В ходе проверки защищенных соединений используется сертификат "Лаборатории Касперского". Этот сертификат автоматически устанавливается в хранилище доверенных сертификатов на защищенной виртуальной машине в результате установки программы Kaspersky Security и удаляется при удалении программы.

Kaspersky Security изменяет параметры браузера Mozilla™ Firefox™ на защищенной виртуальной машине, чтобы браузер использовал системное хранилище доверенных сертификатов.

В этом разделе

Включение и выключение проверки защищенных соединений

По умолчанию проверка защищенных соединений включена и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить проверку защищенных соединений при необходимости.

► *Чтобы включить или выключить через Kaspersky Security Center проверку защищенных соединений, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.
6. В правой части окна в блоке **Проверка защищенных соединений** выполните одно из следующих действий:
   - Установите флажок **Проверять защищенные соединения**, если вы хотите, чтобы компоненты Kaspersky Security проверяли трафик, передаваемый по защищенным соединениям.
   - Снимите флажок **Проверять защищенные соединения**, если не требуется расшифровывать и проверять трафик, передаваемый по защищенным соединениям.
7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить в локальном интерфейсе проверку защищенных соединений, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункт 6 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Просмотр списка предустановленных исключений

Список предустановленных исключений содержит соединения, которые могут устанавливаться между программами и веб-ресурсами доменов. Для этих соединений не предусмотрена возможность расшифровки трафика, поэтому Kaspersky Security не проверяет эти соединения в ходе проверки защищенных соединений.

Вы можете посмотреть список предустановленных исключений из проверки защищенных соединений в локальном интерфейсе Легкого агента для Windows. Список сформирован специалистами "Лаборатории Касперского" и обновляется автоматически при обновлении баз программы.

► *Чтобы посмотреть список предустановленных исключений из проверки защищенных соединений, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.

3. В блоке **Проверка защищенных соединений** перейдите по ссылке, чтобы открыть окно **Предустановленные исключения из проверки защищенных соединений**.

Соединения в списке заданы с помощью следующих условий:

- Домен, с которым устанавливается соединение. Домен может быть задан с помощью маски. Символ * в маске заменяет любую последовательность из нуля или более символов. Если домен не указан или в графе **Домен** указана маска *, то из проверки исключаются соединения с любым доменом.
- Имя исполняемого файла программы, которая устанавливает соединение. Если программа не указана, то из проверки исключаются соединения, инициированные программами с любым именем исполняемого файла.
- Издатель программы, которая устанавливает соединение. Если издатель не указан, то из проверки исключаются соединения, инициированные программами любого издателя.
- Владелец цифровой подписи программы, которая устанавливает соединение. Если владелец

цифровой подписи не указан, то из проверки исключаются соединения, инициированные программами независимо от их цифровой подписи.

Настройка параметров проверки защищенных соединений

Вы можете настраивать параметры проверки защищенных соединений через Kaspersky Security Center или в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить через Kaspersky Security Center параметры проверки защищенных соединений, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.
6. В правой части окна в блоке **Проверка защищенных соединений** нажмите на кнопку **Параметры проверки**.

   Откроется окно **Параметры проверки защищенных соединений**.
7. Выберите действие, которое Kaspersky Security выполняет при обнаружении ошибки сертификата веб-ресурса:
   - **Разрешать**. Kaspersky Security разрешает установить соединение с веб-ресурсом.

     Если соединение устанавливается через браузер, то при переходе на веб-сайт с ошибкой сертификата откроется HTML-страница с предупреждением о том, что этот веб-сайт не рекомендован для посещения, и с описанием обнаруженной ошибки сертификата. По ссылке на HTML-странице пользователь может перейти на запрошенный веб-сайт. После этого Kaspersky Security в течении часа не будет отображать предупреждения об ошибке сертификата этого веб-сайта, а также при обращении к другим ресурсам в том же домене.

     Это действие выбрано по умолчанию.
   - **Блокировать**. Kaspersky Security блокирует соединение с веб-ресурсом.

     Если соединение устанавливается через браузер, то при переходе на веб-сайт с ошибкой сертификата откроется HTML-страница с предупреждением о том, что переход на веб-сайт заблокирован, и с описанием обнаруженной ошибки сертификата.
8. Выберите действие, которое Kaspersky Security выполняет при возникновении ошибок проверки защищенного соединения:
   - **Исключать домен из проверки**. Если проверка защищенного соединения с веб-ресурсом завершилась с ошибкой, Kaspersky Security добавляет домен веб-ресурса в список доменов с ошибками защищенных соединений. Все веб-ресурсы доменов, находящихся в этом списке,

исключаются из проверки защищенных соединений. При повторном обращении к веб-ресурсам этого домена Kaspersky Security разрешает установить соединение, но не выполняет расшифровку и проверку трафика.

Это действие выбрано по умолчанию.

> Список доменов с ошибками проверки защищенных соединений доступен для просмотра в окне **Параметры проверки защищенных соединений** в локальном интерфейсе Легкого агента для Windows.

- **Разрывать соединение**. Если проверка защищенного соединения с веб-ресурсом завершилась с ошибкой, Kaspersky Security блокирует все последующие попытки соединения с этим веб-ресурсом.

> Если вы выбрали действие **Разрывать соединение**, все домены, ранее добавленные в список доменов с ошибками проверки защищенных соединений, автоматически удаляются из этого списка.

9. Если вы хотите, чтобы программа Kaspersky Security блокировала соединения, которые устанавливаются с использованием протоколов TLS 1.0, SSL 2.0 и SSL 3.0, установите флажок **Блокировать соединения по протоколам TLS 1.0, SSL 2.0 и SSL 3.0 (рекомендуется)**.

   По умолчанию программа Kaspersky Security не блокирует сетевые соединения, которые устанавливаются с использованием протоколов TLS 1.0, SSL 2.0 и SSL 3.0. При этом Kaspersky Security контролирует сетевой трафик, передаваемый по соединениям, которые устанавливаются с использованием протоколов TLS 1.0 и SSL 3.0. Сетевой трафик, передаваемый с использованием протокола SSL 2.0, не контролируется.

   > Протоколы TLS 1.0, SSL 2.0 и SSL 3.0 имеют недостатки, которые влияют на безопасность передачи данных.

10. Нажмите на кнопку **OK** в окне **Параметры проверки защищенных соединений**.
11. Нажмите на кнопку **Применить**.

► *Чтобы настроить в локальном интерфейсе параметры проверки защищенных соединений, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–10 предыдущей инструкции.

   По ссылке **Домены с ошибками проверки** в окне **Параметры проверки защищенных**

соединений вы можете посмотреть список доменов, проверка защищенных соединений с которыми завершается с ошибкой.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Исключение веб-ресурсов из проверки защищенных соединений

Kaspersky Security не расшифровывает трафик и не проверяет сертификаты безопасности для веб-ресурсов доверенных доменов. Вы можете сформировать список доверенных доменов через Kaspersky Security Center или в локальном интерфейсе Легкого агента для Windows.

► *Чтобы сформировать через Kaspersky Security Center список доверенных доменов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.
6. В правой части окна в блоке **Проверка защищенных соединений** нажмите на кнопку **Доверенные домены**.

   Откроется окно **Доверенные домены**.
7. Если вы хотите добавить домен в список доверенных доменов, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Домен**.
   b. Введите имя, IP-адрес или веб-адрес домена.

      Исключение из проверки не распространяется на веб-ресурсы поддоменов указанного домена. Если вы хотите исключить из проверки защищенных соединений веб-ресурсы поддоменов, введите маску домена в виде `*.example.com`.
   c. Нажмите на кнопку **OK** в окне **Домен**.

      Домен добавится в список доверенных доменов.

      По умолчанию все веб-ресурсы доменов, добавленных в список, исключаются из проверки защищенных соединений. Если требуется, вы можете временно отменить исключение из проверки для веб-ресурсов домена, не удаляя домен из списка доверенных доменов. Для этого снимите флажок напротив домена в списке.
8. Если вы хотите изменить имя или адрес доверенного домена, выполните следующие действия:
   a. Выберите домен в списке и нажмите на кнопку **Изменить**.

      Откроется окно **Домен**.

b. Введите новое доменное имя, IP-адрес, веб-адрес или маску домена в виде `*.example.com` и нажмите на кнопку **OK**.

9. Если вы хотите удалить домен из списка доверенных доменов, выберите его в списке и нажмите на кнопку **Удалить**.
10. Нажмите на кнопку **OK** в окне **Доверенные домены**.
11. Нажмите на кнопку **Применить**.

► *Чтобы сформировать в локальном интерфейсе список доверенных доменов, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–10 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Исключение программ из проверки защищенных соединений

Вы можете настраивать исключение из проверки защищенных соединений для программ через Kaspersky Security Center или в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить через Kaspersky Security Center исключения из проверки защищенных соединений для программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.
6. В правой части окна в блоке **Проверка защищенных соединений** нажмите на кнопку **Доверенные программы**.

   Откроется закладка **Доверенные программы** окна **Доверенная зона**.
7. Выберите программу, для которой вы хотите настроить исключение из проверки защищенных

соединений, одним из следующих способов:

- Если программа отсутствует в списке доверенных программ, нажмите на кнопку **Добавить**. В окне **Исключения для программы** укажите путь к исполняемому файлу программы.
- Если программа присутствует в списке доверенных программ, выберите ее и нажмите на кнопку **Изменить**.

8. В окне **Исключения для программы** настройте параметры проверки сетевого трафика, передаваемого для этой программы, с помощью флажка **Не проверять сетевой трафик** и ссылок, расположенных в нижней части окна.

   Вы можете настроить следующие параметры проверки трафика, передаваемого для этой программы:

   - исключать из проверки весь трафик или только зашифрованный трафик;
   - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных IP-адресов;
   - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных портов.

   Вы можете изменять эти параметры щелчком мыши по ссылке.

9. Нажмите на кнопку **OK** в окне **Исключения для программы**.
10. Нажмите на кнопку **OK** в окне **Доверенная зона**.
11. Нажмите на кнопку **Применить**.

► *Чтобы настроить в локальном интерфейсе исключения из проверки защищенных соединений для программ, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Контроль сетевого трафика**.

   В правой части окна отобразятся параметры контроля сетевых портов и проверки защищенных соединений.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выберите программу, для которой вы хотите настроить исключение из проверки защищенных соединений, одним из следующих способов:

   - Если программа отсутствует в списке доверенных программ, нажмите на кнопку **Добавить** и выберите программу с помощью одного из пунктов контекстного меню.
   - Если программа присутствует в списке доверенных программ, выберите ее и нажмите на кнопку **Изменить**.

4. В окне **Исключения для программы** настройте параметры проверки сетевого трафика, передаваемого для этой программы, с помощью флажка **Не проверять сетевой трафик** и ссылок, расположенных в нижней части окна.

   Вы можете настроить следующие параметры проверки трафика, передаваемого для этой программы:

- исключать из проверки весь трафик или только зашифрованный трафик;
- исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных IP-адресов;
- исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных портов.

Вы можете изменять эти параметры щелчком мыши по ссылке.

5. Нажмите на кнопку **OK** в окне **Исключения для программы**.
6. Нажмите на кнопку **OK** в окне **Доверенная зона**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Мониторинг системы

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с операционной системой Windows для серверов или с операционной системой Windows для рабочих станций.

Выключение компонента приводит к выходу программы из сертифицированного состояния. Настройка некоторых параметров работы компонента может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Компонент Мониторинг системы анализирует поведение программ на защищенной виртуальной машине и предоставляет эту информацию другим компонентам программы для повышения эффективности их работы.

Компонент Мониторинг системы использует *шаблоны опасного поведения программ* (Behavior Stream Signatures) (далее также "шаблоны опасного поведения"). Шаблоны опасного поведения содержат последовательности действий программ, которые программа Kaspersky Security классифицирует как опасные. Если активность программы соответствует одному из шаблонов опасного поведения, программа Kaspersky Security выполняет заданное действие (см. раздел "Изменение действия при обнаружении вредоносной активности программы" на стр. 266). Использование шаблонов опасного поведения позволяет обнаружить совсем новые и неизвестные вредоносные программы по их поведению и остановить их работу, что обеспечивает проактивную защиту виртуальной машины.

На основе информации, полученной компонентом Мониторинг системы, программа Kaspersky Security может выполнять откат действий (см. раздел "Откат действий вредоносных программ при лечении" на стр. 268), произведенных вредоносными программами в операционной системе. Откат действий вредоносной программы может быть инициирован Файловым Антивирусом (см. раздел "Защита файловой системы виртуальной машины. Файловый Антивирус" на стр. 197) или при антивирусной проверке.

Откат действий вредоносной программы не оказывает негативного влияния на работу операционной системы и целостность информации на защищенной виртуальной машине.

Компонент Мониторинг системы также может защищать папки общего доступа (см. раздел "Настройка защиты папок общего доступа от внешнего шифрования" на стр. 269) от внешнего шифрования, отслеживая операции, выполняемые с удаленного компьютера.

Компонент Мониторинг системы отслеживает операции только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы файловой системой EFS.

В этом разделе

Включение и выключение Мониторинга системы

По умолчанию компонент Мониторинг системы включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Мониторинг системы при необходимости.

Не рекомендуется выключать Мониторинг системы без необходимости, так как это снижает эффективность работы компонентов защиты, которые могут запрашивать данные, полученные Мониторингом системы, для уточнения обнаруженной угрозы.

► *Чтобы включить или выключить Мониторинг системы через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
6. Выполните одно из следующих действий:
   - Установите флажок **Мониторинг системы**, если вы хотите включить компонент Мониторинг системы.
   - Снимите флажок **Мониторинг системы**, если вы хотите выключить компонент Мониторинг системы.

7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

► *Чтобы включить или выключить Мониторинг системы на закладке Центр управления главного окна программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.
4. По правой клавише мыши откройте контекстное меню строки **Мониторинг системы** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Мониторинг системы.

     Значок статуса работы компонента , отображающийся слева в строке **Мониторинг системы**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Мониторинг системы.

     Значок статуса работы компонента , отображающийся слева в строке **Мониторинг системы**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

► *Чтобы включить или выключить Мониторинг системы из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Мониторинг системы**, если вы хотите включить компонент Мониторинг системы.
   - Снимите флажок **Включить Мониторинг системы**, если вы хотите выключить компонент

Мониторинг системы.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение защиты от эксплойтов

Эксплойт – это программный код, который использует какую-либо уязвимость в системе или программном обеспечении, чтобы выполнить на компьютере вредоносное действие. Эксплойты часто используются для установки вредоносного программного обеспечения на компьютере без ведома пользователя. Эксплойты чаще всего атакуют браузеры, а также программы Adobe® Flash®, Java и Microsoft Office.

Защита от эксплойтов включает в себя следующие методы:

- Контроль запуска исполняемых файлов из уязвимых программ и браузеров.
- Контроль подозрительных действий уязвимых программ.
- Мониторинг действий программ.
- Отслеживание источника вредоносного кода.
- Предотвращение использования уязвимостей программ.

Списки программ с обнаруженными уязвимостями обновляются вместе с базами программы Kaspersky Security.

По умолчанию защита от эксплойтов включена. Вы можете выключить защиту от эксплойтов при необходимости.

► *Чтобы включить или выключить защиту от эксплойтов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
6. В блоке **Общие параметры** выполните одно из следующих действий:
   - Установите флажок **Включить защиту от эксплойтов**, если вы хотите, чтобы программа Kaspersky Security отслеживала исполняемые файлы, запускаемые уязвимыми программами.

     Если программа Kaspersky Security обнаруживает, что исполняемый файл из уязвимой программы запущен не пользователем, она блокирует запуск этого файла.
   - Снимите флажок **Включить защиту от эксплойтов**, если вы не хотите, чтобы программа Kaspersky Security отслеживала исполняемые файлы, запускаемые уязвимыми программами.
7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить защиту от эксплойтов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить защиту от эксплойтов**, если вы хотите, чтобы программа Kaspersky Security отслеживала исполняемые файлы, запускаемые уязвимыми программами.

     Если программа Kaspersky Security обнаруживает, что исполняемый файл из уязвимой программы запущен не пользователем, она блокирует запуск этого файла.
   - Снимите флажок **Включить защиту от эксплойтов**, если вы не хотите, чтобы программа Kaspersky Security отслеживала исполняемые файлы, запускаемые уязвимыми программами.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия при обнаружении вредоносной активности программы

При обнаружении вредоносной активности программы Kaspersky Security выполняет действие, заданное в параметрах компонента Мониторинг системы. По умолчанию при обнаружении вредоносной активности программы Kaspersky Security завершает работу вредоносной программы и удаляет исполняемый файл этой программы.

► *Чтобы изменить действие Мониторинга системы через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
6. В блоке **Проактивная защита** в раскрывающемся списке **При обнаружении вредоносной активности программы** выберите нужное действие:
   - **Выбирать действие автоматически**. Если выбран этот элемент, то при обнаружении

вредоносной активности программы Kaspersky Security выполняет действия, установленные специалистами "Лаборатории Касперского" по умолчанию: завершает работу вредоносной программы и удаляет исполняемый файл этой программы.

Этот вариант действия выбран по умолчанию.

- **Завершать работу вредоносной программы и удалять исполняемый файл**. Если выбран этот элемент, то при обнаружении вредоносной активности программы Kaspersky Security завершает работу этой программы и удаляет исполняемый файл этой программы.
- **Завершать работу вредоносной программы**. Если выбран этот элемент, то при обнаружении вредоносной активности программы Kaspersky Security завершает работу этой программы.
- **Пропускать**. Если выбран этот элемент, то при обнаружении вредоносной активности программы Kaspersky Security не выполняет действий над исполняемым файлом этой программы.

7. Нажмите на кнопку **Применить**.

► *Чтобы изменить действие Мониторинга системы в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. В блоке **Проактивная защита** в раскрывающемся списке **При обнаружении вредоносной активности программы** выберите нужное действие:
   - **Выбирать действие автоматически**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, программа Kaspersky Security выполняет действия, установленные специалистами "Лаборатории Касперского" по умолчанию: Kaspersky Security завершает работу вредоносной программы и удаляет исполняемый файл этой программы.

     Этот вариант действия выбран по умолчанию.
   - **Завершать работу вредоносной программы и удалять исполняемый файл**. Если выбран этот элемент, то при обнаружении вредоносной активности программы Kaspersky Security завершает работу этой программы и удаляет исполняемый файл этой программы.
   - **Завершать работу вредоносной программы**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, программа Kaspersky Security завершает работу этой программы.
   - **Пропускать**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, программа Kaspersky Security не выполняет действий над исполняемым файлом этой программы.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Откат действий вредоносных программ при лечении

► *Чтобы включить или выключить откат действий вредоносных программ через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
6. В блоке **Откат действий вредоносных программ** выполните одно из следующих действий:
   - Установите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы программа Kaspersky Security выполняла откат действий, которые вредоносные программы совершили в операционной системе.
   - Снимите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы программа Kaspersky Security не выполняла откат действий, которые вредоносные программы совершили в операционной системе.
7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить откат действий вредоносных программ в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. В блоке **Откат действий вредоносных программ** выполните одно из следующих действий:
   - Установите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы программа Kaspersky Security выполняла откат действий, которые вредоносные программы совершили в операционной системе.
   - Снимите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы программа Kaspersky Security не выполняла откат действий, которые вредоносные программы совершили в операционной системе.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка защиты папок общего доступа от внешнего шифрования

Функция защиты папок общего доступа от внешнего шифрования обеспечивает анализ активности в папках общего доступа. Kaspersky Security отслеживает следующие операции, выполняемые с удаленного компьютера:

- удаление файла;
- изменение содержимого файла;
- изменение размера файла;
- перемещение файла.

Kaspersky Security отслеживает операции только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы файловой системой EFS.

При обнаружении попытки изменения файлов в папках общего доступа Kaspersky Security создает резервные копии измененных файлов и анализирует обнаруженную активность. Если активность в папках общего доступа совпадает с одним из шаблонов опасного поведения, характерного для внешнего шифрования, Kaspersky Security выполняет выбранное действие (см. раздел "Изменение действия при обнаружении внешнего шифрования папок общего доступа" на стр. 271). По умолчанию при обнаружении внешнего шифрования папок общего доступа Kaspersky Security блокирует сетевую активность компьютера, осуществляющего шифрование, а также записывает в отчет локального интерфейса (см. раздел "Работа с отчетами в локальном интерфейсе" на стр. 431) и отправляет в Kaspersky Security Center информацию об обнаруженной вредоносной активности.

Если в параметрах Мониторинга системы включен откат действий вредоносных программ (см. раздел "Откат действий вредоносных программ при лечении" на стр. 268), то при обнаружении внешнего шифрования файлов в папках общего доступа Kaspersky Security также может восстановить измененные файлы из резервных копий. Информация об этом также записывается в отчет локального интерфейса и отправляется в Kaspersky Security Center.

Вы можете выполнить следующие действия для настройки защиты папок общего доступа от внешнего шифрования:

- изменить действие (см. раздел "Изменение действия при обнаружении внешнего шифрования папок общего доступа" на стр. 271), которое Kaspersky Security выполняет при обнаружении внешнего шифрования папок общего доступа;
- настроить исключения (см. раздел "Настройка исключений из защиты от внешнего шифрования" на стр. 272) из защиты папок общего доступа от внешнего шифрования.

В этом разделе

Включение и выключение защиты папок общего доступа от внешнего шифрования

По умолчанию защита папок общего доступа от внешнего шифрования включена.

> После установки программы Kaspersky Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки виртуальной машины.

► *Чтобы включить или выключить защиту папок общего доступа от внешнего шифрования через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
6. В блоке **Общие параметры** выполните одно из следующих действий:
   - Установите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы хотите, чтобы программа Kaspersky Security отслеживала операции с файлами в папках общего доступа, выполняемые с удаленного компьютера.
   - Снимите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы не хотите, чтобы программа Kaspersky Security отслеживала операции с файлами в папках общего доступа, выполняемые с удаленного компьютера.
7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить защиту папок общего доступа от внешнего шифрования в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы хотите, чтобы программа Kaspersky Security отслеживала операции с файлами в папках

общего доступа, выполняемые с удаленного компьютера.

- Снимите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы не хотите, чтобы программа Kaspersky Security отслеживала операции с файлами в папках общего доступа, выполняемые с удаленного компьютера.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия при обнаружении внешнего шифрования папок общего доступа

По умолчанию при обнаружении шифрования файлов в папках общего доступа программа Kaspersky Security блокирует сетевую активность компьютера, осуществляющего шифрование, а также записывает в отчет локального интерфейса (см. раздел "Работа с отчетами в локальном интерфейсе" на стр. 431) и отправляет в Kaspersky Security Center информацию об обнаруженной вредоносной активности. Если в параметрах Мониторинга системы включен откат действий вредоносных программ (см. раздел "Откат действий вредоносных программ при лечении" на стр. 268), то Kaspersky Security также может восстановить измененные файлы из резервных копий.

Вы можете изменить действие, которое программа Kaspersky Security будет выполнять при обнаружении внешнего шифрования папок общего доступа.

► *Чтобы выбрать действие Мониторинга системы через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
6. В блоке **Общие параметры** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры**.
7. В окне **Параметры** выберите нужное действие:

   - **Информировать**.

     Если выбран этот вариант, то при обнаружении шифрования файлов в папках общего доступа Kaspersky Security записывает в отчет локального интерфейса и отправляет в Kaspersky Security Center информацию об обнаруженной вредоносной активности, а также добавляет информацию об этом в список необработанных объектов.

     Kaspersky Security не восстанавливает измененные файлы из резервных копий, даже если в параметрах Мониторинга системы включен откат действий вредоносных программ (см. раздел "Откат действий вредоносных программ при лечении" на стр. 268).

   - **Блокировать соединение**.

     Если выбран этот вариант, то при обнаружении шифрования файлов в папках общего доступа

Kaspersky Security блокирует сетевую активность компьютера, осуществляющего шифрование, а также записывает в отчет локального интерфейса и отправляет в Kaspersky Security Center информацию об обнаруженной вредоносной активности. В поле **Блокировать соединение на N минут** вы можете указать время в минутах, на которое будет заблокировано сетевое соединение. По умолчанию установлено значение 60 минут.

Если в параметрах Мониторинга системы включен откат действий вредоносных программ (см. раздел "Откат действий вредоносных программ при лечении" на стр. 268), то Kaspersky Security также выполняет восстановление измененных файлов из резервных копий.

Этот вариант действия выбран по умолчанию.

Если сетевая активность компьютера была ранее заблокирована (выбрано действие **Блокировать соединение**), то при смене действия на **Информировать** она остается заблокированной на указанное время.

8. Нажмите на кнопку **OK** в окне **Параметры**.
9. Нажмите на кнопку **Применить**.

► *Чтобы выбрать действие Мониторинга системы в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Параметры**.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
4. Выполните пункты 7–8 предыдущей инструкции.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка исключений из защиты от внешнего шифрования

Вы можете исключить удаленный компьютер из защиты папок общего доступа от внешнего шифрования, добавив в список исключений имя или IP-адрес удаленного компьютера. Программа не будет отслеживать сетевую активность с этого компьютера в отношении папок общего доступа.

Для работы функциональности исключений из защиты папок общего доступа от внешнего шифрования требуется в политике безопасности Windows включить ведение аудита успешных попыток входа в систему (для параметра "Аудит событий входа в систему" установить флажок **Успех**). См. подробнее на сайте корпорации Microsoft (https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events).

Если вы добавили в список исключений из защиты папок общего доступа адрес удаленного компьютера, который подключался к папке общего доступа до запуска программы Kaspersky Security, для этого компьютера не будет применяться исключение. Вам нужно перезагрузить этот компьютер после запуска программы Kaspersky Security, чтобы не учитывать сетевую активность с этого компьютера при защите папок общего доступа от внешнего шифрования.

► *Чтобы исключить удаленный компьютер из защиты папок общего доступа от внешнего шифрования через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
6. В блоке **Общие параметры** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры**.
7. В окне **Параметры** нажмите на кнопку **Исключения**.

   Откроется окно **Исключения**.
8. В окне **Исключения** выполните одно из следующих действий:
   - Если вы хотите добавить IP-адрес или имя компьютера в список исключений, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить IP-адрес или имя компьютера, выберите его в списке исключений и нажмите на кнопку **Изменить**.

   Откроется окно **Компьютер**.
9. В окне **Компьютер** введите IP-адрес компьютера или имя компьютера, для которого не будут отслеживаться попытки изменения файлов в папках общего доступа.
10. Нажмите на кнопку **OK** в окне **Компьютер**.
11. Нажмите на кнопку **OK** в окне **Исключения**.
12. Нажмите на кнопку **Применить**.

► *Чтобы исключить удаленный компьютер из защиты папок общего доступа от внешнего шифрования в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента Мониторинг системы.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Параметры**.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

4. Выполните пункты 7–11 предыдущей инструкции.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль запуска программ

Описанная в этом разделе функциональность программы Kaspersky Security доступна на виртуальных машинах с операционными системами Windows для рабочих станций. Если программа установлена на виртуальной машине с операционной системой Windows для серверов, эта функциональность доступна, только если вы используете программу по расширенной лицензии.

Контроль запуска программ отслеживает попытки запуска программ на виртуальной машине и регулирует запуск программ с помощью *правил контроля запуска программ* (см. раздел "*О правилах контроля запуска программ*" на стр. 277).

Контроль запуска программ может работать в двух режимах:

- *Список запрещенных программ*. Режим, при котором Контроль запуска программ разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля запуска программ.
- *Список разрешенных программ*. Режим, при котором Контроль запуска программ запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля запуска программ. Таким образом, если правила контроля запуска программ сформированы максимально полно, Контроль запуска программ запрещает запуск всех новых, не проверенных администратором локальной сети организации программ, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

  Этот режим работы Контроля запуска программ настроен по умолчанию.

Для каждого режима работы Контроля запуска программ вы можете создать отдельные правила (см. раздел "Создание и изменение правила контроля запуска программ" на стр. 283), а также выбрать действие, которое Контроль запуска программ должен выполнять при обнаружении попытки запуска программы, не разрешенной правилом: информировать о запуске программы или блокировать запуск программы.

При блокировке запуска программы пользователь виртуальной машины может отправить жалобу администратору локальной сети организации по ссылке из текста сообщения о блокировке, если блокировка запуска программы, по мнению пользователя, произошла ошибочно. Для сообщения о блокировке запуска программы и для жалобы администратору на ошибочную блокировку предусмотрены шаблоны. Вы можете изменять шаблоны этих сообщений (см. раздел "Изменение шаблонов сообщений Контроля запуска программ" на стр. 287).

Все попытки запуска на защищенной виртуальной машине программ, не разрешенных правилами контроля запуска программ, фиксируются в отчетах.

По умолчанию компонент Контроль запуска программ выключен, вы можете включить Контроль запуска программ при необходимости (см. раздел "Включение и выключение Контроля запуска программ" на стр. 278).

kaspersky

Если вы используете программу Kaspersky Security для защиты виртуальной инфраструктуры на основе решения Citrix Virtual Apps and Desktops (Citrix XenApp and XenDesktop) и планируете использовать слои Citrix App Layer для сохранения данных пользователя, Контроль запуска программ может блокировать взаимодействие между Citrix Virtual Apps and Desktops и Citrix App Layer. Если вы хотите использовать Контроль запуска программ в режиме Список разрешенных программ, вам нужно создать разрешающее правило для файла LayerInfo.exe. Для этого вам нужно создать категорию программ, пополняемую вручную, добавить в нее путь c:\program files\unidesk\layering services\LayerInfo.exe и создать разрешающее правило на основе этой категории.

Настройка Контроля запуска программ осуществляется в Kaspersky Security Center. Вы можете выполнить следующие действия для настройки Контроля запуска программ в Kaspersky Security Center:

- Получить информацию о программах, которые установлены на защищенных виртуальных машинах локальной сети организации (см. раздел "Получение информации о программах, которые установлены на защищенных виртуальных машинах" на стр. 280).
- Создать и изменить правило контроля запуска программ (см. раздел "Создание и изменение правила контроля запуска программ" на стр. 283).
- Изменить статус работы правила контроля запуска программ (см. раздел "Изменение статуса работы правила контроля запуска программ" на стр. 285).
- Удалить правило контроля запуска программ (см. раздел "Удаление правила контроля запуска программ" на стр. 285).
- Настроить контроль запуска исполняемых модулей и драйверов (см. раздел "Настойка контроля запуска исполняемых модулей и драйверов" на стр. 286).
- Изменить шаблоны сообщений Контроля запуска программ (см. раздел "Изменение шаблонов сообщений Контроля запуска программ" на стр. 287).

В этом разделе

О правилах контроля запуска программ

Правило контроля запуска программ представляет собой набор параметров, необходимых для работы компонента Контроль запуска программ:

- Принадлежность программы к категории программ. *Категория программ* – это группа программ, обладающих общими признаками. Например, категория, в которую входят исполняемые файлы с выбранных защищенных виртуальных машин, или категория "Программы для работы", в которую входит стандартный набор программ, используемых в организации. Вы можете создавать категории на основе разных условий, в том числе на основе KL-категорий. KL-категория – это список программ, сформированный специалистами "Лаборатории Касперского". Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft Office, Adobe Acrobat® и другие. Подробнее о работе с категориями см. в документации Kaspersky Security Center.

  Если у файлов отсутствует цифровая подпись, компонент Контроль запуска программ не может определить KL-категорию для этих файлов и запрещает их запуск. Поэтому, если в параметрах компонента Контроль запуска программ выбрано действие "Блокировать", запуск файлов без цифровой подписи будет заблокирован. В случае, если вы хотите разрешить запуск каких-либо файлов без цифровой подписи, рекомендуется в параметрах компонента Контроль запуска программ выбрать действие (см. раздел "Создание и изменение правила контроля запуска программ" на стр. 283) "Информировать" и после получения события в Kaspersky Security Center добавить нужные файлы в предварительно созданную категорию программ.

- Разрешение или запрещение выбранным пользователям и / или группам пользователей запускать программы. Вы можете указать пользователя и / или группу пользователей, которым разрешен или запрещен запуск программ из указанной категории.

Для каждого режима работы Контроля запуска программ нужно создать отдельные правила, а также выбрать действие, которое Контроль запуска программ должен выполнять при обнаружении попытки запуска программы, не разрешенной правилом: информировать о запуске программы или блокировать запуск программы.

Статус работы правила контроля запуска программ

Правила контроля запуска программ могут иметь три статуса работы:

- *Вкл.* Статус работы правила означает, что правило включено.
- *Выкл*. Статус работы правила означает, что правило выключено.
- *Тест*. Статус работы правила означает, что Kaspersky Security не запрещает запуск программ, на которые распространяется действие правила, но фиксирует информацию о запуске этих программ в отчетах. Статус работы правила *Тест* удобно использовать для проверки работы сформированного правила контроля запуска программ. Пользователь не ограничен в запуске программ, удовлетворяющих правилу со статусом работы *Тест*. Разрешение или запрет на запуск программы формируются отдельно для тестовых и не тестовых правил.

По умолчанию после создания правило контроля запуска программ включено (имеет статус работы *Вкл)*. Вы можете выключить правило контроля запуска программ (см. раздел "Изменение статуса работы правила контроля запуска программ" на стр. 285). Если правило контроля запуска программ выключено, программа временно не применяет это правило.

Предустановленные правила контроля запуска программ

После установки программы Kaspersky Security по умолчанию созданы следующие правила контроля

запуска программ для режима работы Список разрешенных программ:

- **Доверенные программы обновления**. Правило разрешает всем пользователям запускать программы, которые установлены или обновлены программами из KL-категории "Доверенные программы обновления". В KL-категорию "Доверенные программы обновления" включены программы обновления наиболее известных производителей программного обеспечения. По умолчанию правило выключено.
- **Операционная система и ее компоненты**. Правило разрешает всем пользователям запускать программы, принадлежащие к KL-категории "Золотая категория". В KL-категорию "Золотая категория" включены программы, необходимые для запуска и работы операционной системы. По умолчанию правило включено.
- **Программы для виртуализации**. Правило разрешает всем пользователям запускать программы, принадлежащие к KL-категории "Программы для виртуализации". В KL-категорию "Программы для виртуализации" включены программы, предназначенные для виртуализации платформ и ресурсов. По умолчанию правило включено.

Действия с правилами контроля запуска программ

Вы можете выполнить следующие действия с правилами контроля запуска программ:

- Добавить новое правило (см. раздел "Создание и изменение правила контроля запуска программ" на стр. 283).
- Изменить правило (см. раздел "Создание и изменение правила контроля запуска программ" на стр. 283).
- Включить и выключить правило (см. раздел "Изменение статуса работы правила контроля запуска программ" на стр. 285).
- Удалить правило (см. раздел "Удаление правила контроля запуска программ" на стр. 285).

Вы не можете изменить или удалить предустановленные правила контроля запуска программ.

Включение и выключение Контроля запуска программ

По умолчанию Контроль запуска программ выключен, вы можете включить Контроль запуска программ при необходимости.

► *Чтобы включить или выключить Контроль запуска программ через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел

Контроль запуска программ.

В правой части окна отобразятся параметры компонента Контроль запуска программ.

6. Выполните одно из следующих действий:
   - Установите флажок **Контроль запуска программ**, если вы хотите включить компонент Контроль запуска программ.
   - Снимите флажок **Контроль запуска программ**, если вы хотите выключить компонент Контроль запуска программ.
7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

► *Чтобы включить или выключить Контроль запуска программ на закладке Центр управления главного окна программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки **Контроль запуска программ** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль запуска программ.

     Значок статуса работы компонента , отображающийся слева в строке **Контроль запуска программ**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль запуска программ.

     Значок статуса работы компонента , отображающийся слева в строке **Контроль запуска программ**, изменится на значок .

Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

► *Чтобы включить или выключить Контроль запуска программ из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите раздел **Контроль рабочего места**.
3. В правой части окна выполните одно из следующих действий:
   - Установите флажок **Включить Контроль запуска программ**, если вы хотите включить

компонент Контроль запуска программ.

- Снимите флажок **Включить Контроль запуска программ**, если вы хотите выключить компонент Контроль запуска программ.

Если флажок недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Получение информации о программах, которые установлены на защищенных виртуальных машинах

Для создания правила контроля запуска программ (см. раздел «Создание и изменение правила контроля запуска программ» на стр. 283) рекомендуется получить представление о программах, используемых на защищенных виртуальных машинах локальной сети организации. Вы можете получить следующую информацию:

- производители, версии и локализации программ, которые используются в локальной сети организации;
- регулярность обновлений программ;
- политики использования программ, принятые в организации (это могут быть политики безопасности или административные политики);
- расположение хранилища инсталляционных пакетов программ.

Чтобы получить информацию о программах, которые используются на защищенных виртуальных машинах в локальной сети организации, вы можете использовать данные, представленные в списках **Реестр программ** и **Исполняемые файлы**.

Вы можете просматривать эти списки в Консоли администрирования: **Дополнительно** → **Управление программами**.

Список **Реестр программ** содержит программы, которые обнаружил на защищенных виртуальных машинах установленный на них Агент администрирования.

Список **Исполняемые файлы** содержит исполняемые файлы, которые когда-либо запускались на защищенных виртуальных машинах или были обнаружены в процессе работы задачи инвентаризации программы Kaspersky Security (см. раздел "Создание задачи инвентаризации" на стр. 281).

В окне свойств программы, выбранной в одном из этих списков вы можете получить общую информацию о программе и информацию об исполняемых файлах программы, а также просмотреть список защищенных виртуальных машин, на которых установлена эта программа.

Списки программ и исполняемых файлов создаются Агентом администрирования, если в свойствах политики для Легкого агента для Windows в разделе **Отчеты и хранилища** в блоке **Информировать Сервер администрирования** установлен флажок **О запускаемых программах**.

Создание задачи инвентаризации

► *Чтобы создать задачу инвентаризации в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех виртуальных машин, входящих в эту группу. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин (задачу для набора устройств).
3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows** выберите **Инвентаризация**.

   Перейдите к следующему шагу мастера создания задачи.
5. В окне **Область инвентаризации** сформируйте список объектов, которые будут составлять область инвентаризации:
   a. Выполните одно из следующих действий:
      - Если вы хотите добавить новый объект в область инвентаризации, нажмите на кнопку **Добавить**.

        Откроется окно **Выбор объекта**.
      - Если вы хотите изменить объект, выберите его в списке объектов и нажмите на кнопку **Изменить**.

        Откроется окно **Выбор объекта**.
      - Если вы хотите удалить объект из области инвентаризации, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

        Откроется окно подтверждения удаления.

        > Вы не можете удалить или изменить объекты, включенные в область инвентаризации по умолчанию.

   b. Выполните одно из следующих действий:
      - Если вы хотите добавить новый объект, в окне **Выбор объекта** выберите объект в дереве или укажите путь к объекту в поле **Объект** и нажмите на кнопку **Добавить**.

        Объект, добавленный в окне **Выбор объекта**, отобразится в списке объектов в окне **Область инвентаризации**.

        Нажмите на кнопку **ОК**.
      - Если вы хотите изменить объект, в окне **Выбор объекта** в поле **Объект** укажите другой

объект или путь к объекту и нажмите на кнопку **OK**.

- Если вы хотите удалить объект, в окне подтверждения удаления нажмите на кнопку **Да**.

c. Если требуется, повторите пункты a и b для добавления, изменения или удаления объектов из области инвентаризации.

d. Если вы хотите исключить объект из области инвентаризации, в списке объектов окна **Область инвентаризации** снимите флажок рядом с ним. Объект остается в списке, но не учитывается во время выполнения задачи инвентаризации.

6. В окне **Область инвентаризации** выполните следующие действия:

- Установите флажок **Приостанавливать проверку по расписанию, если защищенная виртуальная машина разблокирована**, если вы хотите, чтобы программа приостанавливала запуск задачи инвентаризации, если ресурсы виртуальной машины заняты.
- Установите флажок **Инвентаризация DLL-модулей**, если вы хотите, чтобы программа проверяла наличие DLL-модулей на виртуальных машинах и передавала информацию о DLL-модулях на Сервер администрирования.
- Установите флажок **Инвентаризация файлов скриптов**, если вы хотите, чтобы программа проверяла наличие на виртуальных машинах файлов, содержащих скрипты, и передавала информацию о таких файлах на Сервер администрирования.

7. Нажмите на кнопку **Дополнительно**, если вы хотите настроить параметры оптимизации проверки (см. раздел "Оптимизация проверки файлов" на стр. 363) и параметры проверки составных файлов (см. раздел "Проверка составных файлов" на стр. 362) во время выполнения задачи инвентаризации.

8. Нажмите на кнопку **OK** в окне **Область инвентаризации**.

   Перейдите к следующему шагу мастера создания задачи.

9. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора виртуальных машин, для которых вы создаете задачу. Вы можете выбрать виртуальные машины из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса виртуальных машин вручную, импортировать список виртуальных машин из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора виртуальных машин в открывшемся окне выполните одно из следующих действий:

- В списке обнаруженных виртуальных машин укажите виртуальные машины, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия виртуальной машины.
- Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса виртуальных машин вручную.
- Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов виртуальных машин.
- Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей виртуальные машины, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.

10. Далее следуйте указаниям мастера создания задачи.

Задача инвентаризации завершается с ошибкой, если на виртуальной машине, на которой запущена задача, не установлен компонент Контроль запуска программ.

Создание и изменение правила контроля запуска программ

Вы можете создавать правила контроля запуска программ, которые разрешают или запрещают пользователям локальной сети организации запускать программы на защищенных виртуальных машинах.

► *Чтобы создать или изменить правило контроля запуска программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
6. В блоке **Параметры Контроля запуска программ** в раскрывающемся списке выберите режим работы Контроля запуска программ:
   - **Список разрешенных программ**. Если выбран этот режим, то Контроль запуска программ запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в создаваемом правиле контроля запуска программ.

     Этот режим работы выбран по умолчанию.
   - **Список запрещенных программ**. Если выбран этот режим, то Контроль запуска программ разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в создаваемом правиле контроля запуска программ.
7. В раскрывающемся списке **Действие** выберите действие, которое программа Kaspersky Security должна выполнять при обнаружении попытки пользователя запустить программу, запуск которой не разрешен правилом контроля запуска программ:
   - **Блокировать**. Если выбран этот элемент, при попытке пользователя запустить программу, не разрешенную правилом, программа Kaspersky Security блокирует запуск этой программы.
   - **Информировать**. Если выбран этот элемент, при попытке пользователя запустить программу, не разрешенную правилом, программа Kaspersky Security разрешает запуск этой программы, но записывает в отчет локального интерфейса и отправляет в Kaspersky Security Center информацию об этом.

     Этот вариант действия выбран по умолчанию.
8. В блоке **Параметры Контроля запуска программ** выполните одно из следующих действий:

- Если вы хотите создать новое правило, нажмите на кнопку **Добавить**.
- Если вы хотите изменить существующее правило, выберите его в списке и нажмите на кнопку **Изменить**.

> Вы не можете изменить или удалить предустановленные правила контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. 277).

Откроется окно **Правило контроля запуска программ**.

9. Выполните одно из следующих действий:
   - Если вы хотите создать правило на основе ранее созданных категорий программ, в раскрывающемся списке **Категория** выберите созданную категорию программ.
   - Если вы хотите создать новую категорию программ и на ее основе создать правило, нажмите на кнопку **Создать категорию** и следуйте указаниям мастера создания категории (подробнее о работе с категориями см. в документации Kaspersky Security Center).
10. В поле **Описание** введите описание категории программ.
11. В таблице **Пользователи и / или группы** укажите имена пользователей и / или групп пользователей, которым разрешено или запрещено запускать программы указанной выше категории. Для этого выполните следующие действия:
    a. Нажмите на кнопку **Добавить**.

       Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

    b. Введите имена пользователей и / или группы пользователей.

    c. Нажмите на кнопку **ОК**.

    Выбранные пользователи и группы отобразятся в окне **Правило контроля запуска программ** в таблице в графе **Пользователь и / или группа**.
12. В окне **Правило контроля запуска программ** выполните одно из следующих действий:
    - Если вы выбрали режим работы **Список разрешенных программ**, установите флажок **Разрешить** напротив пользователя или группы, которым вы хотите разрешить запуск программ указанной выше категории.
    - Если вы выбрали режим работы **Список запрещенных программ**, установите флажок **Запретить** напротив пользователя или группы, которым вы хотите запретить запуск программ указанной выше категории.
13. Установите флажок **Запретить остальным пользователям**, если вы хотите запретить запуск программ указанной выше категории остальным пользователям, не указанным таблице **Пользователи и / или группы**.
14. Установите флажок **Доверенные программы обновления**, если вы хотите, чтобы программа Kaspersky Security считала программы из категории, указанной в правиле, доверенными программами обновления и разрешала им запускать другие программы, для которых не определены правила контроля их запуска.
15. Нажмите на кнопку **ОК** в окне **Правило контроля запуска программ**.
16. Нажмите на кнопку **Применить**.

Изменение статуса работы правила контроля запуска программ

Все предустановленные правила контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. 277) имеют статус *Включено*. Если правило контроля запуска программ включено, Контроль запуска программ применяет это правило. Новое правило контроля запуска программ также после создания имеет статус *Включено*.

Вы можете выключить любое правило контроля запуска программ. Если правило контроля запуска программ выключено, Контроль запуска программ временно не применяет это правило.

Также вы можете протестировать работу любого правила контроля запуска программ.

► *Чтобы изменить статус работы правила контроля запуска программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль запуска программ**.
6. В правой части окна отобразятся параметры компонента Контроль запуска программ.
7. В блоке **Параметры Контроля запуска программ** в раскрывающемся списке выберите режим работы Контроля запуска программ, для которого вы хотите изменить статус правила: **Список разрешенных программ** или **Список запрещенных программ**.
8. В таблице правил выберите правило контроля запуска программ, статус работы которого вы хотите изменить.
9. В графе **Статус** выполните одно из следующих действий:
   - Если вы хотите включить правило, выберите значение **Вкл**.
   - Если вы хотите выключить правило, выберите значение **Выкл**.
   - Если вы хотите проверить работу правила, выберите значение **Тест**. Этот статус работы правила означает, что Kaspersky Security не запрещает запуск программ, на которые распространяется действие правила, но фиксирует информацию о запуске этих программ в отчетах.
10. Нажмите на кнопку **Применить**.

Удаление правила контроля запуска программ

Вы можете удалить правило контроля запуска программ, если вы не хотите, чтобы программа Kaspersky Security применяла это правило для обнаружения попыток запуска программ пользователями. Также вы можете временно выключить правило контроля запуска программ (см. раздел "Изменение статуса работы правила контроля запуска программ" на стр. 285), не удаляя его из списка правил.

► *Чтобы удалить правило контроля запуска программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
6. В блоке **Параметры Контроля запуска программ** в раскрывающемся списке выберите режим работы Контроля запуска программ, правило для которого вы хотите удалить: **Список разрешенных программ** или **Список запрещенных программ**.
7. В таблице правил контроля запуска программ выберите правило, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено из списка правил для выбранного режима работы Контроля запуска программ.

   Вы не можете удалить предустановленные правила контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. 277).
8. Нажмите на кнопку **Применить**.

Настойка контроля запуска исполняемых модулей и драйверов

► *Чтобы настроить контроль запуска исполняемых модулей и драйверов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
6. Выполните одно из следующих действий:
   - Установите флажок **Контролировать DLL и драйверы**, если вы хотите, чтобы программа Kaspersky Security контролировала загрузку исполняемых модулей и драйверов при запуске

программ пользователями.

> Включение контроля загрузки исполняемых модулей и драйверов требует значительных ресурсов операционной системы Windows.

- Снимите флажок **Контролировать DLL и драйверы**, если вы не хотите, чтобы программа Kaspersky Security контролировала загрузку исполняемых модулей и драйверов при запуске программ пользователями.

  По умолчанию флажок снят.

7. Нажмите на кнопку **Применить**.

Изменение шаблонов сообщений Контроля запуска программ

Для сообщения о блокировке запуска программы и для жалобы администратору на ошибочную блокировку предусмотрены шаблоны. Вы можете изменять шаблоны этих сообщений.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
6. В нижней части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны сообщений**.
7. Выполните одно из следующих действий:
   - Если вы хотите изменить шаблон сообщения о блокировке запуска программы, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон жалобы администратору локальной сети организации, выберите закладку **Жалоба**.
8. Измените шаблон сообщения о блокировке или жалобы администратору. Для этого используйте кнопки **По умолчанию** и **Переменные**.
9. Нажмите на кнопку **ОК** в окне **Шаблоны сообщений**.
10. Нажмите на кнопку **Применить**.

Контроль активности программ

Описанная в этом разделе функциональность программы Kaspersky Security доступна, только если программа установлена на виртуальной машине с операционной системой Windows для рабочих станций.

Выключение компонента приводит к выходу программы из сертифицированного состояния.

Компонент Контроль активности программ предотвращает выполнение программами опасных для операционной системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным.

Компонент контролирует работу программ на защищенной виртуальной машине, в том числе доступ программ к защищаемым ресурсам (например, к файлам и папкам, ключам реестра), с помощью *правил контроля программ* (см. раздел "*Работа с правилами контроля программ*" на стр. 293). Правила контроля программ представляют собой набор ограничений для различных действий программ в операционной системе и прав доступа к ресурсам защищенной виртуальной машины.

Инициатором запуска программы может быть как пользователь, так и другая запущенная программа. Если инициатором запуска программы является другая программа, образуется последовательность запуска, состоящая из родительских и дочерних процессов.

Когда программа пытается получить доступ к защищаемому ресурсу, Контроль активности программ анализирует права всех родительских процессов этой программы на доступ к защищаемому ресурсу. При этом выполняется правило минимального приоритета: при сравнении прав доступа программы и родительского процесса к активности программы применяются права доступа с минимальным приоритетом.

Приоритет прав доступа следующий:

1. **Разрешать**. Это право доступа имеет высший приоритет.
2. **Запрещать**. Это право доступа имеет низший приоритет.

Этот механизм предотвращает использование доверенных программ недоверенными или ограниченными в правах программами с целью выполнения привилегированных действий.

Если действие программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права (см. раздел "Изменение правила контроля программы в локальном интерфейсе" на стр. 296) или можете выключить наследование ограничений родительского процесса в локальном интерфейсе.

Во время первого запуска программы на защищенной виртуальной машине компонент Контроль активности программ проверяет безопасность программы и помещает программу в одну из *групп доверия* (см. раздел "*Работа с группами доверия*" на стр. 291). Группа доверия определяет правила контроля программ, которые программа Kaspersky Security применяет для контроля работы программ.

Для более эффективной работы Контроля активности программ рекомендуется включить использование Kaspersky Security Network в работе программы Kaspersky Security (см. раздел "Участие в Kaspersky Security Network" на стр. 399). Данные, полученные с помощью Kaspersky Security Network, позволяют точнее относить программы к той или иной группе доверия, а также применять оптимальные правила контроля программ.

Во время повторного запуска программы Контроль активности программ проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие правила контроля программ. Если программа была изменена, Контроль активности программ исследует программу как при первом запуске.

В этом разделе

Включение и выключение Контроля активности программ

По умолчанию Контроль активности программ включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Контроль активности программ при необходимости.

► *Чтобы включить или выключить Контроль активности программ через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
6. Выполните одно из следующих действий:
   - Установите флажок **Контроль активности программ**, если вы хотите включить компонент Контроль активности программ.
   - Снимите флажок **Контроль активности программ**, если вы хотите выключить компонент

Контроль активности программ.

7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

► *Чтобы включить или выключить Контроль активности программ на закладке Центр управления главного окна программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки **Контроль активности программ** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль активности программ.

     Значок статуса работы компонента , отображающийся слева в строке **Контроль активности программ**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль активности программ.

     Значок статуса работы компонента , отображающийся слева в строке **Контроль активности программ**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

► *Чтобы включить или выключить Контроль активности программ из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить Контроль активности программ**, если вы хотите включить

компонент Контроль активности программ.

- Снимите флажок **Включить Контроль активности программ**, если вы хотите выключить компонент Контроль активности программ.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с группами доверия

Во время первого запуска программы на защищенной виртуальной машине компонент Контроль активности программ проверяет безопасность программы и помещает программу в одну из групп доверия.

На первом этапе проверки программы Контроль активности программ ищет запись о программе во внутренней базе известных программ, а затем отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). Если запись о программе найдена в базе Kaspersky Security Network, то программа помещается в группу доверия, зарегистрированную в базе Kaspersky Security Network. При каждом повторном запуске программы Контроль активности программ отправляет новый запрос в базу KSN и перемещает программу в другую группу доверия, если репутация программы в базе KSN изменилась.

Чтобы распределять по группам доверия неизвестные программы (отсутствующие в базе KSN и не имеющие цифровой подписи доверенного производителя), программа Kaspersky Security по умолчанию использует эвристический анализ. В процессе эвристического анализа программа Kaspersky Security определяет степень угрозы программы и на основании степени угрозы помещает программу в ту или иную группу доверия. Вместо использования эвристического анализа вы можете указать группу доверия, в которую программа Kaspersky Security должна автоматически помещать все неизвестные программы.

По умолчанию Контроль активности программ проверяет программу в течение 30 секунд. Если по истечении этого времени определение степени угрозы программы не завершено, Контроль активности программ помещает программу в группу доверия "Слабые ограничения" и продолжает определять степень угрозы программы в фоновом режиме. Затем Контроль активности программ помещает программу в подходящую группу доверия. Вы можете изменить время, которое отводится для проверки степени угрозы запускаемых программ. Если вы уверены, что все запускаемые на защищенной виртуальной машине программы не представляют угрозы для ее безопасности, то можно уменьшить время, отведенное для определения степени угрозы программы. Если же вы устанавливаете на защищенную виртуальную машину программы, в безопасности которых вы не уверены, рекомендуется увеличить время определения степени угрозы программ.

Если степень угрозы программы высока, то программа Kaspersky Security уведомляет вас об этом и предлагает выбрать группу доверия, в которую следует поместить эту программу. Уведомление содержит статистику использования этой программы участниками Kaspersky Security Network. На основании этой статистики, а также зная историю появления программы на виртуальной машине, вы можете принять более объективное решение о том, в какую группу доверия следует поместить эту программу.

В этом разделе

Распределение программ по группам доверия

► *Чтобы настроить через Kaspersky Security Center распределение программ по группам доверия, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
6. Если вы хотите автоматически помещать программы с цифровой подписью в группу доверия "Доверенные", установите флажок **Доверять программам, имеющим цифровую подпись**.
7. Выберите способ распределения неизвестных программ по группам доверия:
   - Если вы хотите использовать эвристический анализ для распределения неизвестных программ по группам доверия, выберите вариант **Использовать эвристический анализ для определения группы** и укажите время, которое отводится для проверки запускаемой программы, в поле **Максимальное время определения группы**.
   - Если вы хотите помещать все неизвестные программы в указанную группу доверия, выберите вариант **Автоматически помещать в группу** и выберите нужную группу доверия в раскрывающемся списке.
8. Нажмите на кнопку **Применить**.

► *Чтобы настроить распределение программ по группам доверия в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–7 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Перемещение программы в группу доверия в локальном интерфейсе

Во время первого запуска программы Контроль активности программ автоматически помещает программу в ту или иную группу доверия. При необходимости вы можете вручную переместить программу в другую группу доверия в локальном интерфейсе.

> Специалисты "Лаборатории Касперского" не рекомендуют перемещать программы из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого вы можете при необходимости изменить правило контроля отдельной программы (см. раздел "Изменение правила контроля программы в локальном интерфейсе" на стр. 296).

► *Чтобы переместить программу в группу доверия, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Нажмите на кнопку **Программы**.
4. Откроется окно **Программы** на закладке **Правила Контроля активности программ**.
5. В списке программ выберите нужную программу и выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню программы и выберите пункт **Переместить в группу** / **<Название группы>**.
   - По ссылке **Доверенные** / **Слабые ограничения** / **Сильные ограничения** / **Недоверенные** в левом нижнем углу закладки **Правила контроля программ** откройте контекстное меню и выберите нужную группу доверия.
6. Нажмите на кнопку **OK** в окне **Программы**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с правилами контроля программ

По умолчанию для контроля работы программы применяются правила контроля программ, определенные для той группы доверия, в которую компонент Контроль активности программ поместил программу при первом ее запуске. При необходимости вы можете изменить правила контроля программ для всей группы доверия (см. раздел "Изменение правил контроля программ для групп доверия и для групп программ" на стр. 294), для отдельной программы (см. раздел "Изменение правила контроля программы в локальном интерфейсе" на стр. 296) или группы программ внутри группы доверия (см. раздел "Изменение правил контроля программ для групп доверия и для групп программ" на стр. 294).

Правила контроля программ, определенные для отдельных программ или групп программ внутри группы доверия, имеют более высокий приоритет, чем правила контроля программ, определенные для группы доверия. То есть, если параметры правил контроля программ, определенные для отдельной программы или группы программ внутри группы доверия, отличны от параметров правил контроля программ, определенных для группы доверия, Контроль активности программ контролирует работу программы или группы программ внутри группы доверия в соответствии с правилами контроля программ, определенными для программы или группы программ.

В этом разделе

Изменение правил контроля программ для групп доверия и для групп программ

По умолчанию для разных групп доверия созданы оптимальные правила контроля программ. Параметры правил контроля групп программ, входящих в группу доверия, наследуют значения параметров правил контроля программ для групп доверия. Вы можете изменить предустановленные правила контроля программ для групп доверия и для групп программ.

► *Чтобы изменить правила контроля программ для группы доверия или для группы программ через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
6. В блоке **Правила программ** нажмите на кнопку **Настройка**, расположенную в верхней части блока.

   Откроется окно **Программы** на закладке **Правила Контроля активности программ**.
7. В списке программ выберите группу доверия или группу программ, для которой вы хотите изменить правило контроля программ.

8. Нажмите на кнопку **Изменить** или по правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.

9. Выполните одно из следующих действий:

   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить правила контроля группы доверия или правила контроля группы программ, регулирующие права группы доверия или группы программ на операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить правила контроля группы доверия или правила контроля группы программ, регулирующие права группы доверия или группы программ на доступ к процессам и объектам операционной системы.

10. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт:

    - **Наследовать**.
    - **Разрешать**.
    - **Запрещать**.
    - **Записывать в отчет**.

    Если вы изменяете правила контроля группы доверия, то пункт **Наследовать** недоступен для выбора.

11. Нажмите на кнопку **OK** в окне **Правила контроля группы программ**.
12. Нажмите на кнопку **OK** в окне **Программы**.
13. Нажмите на кнопку **Применить**.

► *Чтобы изменить правила контроля программ для группы доверия или для группы программ в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы** на закладке **Правила Контроля активности программ**.

4. Выполните пункты 7–12 предыдущей инструкции.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение правила контроля программы в локальном интерфейсе

По умолчанию параметры правил контроля программ, входящих в группу программ или в группу доверия, наследуют значения параметров правил контроля группы доверия. При необходимости вы можете изменить параметры правила контроля программы в локальном интерфейсе.

► *Чтобы изменить правило контроля программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы** на закладке **Правила контроля программ**.
4. В списке программ выберите нужную программу.
5. Выполните одно из следующих действий:
   - Нажмите на кнопку **Изменить**, расположенную над списком программ.
   - По правой клавише мыши откройте контекстное меню программы и выберите пункт **Правила программы**.
   - Нажмите на кнопку **Дополнительно**, расположенную в правом нижнем углу закладки **Правила контроля программ**.

   Откроется окно **Правила контроля программы**.
6. Выполните одно из следующих действий:
   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить правила контроля программы, регулирующие права программы на операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить правила контроля программы, регулирующие права программы на доступ к процессам и объектам операционной системы.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт:
   - **Наследовать**.
   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.
8. Нажмите на кнопку **OK** в окне **Правила контроля программы**.
9. Нажмите на кнопку **OK** в окне **Программы**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выключение загрузки и обновления правил контроля программ из базы Kaspersky Security Network

По умолчанию для программ, найденных в базе Kaspersky Security Network, применяются правила контроля программ, загруженные из этой базы. Если на момент первого своего запуска программа отсутствовала в базе Kaspersky Security Network, но затем информация о ней была добавлена в базу Kaspersky Security Network, то программа Kaspersky Security по умолчанию автоматически обновляет правила контроля этой программы. Вы можете выключить загрузку правил контроля программ из базы Kaspersky Security Network и автоматическое обновление правил контроля для ранее неизвестных программ.

► *Чтобы выключить загрузку и обновление правил контроля программ из базы Kaspersky Security Network через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
6. Снимите флажок **Обновлять правила контроля ранее неизвестных программ из базы KSN**.
7. Нажмите на кнопку **Применить**.

► *Чтобы выключить загрузку и обновление правил контроля программ из базы Kaspersky Security Network в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Снимите флажок **Обновлять правила контроля ранее неизвестных программ из базы KSN**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выключение наследования ограничений родительского процесса в локальном интерфейсе

Если действие программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права (см. раздел "Изменение правила контроля программы в локальном интерфейсе" на стр. 296) или можете выключить наследование ограничений родительского процесса в

локальном интерфейсе.

► *Чтобы выключить наследование ограничений родительского процесса, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы** на закладке **Правила Контроля активности программ**.
4. В списке программ выберите нужную программу.
5. По правой клавише мыши откройте контекстное меню программы и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. Выберите закладку **Исключения**.
7. Установите флажок **Не наследовать ограничения родительского процесса (программы)**.
8. Нажмите на кнопку **OK** в окне **Правила контроля программы**.
9. Нажмите на кнопку **OK** в окне **Программы**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Исключение некоторых действий программы из правил контроля программы в локальном интерфейсе

► *Чтобы исключить некоторые действия программы из правил контроля программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы** на закладке **Правила Контроля активности программ**.

4. В списке программ выберите нужную программу.
5. По правой клавише мыши откройте контекстное меню программы и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. Выберите закладку **Исключения**.
7. Установите флажки напротив действий программы, которые не нужно контролировать или нужно разрешить:
   - **Не проверять открываемые файлы**.
   - **Не контролировать активность программы**.
   - **Не наследовать ограничения родительского процесса (программы)**.
   - **Не контролировать активность дочерних программ**.
   - **Разрешать взаимодействие с интерфейсом программы**.
   - **Не проверять сетевой трафик**.

   Если вы установили флажок **Не проверять сетевой трафик**, то с помощью ссылок в нижней части окна вы можете настроить следующие параметры проверки трафика, передаваемого для этой программы:
   - исключать из проверки весь трафик или только зашифрованный трафик (см. раздел "Проверка защищенных соединений" на стр. 252);
   - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных IP-адресов;
   - исключать из проверки трафик, передаваемый для этой программы с любых или только с указанных портов.

   Вы можете изменять эти параметры щелчком мыши по ссылке.
8. Нажмите на кнопку **OK** в окне **Правила контроля программы**.
9. Нажмите на кнопку **OK** в окне **Программы**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка параметров хранения правил контроля неиспользуемых программ

По умолчанию правила контроля программ, которые не запускались в течение 60 дней, автоматически удаляются. Вы можете изменить время хранения правил контроля неиспользуемых программ или выключить их автоматическое удаление.

► *Чтобы настроить параметры хранения правил контроля неиспользуемых программ через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.

4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
6. Выполните одно из следующих действий:
   - Если вы хотите, чтобы программа Kaspersky Security удаляла правила контроля неиспользуемых программ по истечении заданного времени, установите флажок **Удалять правила контроля программ, не запускавшихся более** и в поле справа укажите длительность хранения правил контроля неиспользуемых программ в днях.
   - Если вы хотите выключить автоматическое удаление правил контроля неиспользуемых программ, снимите флажок **Удалять правила контроля программ, не запускавшихся более**.
7. Нажмите на кнопку **Применить**.

► *Чтобы настроить параметры хранения правил контроля неиспользуемых программ в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните одно из следующих действий:
   - Если вы хотите, чтобы программа Kaspersky Security удаляла правила контроля неиспользуемых программ по истечении заданного времени, установите флажок **Удалять правила контроля программ, не запускавшихся более** и в поле справа укажите длительность хранения правил контроля неиспользуемых программ в днях.
   - Если вы хотите выключить автоматическое удаление правил контроля неиспользуемых программ, снимите флажок **Удалять правила контроля программ, не запускавшихся более**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита ресурсов операционной системы и персональных данных

Компонент Контроль активности программ управляет правами программ на операции над различными категориями ресурсов операционной системы и персональных данных.

Специалисты "Лаборатории Касперского" выделили предустановленные категории защищаемых ресурсов. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

Вы можете выполнить следующие действия:

- Создать новую категорию защищаемых ресурсов (см. раздел "Создание категории защищаемых ресурсов" на стр. 301).
- Создать новый защищаемый ресурс (см. раздел "Создание защищаемого ресурса" на стр. 302).
- Исключить ресурс из защиты (см. раздел "Исключение ресурса из защиты" на стр. 303).

В этом разделе

Создание категории защищаемых ресурсов

► *Чтобы создать категорию защищаемых ресурсов через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
6. В блоке **Правила программ** нажмите на кнопку **Настройка**, расположенную в нижней части блока.

   Откроется окно **Программы** на закладке **Защищаемые ресурсы**.
7. В левой части закладки **Защищаемые ресурсы** выберите раздел или категорию защищаемых ресурсов, в которые вы хотите добавить новую категорию защищаемых ресурсов.
8. В верхней левой части закладки **Защищаемые ресурсы** по левой клавише мыши откройте контекстное меню кнопки **Добавить** и выберите в меню пункт **Категорию**.

   Откроется окно **Категория защищаемых ресурсов**.
9. Введите название новой категории защищаемых ресурсов.
10. Нажмите на кнопку **OK** в окне **Категория защищаемых ресурсов**.

    В списке категорий защищаемых ресурсов появится новый элемент.
11. Нажмите на кнопку **OK** в окне **Программы**.
12. Нажмите на кнопку **Применить**.

► *Чтобы создать категорию защищаемых ресурсов в локальном интерфейсе, выполните*

следующие действия:

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Ресурсы**.

   Откроется окно **Программы** на закладке **Защищаемые ресурсы**.
4. Выполните пункты 7–11 предыдущей инструкции.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

После того как вы создали категорию защищаемых ресурсов, вы можете изменить или удалить ее с помощью кнопок **Изменить** и **Удалить** в верхней левой части закладки **Защищаемые ресурсы**.

Создание защищаемого ресурса

► *Чтобы создать защищаемый ресурс через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
6. В блоке **Правила программ** нажмите на кнопку **Настройка**, расположенную в нижней части блока.

   Откроется окно **Программы** на закладке **Защищаемые ресурсы**.
7. В левой части закладки **Защищаемые ресурсы** выберите раздел или категорию защищаемых ресурсов, в которые вы хотите добавить новый защищаемый ресурс.
8. В верхней левой части закладки **Защищаемые ресурсы** по левой клавише мыши откройте контекстное меню кнопки **Добавить** и выберите тип ресурса, который вы хотите добавить: **Файл или папку** или **Ключ реестра**.

   Откроется окно **Защищаемый ресурс**.

9. В поле **Название** введите название защищаемого ресурса.
10. Нажмите на кнопку **Обзор**.
11. В открывшемся окне укажите необходимые параметры в зависимости от типа добавляемого защищаемого ресурса и нажмите на кнопку **OK**.
12. Нажмите на кнопку **OK** в окне **Защищаемый ресурс**.

    На закладке **Защищаемые ресурсы** в списке защищаемых ресурсов выбранной категории появится новый элемент.
13. Нажмите на кнопку **OK** в окне **Программы**.
14. Нажмите на кнопку **Применить**.

► *Чтобы создать защищаемый ресурс в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Ресурсы**.

   Откроется окно **Программы** на закладке **Защищаемые ресурсы**.
4. Выполните пункты 7–13 предыдущей инструкции.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

После того как вы добавили защищаемый ресурс, вы можете изменить или удалить его с помощью кнопок **Изменить** и **Удалить** в верхней левой части закладки **Защищаемые ресурсы**.

Исключение ресурса из защиты

► *Чтобы исключить ресурс из защиты через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

6. В блоке **Правила программ** нажмите на кнопку **Настройка**, расположенную в нижней части блока.

   Откроется окно **Программы** на закладке **Защищаемые ресурсы**.

7. Исключите ресурс из защиты одним из следующих способов:

   - Выключите защиту ресурса. Для этого в левой части закладки в списке защищаемых ресурсов выберите ресурс, защиту которого вы хотите выключить, и снимите флажок рядом с его названием.
   - Добавьте ресурс в список исключений из защиты компонентом Контроль активности программ. Для этого выполните следующие действия:

     a. В верхней правой части закладки **Защищаемые ресурсы** нажмите на кнопку **Исключения**.

     b. В открывшемся окне **Исключения** по левой клавише мыши откройте контекстное меню кнопки **Добавить** и выберите тип ресурса, который вы хотите добавить в список исключений из защиты компонента Контроль активности программ: **Файл или папку** или **Ключ реестра**.

        Откроется окно **Защищаемый ресурс**.

     c. В поле **Название** введите название защищаемого ресурса.

     d. Нажмите на кнопку **Обзор**.

     e. В открывшемся окне укажите необходимые параметры в зависимости от типа защищаемого ресурса, добавляемого в список исключений из защиты компонентом Контроль активности программ, и нажмите на кнопку **OK**.

     f. Нажмите на кнопку **OK** в окне **Защищаемый ресурс**.

        В списке ресурсов, исключенных из защиты компонента Контроль активности программ, появится новый элемент.

     g. Нажмите на кнопку **OK** в окне **Исключения**.

8. Нажмите на кнопку **OK** в окне **Программы**.
9. Нажмите на кнопку **Применить**.

► *Чтобы исключить ресурс из защиты в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Ресурсы**.

   Откроется окно **Программы** на закладке **Защищаемые ресурсы**.

4. Выполните пункты 7–8 предыдущей инструкции.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Веб-Контроль

Описанная в этом разделе функциональность программы Kaspersky Security доступна, только если программа установлена на виртуальной машине с операционной системой Windows для рабочих станций.

Выключение компонента приводит к выходу программы из сертифицированного состояния.

Компонент Веб-Контроль позволяет контролировать действия пользователей локальной сети организации: ограничивать или запрещать доступ к веб-ресурсам. Под веб-ресурсом подразумевается как отдельная веб-страница или несколько веб-страниц, так и веб-сайт или несколько веб-сайтов, сгруппированных по общему признаку.

Веб-Контроль может контролировать доступ к веб-ресурсам, при обращении к которым используются защищенные соединения (см. раздел "Проверка защищенных соединений" на стр. 252).

Веб-Контроль предоставляет следующие возможности:

- Экономия трафика.

  Расход трафика контролируется путем ограничения или запрета загрузок мультимедийных файлов и ограничения или запрета доступа на не связанные с работой веб-ресурсы.

- Разграничение доступа по категориям содержания веб-ресурсов (см. раздел "Категории содержания веб-ресурсов" на стр. 308).

  Для уменьшения расхода трафика и потенциальных потерь из-за нецелевого использования рабочего времени вы можете ограничить или запретить доступ к веб-ресурсам определенных категорий (например, запретить доступ к веб-ресурсам категории "Новостные ресурсы").

- Централизованное управление доступом к веб-ресурсам.

  При использовании Kaspersky Security Center доступны персональные и групповые параметры доступа к веб-ресурсам.

Все ограничения и запреты на доступ к веб-ресурсам реализуются в виде правил доступа к веб-ресурсам (см. раздел "О правилах доступа к веб-ресурсам" на стр. 307).

kaspersky

В этом разделе

О правилах доступа к веб-ресурсам

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое программа Kaspersky Security выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

В программе предусмотрены следующие фильтры:

- **Фильтр по содержанию**. Веб-Контроль разделяет веб-ресурсы по категориям содержания и категориям типа данных. Вы можете контролировать доступ пользователей к веб-ресурсам определенных категорий содержания и / или категорий типа данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, программа Kaspersky Security выполняет действие, указанное в правиле.
- **Фильтр по адресам веб-ресурсов**. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

  Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, программа Kaspersky Security контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам веб-ресурсов и / или группам адресов веб-ресурсов.
- **Фильтр по именам пользователей и групп пользователей**. Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.
- **Расписание работы правила**. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда программа Kaspersky Security контролирует доступ к веб-ресурсам, указанным в правиле.

После установки программы Kaspersky Security по умолчанию созданы следующие правила доступа к веб-ресурсам:

- **Сценарии и таблицы стилей**. Правило разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат названия файлов с расширением css, js, vbs. Например: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- **Правило по умолчанию**. Правило разрешает всем пользователям в любое время доступ к любым веб-ресурсам.

Категории содержания веб-ресурсов

Для ограничения доступа пользователей виртуальной машины к веб-ресурсам вы можете использовать категории содержания веб-ресурсов, перечисленные в списке ниже.

Порядок категорий в списке не отражает относительной важности или распространенности категорий в интернете. Названия категорий являются условными и используются лишь для программ и веб-сайтов "Лаборатории Касперского". Названия не обязательно соответствуют значению, которое им придает применимое законодательство. Один веб-ресурс может относиться к нескольким категориям одновременно.

Для взрослых

Категория включает веб-ресурсы, относящиеся к сексуальной стороне человеческих отношений. Это может быть содержимое в любом формате и виде.

- Порнография, эротика – веб-ресурсы, содержащие любые фото- или видеоматериалы с изображением половых органов людей или человекоподобных существ, полового акта или самоудовлетворения, совершенного людьми или человекоподобными существами. А так же веб-ресурсы, содержащие любые текстовые, в том числе литературные и художественные материалы с описанием половых органов людей или человекоподобных существ, полового акта или самоудовлетворения, совершенного людьми или человекоподобными существами. Кроме того, веб-ресурсы, содержащие эротические материалы, произведения, натуралистично освещающие половую жизнь человека, или произведения искусства, рассчитанные на стимулирование сексуального возбуждения.
- Нудизм – веб-ресурсы, посвященные явлению нудизм: сайты сообществ, специальных мест отдыха, фото-хостингов, так или иначе связанные с нудизмом. А также сайты содержащие соответствующие изображения.
- Белье – веб-ресурсы, которые продают нижнее белье, так же сайты выставок, показов в нижнем белье, контент эротической направленности в котором есть люди в белье.
- Секс-образование – веб-ресурсы, которые содержат:
  - статьи и блоги на тему полового воспитания, как научные, так и популярные;
  - медицинские энциклопедии, их разделы о половом размножении;
  - ресурсы медицинских учреждений, их разделы про лечение половых органов.
- Знакомства для взрослых – веб-ресурсы, которые предлагают сервис знакомств, в том числе с сексуальным подтекстом.
- ЛГБТ+ – веб-ресурсы, которые содержат любую информацию о ЛГБТ. Это могут быть энциклопедии, форумы, сайты соответствующих объединений. Любая информация на любом сайте этой тематики.
- Интим-магазины – веб-ресурсы, посвященные интим-магазинам, описание этих магазинов и прочее.
- Аборты – веб-ресурсы содержащие информацию об абортах. В том числе на сайтах медицинских учреждений.

Программное обеспечение, аудио, видео

Категория включает веб-ресурсы, где пользователи могут загружать пакеты программного обеспечения:

- Веб-ресурсы, распространяющие аудио- и видеоматериалы: фильмы, записи спортивных трансляций, записи концертов, песни, клипы, видеоролики, учебные аудио- и видеозаписи и прочее.
- Торрент-трекеры и сайты файлообмена вне зависимости от физического нахождения распространяемых файлов.

Алкоголь, табак, наркотики и психотропы

Категория включает веб-ресурсы, на которых есть упоминание алкоголя, наркотиков, табака в любых видах, в том числе рекламные, исторические, медицинские и обучающие ресурсы. А также веб-ресурсы, где описаны или продаются приспособления для употребления указанных веществ.

- Наркотики – веб-ресурсы, содержимое которых связано с наркотической продукцией, в частности, ресурсы, которые посвящены реализации, рекламе, описанию, историческим и медицинским фактам о наркотической продукции.
- Алкоголь – веб-ресурсы содержимое которых связано с алкогольной и спиртосодержащей продукцией, в частности, ресурсы, которые посвящены реализации, рекламе, описанию, историческим и медицинским фактам о спиртной продукции.
- Табак – веб-ресурсы содержимое которых связано с табачной продукцией, в частности, ресурсы, которые посвящены реализации, рекламе, описанию, историческим и медицинским фактам о табачной продукции.

Насилие

Категория включает веб-ресурсы, содержащие фото-, видео- и текстовые материалы, описывающие акты физического или психического насилия над людьми, а также жестокого отношения к животным. Произведения искусства могут быть исключениями в этой категории.

Оружие, взрывчатые вещества, пиротехника

Категория включает веб-ресурсы, содержащие информацию об оружии, взрывчатых веществах и пиротехнической продукции.

Под "оружием" понимаются устройства, предметы и средства, конструктивно предназначенные для нанесения вреда жизни и здоровью людей и животных и / или выведения из строя техники и сооружений.

Нецензурная лексика

Категория включает веб-ресурсы, на которых обнаружены элементы нецензурной брани.

В эту категорию также попадают веб-ресурсы с лингвистическими и филологическими материалами, содержащими нецензурную лексику в качестве предмета рассмотрения.

Азартные игры, лотереи, тотализаторы

Категория включает веб-ресурсы, содержащие:

- Азартные игры, предусматривающие денежные взносы за участие.
- Тотализаторы, предусматривающие денежные ставки.

- Лотереи, предусматривающие приобретение лотерейных билетов / номеров.

Общение в сети

Категория включает веб-ресурсы, позволяющие тем или иным пользователям (зарегистрированным или нет), отправлять персональные сообщения другим пользователям.

- Веб-почта – исключительно страницы авторизации в почтовом сервисе и страницы почтового ящика, содержащего почтовые сообщения и сопутствующие данные (например, личные контакты). Для остальных веб-страниц интернет-провайдера, предлагающего почтовый сервис, данная категория не назначается.
- Социальные сети – веб-сайты, предназначенные для построения, отражения и организации контактов между людьми, организациями, государством, требующие в качестве условия участия регистрацию учетной записи пользователя.
- Чаты, форумы, IM – веб-чаты, а также веб-ресурсы, предназначенные для распространения и поддержки приложений для мгновенного обмена сообщениями, предоставляющих возможность коммуникации в реальном времени. А также форумы – специальные веб-сервисы для публичного обсуждения различных тем с сохранением переписки.
- Блоги – веб-ресурсы, предназначенные для публичного обсуждения различных тем с помощью специальных веб-приложений, включая блог-платформы (веб-сайты, предоставляющие платные или бесплатные услуги по созданию и обслуживанию блогов).
- Сайты знакомств – веб-ресурсы знакомств, которые помогают организовать знакомства между людьми, в том числе без сексуального подтекста.

Интернет-магазины, банки, платежные системы

Категория включает веб-ресурсы, предназначенные для проведения любых операций с безналичными денежными средствами в режиме онлайн с помощью специальных веб-приложений. А также веб-ресурсы, помогающие снять, сдать, купить или продать недвижимость.

- Интернет-магазины – интернет-магазины и интернет-аукционы, предназначенные для реализации любых товаров, работ или услуг физическим и / или юридическим лицам, в том числе как веб-сайты магазинов, осуществляющих реализацию исключительно в интернете, так и интернет-представительства обычных магазинов, характерной особенностью которых является возможность оплаты в режиме онлайн.
- Банки – веб-ресурсы банков.
- Платежные системы – к этой категории относятся следующие веб-страницы:
  - Специальные веб-страницы банков, предусматривающие услуги интернет-банкинга, включающие безналичные (электронные) переводы между банковскими счетами, открытие банковских вкладов, конвертацию денежных средств, оплату услуг сторонних организаций и т. д.
  - Веб-страницы электронных платёжных систем, предоставляющие доступ к персональной учетной записи пользователя.
- Криптовалюты, майнинг – веб-сайты, предоставляющие сервисы покупки и продажи криптовалют, сервисы информирования о криптовалютах и майнинге.

Поиск работы

Категория включает веб-ресурсы, предназначенные для установления контактов между работодателем и соискателем работы. К ним в частности относятся:

- веб-сайты кадровых агентств (агентств по трудоустройству и / или агентств по подбору персонала);

- веб-страницы работодателей, содержащие описание имеющихся вакансий и их преимуществ;
- независимые порталы, содержащие предложения трудоустройства от работодателей и кадровых агентств;
- социальные сети профессионального характера, которые в том числе позволяют размещать / находить данные о специалистах, которые не находятся в активном поиске работы.

Средства анонимного доступа

Категория включает веб-ресурсы, выступающие в роли посредника для загрузки контента прочих веб-ресурсов с помощью специальных веб-приложений для:

- обхода ограничений администратора локальной сети на доступ к веб-адресам или IP-адресам;
- анонимного доступа к веб-ресурсам, в том числе к веб-ресурсам, которые преднамеренно не принимают HTTP-запросы с определенных IP-адресов или их групп (например, по стране происхождения).

Компьютерные игры

Категория включает веб-ресурсы, посвященные компьютерным играм разнообразных жанров, а также игровые сообщества и сервисы.

Религии, религиозные объединения

Категория включает веб-ресурсы, содержащие материалы об общественных течениях (движениях), объединениях (сообществах) и организациях, подразумевающих наличие религиозной идеологии и / или культа в любых проявлениях.

Новостные ресурсы

Новостные порталы на любые темы, в том числе социальные новости агрегаторы новостей, rss рассылки.

Реклама, тизерные сети

Категория включает веб-ресурсы, содержащие баннеры. Рекламная информация на баннерах может отвлекать пользователей от дел, а загрузка баннеров увеличивает объем трафика.

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен. Вы можете выключить Веб-Контроль при необходимости.

► *Чтобы включить или выключить Веб-Контроль через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел

Веб-Контроль.

В правой части окна отобразятся параметры компонента Веб-Контроль.

6. Выполните одно из следующих действий:
   - Установите флажок **Веб-Контроль**, если вы хотите включить компонент Веб-Контроль.
   - Снимите флажок **Веб-Контроль** если вы хотите выключить компонент Веб-Контроль.
7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

► *Чтобы включить или выключить Веб-Контроль на закладке Центр управления главного окна программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки **Веб-Контроль** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Веб-Контроль.
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Веб-Контроль.

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

► *Чтобы включить или выключить Веб-Контроль из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить Веб-Контроль**, если вы хотите включить компонент Веб-Контроль.

- Снимите флажок **Включить Веб-Контроль**, если вы хотите выключить компонент Веб-Контроль.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Действия с правилами доступа к веб-ресурсам

Вы можете выполнить следующие действия при настройке правил доступа к веб-ресурсам:

- Создать новое правило (см. раздел "Создание и изменение правила доступа к веб-ресурсам" на стр. 313).
- Изменить правило (см. раздел "Создание и изменение правила доступа к веб-ресурсам" на стр. 313).
- Изменить приоритет правила (см. раздел "Изменение приоритета правил доступа к веб-ресурсам" на стр. 315).
- Проверить работу правила (см. раздел "Проверка работы правил доступа к веб-ресурсам" на стр. 316).
- Включить и выключить правило (см. раздел "Включение и выключение правила доступа к веб-ресурсам" на стр. 317).
- Удалить правило (см. раздел "Удаление правила доступа к веб-ресурсам" на стр. 318).

В этом разделе

Создание и изменение правила доступа к веб-ресурсам

► *Чтобы создать или изменить через Kaspersky Security Center правило доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Контроль**.

В правой части окна отобразятся параметры компонента Веб-Контроль.

6. Выполните одно из следующих действий:
   - Если вы хотите создать новое правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить существующее правило, выберите его в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
7. В поле **Название** введите или измените название правила.
8. В раскрывающемся списке **Фильтровать содержание** выберите нужный элемент:
   - **Любое содержание**.
   - **По категориям содержания**.
   - **По типам данных**.
   - **По категориям содержания и типам данных**.

   Если выбран элемент, отличный от **Любое содержание**, откроется блок для выбора категорий содержания и / или категорий типов данных. Установите флажки напротив названий нужных категорий содержания и / или категорий типов данных.

   Установка флажка напротив названия категории содержания и / или категории типов данных означает, что программа в соответствии с правилом контролирует доступ к веб-ресурсам, принадлежащим выбранным категориям содержания и / или категориям типов данных.
9. В раскрывающемся списке **Применять к адресам** выберите нужный элемент:
   - **Ко всем адресам**.
   - **К отдельным адресам**.

   Если выбран элемент **К отдельным адресам**, откроется блок, в котором требуется создать список адресов веб-ресурсов. Вы можете создавать или изменять список адресов веб-ресурсов, используя кнопки **Добавить**, **Изменить**, **Удалить**. Для создания списка адресов веб-ресурсов вы можете также использовать *маски адреса веб-ресурса* (см. раздел "*Правила формирования масок адреса веб-ресурса*" на стр. 319).

   После создания списка адресов веб-ресурсов вы можете экспортировать его в файл (см. раздел "Экспорт и импорт списка адресов веб-ресурсов" на стр. 321), чтобы впоследствии импортировать этот список из файла (см. раздел "Экспорт и импорт списка адресов веб-ресурсов" на стр. 321).
10. Установите флажок **Укажите пользователей и / или группы** и нажмите на кнопку **Выбрать**.

    Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
11. Задайте или измените список пользователей и / или групп пользователей, для которых разрешен или ограничен доступ к веб-ресурсам, описанным в правиле, и нажмите на кнопку **OK**.
12. В раскрывающемся списке **Действие** выберите нужный элемент:
    - **Разрешать**. Если выбрано это значение, то программа разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
    - **Запрещать**. Если выбрано это значение, то программа запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
    - **Предупреждать**. Если выбрано это значение, то при попытке доступа к веб-ресурсам, удовлетворяющим параметрам правила, программа выводит сообщение-предупреждение о возможной небезопасности веб-ресурса. По ссылкам из сообщения-предупреждения

пользователь может получить доступ к запрошенному веб-ресурсу.

13. В раскрывающемся списке **Расписание работы правила** выберите название нужного расписания или на основе выбранного расписания работы правила сформируйте новое расписание. Для этого выполните следующие действия:

    a. Нажмите на кнопку **Настройка** рядом с раскрывающемся списком **Расписание работы правила**.

    Откроется окно **Расписание работы правила**.

    b. Чтобы добавить в расписание работы правила интервал времени, в течение которого правило не работает, в таблице с изображением расписания работы правила левой клавишей мыши нажмите по ячейкам таблицы, соответствующим нужному вам времени и дню недели.

    Цвет ячеек изменится на серый.

    c. Чтобы в расписании работы правила изменить интервал времени, в течение которого работает правило, на интервал времени, в течение которого правило не работает, левой клавишей мыши нажмите по серым ячейкам таблицы, соответствующим нужному вам времени и дню недели.

    Цвет ячеек изменится на зеленый.

    d. Нажмите на кнопку **ОК** или **Сохранить как**, если вы формируете расписание работы правила на основе расписания работы правила "Всегда", сформированного по умолчанию. Нажмите на кнопку **Сохранить как**, если вы формируете расписание работы правила на основе расписания работы правила, сформированного не по умолчанию.

    Откроется окно **Название расписания работы правила**.

    e. Введите название расписания работы правила или оставьте название, предложенное по умолчанию.

    f. Нажмите на кнопку **ОК** в окне **Название расписания работы правила**.

14. Нажмите на кнопку **ОК** в окне **Правило доступа к веб-ресурсам**.
15. Нажмите на кнопку **Применить**.

► *Чтобы создать или изменить в локальном интерфейсе правило доступа к веб-ресурсам, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–14 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение приоритета правил доступа к веб-ресурсам

Приоритет выполнения правила определяется его положением в таблице **Правила доступа в порядке**

приоритета окна параметров компонента Веб-Контроль. Первое правило в таблице имеет самый высокий приоритет.

Если веб-ресурс, к которому пользователь виртуальной машины пытается получить доступ, соответствует параметрам нескольких правил, то действие программы определяет правило с более высоким приоритетом.

Вы можете повысить или понизить приоритет любого правила доступа к веб-ресурсам, кроме правила "Правило по умолчанию", оно всегда имеет самый низкий приоритет и располагается в конце списка правил.

► *Чтобы изменить приоритет правила доступа к веб-ресурсам через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
6. В таблице **Правила доступа в порядке приоритета** выберите правило, приоритет которого вы хотите изменить, и с помощью кнопок **Вверх** и **Вниз** переместите правило на нужную позицию.
7. Нажмите на кнопку **Применить**.

► *Чтобы изменить приоритет правила доступа к веб-ресурсам локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. В таблице **Правила доступа в порядке приоритета** выберите правило, приоритет которого вы хотите изменить, и с помощью кнопок **Вверх** и **Вниз** переместите правило на нужную позицию.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка работы правил доступа к веб-ресурсам

В локальном интерфейсе вы можете проверить согласованность работы правил с помощью функции "Диагностика правил".

► *Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В нижней части окна нажмите на кнопку **Диагностика**.

   Откроется окно **Диагностика правил**.
4. Заполните поля в блоке **Условия**:
   a. Установите флажок **Укажите адрес**, если вы хотите проверить работу правил, в соответствии с которыми программа контролирует доступ к определенному веб-ресурсу. В поле ниже введите адрес веб-ресурса.
   b. Укажите имя пользователя или группы пользователей, если вы хотите проверить работу правил, в соответствии с которыми программа контролирует доступ к веб-ресурсам для определенных пользователей или групп пользователей. Для этого выполните следующие действия:
      1. Установите флажок **Укажите пользователей и / или группы** и нажмите на кнопку **Выбрать**.

         Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
      2. В окне Microsoft Windows **Выбор пользователей или групп** укажите нужного пользователя или группу пользователей и нажмите на кнопку **ОК**.
   c. В раскрывающемся списке **Фильтровать содержание** выберите нужный элемент (**По категориям содержания**, **По типам данных** или **По категориям содержания и типам данных**), если вы хотите проверить работу правил, в соответствии с которыми программа контролирует доступ к веб-ресурсам определенных категорий содержания и / или категорий типов данных, и установите флажки напротив названий нужных категорий содержания и / или категорий типов данных.
   d. Установите флажок **Учитывать время попытки доступа**, если вы хотите проверить работу правил с учетом дня недели и времени совершения попытки доступа к веб-ресурсу(ам), указанным в условиях диагностики правил. Справа укажите день недели и время.
5. Нажмите на кнопку **Проверить**.

В результате проверки работы правил выводится сообщение о действии программы в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу(ам) (разрешение, запрет, предупреждение). Далее проверяются все сработавшие правила.

Справа от кнопки **Проверить** выводится сообщение о действии программы в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу(ам). Первым срабатывает правило, которое находится в списке правил Веб-Контроля выше других правил, удовлетворяющих условиям диагностики. В таблице в нижней части окна **Диагностика правил** выводится список остальных сработавших правил с указанием действия, которое выполняет программа. Правила выводятся в порядке убывания приоритета.

Включение и выключение правила доступа к веб-ресурсам

Все предустановленные правила доступа к веб-ресурсам имеют статус *Включено*. Если правило доступа к веб-ресурсам включено, Веб-Контроль применяет это правило.

Новое правило доступа к веб-ресурсам также после создания имеет статус *Включено*.

Вы можете выключить любое правило доступа к веб-ресурсам, кроме правила "Правило по умолчанию". Если правило доступа к веб-ресурсам выключено, Веб-Контроль временно не применяет это правило.

► *Чтобы включить или выключить через Kaspersky Security Center правило доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
6. В списке правил выберите правило, которое вы хотите включить или выключить.
7. В графе **Статус** по левой клавише мыши откройте контекстное меню и выберите одно из следующих значений:
   - **Вкл**, если вы хотите включить использование правила.
   - **Выкл**, если вы хотите выключить использование правила.
8. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить в локальном интерфейсе правило доступа к веб-ресурсам, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. Выполните пункты 6–7 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Удаление правила доступа к веб-ресурсам

► *Чтобы удалить через Kaspersky Security Center правило доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
6. В списке правил доступа к веб-ресурсам выберите правило, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено из списка правил.

   Вы не можете удалить предустановленное **Правило по умолчанию** (см. раздел "**О правилах доступа к веб-ресурсам**" на стр. 307).
7. Нажмите на кнопку **Применить**.

► *Чтобы удалить в локальном интерфейсе правило доступа к веб-ресурсам, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
3. В списке правил доступа к веб-ресурсам выберите правило, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено из списка правил.

   Вы не можете удалить предустановленное **Правило по умолчанию** (см. раздел "**О правилах доступа к веб-ресурсам**" на стр. 307).
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Правила формирования масок адреса веб-ресурса

Использование маски адреса веб-ресурса (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам (см. раздел "Создание и изменение правила доступа к веб-ресурсам" на стр. 313) требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса используйте следующие правила:

1. Символ * заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса *abc* правило доступа к веб-ресурсам применяется ко всем адресам веб-ресурсов, содержащим последовательность abc. Пример: http://www.example.com/page_0-9abcdef.html.

   Символ ? трактуется как символ знака вопроса.

   Для включения символа * в состав маски адреса нужно вводить два символа *.

2. Последовательность символов www. в начале маски адреса трактуется как последовательность *..

   Пример: маска адреса www.example.com трактуется как *.example.com.

3. Если маска адреса начинается не с символа *, то содержание маски адреса эквивалентно тому же содержанию с префиксом *..

4. Последовательность символов *. в начале маски трактуется как *. или пустая строка.

   Пример: под действие маски адреса http://www.*.example.com попадает адрес веб-ресурса http://www2.example.com.

5. Если маска адреса заканчивается символом, отличным от / или *, то содержание маски адреса эквивалентно тому же содержанию с постфиксом /*.

   Пример: под действие маски адреса http://www.example.com попадают адреса вида http://www.example.com/abc, где a, b, c – любые символы.

6. Если маска адреса заканчивается символом /, то содержание маски адреса эквивалентно тому же содержанию с постфиксом /*.

7. Последовательность символов /* в конце маски адреса трактуется как /* или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес веб-ресурса с любым сетевым протоколом.

     Пример: под действие маски адреса example.com попадают адреса веб-ресурса http://example.com и https://example.com.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса веб-ресурса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса http://*.example.com попадает адрес веб-ресурса http://www.example.com и не попадает адрес https://www.example.com.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа *, если он изначально включен в состав маски адреса. То есть для таких масок адреса не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Таблица 2. Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли адрес маске адреса	Комментарий
2	*.example.com	http://www.123.example.com	Да	См. правило 1.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 2, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	”example.com”	http://www.example.com	Нет	См. правило 9.
15	”http://www.example.com”	http://www.example.com/abc	Нет	См. правило 9.
16	”*.example.com”	http://www.example.com	Да	См. правила 1, 9.
17	”http://www.example.com/*”	http://www.example.com/abc	Да	См. правила 1, 9.
18	”www.example.com”	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше данных, чем адрес веб-ресурса.

Экспорт и импорт списка адресов веб-ресурсов

Если при создании правила доступа к веб-ресурсам (см. раздел "Создание и изменение правила доступа к веб-ресурсам" на стр. 313) вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

► *Чтобы экспортировать список адресов веб-ресурсов в файл через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
6. В списке правил выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать в файл.
7. Нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.

   Под раскрывающимся списком **Применять к адресам** отобразится список адресов веб-ресурсов, к которым применяется правило.
8. Если вы хотите экспортировать не весь список адресов веб-ресурсов, а только его часть, выделите нужные вам адреса веб-ресурсов.
9. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Откроется окно подтверждения действия.
10. Выполните одно из следующих действий:
    - Если вы хотите экспортировать только выделенные элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Да**.
    - Если вы хотите экспортировать все элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Нет**.

    Откроется стандартное окно Microsoft Windows **Сохранить как**.
11. Выберите файл, в который вы хотите экспортировать список адресов веб-ресурсов, и нажмите на кнопку **Сохранить**.

► *Чтобы экспортировать список адресов веб-ресурсов в файл в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. Выполните пункты 6–11 предыдущей инструкции.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

► *Чтобы импортировать в правило список адресов веб-ресурсов из файла через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
6. Выполните одно из следующих действий:
   - Если вы хотите создать новое правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить правило, выберите правило в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
7. Если вы создаете новое правило доступа к веб-ресурсам, в раскрывающемся списке **Применять к адресам** выберите элемент **К отдельным адресам**.
8. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Если вы создаете новое правило, откроется стандартное окно Microsoft Windows **Открыть файл**.

   Если вы изменяете правило, откроется окно подтверждения действия.
9. Если вы изменяете правило доступа к веб-ресурсам, в окне подтверждения действия выполните одно из следующих действий:
   - Если вы хотите добавить к существующим импортируемые элементы списка адресов веб-ресурсов, нажмите на кнопку **Да**.
   - Если вы хотите удалить существующие элементы списка адресов веб-ресурсов и добавить импортируемые, нажмите на кнопку **Нет**.

   Откроется стандартное окно Microsoft Windows **Открыть файл**.
10. В окне Microsoft Windows **Открыть файл** выберите файл со списком адресов веб-ресурсов для импорта и нажмите на кнопку **Открыть**.

    В окне **Правило доступа к веб-ресурсам** под раскрывающимся списком **Применять к адресам** отобразится импортированный список адресов веб-ресурсов.
11. Нажмите на кнопку **OK** в окне **Правило доступа к веб-ресурсам**.
12. Нажмите на кнопку **Применить**.

► *Чтобы импортировать в правило список адресов веб-ресурсов из файла в локальном*

интерфейсе, выполните следующие действия:

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–11 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил доступа к веб-ресурсам, при попытке пользователя виртуальной машины получить доступ к веб-ресурсам программа выводит сообщение одного из следующих типов (подменяет ответ HTTP-сервера HTML-страницей с сообщением):

- **Сообщение-предупреждение**. Сообщение такого типа предупреждает о возможной опасности веб-сайта и / или несоответствии веб-сайта корпоративной политике. Программа выводит сообщение-предупреждение, если в свойствах правила, описывающего этот веб-сайт, в раскрывающемся списке **Действие** выбран элемент **Предупреждать**.

  Если, по мнению пользователя, предупреждение ошибочно, по ссылке из сообщения-предупреждения пользователь может открыть уже сформированное сообщение-жалобу администратору локальной сети организации.

- **Сообщение о блокировке веб-ресурса**. Программа выводит сообщение о блокировке веб-ресурса, если в свойствах правила, которое описывает этот веб-ресурс, в раскрывающемся списке **Действие** выбран элемент **Запрещать**.

  Если, по мнению пользователя, доступ к веб-ресурсу был заблокирован ошибочно, по ссылке из сообщения о блокировке веб-ресурса пользователь может открыть уже сформированное сообщение-жалобу администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения-жалобы для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

► *Чтобы изменить шаблон сообщения Веб-Контроля через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

6. В нижней части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны сообщений**.

7. Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения, предупреждающего о возможной опасности веб-сайта, выберите закладку **Предупреждение**.
   - Если вы хотите изменить шаблон сообщения о блокировке доступа к веб-сайту, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон жалобы администратору локальной сети организации, выберите закладку **Жалоба**.

8. Измените шаблон сообщения. Для этого используйте кнопки **По умолчанию** и **Переменные**.
9. Нажмите на кнопку **OK** в окне **Шаблоны сообщений**.
10. Нажмите на кнопку **Применить**.

► *Чтобы изменить шаблон сообщения Веб-Контроля в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль целостности системы

Описанная в этом разделе функциональность программы Kaspersky Security доступна, только если вы используете программу по расширенной лицензии и программа установлена на виртуальной машине с операционной системой Windows для серверов и файловой системой NTFS или FAT32.

Компонент Контроль целостности системы позволяет отслеживать изменения в операционной системе Windows, установленной на защищенной виртуальной машине. Вы можете контролировать следующие объекты:

- **Файлы и реестр**. Компонент Контроль целостности системы отслеживает изменения в файлах и реестре, включенных в область контроля.
- **Внешние устройства**. Компонент Контроль целостности системы отслеживает подключение внешних устройств следующих типов:
  - Дисководы для жестких дисков.
  - Дисководы для оптических дисков (CD/DVD/Blu-ray).
  - Устройства USB.
  - Камеры и сканеры.
  - Внешние сетевые адаптеры.

Компонент Контроль целостности системы может работать в режиме реального времени, а также выполнять проверку целостности системы по расписанию или по требованию.

При работе в режиме реального времени Контроль целостности системы позволяет отслеживать изменения в объектах контроля, которые вы включили в область действия контроля целостности системы.

Проверка целостности системы по расписанию или по требованию выполняется с помощью *задачи проверки целостности системы* (см. раздел "*Проверка целостности системы по расписанию или по требованию*" на стр. 340). Проверка осуществляется путем сравнения текущего состояния объектов, включенных в область действия проверки целостности системы, с состоянием этих объектов, которое предварительно зафиксировано в виде *снимка состояния системы*.

Вы можете выполнять проверку целостности системы в одном из следующих режимов:

- Полная проверка. При проверке изменений в файлах учитываются все атрибуты файлов и их содержимое.
- Быстрая проверка. При проверке изменений в файлах учитываются только атрибуты файлов, их содержимое не проверяется.

Проверка изменений в реестре и проверка подключения внешних устройств выполняется в любом режиме в соответствии с заданной областью действия проверки целостности системы.

Снимок состояния системы формируется на виртуальной машине в результате выполнения *задачи обновления снимка состояния системы* (см. раздел "*Создание и обновление снимка состояния системы*" на стр. 338). В результате создания или обновления снимка состояния системы фиксируется состояние объектов, включенных в область действия проверки целостности системы.

Вы можете обновлять снимок состояния системы в одном из следующих режимов:

- Полное обновление – по всем объектам, входящим в область проверки.
- Инкрементальное обновление – только по изменившимся или новым объектам из области проверки.

Параметры работы компонента Контроль целостности системы задаются в политике для Легкого агента для Windows или в локальном интерфейсе Легкого агента для Windows. Вы можете включать и выключать работу компонента Контроль целостности системы в режиме реального времени (см. раздел "Включение и выключение контроля целостности системы в режиме реального времени" на стр. 328), а также настраивать следующие параметры:

- Область действия контроля целостности системы в режиме реального времени:
  - Список объектов, которые должен контролировать компонент Контроль целостности системы в режиме реального времени.
  - Список *правил контроля целостности системы*, в соответствии с которыми компонент отслеживает изменения в файлах и реестре. Вы можете создавать правила и использовать предустановленные правила из шаблонов, которые входят в комплект поставки программы.
- Область действия проверки целостности системы. По умолчанию область действия проверки совпадает с областью действия контроля целостности системы. Вы можете задать отдельную область действия для проверки целостности системы по расписанию или по требованию. Эта область действия также используется для задачи обновления снимка состояния системы:
  - Список объектов, состояние которых требуется проверять. Состояние этих объектов фиксируется в снимке состояния системы.
  - Список *правил контроля целостности системы*, в соответствии с которыми компонент проверяет изменения в файлах и реестре. В снимке состояния системы фиксируется состояние файлов и папок, а также ключей реестра, заданных в правилах. Вы можете создавать правила и использовать предустановленные правила из шаблонов, которые входят в комплект поставки программы.

  Если область действия проверки целостности системы не задана, для задачи проверки целостности системы и задачи обновления снимка состояния системы используется область действия контроля целостности системы.
- Уровень важности для событий, которые формирует Контроль целостности системы, когда обнаруживает изменения в системе в режиме реального времени и в результате выполнения задачи проверки целостности системы.

Вы можете посмотреть информацию о результатах работы компонента Контроль целостности системы в Kaspersky Security Center и в локальном интерфейсе Легкого агента для Windows (см. раздел "Просмотр информации о целостности системы на виртуальной машине" на стр. 343).

В этом разделе

Включение и выключение контроля целостности системы в режиме реального времени

По умолчанию контроль целостности системы в режиме реального времени выключен.

Включение и выключение контроля целостности системы в режиме реального времени не влияет на выполнение задачи проверки целостности системы и задачи обновления снимка состояния системы.

► *Чтобы включить или выключить в Консоли администрирования Kaspersky Security Center контроль целостности системы в режиме реального времени, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры Контроля целостности системы.
6. Выполните одно из следующих действий:
   - Установите флажок **Контролировать целостность системы в режиме реального времени**, если вы хотите включить работу компонента Контроль целостности системы в режиме реального времени.
   - Снимите флажок **Контролировать целостность системы в режиме реального времени**, если вы хотите выключить работу компонента Контроль целостности системы в режиме реального времени.
7. Нажмите на кнопку **Применить**.

В локальном интерфейсе Легкого агента для Windows вы можете включить и выключить работу компонента в режиме реального времени двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120);
- из окна настройки параметров программы (см. раздел "Окно настройки параметров программы" на стр. 121).

Если параметры работы компонента в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

► *Чтобы включить или выключить контроль целостности системы в режиме реального*

времени на закладке Центр управления главного окна программы, выполните следующие действия:

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки **Контроль целостности системы** и выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить работу компонента Контроль целостности системы в режиме реального времени.
   - Выберите в меню пункт **Выключить**, если вы хотите выключить работу компонента Контроль целостности системы в режиме реального времени.

► *Чтобы включить или выключить контроль целостности системы в режиме реального времени из окна настройки параметров программы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль целостности системы**.
3. Выполните одно из следующих действий:
   - Установите флажок **Контролировать целостность системы в режиме реального времени**, если вы хотите включить работу компонента Контроль целостности системы в режиме реального времени.
   - Снимите флажок **Контролировать целостность системы в режиме реального времени**, если вы хотите выключить работу компонента Контроль целостности системы в режиме реального времени.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка области действия контроля и области действия проверки целостности системы

Для работы компонента Контроль целостности системы требуется настроить область действия компонента, то есть выбрать объекты, за состоянием которых должен следить Контроль целостности системы. Настройка области действия выполняется в политике Легкого агента для Windows или в локальном интерфейсе Легкого агента для Windows.

Вы можете настроить область действия контроля целостности системы для работы компонента в режиме реального времени и отдельную область действия для проверки целостности системы по расписанию или по требованию. Эта область действия также используется для задачи обновления снимка состояния системы. Если область действия проверки целостности системы не задана, для задачи проверки целостности системы и задачи обновления снимка состояния системы применяется область действия контроля целостности системы.

► *Чтобы настроить область действия компонента Контроль целостности системы в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры Контроля целостности системы.
6. Чтобы настроить область действия контроля целостности системы в режиме реального времени, выполните следующие действия в блоке **Область действия контроля целостности системы**:
   a. Установите флажок **Следить за устройствами**, если вы хотите, чтобы Контроль целостности системы отслеживал подключение внешних устройств на защищенной виртуальной машине в режиме реального времени.
   b. В раскрывающемся списке выберите уровень важности для событий, которые Контроль целостности системы формирует, когда обнаруживает подключение внешнего устройства. По умолчанию формируются события уровня **Информационное**.
   c. Установите флажок **Следить за файлами и реестром**, если вы хотите, чтобы Контроль целостности системы отслеживал изменения в файлах и реестре на защищенной виртуальной машине в режиме реального времени.
   d. Нажмите на кнопку **Настройка**.
   e. В открывшемся окне **Правила контроля целостности системы** сформируйте список правил, которые применяются при работе компонента Контроль целостности системы в режиме реального времени.

      Вы можете выполнять следующие действия при настройке правил контроля целостности системы:
      - Добавлять или изменять правила (см. раздел "Создание и изменение правила контроля целостности системы" на стр. 332).
      - Импортировать и экспортировать правила (см. раздел "Импорт и экспорт правил контроля целостности системы" на стр. 335).
      - Включать или выключать правила (см. раздел "Включение и выключение правила контроля целостности системы" на стр. 337).
      - Удалять правила.
   f. Нажмите на кнопку **ОК** в окне **Правила контроля целостности системы**.
7. Если вы хотите настроить отдельную область действия для проверки целостности системы по расписанию или по требованию, выполните следующие действия в блоке **Область действия проверки целостности системы**:
   a. Установите флажок **Задать область действия проверки целостности системы**.

      Под флажком появится блок параметров **Область действия проверки целостности системы**.
   b. Настройте параметры в блоке **Область действия проверки целостности системы**, как

описано в пункте 6 этой инструкции. Эти параметры будут применяться при выполнении задачи проверки целостности системы и задачи обновления снимка состояния системы.

8. Нажмите на кнопку **Применить**.

► *Чтобы настроить область действия компонента Контроль целостности системы в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры работы компонента Контроль целостности системы.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Чтобы настроить область действия контроля целостности системы в режиме реального времени, выполните следующие действия в блоке **Параметры Контроля целостности системы**:
   a. Установите флажок **Следить за устройствами**, расположенный под названием блока **Параметры Контроля целостности системы**, если вы хотите, чтобы Контроль целостности системы отслеживал подключение внешних устройств на защищенной виртуальной машине в режиме реального времени.
   b. В раскрывающемся списке выберите уровень важности для событий, которые Контроль целостности системы формирует, когда обнаруживает подключение внешнего устройства. По умолчанию формируются события уровня **Информационное**.
   c. Установите флажок **Следить за файлами и реестром**, расположенный в верхней части блока **Параметры Контроля целостности системы**, если вы хотите, чтобы Контроль целостности системы отслеживал изменения в файлах и реестре на защищенной виртуальной машине в режиме реального времени.
   d. Выполните пункты 6d–6f предыдущей инструкции.
4. Если вы хотите настроить отдельную область действия для проверки целостности системы по расписанию или по требованию, выполните следующие действия в блоке **Параметры Контроля целостности системы**:
   a. Установите флажок **Задать область действия проверки целостности системы**.

      Под флажком появится блок параметров.
   b. Настройте параметры в блоке, как описано в пункте 6 предыдущей инструкции. Эти параметры будут применяться при выполнении задачи проверки целостности системы и задачи обновления снимка состояния системы.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

В этом разделе

Создание и изменение правила контроля целостности системы

Вы можете создать правило контроля целостности системы, сформировав область контроля и / или список исключений из области контроля для файлов и папок, ключей и параметров реестра. После создания или импорта правила контроля целостности системы вы можете изменить параметры правила при необходимости.

► *Чтобы создать или изменить правило контроля целостности системы через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры Контроля целостности системы.
6. Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в одном из следующих блоков:
   - в блоке **Область действия контроля целостности системы**, если вы хотите настроить правило для контроля целостности системы в режиме реального времени;
   - в блоке **Область действия проверки целостности системы**, если вы хотите настроить правило для задачи проверки целостности системы и задачи обновления снимка состояния системы.

   Откроется окно **Правила контроля целостности системы**.
7. Выполните одно из следующих действий:
   - Если вы хотите создать правило контроля целостности системы, нажмите на кнопку **Добавить**, расположенную над списком правил.
   - Если вы хотите изменить правило контроля целостности системы, выберите его в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило контроля целостности системы**.
8. Введите имя правила и выберите уровень важности для событий, которые Контроль целостности системы формирует, когда применяет это правило. По умолчанию формируются события уровня

Информационное.

9. Настройте область контроля файлов и папок на закладке **Файлы**.

   Чтобы добавить файл или папку, изменения в которых будет контролировать программа Kaspersky Security, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**, расположенную над полем **Область контроля** на закладке **Файлы**.

      Откроется окно **Файл или папка**.

   b. Введите абсолютный путь к папке или маску пути к папке, изменения в которой нужно контролировать.

      При вводе маски пути вы можете использовать в любой части пути следующие символы:

      - Символ `*` может заменять любые символы, кроме `\ / : ? " < > | *`. При этом:
        - если символ `*` используется для обозначения имени элемента пути целиком (например, для обозначения имени папки: `/*/`), то он может заменять один и более символов;
        - если символ `*` используется для обозначения части имени элемента пути (например, для обозначения части имени папки: `/abc*/`), то он может заменять ноль и более символов.
      - Символ `?` может заменять любой один символ.

      При вводе пути к папке вы можете использовать переменные окружения. Перед именем переменной окружения и после него требуется указывать символ `%`.

   c. Если требуется контролировать изменения файлов в указанной папке, введите имя или маску файла в поле **Имя или маска файла**.

      При вводе маски вы можете использовать следующие символы:

      - `*` – символ, заменяющий ноль и более символов. Может заменять любые символы, кроме `\ / : ? " < > | *`.
      - `?` – символ, заменяющий любой один символ.

      Если вы хотите контролировать изменения указанных файлов также во вложенных папках, установите флажок **Включая файлы во вложенных папках**.

   d. Нажмите на кнопку **ОК** в окне **Файл или папка**.

   Путь к файлу или папке отображается в списке путей в поле **Область контроля**.

   > Kaspersky Security отслеживает изменения файлов и папок только на тех дисках, которые подключены в момент начала работы контроля целостности системы в режиме реального времени, то есть в момент применения политики или в момент включения контроля целостности системы в режиме реального времени. Если диск отключен в момент начала работы контроля целостности системы в режиме реального времени, изменения файлов и папок на этом диске не отслеживаются, даже если эти файлы и папки добавлены в область контроля.

   Вы можете выполнять поиск по ключевым словам в списке, а также удалять файлы и папки из списка с помощью кнопки **Удалить**.

10. Если требуется, аналогичным образом настройте список путей к файлам и / или папкам, которые исключаются из области контроля. Программа Kaspersky Security не контролирует изменения в

файлах и папках, добавленных в список путей в поле **Исключения**.

Для настройки списка исключений используйте кнопки **Добавить** и **Удалить**, расположенные над полем **Исключения** на закладке **Файлы**.

11. Настройте область контроля ключей реестра и параметров ключей на закладке **Реестр**.

    Чтобы добавить ключ реестра или параметр ключа, изменения в которых будет контролировать программа Kaspersky Security, выполните следующие действия:

    a. Нажмите на кнопку **Добавить**, расположенную над полем **Область контроля** на закладке **Реестр**.

       Откроется окно **Ключ реестра**.

    b. Введите имя ключа реестра, изменения в котором требуется контролировать.

       Ключ HKEY_CURRENT_USER не поддерживается. Вы можете указывать путь к ключу в реестре через раздел HKEY_USER в виде HKEY_USERS\<идентификатор профиля пользователя>\<ключ>.

    c. Если вы хотите, чтобы программа Kaspersky Security контролировала также вложенные ключи, установите флажок **Включая вложенные ключи**.

    d. Если требуется контролировать изменения параметра указанного ключа, введите имя или маску параметра в поле **Имя или маска параметра ключа**.

       При вводе маски вы можете использовать символы `*` (любая последовательность символов) и `?` (любой один символ).

    e. Нажмите на кнопку **OK** в окне **Ключ реестра**.

    Имя ключа и параметр ключа, если он был указан, отображается в списке ключей и параметров реестра в поле **Область контроля**.

    Вы можете выполнять поиск по ключевым словам в списке, а также удалять ключи из списка с помощью кнопки **Удалить**.

12. Если требуется, аналогичным образом настройте список ключей и параметров реестра, которые исключаются из области контроля. Программа Kaspersky Security не контролирует изменения ключей и параметров реестра, добавленных в список в поле **Исключения**.

    Для настройки списка исключений используйте кнопки **Добавить** и **Удалить**, расположенные над полем **Исключения** на закладке **Реестр**.

13. Нажмите на кнопку **OK** в окне **Правило контроля целостности системы**.

    Правило отображается в списке правил в окне **Правила контроля целостности системы**.

14. Нажмите на кнопку **OK** в окне **Правила контроля целостности системы**.

15. Нажмите на кнопку **Применить**.

► *Чтобы создать или изменить правило контроля целостности системы в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль целостности системы**.

В правой части окна отобразятся параметры работы компонента Контроль целостности системы.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в верхней части блока **Параметры Контроля целостности системы**, если вы хотите настроить правило для контроля целостности системы в режиме реального времени.
   - Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в нижней части блока **Параметры Контроля целостности системы**, если вы хотите настроить правило для задачи проверки целостности системы и задачи обновления снимка состояния системы.

   Откроется окно **Правила контроля целостности системы**.
4. Выполните пункты 7–14 предыдущей инструкции.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Импорт и экспорт правил контроля целостности системы

Вы можете сохранить настроенный список правил контроля целостности системы в файле и загрузить ранее сохраненный список правил из файла. Для импорта и экспорта списка правил вы можете использовать файл в формате XML.

При настройке параметров компонента Контроль целостности системы через Kaspersky Security Center вы можете импортировать список правил контроля целостности системы из шаблонов, которые входят в комплект поставки программы Kaspersky Security. Шаблон содержит пути к файлам и папкам, а также ключи и параметры реестра, которые используются в работе какой-либо программы. Правила, импортированные из шаблона, позволяют отслеживать изменения, связанные с работой этой программы.

► *Чтобы импортировать или экспортировать список правил контроля целостности системы через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры Контроля целостности системы.
6. Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в одном из следующих блоков:
   - в блоке **Область действия контроля целостности системы**, если вы хотите настроить

правило для контроля целостности системы в режиме реального времени;

- в блоке **Область действия проверки целостности системы**, если вы хотите настроить правило для задачи проверки целостности системы и задачи обновления снимка состояния системы.

Откроется окно **Правила контроля целостности системы**.

7. Если вы хотите импортировать список правил контроля целостности системы, нажмите на кнопку **Импорт** и выполните одно из следующих действий:
   - Чтобы импортировать правило из шаблона, в раскрывающемся списке выберите **Из шаблона**, в открывшемся окне выберите имя шаблона и нажмите на кнопку **OK**.

     В список правил в окне **Правила контроля целостности системы** будет добавлено правило из выбранного шаблона.
   - Чтобы импортировать правила из файла, в раскрывающемся списке выберите **Из файла** и укажите путь к файлу в формате XML в открывшемся окне.

     В список правил в окне **Правила контроля целостности системы** будут добавлены правила из выбранного файла.
8. Если вы хотите экспортировать список правил контроля целостности системы, нажмите на кнопку **Экспорт** и укажите путь к файлу, в котором вы хотите сохранить список правил.
9. Нажмите на кнопку **OK** в окне **Правила контроля целостности системы**.
10. Нажмите на кнопку **Применить**.

► *Чтобы импортировать или экспортировать список правил контроля целостности системы в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры работы компонента Контроль целостности системы.

   > Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в верхней части блока **Параметры Контроля целостности системы**, если вы хотите настроить правило для контроля целостности системы в режиме реального времени.
   - Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в нижней части блока **Параметры Контроля целостности системы**, если вы хотите настроить правило для задачи проверки целостности системы и задачи обновления снимка состояния системы.

   Откроется окно **Правила контроля целостности системы**.
4. Выполните пункты 7–9 предыдущей инструкции.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение правила контроля целостности системы

Все правила контроля целостности системы добавляются в список правил со статусом *Включено*. Если правило включено, Контроль целостности системы применяет это правило.

Вы можете выключить любое правило контроля целостности системы. Если правило выключено, Контроль целостности системы временно не применяет это правило.

► *Чтобы включить или выключить правило контроля целостности системы через Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры Контроля целостности системы.
6. Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в одном из следующих блоков:
   - в блоке **Область действия контроля целостности системы**, если вы хотите настроить правило для контроля целостности системы в режиме реального времени;
   - в блоке **Область действия проверки целостности системы**, если вы хотите настроить правило для задачи проверки целостности системы и задачи обновления снимка состояния системы.

   Откроется окно **Правила контроля целостности системы**.
7. В списке правил контроля целостности системы выберите нужное вам правило и выполните одно из следующих действий в графе **Статус**:
   - Выберите значение **Вкл**, если вы хотите включить правило.
   - Выберите значение **Выкл**, если вы хотите выключить правило.
8. Нажмите на кнопку **ОК** в окне **Правила контроля целостности системы**.
9. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить правило контроля целостности системы в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль целостности системы**.

   В правой части окна отобразятся параметры работы компонента Контроль целостности системы.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в верхней части блока **Параметры Контроля целостности системы**, если вы хотите настроить правило для контроля целостности системы в режиме реального времени.
   - Нажмите на кнопку **Настройка**, расположенную справа от флажка **Следить за файлами и реестром** в нижней части блока **Параметры Контроля целостности системы**, если вы хотите настроить правило для задачи проверки целостности системы и задачи обновления снимка состояния системы.

   Откроется окно **Правила контроля целостности системы**.
4. Выполните пункты 7–8 предыдущей инструкции.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Создание и обновление снимка состояния системы

Вы можете создать и впоследствии обновлять снимок состояния системы защищенных виртуальных машин с помощью задачи обновления снимка состояния системы.

Вы можете создать и настроить задачу обновления снимка состояния системы для защищенных виртуальных машин, которые входят в группу администрирования, с помощью Консоли администрирования Kaspersky Security Center. Вы можете настроить задачу обновления снимка состояния системы для одной виртуальной машины в локальном интерфейсе Легкого агента для Windows.

Задача запускается на виртуальной машине и в специальном формате сохраняет информацию о состоянии объектов контроля, которые вы включили в область действия проверки целостности системы. Если вы не задали область действия проверки целостности системы, состав объектов определяется областью действия контроля целостности системы. Область действия проверки и область действия контроля настраиваются в политике, которая применяется на виртуальной машине, или в локальном интерфейсе Легкого агента для Windows.

► *Чтобы создать или обновить снимок состояния системы на виртуальных машинах с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех виртуальных машин, входящих в эту группу. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или

нескольких виртуальных машин (задачу для набора устройств).

3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows** выберите **Обновление снимка состояния системы**.

   Перейдите к следующему шагу мастера создания задачи.
5. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора виртуальных машин, для которых вы создаете задачу. Вы можете выбрать виртуальные машины из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса виртуальных машин вручную, импортировать список виртуальных машин из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора виртуальных машин в открывшемся окне выполните одно из следующих действий:
   - В списке обнаруженных виртуальных машин укажите виртуальные машины, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия виртуальной машины.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса виртуальных машин вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов виртуальных машин.
   - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей виртуальные машины, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.
6. В поле **Имя** введите имя задачи обновления снимка состояния системы.

   Перейдите к следующему шагу мастера создания задачи.
7. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

   > В результате выполнения задачи с параметрами по умолчанию программа выполняет обновление снимка состояния системы только по изменившимся или новым объектам из области контроля (инкрементальное обновление).

   Завершите работу мастера.

   Созданная задача отобразится в списке задач.
8. Если вы хотите выполнить полное обновление снимка состояния системы, измените параметры задачи следующим образом:
   a. Откройте окно свойств созданной задачи двойным щелчком мыши.
   b. Перейдите в раздел **Параметры** и выберите вариант **Полное обновление**.
   c. Нажмите на кнопку **ОК**.
9. Запустите задачу (см. раздел "Запуск и остановка задач" на стр. 147) обновления снимка состояния системы.

В результате выполнения задачи на каждой виртуальной машине, которую вы указали в параметрах

задачи, создается или обновляется ранее созданный снимок состояния системы.

► *Чтобы создать или обновить снимок состояния системы на виртуальной машине через локальный интерфейс Легкого агента для Windows, выполните следующие действия:*

1. Если требуется, настройте параметры задачи обновления снимка состояния системы. Для этого выполните следующие действия:
   a. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
   b. В левой части окна в блоке **Задачи по расписанию** выберите раздел **Обновление снимка состояния системы**.

      В правой части окна отобразятся параметры задачи обновления снимка состояния системы.

      Если в блоке отсутствует раздел **Обновление снимка состояния системы**, это означает, что отображение и управление локальными задачами запрещены политикой для всех защищенных виртуальных машин группы администрирования. Вы можете включить и выключить отображение и управление локальными задачами в политике Легкого агента для Windows (подраздел **Дополнительные параметры** в разделе **Другие параметры**).

   c. Выберите режим обновления снимка состояния системы:
      - **Полное обновление** – по всем объектам, входящим в область контроля.
      - **Инкрементальное обновление** – только по изменившимся или новым объектам из области контроля.
   d. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.
2. Запустите задачу (см. раздел "Запуск и остановка задач" на стр. 147) обновления снимка состояния системы.

Проверка целостности системы по расписанию или по требованию

Вы можете проверять целостность системы на защищенных виртуальных машинах с помощью задачи проверки целостности системы.

Вы можете создать и настроить задачу проверки целостности системы для защищенных виртуальных машин, которые входят в группу администрирования, с помощью Консоли администрирования Kaspersky Security Center. Вы можете настроить задачу проверки целостности системы для одной виртуальной машины в локальном интерфейсе Легкого агента для Windows.

Для успешного выполнения задачи требуется, чтобы снимок состояния системы (см. раздел "Создание и изменение правила контроля целостности системы" на стр. 332) полностью соответствовал области действия проверки целостности системы на момент запуска задачи проверки целостности системы. Если состав объектов, состояние которых зафиксировано в снимке состояния системы, отличается от состава объектов, входящих в область действия проверки целостности системы, задача проверки целостности системы завершается с ошибкой.

► *Чтобы проверить целостность системы на виртуальных машинах с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех виртуальных машин, входящих в эту группу. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин (задачу для набора устройств).
3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows** выберите **Проверка целостности системы**.

   Перейдите к следующему шагу мастера создания задачи.
5. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора виртуальных машин, для которых вы создаете задачу. Вы можете выбрать виртуальные машины из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса виртуальных машин вручную, импортировать список виртуальных машин из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора виртуальных машин в открывшемся окне выполните одно из следующих действий:
   - В списке обнаруженных виртуальных машин укажите виртуальные машины, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия виртуальной машины.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса виртуальных машин вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов виртуальных машин.
   - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей виртуальные машины, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.
6. В раскрывающемся списке **Запуск по расписанию** выберите **Вручную**.

   Перейдите к следующему шагу мастера создания задачи.

7. В поле **Имя** введите имя задачи проверки целостности системы.

   Перейдите к следующему шагу мастера создания задачи.

8. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

   > В результате выполнения задачи с параметрами по умолчанию программа выполняет проверку целостности системы в режиме **Полная проверка** (при проверке изменений в файлах учитываются все атрибуты файлов и содержимое файлов).

   Завершите работу мастера.

   Созданная задача отобразится в списке задач.

9. Если вы хотите, чтобы при проверке изменений в файлах программа учитывала только атрибуты файлов и не проверяла содержимое файлов, измените параметры задачи следующим образом:

   a. Откройте окно свойств созданной задачи двойным щелчком мыши.

   b. Перейдите в раздел **Параметры** и выберите вариант **Быстрая проверка**.

   c. Нажмите на кнопку **OK**.

10. Запустите задачу (см. раздел "Запуск и остановка задач" на стр. 147) проверки целостности системы.

Проверка целостности системы выполняется на каждой виртуальной машине, которую вы указали в параметрах задачи. Вы можете посмотреть результаты ее выполнения (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 148) в Консоли администрирования.

► *Чтобы проверить целостность системы на виртуальной машине в локальном интерфейсе Легкого агента для Windows, выполните следующие действия:*

1. Если требуется, настройте параметры задачи проверки целостности системы. Для этого выполните следующие действия:

   a. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).

   b. В левой части окна в блоке **Задачи по расписанию** выберите раздел **Проверка целостности системы**.

      В правой части окна отобразятся параметры задачи проверки целостности системы.

      > Если в блоке отсутствует раздел **Проверка целостности системы**, это означает, что отображение локальных задач и управление ими запрещены политикой для всех защищенных виртуальных машин группы администрирования. Вы можете включить и выключить отображение локальных задач и управление ими в политике Легкого агента для Windows (подраздел **Дополнительные параметры** в разделе **Другие параметры**).

   c. Выберите режим проверки:

      - **Полная проверка** – при проверке изменений в файлах учитываются все атрибуты файлов и содержимое файлов. Этот вариант выбран по умолчанию.
      - **Быстрая проверка** – при проверке изменений в файлах учитываются только атрибуты файлов и не проверяется содержимое файлов.

d. Если требуется, измените режим запуска задачи. Рекомендуется использовать режим запуска **Вручную**. Этот режим выбран по умолчанию.

e. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

2. Запустите задачу (см. раздел "Запуск и остановка задач" на стр. 147) проверки целостности системы.

Просмотр информации о целостности системы на виртуальной машине

Информация о результатах работы компонента Контроль целостности системы отображается следующими способами:

- В виде событий Kaspersky Security Center. Компонент Контроль целостности системы отправляет событие в Kaspersky Security Center, если обнаруживает на защищенной виртуальной машине подключение внешнего устройства или изменение в файлах или реестре.

  Все события от компонента Контроль целостности системы отображаются в списке событий Kaspersky Security Center в Консоли администрирования. Вы можете настроить выборку событий, чтобы посмотреть события от компонента Контроль целостности системы. Подробнее о настройке выборки событий см. в документации Kaspersky Security Center.

  События, произошедшие при последнем запуске задачи проверки целостности системы на виртуальной машине отображаются в свойствах программы, установленной на виртуальной машине (см. раздел "Просмотр событий, произошедших во время последнего запуска задачи проверки целостности системы" на стр. 344).

- Путем изменения статуса виртуальной машины в Kaspersky Security Center. При получении от компонента Контроль целостности системы событий с уровнем важности *Критическое* или *Важное* Kaspersky Security Center изменяет статус клиентского устройства для защищенной виртуальной машины на *Критический* или *Предупреждение*.

  > Получение статуса устройства от управляемой программы должно быть включено в Kaspersky Security Center в списках условий назначения статусов *Критический* и *Предупреждение*. Условия назначения статусов устройства настраиваются в окне свойств группы администрирования.

  Статус клиентского устройства и все причины изменения статуса отображаются в списке устройств, входящих в группу администрирования. Подробнее о статусах клиентского устройства см. в документации Kaspersky Security Center.

  Вы можете сбросить статус, полученный от компонента Контроль целостности системы (см. раздел "Сброс статуса целостности системы" на стр. 350).

- В результатах выполненной задачи (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 148) проверки целостности системы в Kaspersky Security Center.

- В виде отчетов в Kaspersky Security Center. В Kaspersky Security Center предусмотрено два типа отчетов:

  - отчет об устройствах, на которых произошло максимальное количество срабатываний правил Контроля целостности системы (см. раздел "Просмотр отчета о виртуальных машинах, на которых произошло максимальное количество срабатываний правил Контроля целостности

системы" на стр. 345);

- отчет о правилах Контроля целостности системы, которые чаще всего срабатывали на защищенных виртуальных машинах (см. раздел "Просмотр отчета о наиболее часто срабатывающих правилах Контроля целостности системы" на стр. 348).

- В виде отчетов в локальном интерфейсе Легкого агента (см. раздел "Работа с отчетами в локальном интерфейсе" на стр. 431). В окне **Отчеты и хранилища** на закладке **Отчеты** вы можете посмотреть следующие отчеты:
  - отчет о работе Контроля целостности системы в реальном времени (отчет Контроль целостности системы);
  - отчет о выполнении задачи проверки целостности системы (отчет Проверка целостности системы);
  - отчет о выполнении задачи обновления снимка состояния системы (отчет Обновление снимка состояния системы).

В этом разделе

Просмотр событий, произошедших во время последнего запуска задачи проверки целостности системы

Вы можете посмотреть список событий, произошедших при последнем запуске задачи проверки целостности системы, в свойствах программы Kaspersky Security, установленной на защищенной виртуальной машине.

► *Чтобы просмотреть с помощью Консоли администрирования список событий, произошедших на виртуальной машине во время последнего запуска задачи проверки целостности системы, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, в которую входит нужная виртуальная машина.
3. В рабочей области выберите закладку **Устройства**.
4. В списке выберите виртуальную машину, для которой вы хотите посмотреть список событий, произошедших при проверке целостности системы.
5. Откройте окно свойств виртуальной машины двойным щелчком мыши.

   Откроется окно **Свойства: <Имя виртуальной машины>**.
6. В списке слева выберите раздел **Программы**.

В правой части окна отобразится список программ, установленных на этой виртуальной машине.

7. Выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент** и откройте окно параметров программы двойным щелчком мыши.

   Откроется окно **Параметры программы Kaspersky Security для виртуальных сред 5.2 Легкий агент**.

8. В списке слева выберите раздел **События Контроля целостности системы**.

   В таблице отображаются следующие сведения о каждом событии:

   - Дата формирования события.
   - Наименование события.
   - Правило, которое применил компонент Контроль целостности системы.
   - Объект контроля, в котором зафиксировано изменение. В зависимости от типа объекта контроля в графе отображается следующая информация:
     - Путь к файлу, если компонент Контроль целостности системы обнаружил изменение в файле.
     - Ключ реестра, если компонент Контроль целостности системы обнаружил изменение в реестре.
     - Название устройства, если компонент Контроль целостности системы обнаружил подключение внешнего устройства.
   - Характер изменения объекта контроля, обнаруженный компонентом Контроль целостности системы. Возможные значения:
     - Создание.
     - Изменение.
     - Удаление.
     - Подключение.

   В списке событий вы можете выполнять следующие действия:

   - обновлять список событий;
   - фильтровать список событий по значениям граф или по условиям сложного фильтра;
   - использовать функцию поиска определенного события;
   - изменять порядок и набор граф, отображаемых в отчете;
   - сортировать список событий по каждой графе;
   - сохранять отчет в текстовый файл формата TXT или CSV.

Просмотр отчета о виртуальных машинах, на которых произошло максимальное количество срабатываний правил Контроля целостности системы

► *Чтобы просмотреть отчет о виртуальных машинах, на которых произошло максимальное количество срабатываний правил Контроля целостности системы, с помощью Консоли*

администрирования, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В рабочей области узла **Сервер администрирования** перейдите на закладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**, чтобы запустить мастер создания шаблона отчета.
4. Следуйте указаниям мастера.
5. В окне **Выбор типа шаблона отчета** в разделе **Другое** выберите тип **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.
6. После создания шаблона отчета выберите его в списке шаблонов на закладке **Отчеты**.

В рабочей области отобразится отчет.

В поле **Период** отображается отчетный период, для которого был построен отчет. По умолчанию отчет создается за последние 30 дней, включая дату создания отчета.

Отчет состоит из двух таблиц:

- таблица сводной информации содержит сведения о защищенных виртуальных машинах, на которых произошло максимальное количество срабатываний правил Контроля целостности системы;
- таблица детальной информации содержит сведения о каждом факте срабатывания правила.

Вы можете настроить отображение граф в каждой таблице. О добавлении и удалении граф в таблицах отчета см. в документации Kaspersky Security Center.

Таблица сводной информации содержит следующие сведения:

- **Имя устройства** – имя защищенной виртуальной машины, на которой сработали правила Контроля целостности системы.
- **Количество событий** – количество срабатываний правил Контроля целостности системы на защищенной виртуальной машине.
- **Количество правил** – количество правил Контроля целостности системы, сработавших на защищенной виртуальной машине.

  В строке ниже отображается следующая сводная информация:

  - **Количество устройств** – общее количество защищенных виртуальных машин, на которых сработали правила Контроля целостности системы.
  - **Количество событий** – общее количество срабатываний правил Контроля целостности системы на защищенных виртуальных машинах.
  - **Достигнуто ограничение приема событий** – информация, о том, было ли достигнуто максимальное количество событий, которое Kaspersky Security Center может получать от компонентов Контроль целостности системы на клиентских компьютерах. Ограничение на количество получаемых событий настраивается в реестре программы Kaspersky Security Center и по умолчанию составляет 15 000 событий в сутки. Если количество полученных событий превысило ограничение, в поле отображается `Да`.

Таблица детальной информации содержит следующие сведения:

- **Виртуальный Сервер** – имя виртуального Сервера администрирования (при наличии), под управлением которого находится защищенная виртуальная машина.
- **Имя группы** – имя группы, в которую входит защищенная виртуальная машина, на которой

сработало правило Контроля целостности системы.

- **IP-адрес** – IP-адрес защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **Время последнего выхода на связь** – дата и время, когда защищенная виртуальная машина, на которой сработало правило Контроля целостности системы, была замечена в сети Сервером администрирования.
- **Время последнего подключения к Агенту администрирования** – дата и время последней синхронизации Агента администрирования с Сервером администрирования.
- **Имя устройства** – имя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **NetBIOS-имя** – имя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **Имя домена** – имя домена, к которому относится защищенная виртуальная машина, на которой сработало правило Контроля целостности системы.
- **DNS-имя** – DNS-имя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **DNS-имя домена** – DNS-имя домена, к которому относится защищенная виртуальная машина, на которой сработало правило Контроля целостности системы.
- **Важность** – уровень важности события Контроля целостности системы. Возможные значения: `Информационное сообщение`, `Важное сообщение`, `Критическое сообщение`.
- **Время возникновения** – дата и время возникновения события.
- **Название сработавшего правила** – название сработавшего правила Контроля целостности системы.
- **Путь к объекту** – путь к объекту контроля, изменение которого обнаружил компонент Контроль целостности системы. В зависимости от типа объекта контроля в графе отображается следующая информация:
  - Путь к файлу или папке, если компонент Контроль целостности системы обнаружил изменение в файле или папке.
  - Ключ реестра, если компонент Контроль целостности системы обнаружил изменение в реестре.
  - Внешнее устройство, если компонент Контроль целостности системы обнаружил подключение внешнего устройства.
- **Действие** – действие, произведенное над объектом контроля. Возможные значения: `Создание`, `Изменение`, `Удаление`, `Подключение`.
- **Тип объекта** – тип объекта контроля, изменение которого обнаружил компонент Контроль целостности системы. Возможные значения: `Файл или папка`, `Ключ реестра`, `Внешнее устройство`.
- **Компонент Контроль целостности системы был отключен** – информация, о том, был ли компонент Контроль целостности системы выключен во время возникновения события. Для программы Kaspersky Security в этом поле всегда отображается `Нет`.
- **Пользователь** – учетная запись пользователя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.

Просмотр отчета о наиболее часто срабатывающих правилах Контроля целостности системы

► *Чтобы просмотреть отчет о наиболее часто срабатывающих правилах Контроля целостности системы с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В рабочей области узла **Сервер администрирования** перейдите на закладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**, чтобы запустить мастер создания шаблона отчета.
4. Следуйте указаниям мастера.
5. В окне **Выбор типа шаблона отчета** в разделе **Другое** выберите тип **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах**.
6. После создания шаблона отчета выберите его в списке шаблонов на закладке **Отчеты**.

В рабочей области отобразится отчет.

В поле **Период** отображается отчетный период, для которого был построен отчет. По умолчанию отчет создается за последние 30 дней, включая дату создания отчета.

Отчет состоит из двух таблиц:

- таблица сводной информации содержит сведения о правилах Контроля целостности системы, которые чаще всего срабатывали на устройствах за отчетный период;
- таблица детальной информации содержит сведения о каждом факте срабатывания правила.

Вы можете настроить отображение граф в каждой таблице. О добавлении и удалении граф в таблицах отчета см. в документации Kaspersky Security Center.

Таблица сводной информации содержит следующие сведения:

- **Название сработавшего правила** – название сработавшего правила Контроля целостности системы.
- **Количество событий** – количество срабатываний правила Контроля целостности системы на защищенных виртуальных машинах.
- **Количество устройств** – количество защищенных виртуальных машин, на которых сработало правило Контроля целостности системы.

  В строке ниже отображается следующая сводная информация:

  - **Количество устройств** – общее количество защищенных виртуальных машин, на которых сработали правила Контроля целостности системы.
  - **Количество событий** – общее количество срабатываний правил Контроля целостности системы на защищенных виртуальных машинах.
  - **Достигнуто ограничение приема событий** – информация, о том, было ли достигнуто максимальное количество событий, которое Kaspersky Security Center может получать от компонентов Контроль целостности системы на клиентских компьютерах. Ограничение на количество получаемых событий настраивается в реестре программы Kaspersky Security Center и по умолчанию составляет 15 000 событий в сутки. Если количество полученных событий превысило ограничение, в поле отображается `Да`.

Таблица детальной информации содержит следующие сведения:

- **Виртуальный Сервер** – имя виртуального Сервера администрирования (при наличии), под управлением которого находится защищенная виртуальная машина.
- **Имя группы** – имя группы, в которую входит защищенная виртуальная машина, на которой сработало правило Контроля целостности системы.
- **IP-адрес** – IP-адрес защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **Время последнего выхода на связь** – дата и время, когда защищенная виртуальная машина, на которой сработало правило Контроля целостности системы, была замечена в сети Сервером администрирования.
- **Время последнего подключения к Агенту администрирования** – дата и время последней синхронизации Агента администрирования с Сервером администрирования.
- **Имя устройства** – имя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **NetBIOS-имя** – имя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **Имя домена** – имя домена, к которому относится защищенная виртуальная машина, на которой сработало правило Контроля целостности системы.
- **DNS-имя** – DNS-имя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.
- **DNS-имя домена** – DNS-имя домена, к которому относится защищенная виртуальная машина, на которой сработало правило Контроля целостности системы.
- **Важность** – уровень важности события Контроля целостности системы. Возможные значения: `Информационное сообщение`, `Важное сообщение`, `Критическое сообщение`.
- **Время возникновения** – дата и время возникновения события.
- **Название сработавшего правила** – название сработавшего правила Контроля целостности системы.
- **Путь к объекту** – путь к объекту контроля, изменение которого обнаружил компонент Контроль целостности системы. В зависимости от типа объекта контроля в графе отображается следующая информация:
  - Путь к файлу или папке, если компонент Контроль целостности системы обнаружил изменение в файле или папке.
  - Ключ реестра, если компонент Контроль целостности системы обнаружил изменение в реестре.
  - Внешнее устройство, если компонент Контроль целостности системы обнаружил подключение внешнего устройства.
- **Действие** – действие, произведенное над объектом контроля. Возможные значения: `Создание`, `Изменение`, `Удаление`, `Подключение`.
- **Тип объекта** – тип объекта контроля, изменение которого обнаружил компонент Контроль целостности системы. Возможные значения: `Файл или папка`, `Ключ реестра`, `Внешнее устройство`.
- **Компонент Контроль целостности системы был отключен** – информация, о том, был ли компонент Контроль целостности системы выключен во время возникновения события. Для

программы Kaspersky Security в этом поле всегда отображается `Нет`.

- **Пользователь** – учетная запись пользователя защищенной виртуальной машины, на которой сработало правило Контроля целостности системы.

Сброс статуса целостности системы

Если причиной изменения статуса виртуальной машины (см. раздел "Статус клиентского устройства в Kaspersky Security Center" на стр. 159) на *Критический* или *Предупреждение* были события Контроля целостности системы, такой статус называется *статусом целостности системы*.

Вы можете сбросить статус целостности системы в Kaspersky Security Center, то есть отменить для виртуальных машин статусы *Критический* и *Предупреждение.*

Вы можете сбросить статус целостности системы для одной виртуальной машины (см. раздел "Сброс статуса целостности системы для одной виртуальной машины" на стр. 350) или создать групповую задачу сброса статуса целостности системы для нескольких защищенных виртуальных машин, входящих в группу администрирования (см. раздел "Создание задачи сброса статуса целостности системы" на стр. 351).

В этом разделе

Сброс статуса целостности системы для одной виртуальной машины

► *Чтобы сбросить статус целостности системы для одной виртуальной машины с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, в которую входит нужная виртуальная машина.
3. В рабочей области выберите закладку **Устройства**.
4. В списке выберите виртуальную машину, для которой вы хотите посмотреть статус, полученный от компонента Контроль целостности системы.
5. Откройте окно свойств виртуальной машины двойным щелчком мыши.

   Откроется окно **Свойства: <Имя виртуальной машины>**.
6. В списке слева выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на этой виртуальной машине.
7. Выберите **Kaspersky Security для виртуальных сред 5.2 Легкий агент** и откройте окно параметров программы двойным щелчком мыши.

   Откроется окно **Параметры программы Kaspersky Security для виртуальных сред 5.2 Легкий агент**.

8. В списке слева выберите раздел **Статус целостности системы на виртуальной машине**.
9. В правой части окна нажмите на кнопку **Сбросить статус**.

Если причиной изменения статуса виртуальной машины на *Критический* или *Предупреждение* были события Контроля целостности системы, виртуальной машине назначается статус *OK*.

Если статус был изменен также по причине других событий или по правилам назначения статусов Kaspersky Security Center, то статус для виртуальной машины не изменяется.

Создание задачи сброса статуса целостности системы

Вы можете создавать задачу сброса статуса целостности системы с помощью Консоли администрирования. Задача запускается вручную (см. раздел "Запуск и остановка задач" на стр. 147). Сброс статуса целостности системы выполняется на каждой виртуальной машине, которую вы указали в параметрах задачи.

► *Чтобы создать задачу сброса целостности системы на виртуальных машинах с помощью Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех виртуальных машин, входящих в эту группу. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин (задачу для набора устройств).
3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows** выберите **Сброс статуса целостности системы**.

   Перейдите к следующему шагу мастера создания задачи.
5. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора виртуальных машин, для которых вы создаете задачу. Вы можете выбрать виртуальные машины из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса виртуальных машин вручную, импортировать список виртуальных машин из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора виртуальных машин в открывшемся окне выполните одно из следующих действий:
   - В списке обнаруженных виртуальных машин укажите виртуальные машины, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия виртуальной машины.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса виртуальных машин вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT,

содержащий перечень адресов виртуальных машин.

- Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей виртуальные машины, для которых вы создаете задачу.

Перейдите к следующему шагу мастера создания задачи.

6. В поле **Имя** введите имя задачи сброса статуса целостности системы.

   Перейдите к следующему шагу мастера создания задачи.

7. 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.

Мониторинг сети

Описанная в этом разделе функциональность программы Kaspersky Security доступна, только если программа установлена на виртуальной машине с операционной системой Windows для серверов или с операционной системой Windows для рабочих станций.

Мониторинг сети – это инструмент, предназначенный для просмотра в локальном интерфейсе Легкого агента для Windows информации о сетевой активности защищенной виртуальной машины в реальном времени.

► *Чтобы запустить мониторинг сети, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.
4. По правой клавише мыши откройте контекстное меню строки **Сетевой экран** и выберите пункт **Мониторинг сети**.

   Откроется окно **Мониторинг сети**. В этом окне информация о сетевой активности защищенной виртуальной машины представлена на четырех закладках:

   - На закладке **Сетевая активность** отображаются все активные на текущий момент сетевые соединения защищенной виртуальной машины. Отображаются как сетевые соединения, инициированные защищенной виртуальной машиной, так и входящие сетевые соединения.
   - На закладке **Открытые порты** перечислены все открытые сетевые порты на защищенной виртуальной машине.
   - На закладке **Сетевой трафик** отображается объем входящего и исходящего сетевого трафика между защищенной виртуальной машиной и другими компьютерами сети, в которой вы работаете в текущий момент.
   - На закладке **Заблокированные компьютеры** представлен список IP-адресов удаленных компьютеров, сетевую активность которых компонент Защита от сетевых атак заблокировал, обнаружив попытку сетевой атаки с этого IP-адреса.

Проверка виртуальной машины

При старте защищенной виртуальной машины вместе с программой Kaspersky Security автоматически включается и непрерывно продолжает работать *постоянная защита* виртуальной машины. Постоянная защита заключается в проверке файлов защищенной виртуальной машины при доступе к ним на наличие вредоносных программ. Когда пользователь или какая-нибудь программа обращается к файлу на защищенной виртуальной машине (например, записывает или считывает его), программа Kaspersky Security перехватывает обращение к этому файлу.

В дополнение к постоянной защите требуется регулярно выполнять *антивирусную проверку* защищенной виртуальной машины, то есть проверку на вирусы и другие программы, представляющие угрозу, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены программой, например, из-за установленного низкого уровня защиты или по другим причинам. Антивирусная проверка является важным фактором для обеспечения безопасности виртуальной машины.

Проверка виртуальных машин выполняется с помощью *задач проверки*.

Задачи Поиск вирусов в Kaspersky Security Center

После установки mmc-плагинов Kaspersky Security в Kaspersky Security Center автоматически создаются следующие задачи проверки:

- Задача **Поиск вирусов** для Легкого агента для Windows. Задача создается для группы администрирования **Управляемые устройства** и может запускаться на всех виртуальных машинах с установленным компонентом Легкий агент для Windows, которые входят в группу **Управляемые устройства** или в любую вложенную группу администрирования. При необходимости вы можете изменить параметры этой задачи или удалить ее и создать новую задачу поиска вирусов.
- Задача **Поиск вирусов** для Легкого агента для Linux. Задача создается для группы администрирования **Управляемые устройства** и может запускаться на всех виртуальных машинах с установленным компонентом Легкий агент для Linux, которые помещены в группу **Управляемые устройства** или в любую вложенную группу администрирования. При необходимости вы можете изменить параметры этой задачи или удалить ее и создать новую задачу поиска вирусов.

В процессе выполнения задачи **Поиск вирусов** программа Kaspersky Security выполняет антивирусную проверку областей защищенной виртуальной машины, указанных в параметрах задачи. Управление задачей осуществляется в Kaspersky Security Center.

Задачи проверки в локальном интерфейсе Легкого агента для Windows

На защищенных виртуальных машинах с установленным компонентом Легкий агент для Windows предусмотрены следующие задачи проверки (см. раздел "Управление задачами через локальный интерфейс Легкого агента для Windows" на стр. 143), которые вы можете настраивать через локальный интерфейс Легкого агента для Windows:

- **Полная проверка**.
- **Проверка важных областей**.
- **Выборочная проверка**.

Задача полной проверки и задача проверки важных областей являются специфическими. Для этих задач не рекомендуется изменять область проверки.

После запуска задач проверки (см. раздел "Запуск и остановка задач" на стр. 147) процесс выполнения проверки отображается в поле напротив названия запущенной задачи проверки в блоке **Управление задачами** на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 120).

Информация о результатах проверки и обо всех событиях, произошедших во время выполнения задач проверки, записывается в отчеты программы (см. раздел "Настройка параметров отчетов" на стр. 429).

Задачи проверки для Легкого агента для Linux

На защищенных виртуальных машинах с установленным компонентом Легкий агент для Linux предусмотрены следующие задачи проверки, которыми вы можете управлять с помощью командной строки (см. раздел «Проверка виртуальной машины» на стр. 486):

- *Полная проверка* (на стр. 487).
- *Выборочная проверка* (на стр. 487).

В этом разделе

Создание задачи поиска вирусов

Вы можете создавать задачу **Поиск вирусов** для Легкого агента для Windows и для Легкого агента для Linux в Консоли администрирования.

Во время создания задачи вы можете задать расписание запуска задачи. Независимо от заданного расписания вы можете в любой момент запустить или остановить задачу (см. раздел "Запуск и остановка задач" на стр. 147) вручную.

► *Чтобы создать задачу поиска вирусов для Легкого агента для Windows в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех виртуальных машин, входящих в эту группу. В рабочей области выберите закладку **Задачи**.

- Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин (задачу для набора устройств).

3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows** выберите **Поиск вирусов**.

   Перейдите к следующему шагу мастера.
5. В окне **Область проверки** сформируйте список объектов, которые проверяет Kaspersky Security (см. раздел "Формирование области проверки задачи" на стр. 360).

   Перейдите к следующему шагу мастера создания задачи.
6. В окне **Действие Kaspersky Security для виртуальных сред 5.2 Легкий агент** выполните следующие действия:

   - Выберите действие, которое выполняет программа Kaspersky Security (см. раздел "Изменение действия над зараженными файлами" на стр. 359), если в результате проверки обнаруживает зараженные файлы.
   - Установите флажок **Выполнять лечение активного заражения немедленно**, если вы хотите, чтобы программа выполняла процедуру лечения активного заражения (см. раздел "Технология лечения активного заражения" на стр. 194) сразу после его обнаружения в процессе выполнения групповой задачи поиска вирусов и перезагружала виртуальную машину после лечения активного заражения без запроса подтверждения у пользователя.
   - Установите флажок **Приостанавливать проверку по расписанию, если защищенная виртуальная машина разблокирована**, если вы хотите, чтобы программа приостанавливала запуск задачи проверки, если ресурсы виртуальной машины заняты.

   Перейдите к следующему шагу мастера.
7. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора виртуальных машин, для которых вы создаете задачу. Вы можете выбрать виртуальные машины из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса виртуальных машин вручную, импортировать список виртуальных машин из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора виртуальных машин в открывшемся окне выполните одно из следующих действий:

   - В списке обнаруженных виртуальных машин укажите виртуальные машины, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия виртуальной машины.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса виртуальных машин вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов виртуальных машин.
   - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей виртуальные машины, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.
8. Далее следуйте указаниям мастера создания задачи.

► *Чтобы создать задачу поиска вирусов для Легкого агента для Linux в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех виртуальных машин, входящих в эту группу. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин (задачу для набора устройств).
3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux** выберите **Поиск вирусов**.

   Перейдите к следующему шагу мастера.
5. В окне **Область проверки** сформируйте список объектов, которые проверяет Kaspersky Security (см. раздел "Формирование области проверки задачи" на стр. 367).

   Перейдите к следующему шагу мастера создания задачи.
6. В окне **Действие Kaspersky Security для виртуальных сред 5.2 Легкий агент** выберите действие, которое выполняет программа Kaspersky Security (см. раздел "Изменение действия над зараженными файлами" на стр. 367), если в результате проверки обнаруживает зараженные файлы.

   Перейдите к следующему шагу мастера.
7. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора виртуальных машин, для которых вы создаете задачу. Вы можете выбрать виртуальные машины из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса виртуальных машин вручную, импортировать список виртуальных машин из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора виртуальных машин в открывшемся окне выполните одно из следующих действий:
   - В списке обнаруженных виртуальных машин укажите виртуальные машины, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия виртуальной машины.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса виртуальных машин вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов виртуальных машин.
   - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей виртуальные машины, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.
8. Далее следуйте указаниям мастера создания задачи.

Настройка параметров задачи поиска вирусов для Легкого агента для Windows

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия для настройки параметров задачи поиска вирусов для Легкого агента для Windows:

- Изменить уровень безопасности (см. раздел "Изменение уровня безопасности" на стр. 359).
- Изменить действие (см. раздел "Изменение действия над зараженными файлами" на стр. 359), которое программа выполняет при обнаружении зараженного файла.
- Сформировать область проверки задачи (см. раздел "Формирование области проверки задачи" на стр. 360).
- Настроить проверку составных файлов (см. раздел "Проверка составных файлов" на стр. 362).
- Оптимизировать проверку файлов (см. раздел "Оптимизация проверки файлов" на стр. 363).
- Настроить использование эвристического анализа (см. раздел "Использование эвристического анализа" на стр. 364).
- Настроить использование технологии проверки iSwift (см. раздел "Использование технологии iSwift" на стр. 364).

В этом разделе

Изменение уровня безопасности

Для выполнения задач проверки программа применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности*. Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. Предусмотрено три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными и рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. 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 настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне с названием задачи проверки.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

Изменение действия над зараженными файлами

► *Чтобы изменить действие над зараженными файлами, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.

6. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Выбирать действие автоматически**.
   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.
   - **Выполнять действие: Лечить**.
   - **Выполнять действие: Удалять**.
   - **Выполнять действие: Блокировать**.

   По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Лечить. Удалять, если лечение невозможно**.

   В отношении файлов, являющихся частью приложения Windows Store, программа Kaspersky Security выполняет действие **Удалять** вне зависимости от выбранного варианта.

   При удалении или лечении копии файлов сохраняются в резервном хранилище.

7. Нажмите на кнопку **Применить**.

Формирование области проверки задачи

Областью проверки называется местоположение файлов, которые программа проверяет во время выполнения задачи проверки. Вы можете расширить или сузить область проверки, добавив или удалив объекты, которые проверяет программа, или изменив тип проверяемых файлов.

► *Чтобы сформировать область проверки, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Область действия** в блоке **Типы файлов** укажите тип файлов, которые должна проверять программа:
   - Выберите **Все файлы**, если вы хотите проверять все файлы.
   - Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее

подвержены заражению.

- Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее подвержены заражению.

Выбирая тип проверяемых файлов, нужно помнить следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.
- Злоумышленник может отправить вирус или другую вредоносную программу на вашу виртуальную машину в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Файловый Антивирус проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие вредоносные программы.
- Список проверяемых расширений и список проверяемых форматов меняются динамически и соответствуют текущей необходимости поддержания безопасности вашей виртуальной машины.

8. Нажмите на кнопку **OK** в окне **Поиск вирусов**.
9. В блоке **Область проверки** нажмите на кнопку **Настройка**.

   Откроется окно **Область проверки**.
10. В окне **Область проверки** выполните одно из следующих действий:
    - Если вы хотите добавить новый объект в список проверяемых объектов, нажмите на кнопку **Добавить**.

      Откроется окно **Выбор объекта**.
    - Если вы хотите изменить путь к объекту, выберите объект в списке объектов и нажмите на кнопку **Изменить**.

      Откроется окно **Выбор объекта**.
    - Если вы хотите удалить объект из области проверки, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

      Откроется окно подтверждения удаления.

      > Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.
11. Выполните одно из следующих действий:
    - Если вы хотите добавить новый объект, в окне **Выбор объекта** выберите объект в дереве или укажите путь к объекту в поле **Объект** и нажмите на кнопку **Добавить**.

      Объект, добавленный в окне **Выбор объекта**, отобразится в списке объектов в окне **Область проверки**.

      Нажмите на кнопку **OK**.
    - Если вы хотите изменить путь к объекту, в окне **Выбор объекта** укажите другой путь к объекту в

поле **Объект** и нажмите на кнопку **OK**.

- Если вы хотите удалить объект, в окне подтверждения удаления нажмите на кнопку **Да**.

12. Если требуется, повторите пункты 10 и 11 для добавления объектов, изменения пути к ним или удаления объектов из области проверки.
13. Если вы хотите исключить объект из области проверки, в списке объектов окна **Область проверки** снимите флажок рядом с ним. Объект остается в списке проверяемых объектов, но не проверяется во время выполнения задачи проверки.
14. Нажмите на кнопку **OK** в окне **Область проверки**.
15. Нажмите на кнопку **Применить**.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Область действия** в блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, самораспаковывающиеся архивы, вложенные OLE-объекты, файлы почтовых форматов или защищенные паролем архивы, установив соответствующие флажки.
8. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.
9. В блоке **Ограничение по размеру** выполните одно из следующих действий:
   - Если вы хотите, чтобы программа распаковывала составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.
   - Если вы не хотите, чтобы программа распаковывала составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.

Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

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

10. Нажмите на кнопку **OK** в окне **Составные файлы**.
11. Нажмите на кнопку **OK** в окне **Поиск вирусов**.
12. Нажмите на кнопку **Применить**.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов при выполнении задачи поиска вирусов: сократить время проверки и увеличить скорость работы программы. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа.

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Область действия** в блоке **Оптимизация проверки** выполните следующие действия:
   - Если вы хотите, чтобы при выполнении задачи поиска вирусов программа проверяла только новые файлы и те файлы, которые изменились с момента их предыдущего анализа, установите флажок **Проверять только новые и измененные файлы**.
   - Если вы хотите, чтобы при выполнении задачи поиска вирусов программа пропускала файлы по истечении заданного времени, установите флажок **Пропускать файлы, если их проверка длится более** и в поле справа от флажка укажите длительность проверки одного файла в секундах.
8. Нажмите на кнопку **OK** в окне **Поиск вирусов**.
9. Нажмите на кнопку **Применить**.

Использование эвристического анализа

Во время своей работы программа использует сигнатурный анализ. В процессе сигнатурного анализа программа сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" сигнатурный анализ всегда включен.

Для повышения эффективности проверки вы можете использовать эвристический анализ. В процессе эвристического анализа программа анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

► *Чтобы настроить использование эвристического анализа, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Дополнительно** в блоке **Методы проверки** выполните одно из следующих действий:
   - Если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи поиска вирусов, установите флажок **Эвристический анализ** и с помощью ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы программа не использовала эвристический анализ во время выполнения задачи поиска вирусов, снимите флажок **Эвристический анализ**.
8. Нажмите на кнопку **OK** в окне **Поиск вирусов**.
9. Нажмите на кнопку **Применить**.

Использование технологии iSwift

Вы можете включить использование технологии iSwift, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы настроить использование технологии iSwift, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы

администрирования, в состав которой входят нужные защищенные виртуальные машины.

3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Windows и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Windows в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Дополнительно** в блоке **Технология проверки** выполните одно из следующих действий:
   - Установите флажок **Технология iSwift**, если вы хотите использовать эту технологию во время выполнения задачи поиска вирусов.
   - Снимите флажок **Технология iSwift**, если вы не хотите использовать эту технологию во время выполнения задачи поиска вирусов.
8. Нажмите на кнопку **OK** в окне **Поиск вирусов**.
9. Нажмите на кнопку **Применить**.

Настройка параметров задачи поиска вирусов для Легкого агента для Linux

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия для настройки параметров задачи поиска вирусов для Легкого агента для Linux:

- Изменить уровень безопасности (см. раздел "Изменение уровня безопасности" на стр. 366).
- Изменить действие (см. раздел "Изменение действия над зараженными файлами" на стр. 367), которое программа выполняет при обнаружении зараженного файла.
- Сформировать область проверки задачи (см. раздел "Формирование области проверки задачи" на стр. 367).

- Настроить проверку составных файлов (см. раздел "Проверка составных файлов" на стр. 368).
- Настроить использование эвристического анализа (см. раздел "Использование эвристического анализа" на стр. 370).
- Настроить использование технологии проверки iChecker (см. раздел "Использование технологии iChecker" на стр. 370).

В этом разделе

Изменение уровня безопасности

Для выполнения задач проверки программа применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности*. Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. Предусмотрено три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными и рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Linux и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Linux в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. 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 настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне с названием задачи проверки.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По**

умолчанию.

7. Нажмите на кнопку **Применить**.

Изменение действия над зараженными файлами

► *Чтобы изменить действие над зараженными файлами, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Linux и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Linux в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Лечить. Удалять, если лечение невозможно**.
   - **Лечить**.
   - **Удалять**.
   - **Информировать**.

   По умолчанию выбран вариант **Лечить. Удалять, если лечение невозможно**.

   > При удалении или лечении копии файлов сохраняются в резервном хранилище.
7. Нажмите на кнопку **Применить**.

Формирование области проверки задачи

Областью проверки называется местоположение файлов, которые программа проверяет во время выполнения задачи проверки. Вы можете расширить или сузить область проверки, добавив или удалив объекты, которые проверяет программа.

► *Чтобы сформировать область проверки, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Linux и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Linux в списке слева выберите раздел

Параметры.

В правой части окна отобразятся параметры задачи.

6. В блоке **Область проверки** нажмите на кнопку **Настройка**.

   Откроется окно **Область проверки**.

7. В окне **Область проверки** выполните одно из следующих действий:

   - Если вы хотите добавить новый объект в список проверяемых объектов, нажмите на кнопку **Добавить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите изменить путь к объекту, выберите объект в списке объектов и нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите удалить объект из области проверки, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

     Откроется окно подтверждения удаления.

     Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

8. Выполните одно из следующих действий:

   - Если вы хотите добавить новый объект, в окне **Выбор объекта** укажите путь к объекту в поле **Объект** и нажмите на кнопку **Добавить**.

     Объект, добавленный в окне **Выбор объекта**, отобразится в списке объектов в окне **Область проверки**.

     Нажмите на кнопку **ОК** в окне **Выбор объекта**.

   - Если вы хотите изменить путь к объекту, в окне **Выбор объекта** укажите другой путь к объекту в поле **Объект** и нажмите на кнопку **ОК**.

   - Если вы хотите удалить объект, в окне подтверждения удаления нажмите на кнопку **Да**.

9. Если требуется, повторите пункты 7 и 8 для добавления объектов, изменения пути к ним или удаления объектов из области проверки.

10. Если вы хотите исключить объект из области проверки, в списке объектов окна **Область проверки** снимите флажок рядом с объектом. Объект остается в списке проверяемых объектов, но не проверяется во время выполнения задачи проверки.

11. Нажмите на кнопку **ОК** в окне **Область проверки**.

12. Нажмите на кнопку **Применить**.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив

скорость проверки.

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Linux и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Linux в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Область действия** в блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: упакованные файлы, архивы, самораспаковывающиеся архивы, почтовые базы или файлы почтовых форматов, установив соответствующие флажки.
8. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.
9. В блоке **Ограничение по времени** выполните одно из следующих действий:
   - Если вы хотите, чтобы программа пропускала файлы по истечении заданного времени, установите флажок **Пропускать файлы, если их проверка длится более** и в поле **Максимальное время проверки** укажите нужное значение.
   - Если вы не хотите, чтобы программа пропускала файлы по истечении заданного времени, снимите флажок **Пропускать файлы, если их проверка длится более**.
10. В блоке **Ограничение по размеру** выполните одно из следующих действий:
    - Если вы хотите, чтобы программа распаковывала составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.
    - Если вы не хотите, чтобы программа распаковывала составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.

      Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

    Программа Kaspersky Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
11. Нажмите на кнопку **OK** в окне **Составные файлы**.
12. Нажмите на кнопку **OK** в окне **Поиск вирусов**.

13. Нажмите на кнопку **Применить**.

Использование эвристического анализа

Во время своей работы программа использует сигнатурный анализ. В процессе сигнатурного анализа программа сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" сигнатурный анализ всегда включен.

Для повышения эффективности проверки вы можете использовать эвристический анализ. В процессе эвристического анализа программа анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

► *Чтобы настроить использование эвристического анализа, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Linux и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Linux в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Дополнительно** в блоке **Методы проверки** выполните одно из следующих действий:
   - Если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи поиска вирусов, установите флажок **Эвристический анализ** и с помощью ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы программа не использовала эвристический анализ во время выполнения задачи поиска вирусов, снимите флажок **Эвристический анализ**.
8. Нажмите на кнопку **ОК** в окне **Поиск вирусов**.
9. Нажмите на кнопку **Применить**.

Использование технологии iChecker

Вы можете включить использование технологии iChecker, которая позволяет увеличить скорость проверки за счет исключения из проверки некоторых файлов по специальному алгоритму, учитывающему дату выпуска баз программы, дату предыдущей проверки файла, а также изменение параметров проверки.

► *Чтобы настроить использование технологии iChecker, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите задачу поиска вирусов для Легкого агента для Linux и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.
5. В окне свойств задачи поиска вирусов для Легкого агента для Linux в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Поиск вирусов**.
7. В окне **Поиск вирусов** на закладке **Дополнительно** в блоке **Технология проверки** выполните одно из следующих действий:
   - Установите флажок **Технология iChecker**, если вы хотите использовать эту технологию во время выполнения задачи поиска вирусов.
   - Снимите флажок **Технология iChecker**, если вы не хотите использовать эту технологию во время выполнения задачи поиска вирусов.
8. Нажмите на кнопку **OK** в окне **Поиск вирусов**.
9. Нажмите на кнопку **Применить**.

Настройка параметров задач проверки в локальном интерфейсе

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

Вы можете выполнить следующие действия для настройки параметров задач проверки в локальном интерфейсе:

- Изменить уровень безопасности (см. раздел "Изменение уровня безопасности" на стр. 372).
- Изменить действие (см. раздел "Изменение действия над зараженными файлами" на стр. 373),

которое программа выполняет при обнаружении зараженного файла.

- Сформировать область проверки (см. раздел "Формирование области проверки задачи" на стр. 374).
- Настроить проверку составных файлов (см. раздел "Проверка составных файлов" на стр. 376).
- Оптимизировать проверку файлов (см. раздел "Оптимизация проверки файлов" на стр. 377).
- Настроить использование эвристического анализа (см. раздел "Использование эвристического анализа" на стр. 378).
- Настроить использование технологии проверки iSwift (см. раздел "Использование технологии iSwift" на стр. 379).
- Выбрать режим запуска задач проверки (см. раздел "Настройка режима запуска задачи проверки" на стр. 379).
- Настроить запуск задач проверки с правами другого пользователя (см. раздел "Настройка запуска задачи проверки с правами другого пользователя" на стр. 381).

В этом разделе

Изменение уровня безопасности

Для выполнения задач проверки программа применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности*. Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. Предусмотрено три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными и рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

> Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

В правой части окна отобразятся параметры выбранной задачи проверки.

3. 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 настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне с названием задачи проверки.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия над зараженными файлами

► *Чтобы изменить действие над зараженными файлами в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Выбирать действие автоматически**.
   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.
   - **Выполнять действие: Лечить**.
   - **Выполнять действие: Удалять**.
   - **Выполнять действие: Информировать**.

   По умолчанию выбран вариант **Выбирать действие автоматически**. Программа выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию: **Лечить. Удалять, если лечение невозможно**.

> В отношении файлов, являющихся частью приложения Windows Store, программа Kaspersky Security выполняет действие **Удалять** вне зависимости от выбранного варианта.

> При удалении или лечении копии файлов сохраняются в резервном хранилище.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование области проверки задачи

Областью проверки называется местоположение и тип файлов (например, все жесткие диски, объекты автозапуска, почтовые базы), которые программа проверяет во время выполнения задачи проверки. Вы можете расширить или сузить область проверки, добавив или удалив объекты, которые проверяет программа, или изменив тип проверяемых файлов.

> Не рекомендуется изменять область проверки задачи полной проверки и задачи проверки важных областей.

► *Чтобы сформировать область проверки в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление задачами**.
4. Нажмите на строку с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

   Откроется меню действий с задачей проверки.
5. Выберите в меню пункт **Область проверки**.

   Откроется окно **Область проверки**.
6. В окне **Область проверки** выполните одно из следующих действий:
   - Если вы хотите добавить новый объект в список проверяемых объектов, нажмите на кнопку **Добавить**.

     Откроется окно **Выбор объекта**.
   - Если вы хотите изменить путь к объекту, выберите объект в списке объектов и нажмите на кнопку **Изменить**.

Откроется окно **Выбор объекта**.

- Если вы хотите удалить объект из области проверки, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

  Откроется окно подтверждения удаления.

  > Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

7. Выполните одно из следующих действий:
   - Если вы хотите добавить новый объект, в окне **Выбор объекта** выберите объект и нажмите на кнопку **Добавить**.

     Все объекты, выбранные в окне **Выбор объекта**, отобразятся в списке объектов в окне **Область проверки**.

     Нажмите на кнопку **ОК**.
   - Если вы хотите изменить путь к объекту из списка объектов, в окне **Выбор объекта** укажите другой путь к объекту в поле **Объект** и нажмите на кнопку **ОК**.
   - Если вы хотите удалить объект, нажмите на кнопку **Да** в окне подтверждения удаления.
8. Если требуется, повторите пункты 6 и 7 для добавления объектов, изменения пути к ним или удаления объектов из области проверки.
9. Если вы хотите исключить объект из области проверки, в списке объектов окна **Область проверки** снимите флажок рядом с ним. Объект остается в списке проверяемых объектов, но не проверяется во время выполнения задачи проверки.
10. Нажмите на кнопку **ОК** в окне **Область проверки**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

► *Чтобы выбрать тип проверяемых файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.
4. В окне с названием выбранной задачи проверки на закладке **Область действия** в блоке **Типы файлов** укажите тип файлов, которые должна проверять программа во время выполнения выбранной задачи проверки:
   - Выберите **Все файлы**, если вы хотите проверять все файлы.

- Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее подвержены заражению.
- Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, которые, по мнению специалистов «Лаборатории Касперского», в настоящее время наиболее подвержены заражению.

Выбирая тип проверяемых файлов, нужно помнить следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.
- Злоумышленник может отправить вирус или другую вредоносную программу на вашу виртуальную машину в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Файловый Антивирус проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие вредоносные программы.
- Список проверяемых расширений и список проверяемых форматов меняются динамически и соответствуют текущей необходимости поддержания безопасности вашей виртуальной машины.

5. Нажмите на кнопку **ОК** в окне с названием задачи проверки.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, самораспаковывающиеся архивы, вложенные OLE-объекты, файлы почтовых форматов или защищенные паролем архивы, установив соответствующие флажки.
5. Если в блоке **Оптимизация проверки** снят флажок **Проверять только новые и измененные файлы**, для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы этого типа или только новые. Для выбора нажмите на ссылку **все / новые**, расположенную рядом с названием типа составного файла. Ссылка меняет свое значение при нажатии на нее левой клавишей мыши.

   Если флажок **Проверять только новые и измененные файлы** установлен, то проверяются только новые файлы.
6. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.
7. В блоке **Ограничение по размеру** выполните одно из следующих действий:
   - Если вы не хотите, чтобы программа распаковывала составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.
   - Если вы хотите, чтобы программа распаковывала составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

   > Программа проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
8. Нажмите на кнопку **OK** в окне **Составные файлы**.
9. Нажмите на кнопку **OK** в окне с названием задачи проверки.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы программы. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы. Вы можете также ограничить длительность проверки одного файла, в этом случае по истечении заданного времени программа исключит файл из текущей проверки (кроме архивов и составных файлов).

► *Чтобы оптимизировать проверку файлов в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

> Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

В правой части окна отобразятся параметры выбранной задачи проверки.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** выполните следующие действия:

   - Если вы хотите, чтобы при выполнении задачи проверки программа проверяла только новые файлы и те файлы, которые изменились с момента их предыдущего анализа, установите флажок **Проверять только новые и измененные файлы**.
   - Если вы хотите, чтобы при выполнении задачи проверки программа пропускала файлы по истечении заданного времени, установите флажок **Пропускать файлы, если их проверка длится более** и в поле справа от флажка укажите длительность проверки одного файла в секундах.

5. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа

Во время своей работы программа использует сигнатурный анализ. В процессе сигнатурного анализа программа сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" сигнатурный анализ всегда включен.

Для повышения эффективности проверки вы можете использовать эвристический анализ. В процессе эвристического анализа программа анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

► *Чтобы настроить использование эвристического анализа в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

   В правой части окна отобразятся параметры выбранной задачи проверки.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** выполните следующие действия:
   - Если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи проверки, установите флажок **Эвристический анализ** и с помощью ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы программа не использовала эвристический анализ во время выполнения задачи проверки, снимите флажок **Эвристический анализ**.
5. Нажмите на кнопку **OK** в окне с названием задачи проверки.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование технологии iSwift

Вы можете включить использование технологии iSwift, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы настроить использование технологии iSwift в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Технология проверки** выполните одно из следующих действий:
   - Установите флажок **Технология iSwift**, если вы хотите использовать эту технологию во время проверки.
   - Снимите флажок **Технология iSwift**, если вы не хотите использовать эту технологию во время проверки.
5. Нажмите на кнопку **OK** в окне с названием задачи проверки.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка режима запуска задачи проверки

Если по каким-либо причинам запуск задачи проверки невозможен (например, в это время защищенная виртуальная машина выключена), вы можете настроить автоматический запуск пропущенной задачи

проверки, как только это станет возможным.

Вы можете отложить запуск задачи проверки после старта программы для случаев, если вы выбрали режим запуска задачи проверки **По расписанию** и время запуска программы совпадает с расписанием запуска задачи проверки. Задача проверки запускается только по истечении указанного времени после старта программы.

► *Чтобы настроить режим запуска задачи проверки в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

3. Нажмите на кнопку **Режим запуска**.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне на закладке **Режим запуска** выберите один из следующих вариантов режима запуска задачи проверки:
   - Выберите вариант **Вручную**, если вы хотите запускать задачу проверки вручную.
   - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи проверки.
5. Выполните одно из следующих действий:
   - Если вы выбрали вариант **Вручную**, перейдите к пункту 6 инструкции.
   - Если вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи проверки. Для этого выполните следующие действия:
     a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу проверки. Выберите один из следующих вариантов: **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**, **После каждого обновления**.
     b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значение параметров, которые уточняют время запуска задачи проверки.
     c. Если вы выбрали режим запуска задачи проверки **По расписанию** и время запуска программы совпадает с расписанием запуска задачи проверки, вы можете отложить запуск задачи проверки после старта программы. Для этого укажите интервал времени после старта программы, на который задерживается запуск задачи проверки. Задача проверки запускается только по истечении указанного времени после старта программы.

     > Параметр недоступен, если в раскрывающемся списке **Периодичность** выбран элемент **После запуска программы** или **После каждого обновления**.

     d. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы программа

запускала не запущенные вовремя задачи проверки при первой возможности.

> Флажок недоступен, если в раскрывающемся списке **Периодичность** выбраны элементы **Минуты**, **Часы**, **После запуска программы** или **После каждого обновления**.

e. Установите флажок **Приостанавливать проверку по расписанию, если защищенная виртуальная машина разблокирована**, если вы хотите, чтобы программа приостанавливала задачу проверки, когда ресурсы виртуальной машины заняты. Это позволяет экономить вычислительную мощность виртуальной машины во время работы.

6. Нажмите на кнопку **OK** в окне с названием задачи проверки.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка запуска задачи проверки с правами другого пользователя

По умолчанию задача проверки запускается от имени учетной записи, с правами которой вы зарегистрированы в гостевой операционной системе на защищенной виртуальной машине. Однако может возникнуть необходимость запустить задачу проверки с правами другого пользователя. Вы можете указать пользователя, обладающего этими правами, в параметрах задачи проверки и запускать задачу проверки от имени этого пользователя.

► *Чтобы настроить запуск задачи проверки с правами другого пользователя в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей** или **Выборочная проверка**.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. Нажмите на кнопку **Режим запуска**.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**.
5. В поле **Имя** введите имя учетной записи пользователя, права которого требуется использовать для запуска задачи проверки.
6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для запуска задачи проверки.
7. Нажмите на кнопку **OK** в окне с названием задачи проверки.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка съемных дисков при подключении к виртуальной машине

Некоторые вредоносные программы используют уязвимости операционной системы для распространения через локальные сети и съемные диски. Программа позволяет проверять съемные диски на вирусы и другие вредоносные программы при подключении съемных дисков к виртуальной машине.

Вы можете настраивать проверку съемных дисков в свойствах политики для Легкого агента для Windows с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить в Консоли администрирования проверку съемных дисков при подключении к виртуальной машине, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Дополнительные параметры**.
6. В правой части окна в блоке **Проверка съемных дисков при подключении** в раскрывающемся списке **Действие при подключении съемного диска** выберите нужное действие:
   - **Не проверять**.
   - **Полная проверка**.
   - **Быстрая проверка**.
7. Установите флажок **Максимальный размер съемного диска** и в поле рядом укажите значение в мегабайтах, если вы хотите, чтобы программа проверяла съемные диски, размер которых меньше или равен указанному значению.

   Флажок доступен, если в раскрывающемся списке **Действие при подключении съемного диска** выбрано действие **Полная проверка** или **Быстрая проверка**.

8. Нажмите на кнопку **Применить**.

► *Чтобы настроить в локальном интерфейсе проверку съемных дисков при подключении к виртуальной машине, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите раздел **Задачи по расписанию**.

   В правой части окна отобразятся общие параметры задач по расписанию.
3. В блоке **Проверка съемных дисков при подключении** в раскрывающемся списке **Действие при**

подключении съемного диска выберите нужное действие:

- **Не проверять**.
- **Полная проверка**.
- **Быстрая проверка**.

Если блок недоступен, это означает, что настройка параметров проверки съемных дисков запрещена политикой для всех защищенных виртуальных машин группы администрирования.

4. Установите флажок **Максимальный размер съемного диска** и в поле рядом укажите значение в мегабайтах, если вы хотите, чтобы программа проверяла съемные диски, размер которых меньше или равен указанному значению.

   Флажок доступен, если в раскрывающемся списке **Действие при подключении съемного диска** выбрано действие **Полная проверка** или **Быстрая проверка**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Особенности проверки символических и жестких ссылок

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

Проверка символических ссылок

Во время постоянной защиты программа Kaspersky Security проверяет файл, обращение к которому происходит по символической ссылке, только если этот файл входит в область действия постоянной защиты.

Если файл, обращение к которому происходит по символической ссылке, не входит в область действия постоянной защиты, программа не проверяет этот файл. Если такой файл содержит вредоносный код, безопасность виртуальной машины окажется под угрозой.

Задача проверки проверяет файл, обращение к которому происходит по символической ссылке, независимо от места расположения файла. При обнаружении зараженного файла, обращение к которому происходит по символической ссылке, программа лечит исходный файл. Если лечение невозможно, программа удаляет зараженный файл и оставляет символическую ссылку.

Проверка жестких ссылок компонентом Легкий агент для Linux

При обнаружении зараженного файла, у которого больше одной жесткой ссылки, Легкий агент для Linux лечит исходный файл. Если лечение невозможно, Легкий агент для Linux удаляет обрабатываемую жесткую ссылку на файл. При этом остальные жесткие ссылки на этот файл обработаны не будут.

При восстановлении файла с жесткой ссылкой из резервного хранилища программа создает копию исходного файла с именем жесткой ссылки, которая была помещена в резервное хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

Проверка жестких ссылок компонентом Легкий агент для Windows

Когда Легкий агент для Windows обрабатывает файл, у которого больше одной жесткой ссылки, в зависимости от заданного действия над файлами возможны следующие сценарии:

- Если выбрано действие **Удалять**, Kaspersky Security удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.
- Если выбрано действие **Лечить**, Kaspersky Security лечит исходный файл. Если лечение невозможно, программа удаляет обрабатываемую жесткую ссылку и создает вместо нее копию исходного файла с именем удаленной жесткой ссылки. При этом остальные жесткие ссылки на этот файл обработаны не будут.

Зараженный файл считается *обработанным*, если программа в процессе проверки защищенной виртуальной машины совершила одно из следующих действий с зараженным файлом согласно заданным параметрам:

- Лечить.
- Удалять.
- Удалять, если лечение невозможно.

Зараженный файл считается *необработанным*, если программа в процессе проверки защищенной виртуальной машины не совершила действие с зараженным файлом согласно заданным параметрам.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем устройстве без прав на запись данных).
- В параметрах программы для задач проверки в блоке **Действие при обнаружении угрозы** выбрано действие **Информировать**.

Программа Kaspersky Security записывает информацию о необработанных файлах в таблицу необработанных объектов в виде событий. Кроме того, программа добавляет в таблицу необработанных объектов информацию о попытке изменения файлов в папках общего доступа, если в параметрах Мониторинга системы выбрано действие (см. раздел "Изменение действия при обнаружении внешнего шифрования папок общего доступа" на стр. 271) **Информировать**.

В этом разделе описаны действия, которые вы можете выполнять с необработанными объектами в локальном интерфейсе Легкого агента для Windows. Информация о необработанных объектах, обнаруженных на устройствах, также отображается в Консоли администрирования Kaspersky Security Center (в папке **Хранилища** → **Активные угрозы**).

В этом разделе

Запуск задачи выборочной проверки для необработанных файлов

Вы можете вручную запустить задачу выборочной проверки для необработанных файлов, например, если

проверка была прервана по какой-либо причине или вы хотите, чтобы программа Kaspersky Security проверила файлы после очередного обновления баз программы.

► *Чтобы запустить задачу выборочной проверки для необработанных файлов, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Необработанные объекты**.
4. В таблице на закладке **Необработанные объекты** выберите один или несколько файлов, которые вы хотите проверить. Для выбора нескольких файлов используйте клавишу **CTRL**.
5. Запустите задачу выборочной проверки файлов одним из следующих способов:
   - Нажмите на кнопку **Перепроверить**.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Перепроверить**.

   После завершения проверки на экране отобразится уведомление о количестве проверенных файлов и количестве обнаруженных угроз.

Восстановление необработанных файлов

При необходимости вы можете восстановить файлы из таблицы необработанных объектов в папки их исходного размещения.

Рекомендуется восстанавливать необработанные файлы только в том случае, если файлам присвоен статус *Вылечен* или *Не заражен*.

► *Чтобы восстановить необработанные файлы, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Необработанные объекты**.
4. Если вы хотите восстановить все файлы, выполните следующие действия:
   a. По правой клавише мыши в любом месте таблицы на закладке **Необработанные объекты** откройте контекстное меню.
   b. Выберите пункт **Восстановить все**.

      Программа переместит все необработанные файлы из таблицы необработанных объектов в папки их исходного размещения, если эти папки доступны для записи.
   c. Если при восстановлении папка исходного размещения одного из файлов недоступна для записи, откроется стандартное окно Microsoft Windows **Сохранить как**. В этом окне вы можете указать папку для сохранения файла.
5. Если вы хотите восстановить один или несколько файлов, выполните следующие действия:

a. В таблице на закладке **Необработанные объекты** выберите один или несколько необработанных файлов, которые вы хотите восстановить. Для выбора нескольких файлов используйте клавишу **CTRL**.

b. Восстановите файлы одним из следующих способов:

- Нажмите на кнопку **Восстановить**.
- По правой клавише мыши откройте контекстное меню и выберите пункт **Восстановить**.

Программа переместит выбранные файлы в папки их исходного размещения, если эти папки доступны для записи.

c. Если при восстановлении папка исходного размещения одного из файлов недоступна для записи, откроется стандартное окно Microsoft Windows **Сохранить как**. В этом окне вы можете указать папку для сохранения файла.

Удаление файлов из списка необработанных объектов

Вы можете удалить зараженный файл, помещенный в таблицу необработанных объектов.

► *Чтобы удалить файлы из таблицы необработанных объектов, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Необработанные объекты**.
4. В таблице на закладке **Необработанные объекты** выберите один или несколько файлов, которые вы хотите удалить. Для выбора нескольких файлов используйте клавишу **CTRL**.
5. Удалите файлы одним из следующих способов:
   - Нажмите на кнопку **Удалить**.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Удалить**.

Перед тем как удалить файл, программа создает резервную копию файла и сохраняет ее в резервном хранилище на тот случай, если впоследствии вам потребуется восстановить файл (см. раздел "Восстановление файлов из резервного хранилища в локальном интерфейсе" на стр. 420). После этого удаляет выбранные файлы из таблицы необработанных объектов.

Взаимодействие с другими решениями "Лаборатории Касперского"

Программа Kaspersky Security может взаимодействовать со следующими решениями «Лаборатории Касперского»:

- Kaspersky Endpoint Agent.
- Kaspersky Managed Detection and Response.

В этом разделе

Kaspersky Endpoint Agent

Вы можете установить программу Kaspersky Endpoint Agent на виртуальную машину с установленным компонентом Легкий агент для Windows. Программа Kaspersky Endpoint Agent обеспечивает взаимодействие между программой Kaspersky Security и решениями "Лаборатории Касперского", предназначенными для обнаружения сложных угроз: Kaspersky Anti Targeted Attack Platform (https://support.kaspersky.com/KATA/3.7.2/ru-RU/index.htm), Kaspersky Sandbox (https://support.kaspersky.com/KSB/1.0/ru-RU/index.htm), Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/1.0/ru-RU/index.htm).

Не поддерживается взаимодействие с решением Kaspersky Anti Targeted Attack Platform, если вы используете программу Kaspersky Security для защиты инфраструктуры виртуальных рабочих столов (VDI).

► *Чтобы использовать Kaspersky Endpoint Agent в работе программы Kaspersky Security, выполните следующие действия:*

1. Во время установки Легкого агента для Windows включите интеграцию с Kaspersky Endpoint Agent. Для этого вам нужно установить флажок / выбрать параметр **Интеграция с Kaspersky Endpoint Agent** в списке компонентов или использовать соответствующий параметр командной строки, в зависимости от способа установки или обновления.

   Если на виртуальной машине установлен Kaspersky Endpoint Agent, но не включена интеграция с Kaspersky Endpoint Agent, то взаимодействие между Kaspersky Endpoint Agent и программой Kaspersky Security выключено. В работе программы не используются решения "Лаборатории Касперского", предназначенные для обнаружения сложных угроз.

2. Выполните установку Kaspersky Endpoint Agent на виртуальной машине штатными средствами Kaspersky Endpoint Agent.

Подробнее об установке, обновлении и удалении Kaspersky Endpoint Agent см. в документации того решения "Лаборатории Касперского", для интеграции с которым вы используете Kaspersky Endpoint Agent.

Managed Detection and Response

Решение Kaspersky Managed Detection and Response позволяет осуществлять непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию. При взаимодействии с Kaspersky Managed Detection and Response программа Kaspersky Security выполняет следующие функции:

- Отправка в Kaspersky Managed Detection and Response данных телеметрии Легкого агента для Windows для обнаружения угроз.
- Выполнение команд от Kaspersky Managed Detection and Response, направленных на предотвращение угроз.

Подробную информацию о работе решения, а также инструкции по развертыванию решения см. в документации Kaspersky Managed Detection and Response (https://support.kaspersky.com/MDR/ru-RU/).

Не поддерживается взаимодействие с решением Kaspersky Managed Detection and Response, если вы используете программу Kaspersky Security для защиты инфраструктуры виртуальных рабочих столов (VDI).

Программа Kaspersky Security может взаимодействовать с решением с Kaspersky Managed Detection and Response, только если выполняются следующие условия:

- На виртуальной машине установлен и включен компонент Мониторинг системы.
- В работе программы Kaspersky Security используется Kaspersky Security Network в расширенном режиме.

  Использование Локального KSN при взаимодействии с Kaspersky Managed Detection and Response гарантирует отправку телеметрии на выделенные серверы, соответствующие требованиям Общего регламента по защите данных (GDPR). Если Локальный KSN не используется, телеметрия может отправляться в Глобальный KSN, что может являться нарушением законов вашей страны.

Для оптимального использования Kaspersky Managed Detection and Response в работе программы Kaspersky Security рекомендуется включить на виртуальной машине следующие функциональные компоненты Легкого агента:

- Файловый Антивирус.
- Почтовый Антивирус.
- Веб-Антивирус.
- Сетевой экран.

- Защита от сетевых атак.

Включение указанных компонентов не является обязательным условием для использования Kaspersky Managed Detection and Response. Если компоненты выключены на виртуальной машине, в Kaspersky Managed Detection and Response отправляются ограниченные данные телеметрии Легкого агента для Windows, установленного на этой виртуальной машине.

Чтобы использовать решение Kaspersky Managed Detection and Response в работе программы Kaspersky Security, вам нужно включить взаимодействие с Kaspersky Managed Detection and Response и загрузить конфигурационный файл MDR в политике для Легкого агента для Windows. Конфигурационный файл предоставляется в ZIP-архиве и имеет расширение P7 или P7B.

Информация из конфигурационного файла передается на защищенные виртуальные машины при следующей синхронизации с Kaspersky Security Center. После применения на защищенной виртуальной машине политики, в которой настроено использование Managed Detection and Response, и обновления баз программы Kaspersky Security установленный на виртуальной машине Легкий агент для Windows начинает отправлять телеметрию в Kaspersky Managed Detection and Response и может выполнять команды от Kaspersky Managed Detection and Response.

► *Чтобы включить или выключить использование функциональности Managed Detection and Response в работе программы Kaspersky Security, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Managed Detection and Response**.

   В правой части окна отобразятся параметры взаимодействия с Kaspersky Managed Detection and Response.
6. Выполните одно из следующих действий:
   - Установите флажок **Managed Detection and Response**, если вы хотите включить использование функциональности Managed Detection and Response в работе программы Kaspersky Security.
   - Снимите флажок **Managed Detection and Response**, если вы хотите выключить использование функциональности Managed Detection and Response в работе программы Kaspersky Security.
7. Если вы включили использование функциональности Managed Detection and Response, нажмите на кнопку **Загрузить** и выберите конфигурационный файл MDR с расширением P7 или P7B.

   Если требуется удалить ранее загруженный конфигурационный файл, нажмите на кнопку **Удалить**.
8. Нажмите на кнопку **Применить**.

Информацию о том, используется ли функциональность Managed Detection and Response в работе программы Kaspersky Security на виртуальной машине, вы можете получить в Kaspersky Security Center в списке функциональных компонентов Легкого агента, который отображается в свойствах программы Kaspersky Security, установленной на виртуальной машине с Легким агентом для Windows, или в отчете о статусе компонентов программы.

Обновление баз программы

Обновление баз программы Kaspersky Security обеспечивает актуальность защиты виртуальных машин. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах программы. Чтобы программа своевременно обнаруживала угрозы, вам нужно регулярно обновлять базы программы.

Если базы программы давно не обновлялись, сообщение об этом появляется в окне **События** свойств SVM.

Обновления баз могут изменить некоторые параметры программы, например параметры эвристического анализа, повышающие эффективность защиты и проверки.

Для обновления баз программы требуется действующая лицензия на использование программы.

Источник обновлений – это ресурс, содержащий обновления баз для программ "Лаборатории Касперского". Источником обновлений для программы Kaspersky Security для виртуальных сред 5.2 Легкий агент является хранилище Сервера администрирования Kaspersky Security Center. Обновление баз программы выполняется следующим образом:

1. Компонент Сервер защиты загружает пакет обновлений из хранилища Сервера администрирования в папку на SVM.

   По умолчанию пакет обновлений содержит обновления баз программы, необходимых для работы Сервера защиты и Легкого агента. Вы также можете обновлять модули компонента Легкий агент для Windows.

   Допускается устанавливать только обновления модулей, прошедшие инспекционный контроль. Включение автоматического обновления модулей Легкого агента для Windows приводит к выходу программы из сертифицированного состояния.

   Загрузка пакета обновлений выполняется с помощью *задачи обновления* на Сервере защиты. Задача запускается из Kaspersky Security Center и выполняется на SVM (см. раздел "Автоматическое получение пакета обновлений баз программы на SVM" на стр. 392).

   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. Загрузка такого пакета обновлений может создать дополнительный сетевой трафик (до нескольких десятков мегабайт).

2. Обновления баз программы устанавливаются из папки, расположенной на SVM:
   - После загрузки пакета обновлений компонент Сервер защиты автоматически устанавливает на SVM обновления баз, необходимых для работы Сервера защиты.
   - Компонент Легкий агент проверяет наличие пакета обновлений в папке на той SVM, к которой он подключен.

     Чтобы получать обновления баз, Легкий агент должен взаимодействовать с SVM по протоколу HTTP.

     При наличии пакета обновлений Легкий агент устанавливает на защищенной виртуальной машине обновления баз, необходимых для работы Легкого агента. Обновление баз Легкого агента выполняется с помощью *задачи обновления* на защищенной виртуальной машине. Запуск задачи обновления на защищенной виртуальной машине выполняется по расписанию. По умолчанию задан автоматический режим запуска задачи. Задача запускается каждые два часа.

     На защищенной виртуальной машине с установленным компонентом Легкий агент для Windows вы можете настроить в локальном интерфейсе расписание запуска задачи обновления (см. раздел "Настройка режима запуска задачи обновления в локальном интерфейсе" на стр. 394) или запустить задачу обновления вручную (см. раздел "Запуск и остановка задачи обновления в локальном интерфейсе" на стр. 395), если эти функции не запрещены политикой для всех защищенных виртуальных машин группы администрирования. Если по каким-либо причинам запуск задачи обновления невозможен (например, в это время виртуальная машина выключена), вы можете настроить автоматический запуск пропущенной задачи обновления, как только это станет возможным.

     На защищенной виртуальной машине с установленным компонентом Легкий агент для Linux вы можете вручную запустить задачу обновления из командной строки (см. раздел "Запуск и остановка задачи" на стр. 482).

Для получения и установки обновлений баз программы из локальной или сетевой папки (см. раздел "Обновление баз программы из локальной или сетевой папки" на стр. 398) вы можете использовать утилиту Updater Utility, которую можно загрузить с веб-сайта Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/updater4).

Для обеспечения актуальности защиты временных виртуальных машин, рекомендуется регулярно обновлять базы и модули Легкого агента на шаблоне виртуальных машин, из которого созданы временные защищенные виртуальные машины.

Если при установке Легкого агента на шаблон виртуальных машин вы установили флажок **Установка на шаблон для временных пулов VDI**, обновления, требующие перезагрузки защищенной виртуальной машины, не устанавливаются на временных виртуальных машинах. При получении обновлений, требующих перезагрузки защищенной виртуальной машины, Легкий агент, установленный на временной виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновления шаблона защищенных виртуальных машин.

kaspersky

В этом разделе

Автоматическое получение пакета обновлений баз программы на SVM

Kaspersky Security Center позволяет автоматически загружать пакеты обновлений баз программы на SVM. Для этого используются следующие задачи:

- **Задача загрузки обновлений в хранилище**. Задача позволяет загружать пакет обновлений из источника обновлений для Kaspersky Security Center в хранилище Сервера администрирования. Задача загрузки обновлений в хранилище создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище может быть создана в одном экземпляре. Поэтому вы можете создать задачу загрузки обновлений в хранилище только в случае, если она была удалена из списка задач Сервера администрирования. Подробнее см. в документации Kaspersky Security Center.
- **Задача обновления на Сервере защиты**. Задача позволяет загружать пакеты обновлений баз программы на SVM, входящие в выбранную группу администрирования, в соответствии с настроенным расписанием.

  После установки mmc-плагинов управления Kaspersky Security в Kaspersky Security Center автоматически создается задача обновления баз на Сервере защиты. Задача создается для группы администрирования **Управляемые устройства** и позволяет загружать пакет обновлений баз и модулей программы на все SVM, которые входят в группу **Управляемые устройства** или в любую вложенную группу администрирования.

  Для загрузки пакетов обновлений баз и модулей программы на SVM вы можете использовать автоматически созданную задачу обновления баз на Сервере защиты. Задача запускается при каждой загрузке пакета обновлений в хранилище Сервера администрирования Kaspersky Security Center. При необходимости вы можете изменить параметры этой задачи или удалить ее и создать новую задачу обновления баз на Сервере защиты.

► *Чтобы настроить автоматическое получение пакета обновлений баз программы, выполните следующие действия:*

1. Убедитесь, что в Kaspersky Security Center создана задача загрузки обновлений в хранилище. Если задача загрузки обновлений в хранилище отсутствует, создайте ее (см. в документации Kaspersky Security Center).
2. Убедитесь, что в Kaspersky Security Center создана задача обновления баз на Сервере защиты или создайте задачу обновления для SVM, на которых вы хотите обновлять базы программы (см. раздел

"Создание задачи обновления баз на Сервере защиты" на стр. 393).

Создание задачи обновления баз на Сервере защиты

► *Чтобы создать в Консоли администрирования задачу обновления баз на Сервере защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для SVM, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех SVM, входящих в эту группу. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких SVM (задачу для набора устройств).
3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты** выберите **Обновление баз**.

   Перейдите к следующему шагу мастера создания задачи.
5. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора SVM, для которых вы создаете задачу. Вы можете выбрать SVM из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать список SVM из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:
   - В списке обнаруженных виртуальных машин укажите SVM, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия SVM.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
   - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.
6. В раскрывающемся списке **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**. Настройте остальные параметры расписания запуска задачи. Подробнее о параметрах расписания запуска задачи см. в документации Kaspersky Security Center.

   Перейдите к следующему шагу мастера создания задачи.
7. Введите название задачи обновления антивирусных баз.

   Перейдите к следующему шагу мастера создания задачи.
8. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания

задачи, установите флажок **Запустить задачу после завершения работы мастера**. Завершите работу мастера создания задачи. Созданная задача отобразится в списке задач.

Задача будет запускаться каждый раз при загрузке пакета обновлений в хранилище Сервера администрирования. Также вы можете запускать и останавливать задачу вручную (см. раздел "Запуск и остановка задач" на стр. 147).

Настройка режима запуска задачи обновления в локальном интерфейсе

► *Чтобы выбрать режим запуска задачи обновления, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз программы.

   Если в блоке отсутствует раздел **Обновление**, это означает, что настройка параметров обновления баз программы запрещена политикой для всех защищенных виртуальных машин группы администрирования.

3. Нажмите на кнопку **Режим запуска**.

   Откроется окно **Обновление**.

4. В блоке **Режим запуска** выберите один из следующих вариантов режима запуска задачи обновления:
   - Выберите вариант **Автоматически**, если вы хотите, чтобы программа Kaspersky Security запускала задачу обновления в зависимости от наличия пакета обновлений на SVM, к которой подключена защищенная виртуальная машина. Частота проверки программой наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии.

     Если новых обновлений на SVM нет, то задача обновления не запустится.

   - Выберите вариант **Вручную**, если вы хотите запускать задачу обновления вручную.
   - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи обновления.
5. Выполните одно из следующих действий:
   - Если вы выбрали вариант **Автоматически** или **Вручную**, перейдите к пункту 6 инструкции.
   - Если вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи обновления. Для этого выполните следующие действия:

     a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу обновления. Выберите один из следующих вариантов: **Минуты**, **Часы**, **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**.

     b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значение параметров, которые уточняют время запуска задачи обновления.

> При настройке периодичности запуска задачи обновления рекомендуется учитывать периодичность обновления баз программы на SVM, к которой подключена защищенная виртуальная машина.

c. В поле **Отложить запуск после старта программы на** укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Security.

> Если в раскрывающемся списке **Периодичность** выбран элемент **После запуска программы**, поле **Отложить запуск после старта программы на** недоступно.

d. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы программа Kaspersky Security запускала при первой возможности не запущенные вовремя задачи обновления.

> Если в раскрывающемся списке **Периодичность** выбран элемент **Часы**, **Минуты** или **После запуска программы**, то флажок **Запускать пропущенные задачи** недоступен.

6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка задачи обновления в локальном интерфейсе

Независимо от выбранного режима запуска задачи обновления вы можете запустить или остановить задачу обновления Kaspersky Security в любой момент.

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

1. Откройте главное окно программы (на стр. 120).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление задачами**.
4. По правой клавише мыши откройте контекстное меню строки с названием задачи **Обновление**.

   Откроется меню действий с задачей обновления.

   > Если в блоке отсутствуют задачи обновления, это означает, что настройка параметров обновления баз и модулей программы запрещена политикой для всех защищенных виртуальных машин группы администрирования.

5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Запустить обновление**, если вы хотите запустить задачу обновления.

     Статус выполнения задачи обновления, отображающийся справа от названия задачи **Обновление**, изменится на *Выполняется*.

- Выберите в меню пункт **Остановить обновление**, если вы хотите остановить задачу обновления.

  Статус выполнения задачи обновления, отображающийся справа от названия задачи **Обновление**, изменится на *Остановлено*.

После запуска задачи обновления процесс ее выполнения отображается в поле напротив названия задачи **Обновление** в блоке **Управление задачами** на закладке **Центр управления** главного окна программы.

Откат последнего обновления баз программы

После первого обновления баз программы становится доступна функция отката к предыдущему набору баз программы.

Каждый раз, когда на SVM запускается обновление, программа Kaspersky Security создает резервную копию используемых баз программы и только потом приступает к их обновлению. Это позволяет при необходимости вернуться к использованию предыдущего набора баз программы. Возможность отката последнего обновления полезна, например, в том случае, если новая версия баз программы содержит некорректную сигнатуру, из-за которой Kaspersky Security блокирует безопасную программу.

Откат последнего обновления баз программы Kaspersky Security выполняется в следующем порядке:

1. Откат последнего обновления баз программы на SVM. Вы можете откатить последнее обновление баз программы на одной или нескольких SVM. Откат последнего обновления на SVM выполняется с помощью *задачи отката обновления* на Сервере защиты. Задача запускается из Kaspersky Security Center и выполняется на SVM.
2. Откат последнего обновления баз программы на защищенных виртуальных машинах. После отката обновления баз программы на SVM автоматически выполняется откат последнего обновления на всех защищенных виртуальных машинах, которые подключены к этой SVM. Если защищенная виртуальная машина выключена или приостановлена, откат последнего обновления баз на этой машине будет выполнен после ее включения в соответствии с расписанием запуска *задачи обновления* на Легком агенте. По умолчанию задан автоматический режим запуска задачи. Задача запускается каждые два часа.

   На защищенной виртуальной машине с установленным компонентом Легкий агент для Windows пользователь может настроить в локальном интерфейсе расписание запуска задачи обновления или запустить задачу обновления вручную, если эти функции не запрещены политикой для всех защищенных виртуальных машин группы администрирования.

   На защищенной виртуальной машине с установленным компонентом Легкий агент для Linux пользователь может вручную запустить задачу обновления из командной строки (см. раздел "Обновление баз" на стр. 490).

► *Чтобы откатить последнее обновление баз программы на SVM, выполните следующие действия:*

1. Создайте задачу отката обновления на Сервере защиты для SVM, на которых вы хотите откатить обновление баз программы (см. раздел "Создание задачи отката обновления баз на Сервере защиты" на стр. 397).
2. Запустите задачу отката обновления на Сервере защиты (см. раздел "Запуск и остановка задач" на стр. 147).

Создание задачи отката обновления баз на Сервере защиты

► *Чтобы создать в Консоли администрирования задачу отката обновления баз на Сервере защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для SVM, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу для всех SVM, входящих в эту группу. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких SVM (задачу для набора устройств).
3. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты** выберите **Откат обновления**.

   Перейдите к следующему шагу мастера создания задачи.
5. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора SVM, для которых вы создаете задачу. Вы можете выбрать SVM из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать список SVM из файла или указать ранее настроенную выборку устройств (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:
   - В списке обнаруженных виртуальных машин укажите SVM, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия SVM.
   - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
   - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, для которых вы создаете задачу.

   Перейдите к следующему шагу мастера создания задачи.
6. В поле **Запуск по расписанию** выберите **Вручную**. Настройте остальные параметры расписания запуска задачи. Подробнее о параметрах расписания запуска задачи см. в документации Kaspersky Security Center.

   Перейдите к следующему шагу мастера создания задачи.
7. В поле **Имя** введите имя задачи отката обновления.

   Перейдите к следующему шагу мастера создания задачи.
8. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**. Завершите работу мастера создания задачи.

Созданная задача отобразится в списке задач. Вы можете запускать и останавливать задачу вручную (см. раздел "Запуск и остановка задач" на стр. 147).

Обновление баз программы из локальной или сетевой папки

► *Чтобы настроить обновление баз из локальной или сетевой папки, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** дерева консоли.
3. В рабочей области в списке задач выберите задачу **Загрузка обновлений в хранилище Сервера администрирования** и откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню задачи и выберите пункт **Свойства**.
   - По ссылке **Изменить параметры задачи**, расположенной справа от списка задач в блоке с параметрами задачи.
4. В окне свойств задачи в списке слева выберите раздел **Параметры**.

   В правой части окна отобразятся параметры задачи.
5. В блоке **Источники обновлений** по ссылке **Настроить** откройте окно **Источники обновлений**.
6. В окне **Источники обновлений** нажмите на кнопку **Добавить**.

   Откроется окно **Свойства источника обновлений баз**.
7. Выберите вариант **Локальная или сетевая папка**, нажмите на кнопку **Обзор** и в открывшемся окне укажите папку, в которую вы предварительно загрузили обновления баз программы с помощью утилиты Updater Utility. О работе с утилитой см. подробнее на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/updater4).
8. Нажмите на кнопку **OK** в окне **Свойства источника обновлений баз**.
9. Нажмите на кнопку **OK** в окне **Источники обновлений**.
10. Нажмите на кнопку **Применить**.

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, а также сведения о репутации проверяемых веб-адресов.

В зависимости от расположения инфраструктуры различают:

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

Информация о том, какой тип KSN использует программа Kaspersky Security, отображается в свойствах политики для Сервера защиты (см. раздел "Настройка использования Kaspersky Security Network в политике Сервера защиты" на стр. 401), в локальном интерфейсе Легкого агента для Windows (см. раздел "Проверка подключения к Kaspersky Security Network в локальном интерфейсе" на стр. 402) и в командной строке Легкого агента для Linux (см. раздел "Просмотр информации о программе" на стр. 481).

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

Взаимодействие между SVM и защищенными виртуальными машинами, находящимися под управлением Kaspersky Security Center, и инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Для использования KSN в работе Kaspersky Security служба прокси-сервера KSN должна быть включена в Kaspersky Security Center.

Для использования Локального KSN требуется включить и настроить использование Локального KSN в Kaspersky Security Center.

Выбор типа KSN, который используется в работе программы Kaspersky Security, а также 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 для Сервера защиты (см. раздел "Настройка использования Kaspersky Security Network в политике Сервера защиты" на стр. 401).

Легкий агент использует в своей работе KSN в соответствии с параметрами, полученными от SVM, к которой он подключен. Если Легкий агент теряет подключение к SVM, он продолжает использовать параметры, полученные при последнем подключении.

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

Компоненты Kaspersky Security отправляют информацию (см. раздел "О предоставлении данных при использовании Kaspersky Security Network" на стр. 400) в "Лабораторию Касперского" 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.

Участие в Kaspersky Security Network является добровольным. Решение об участии в KSN принимается при создании политики для Сервера защиты, его можно изменить в любой момент.

В этом разделе

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, необходимую для получения репутации веб-адресов: проверяемый веб-адрес, тип протокола соединения, номер используемого порта и веб-адрес, с которого осуществлен переход на проверяемый веб-адрес.
- 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 для Сервера защиты.

Текст Положения о Kaspersky Security Network вы можете посмотреть в свойствах политики для Сервера защиты в разделе **Параметры Kaspersky Security Network**.

Параметры, определяющие состав и получателя данных, отправляемых в "Лабораторию Касперского" при

использовании KSN, хранятся в конфигурационных файлах на защищенной виртуальной машине. Безопасность конфигурационных файлов на защищенной виртуальной машине обеспечивает механизм самозащиты (см. раздел "Самозащита программы" на стр. 405). Если вы выключили механизм самозащиты, вам нужно обеспечить защиту этих конфигурационных файлов от несанкционированного доступа. За подробной информацией вы можете обратиться к специалистам Службы технической поддержки.

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" (https://www.kaspersky.com/products-and-services-privacy-policy).

Если вы не участвуете в Kaspersky Security Network, то данные, перечисленные в Положении о Kaspersky Security Network, не передаются в "Лабораторию Касперского".

Настройка использования Kaspersky Security Network в политике Сервера защиты

Вы можете настроить использование KSN в работе Kaspersky Security в параметрах политики для Сервера защиты с помощью Консоли администрирования

Если использование KSN включено в активной политике для Сервера защиты, службы KSN используются в работе программы 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, KSN не используется 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 также 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 Консоли администрирования – в разделе **Прокси-сервер KSN**). См. подробнее в документации Kaspersky Security Center.

► *Чтобы настроить использование KSN в работе программы Kaspersky Security в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, политику которой вы хотите изменить.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
   - Двойным щелчком мыши.

- По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.

5. В списке слева выберите раздел **Параметры Kaspersky Security Network**.
6. Если вы хотите включить использование KSN, выполните следующие действия:
   a. Установите флажок **Использовать KSN для проверки файлов и веб-адресов**.
   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 **OK**.
   d. По умолчанию KSN используется в расширенном режиме. Режим KSN влияет на объем данных, которые автоматически передаются в "Лабораторию Касперского" (см. раздел "О предоставлении данных при использовании Kaspersky Security Network" на стр. 400) при использовании KSN. Если вы хотите выключить использование расширенного KSN, снимите флажок **Использовать расширенный KSN**.

Выбор типа KSN, который используется в работе программы Kaspersky Security, а также настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

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

7. Если вы хотите выключить использование KSN, снимите флажок **Использовать KSN для проверки файлов и веб-адресов**.
8. Нажмите на кнопку **Применить**.

Проверка подключения к Kaspersky Security Network в локальном интерфейсе

► *Чтобы проверить подключение к Kaspersky Security Network, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 120).
2. В верхней части окна нажмите на кнопку **Kaspersky Security Network**.

   Откроется окно **Kaspersky Security Network**.

   Круглая кнопка **KSN** в левой части окна обозначает статус использования служб KSN в работе программы Kaspersky Security:

   - Если в работе программы Kaspersky Security используются службы KSN, то кнопка **KSN** имеет зеленый цвет. Под кнопкой **KSN** отображаются следующие сведения:
     - статус `Включено`;

- тип используемого KSN: Локальный KSN или Глобальный KSN;
- режим использования KSN: стандартный или расширенный KSN;
- дата последней синхронизации с серверами KSN.

В правой части окна отображается статистика о репутации файлов и веб-ресурсов.

> Получение статистических данных по использованию программой Kaspersky Security служб KSN происходит при открытии окна **Kaspersky Security Network**. Обновление статистики в реальном времени не производится.

- Если в работе программы Kaspersky Security не используются службы KSN, то кнопка **KSN** имеет серый цвет. Под кнопкой **KSN** отображается статус `Выключено`.

  Подключение к серверам KSN может отсутствовать по следующим причинам:

  - использование KSN выключено в политике для Сервера защиты;
  - программа не активирована или срок действия лицензии истек;
  - виртуальная машина не подключена к интернету;
  - служба прокси-сервера KSN выключена в Kaspersky Security Center (см. в документации Kaspersky Security Center).

Настройка дополнительных параметров программы

Вы можете выполнить следующие действия для настройки дополнительных функций программы:

- Настроить механизмы самозащиты программы и защиты от внешнего управления программой (см. раздел "Самозащита программы" на стр. 405).
- Настроить защиту доступа к функциям программы с помощью пароля (см. раздел "Защита паролем доступа к параметрам программы в локальном интерфейсе" на стр. 408).
- Настроить взаимодействие локального интерфейса Легкого агента с пользователем (см. раздел "Настройка взаимодействия пользователя с локальным интерфейсом" на стр. 412).
- Восстановить стандартные параметры программы в локальном интерфейсе (см. раздел "Восстановление стандартных параметров программы в локальном интерфейсе" на стр. 414).
- Создать и использовать конфигурационный файл (см. раздел "Использование конфигурационного файла" на стр. 415), содержащий параметры работы программы.

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

В этом разделе

Самозащита программы

Программа Kaspersky Security обеспечивает безопасность защищенной виртуальной машины с компонентом Легкий агент для Windows от вредоносных программ, включая вредоносные программы, которые пытаются заблокировать работу программы Kaspersky Security или удалить ее с защищенной виртуальной машины.

Стабильность системы безопасности защищенной виртуальной машины с компонентом Легкий агент для Windows обеспечивают реализованные в программе Kaspersky Security механизмы самозащиты и защиты от внешнего управления.

Механизм самозащиты предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

Механизм защиты от внешнего управления позволяет блокировать все попытки управления службами программы с удаленного компьютера.

В этом разделе

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты программы Kaspersky Security включен. При необходимости вы можете выключить механизм самозащиты.

Выключение самозащиты снижает уровень защиты виртуальной машины от вредоносных программ.

Вы можете включать и выключать механизм самозащиты в свойствах политики для Легкого агента для Windows с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы включить или выключить механизм самозащиты в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Дополнительные параметры**.
6. В правой части окна в блоке **Параметры самозащиты** выполните одно из следующих действий:

- Установите флажок **Включить самозащиту**, если вы хотите включить механизм самозащиты.
- Снимите флажок **Включить самозащиту**, если вы хотите выключить механизм самозащиты.

7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить механизм самозащиты в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите раздел **Другие параметры**.

   В правой части окна отобразятся дополнительные параметры защиты.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить самозащиту**, если вы хотите включить механизм самозащиты.
   - Снимите флажок **Включить самозащиту**, если вы хотите выключить механизм самозащиты.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение механизма защиты от внешнего управления

По умолчанию механизм защиты от внешнего управления включен. При необходимости вы можете выключить механизм защиты от внешнего управления.

Вы можете включать и выключать механизм защиты от внешнего управления в свойствах политики для Легкого агента для Windows с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы включить или выключить в Консоли администрирования механизм защиты от внешнего управления, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Дополнительные параметры**.
6. В правой части окна в блоке **Параметры самозащиты** выполните одно из следующих действий:
   - Установите флажок **Выключить внешнее управление системной службой**, если вы хотите включить механизм защиты от внешнего управления.

- Снимите флажок **Выключить внешнее управление системной службой**, если вы хотите выключить механизм защиты от внешнего управления.

7. Нажмите на кнопку **Применить**.

► *Чтобы включить или выключить в локальном интерфейсе механизм защиты от внешнего управления, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите блок **Другие параметры**.

   В правой части окна отобразятся дополнительные параметры программы.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните одно из следующих действий:
   - Установите флажок **Выключить внешнее управление системной службой**, если вы хотите включить механизм защиты от внешнего управления.
   - Снимите флажок **Выключить внешнее управление системной службой**, если вы хотите выключить механизм защиты от внешнего управления.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Обеспечение работы программ удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость использовать программы удаленного администрирования. В локальном интерфейсе вы можете настроить работу программы удаленного администрирования на защищенной виртуальной машине.

► *Чтобы настроить работу программ удаленного администрирования, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.
4. Выберите закладку **Доверенные программы**.
5. Нажмите на кнопку **Добавить**.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

6. В раскрывшемся контекстном меню выполните одно из следующих действий:
   - Выберите пункт **Программы**, если хотите найти программу удаленного администрирования в списке установленных на защищенной виртуальной машине программ. Откроется окно **Выбор программы**.
   - Выберите пункт **Обзор**, если хотите указать путь к исполняемому файлу программы удаленного администрирования. Откроется окно **Выбор файла**.
7. Выберите программу.

   Откроется окно **Исключения для программы**.
8. Установите флажок **Не контролировать активность программы**.
9. Нажмите на кнопку **OK** в окне **Исключения для программы**.

   В списке доверенных программ появится добавленная доверенная программа.
10. Нажмите на кнопку **OK** в окне **Доверенная зона**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита паролем доступа к параметрам программы в локальном интерфейсе

Защищенную виртуальную машину могут использовать несколько пользователей с разным уровнем компьютерной грамотности. Неограниченный доступ пользователей к программе Kaspersky Security и ее параметрам может привести к снижению уровня безопасности защищенной виртуальной машины в целом.

Для ограничения доступа к программе вы можете задать имя пользователя и пароль и указать операции, для выполнения которых программа должна запрашивать эти данные.

Рекомендуется с осторожностью использовать пароль для ограничения доступа к программе. Если вы забыли пароль, вам нужно обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. 503) для получения инструкций по отмене защиты паролем.

Включение и выключение защиты паролем

► *Чтобы включить или выключить защиту паролем в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел

Интерфейс.

В правой части окна отобразятся параметры локального интерфейса.

6. Если вы хотите ограничить доступ к программе с помощью пароля, выполните следующие действия:
   a. В блоке **Защита паролем** установите флажок **Включить защиту паролем** и нажмите на кнопку **Настройка**.

      Откроется окно **Защита паролем**.

   b. В поле **Новое имя пользователя** введите имя пользователя, от имени которого будет осуществляться доступ к программе.

   c. В поле **Новый пароль** введите пароль для доступа к программе.

      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.

   d. В поле **Подтверждение пароля** повторите пароль.

   e. В блоке **Область действия пароля** укажите операции с программой, для выполнения которых пользователь виртуальной машины должен ввести пароль:

      - Выберите вариант **Все операции (кроме уведомлений об опасности)**, если хотите ограничить доступ ко всем операциям с программой.
      - Выберите вариант **Отдельные операции**, если хотите указать операции, для выполнения которых требуется ввести пароль, и в блоке ниже установите флажки напротив названий нужных операций.

   f. Нажмите на кнопку **ОК** в окне **Защита паролем**.

7. Если вы хотите отменить ограничение доступа к программе с помощью пароля, снимите флажок **Включить защиту паролем**.
8. Нажмите на кнопку **Применить**.

После включения защиты паролем каждый раз, когда пользователь виртуальной машины совершает какую-либо операцию, защищенную паролем, будет открываться окно **Проверка пароля**.

Вы можете установить флажок **Запомнить пароль на текущую сессию работы программы** в окне **Проверка пароля**, если вы хотите, чтобы во время текущей сессии работы программа больше не требовала ввода пароля при попытке выполнения защищенной операции.

Снятый флажок **Запомнить пароль на текущую сессию работы программы** означает, что программа запрашивает пароль каждый раз при попытке выполнения защищенной операции.

► *Чтобы включить или выключить защиту паролем в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

3. Если вы хотите ограничить доступ к программе с помощью пароля, выполните пункт 6 предыдущей инструкции.

> Если флажок **Включить защиту паролем** недоступен, это означает, что вы не можете включить или выключить защиту паролем, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой.

4. Если вы хотите отменить ограничение доступа к программе с помощью пароля, выполните следующие действия:
   a. Снимите флажок **Включить защиту паролем**.
   b. Нажмите на кнопку **Сохранить**.

      Откроется окно **Проверка пароля**.
   c. В поле **Имя пользователя** введите имя пользователя.
   d. В поле **Пароль** введите пароль доступа к программе.
   e. Нажмите на кнопку **OK** в окне **Проверка пароля**.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение пароля доступа к программе

► *Чтобы изменить в Консоли администрирования пароль доступа к программе, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.
6. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.
7. В поле **Новое имя пользователя** введите новое имя пользователя, от имени которого будет осуществляться доступ к программе.
8. В поле **Новый пароль** введите новый пароль для доступа к программе.

   > 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.
9. В поле **Подтверждение пароля** повторите новый пароль.
10. Нажмите на кнопку **OK**.

    Программа проверяет введенные пароли. Если пароли совпадают, программа применяет новый

пароль и закрывает окно **Защита паролем**. Если пароли не совпадают, программа выводит сообщение об этом.

11. Нажмите на кнопку **Применить**.

► *Чтобы изменить в локальном интерфейсе пароль доступа к программе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–10 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Указание причины при завершении работы программы и выключении компонентов защиты в локальном интерфейсе

Специалисты "Лаборатории Касперского" не рекомендуют завершать работу программы и выключать компоненты защиты без необходимости, поскольку в этом случае защита виртуальной машины и ваших персональных данных окажется под угрозой.

Вы можете настроить запрос причины, по которой пользователь завершает работу программы или выключает компоненты защиты в локальном интерфейсе Легкого агента. Причина выключения отправляется в Kaspersky Security Center в виде события вместе с соответствующими событиями *Программа успешно остановлена* или *Задача остановлена*.

Вы можете настраивать запрос причины завершения работы программы или выключения компонентов защиты в свойствах политики для Легкого агента для Windows в Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить в Консоли администрирования запрос причины завершения работы программы или выключения компонентов защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Интерфейс**.

В правой части окна отобразятся параметры локального интерфейса.

6. В блоке **Причины выключения** нажмите на кнопку **Настройка**.

   Откроется окно **Причины выключения**.

7. Установите флажки напротив тех действий, для выполнения которых пользователю нужно указать причину и нажмите на кнопку **OK**.

8. Нажмите на кнопку **Применить**.

Теперь при попытке пользователя в локальном интерфейсе завершить работу программы или выключить компоненты защиты откроется окно **Причина выключения**, в котором требуется ввести причину совершения действия.

► *Чтобы настроить в локальном интерфейсе запрос причины завершения работы программы или выключения компонентов защиты, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).

2. В левой части окна в блоке **Другие параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

   > Если параметры в локальном интерфейсе недоступны, это означает, что вы не можете настроить запрос причины, так как для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–7 предыдущей инструкции.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка взаимодействия пользователя с локальным интерфейсом

Вы можете настраивать параметры взаимодействия пользователя с локальным интерфейсом в свойствах политики для Легкого агента для Windows с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить в Консоли администрирования параметры взаимодействия пользователя с локальным интерфейсом, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.

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

4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

6. Настройте параметры запуска и отображения локального интерфейса на виртуальной машине.

   Чтобы обеспечить возможность работы программы Kaspersky Security на виртуальной машине, на которой используется технология Windows Terminal Services, требуется снять флажок **Запускать локальный интерфейс программы**.

   Если вы используете Легкий агент в инфраструктуре виртуальных рабочих столов (VDI) с операционной системой Microsoft Windows для рабочих станций, то для повышения производительности виртуальной инфраструктуры рекомендуется снять флажок **Запускать локальный интерфейс программы**.

7. Если вы хотите настроить отображение информации о поддержке пользователей, выполните следующие действия:

   a. Нажмите на кнопку **Настройка** в блоке **Поддержка пользователей**.

      Откроется окно **Информация о поддержке**.

   b. Сформируйте список ссылок на веб-ресурсы, который будет отображаться в локальном интерфейсе. Для добавления, изменения, удаления и перемещения ссылок в списке используйте кнопки, расположенные над списком.

   c. Нажмите на кнопку **OK** в окне **Информация о поддержке**, чтобы сохранить изменения и закрыть окно.

8. Нажмите на кнопку **Применить**.

► *Чтобы настроить в локальном интерфейсе параметры взаимодействия пользователя с локальным интерфейсом, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

   Если параметры в локальном интерфейсе недоступны, это означает, что вы не можете настроить параметры отображения локального интерфейса, так как для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Настройте параметры отображения локального интерфейса: параметры защиты паролем, параметры уведомлений, параметры запроса причины выключения компонентов программы, анимацию значка программы (см. раздел "Значок программы в области уведомлений" на стр. 119) в области уведомлений при выполнении задач.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Восстановление стандартных параметров программы в локальном интерфейсе

На основе информации об операционной системе и установленных на защищенной виртуальной машине программах специалисты "Лаборатории Касперского" рекомендуют вам оптимальные параметры защиты виртуальной машины. В процессе работы с программой Kaspersky Security вы всегда можете восстановить стандартные параметры программы на защищенной виртуальной машине. Восстановление параметров выполняется в локальном интерфейсе с помощью мастера первоначальной настройки программы.

► *Чтобы восстановить стандартные параметры программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите блок **Другие параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
3. В блоке **Управление параметрами** нажмите на кнопку **Восстановить**.

   Запустится мастер первоначальной настройки программы.
4. В окне **Добро пожаловать** нажмите на кнопку **Далее**, чтобы начать работу мастера первоначальной настройки программы.
5. В окне **Восстановление параметров** представлены компоненты и задачи программы, параметры которых были изменены.

   Если для какого-либо компонента в процессе работы программы были сформированы уникальные параметры, они также отображаются в этом окне. В число уникальных параметров входят, например, списки доверенных веб-адресов, созданные исключения, сетевые правила, правила контроля программ и другие.

   Эти уникальные параметры формируются в процессе работы с программой с учетом индивидуальных задач и требований безопасности. Формирование уникальных параметров зачастую занимает много времени, поэтому специалисты "Лаборатории Касперского" рекомендуют сохранять их, иначе все сформированные в процессе работы программы параметры будут утеряны.

   Установите флажки для тех компонентов и задач, для которых вы хотите восстановить стандартные параметры.
6. Нажмите на кнопку **Далее**.
7. На следующем этапе мастер первоначальной настройки программ анализирует информацию о программах, входящих в состав Microsoft Windows. Эти программы попадают в список доверенных программ (см. раздел "Добавление программы в список доверенных программ" на стр. 186), которые не имеют ограничений на действия, совершаемые в операционной системе. Выполнение анализа информации отображается в окне **Анализ системы**.

   Завершив анализ операционной системы, мастер первоначальной настройки программы автоматически переходит к следующему шагу.
8. В окне **Завершение первоначальной настройки программы** нажмите на кнопку **Завершить**.

   Мастер первоначальной настройки программы закроется, стандартные параметры программы восстановятся.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование конфигурационного файла

Вы можете сохранить параметры Легкого агента в конфигурационном файле в формате CFG.

Конфигурационный файл с параметрами работы Легкого агента позволяет решить следующие задачи:

- Создать политику для Легкого агента для Windows и перенести в создаваемую политику параметры Легкого агента для Windows, ранее сохраненные на защищенной виртуальной машине.
- Создать политику для Легкого агента для Linux и перенести в создаваемую политику параметры Легкого агента для Linux, ранее сохраненные на защищенной виртуальной машине.
- Перенести параметры работы программы с одной защищенной виртуальной машины на другую. В результате программа Kaspersky Security на обеих защищенных виртуальных машинах будет настроена одинаково.
- Импортировать ранее настроенные параметры Легкого агента во время установки Легкого агента для Windows из командной строки.

Вы можете экспортировать и импортировать параметры Легкого агента для Windows в локальном интерфейсе для Легкого агента для Windows (см. раздел "Экспорт и импорт параметров Легкого агента для Windows в локальном интерфейсе" на стр. 416) или из командной строки (см. раздел "Управление Легким агентом для Windows из командной строки" на стр. 493).

Вы можете экспортировать и импортировать параметры Легкого агента для Linux из командной строки (см. раздел "Экспорт и импорт параметров Легкого агента для Linux из командной строки" на стр. 415).

В этом разделе

Экспорт и импорт параметров Легкого агента для Linux из командной строки

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

```
lightagent export <путь к конфигурационному файлу>
```

где <путь к конфигурационному файлу> – путь к файлу, в который вы хотите сохранить параметры программы. Укажите полный путь к конфигурационному файлу.

Программа создаст конфигурационный файл в формате XML.

► *Чтобы импортировать параметры программы из конфигурационного файла, выполните следующую команду:*

```
lightagent import <путь к конфигурационному файлу>
```

где <путь к конфигурационному файлу> – путь к файлу, из которого вы хотите импортировать параметры программы. Укажите полный путь к конфигурационному файлу.

Вы можете использовать только конфигурационный файл, созданный в программе версии Kaspersky Security для виртуальных сред 5.2 Легкий агент.

Экспорт и импорт параметров Легкого агента для Windows в локальном интерфейсе

► *Чтобы экспортировать параметры программы в конфигурационный файл в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите блок **Другие параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
3. В блоке **Управление параметрами** нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.
4. Введите имя конфигурационного файла и укажите путь, по которому вы хотите его сохранить.
5. Нажмите на кнопку **Сохранить**.

► *Чтобы импортировать параметры программы из конфигурационного файла в локальном интерфейсе, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна выберите блок **Другие параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
3. В блоке **Управление параметрами** нажмите на кнопку **Загрузить**.

   Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.
4. Выберите файл, из которого вы хотите импортировать параметры программы и нажмите на кнопку **Открыть**.

   Вы можете использовать только конфигурационный файл, созданный в программе версии Kaspersky Security для виртуальных сред 5.2 Легкий агент.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Резервное хранилище

Если во время проверки защищенной виртуальной машины программа Kaspersky Security обнаруживает в файле вредоносный код, программа блокирует этот файл, присваивает ему статус *Заражен*, помещает его копию в резервное хранилище и пытается провести лечение файла.

Резервное хранилище – это список резервных копий файлов, которые были удалены или изменены программой в процессе лечения. *Резервная копия* – копия файла, которую программа создает перед лечением или удалением этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, программа Kaspersky Security не помещает копию файла в резервное хранилище, а сразу удаляет его. Восстановить целостность приложения Windows Store вы можете средствами операционной системы Microsoft Windows.

Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. После этого можете восстановить файл из его вылеченной резервной копии в папку исходного размещения (см. раздел "Восстановление файлов из резервного хранилища в локальном интерфейсе" на стр. 420).

В Kaspersky Security Center в резервном хранилище отображается общий список файлов, помещенных в резервное хранилище программами "Лаборатории Касперского" на устройствах. Вы можете просматривать свойства файлов, находящихся в резервных хранилищах на защищенных виртуальных машинах, запускать антивирусную проверку файлов в резервном хранилище и удалять из него файлы через Консоль администрирования. Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных виртуальных машинах. Восстановление файлов выполняется на защищенной виртуальной машине (см. раздел "Восстановление файлов из резервного хранилища в локальном интерфейсе" на стр. 420).

Вы можете работать с резервным хранилищем на защищенной виртуальной машине в локальном интерфейсе Легкого агента для Windows (см. раздел "Работа с резервным хранилищем в локальном интерфейсе" на стр. 419) или через командную строку Легкого агента для Linux (см. раздел "Работа с резервным хранилищем" на стр. 491).

При удалении программы файлы резервного хранилища удаляются с защищенной виртуальной машины.

По истечении заданного времени и при достижении максимального размера резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 418) программа автоматически удаляет из резервного хранилища резервные копии файлов с любым статусом.

Также вы можете самостоятельно удалить резервную копию как восстановленного, так и невосстановленного файла (см. раздел "Удаление резервных копий файлов из резервного хранилища в локальном интерфейсе" на стр. 421).

kaspersky

В этом разделе

Настройка параметров резервного хранилища

Вы можете настраивать следующие параметры резервного хранилища:

- Максимальный срок хранения резервных копий файлов в резервном хранилище.

  По умолчанию максимальный срок хранения резервных копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения программа автоматически удаляет наиболее старые файлы из хранилища. Вы можете отменить ограничение по времени или изменить максимальный срок хранения файлов.

- Максимальный размер резервного хранилища.

  По умолчанию максимальный размер резервного хранилища составляет 100 МБ. После достижения максимального размера программа автоматически удаляет наиболее старые файлы из резервного хранилища таким образом, чтобы не превышался его максимальный размер.

Вы можете настраивать параметры резервного хранилища в свойствах политики для Легкого агента с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить параметры резервного хранилища на виртуальных машинах в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows, если вы хотите настроить параметры резервного хранилища для Легкого агента для Windows, или политику для Легкого агента для Linux, если вы хотите настроить параметры резервного хранилища для Легкого агента для Linux.
5. Откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
6. В списке слева выберите раздел **Отчеты и хранилища**.
7. Если вы хотите настроить срок хранения резервных копий файлов в резервном хранилище, в правой части окна в блоке **Параметры резервного хранилища** выполните одно из следующих действий:

   - Если вы хотите ограничить срок хранения резервных копий файлов в резервном хранилище, установите флажок **Хранить файлы не более** и в поле справа от флажка укажите максимальный срок хранения резервных копий файлов.

     По умолчанию максимальный срок хранения резервных копий файлов в резервном хранилище составляет 30 дней.

- Если вы хотите отменить ограничение срока хранения резервных копий файлов в резервном хранилище, снимите флажок **Хранить файлы не более**.

8. Если вы хотите настроить размер резервного хранилища, в правой части окна в блоке **Параметры резервного хранилища** выполните одно из следующих действий:
   - Если вы хотите ограничить размер резервного хранилища, установите флажок **Максимальный размер хранилища** и в поле справа от флажка укажите максимальный размер.

     По умолчанию задан максимальный размер 100 МБ.
   - Если вы хотите отменить ограничение на размер резервного хранилища, снимите флажок **Максимальный размер хранилища**.
9. Нажмите на кнопку **Применить**.

► *Чтобы настроить параметры резервного хранилища для виртуальной машины с Легким агентом для Windows в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Отчеты и хранилища**.
3. Выполните пункты 7–8 предыдущей инструкции.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с резервным хранилищем в локальном интерфейсе

В локальном интерфейсе Легкого агента для Windows резервные копии файлов в резервном хранилище представлены в виде таблицы.

Вы можете выполнить следующие действия с резервными копиями файлов:

- просмотреть список резервных копий файлов;
- восстановить файлы (см. раздел "Восстановление файлов из резервного хранилища в локальном интерфейсе" на стр. 420) из резервных копий в папки их исходного размещения;
- удалить резервные копии файлов (см. раздел "Удаление резервных копий файлов из резервного хранилища в локальном интерфейсе" на стр. 421) из резервного хранилища.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать список резервных копий файлов по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска резервных копий файлов;
- сортировать резервные копии файлов;
- изменять порядок и набор граф, отображаемых в списке резервных копий файлов;

- копировать выбранные резервные копии файлов в буфер обмена.

В этом разделе

Восстановление файлов из резервного хранилища в локальном интерфейсе

В локальном интерфейсе Легкого агента для Windows вы можете восстановить файл из его резервной копии в папку исходного размещения.

Рекомендуется восстанавливать файлы из резервных копий только в том случае, если им присвоен статус *Вылечен*.

► *Чтобы восстановить файлы из резервного хранилища в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Резервное хранилище**.
4. Если вы хотите восстановить все файлы из резервного хранилища, выполните следующие действия:
   a. По правой клавише мыши в любом месте таблицы на закладке **Резервное хранилище** откройте контекстное меню.
   b. Выберите пункт **Восстановить все**.

   Программа восстановит все файлы из их резервных копий в папки их исходного размещения.
5. Если вы хотите восстановить один или несколько файлов из резервного хранилища, выполните следующие действия:
   a. В таблице на закладке **Резервное хранилище** выберите одну или несколько резервных копий, которые вы хотите восстановить. Для выбора нескольких резервных копий используйте клавишу **CTRL**.
   b. Восстановите файлы из резервных копий одним из следующих способов:
      - Нажмите на кнопку **Восстановить**.
      - По правой клавише мыши откройте контекстное меню и выберите пункт **Восстановить**.

   Программа восстановит файлы из выбранных резервных копий в папки их исходного размещения.

Удаление резервных копий файлов из резервного хранилища в локальном интерфейсе

В локальном интерфейсе Легкого агента для Windows вы можете удалить резервные копии как восстановленных, так и невосстановленных файлов.

► *Чтобы удалить резервные копии файлов из резервного хранилища в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Резервное хранилище**.
4. Если вы хотите удалить все резервные копии файлов из резервного хранилища, выполните одно из следующих действий:
   - Нажмите на кнопку **Очистить хранилище**.
   - По правой клавише мыши в любом месте таблицы на закладке **Резервное хранилище** откройте контекстное меню и выберите пункт **Очистить хранилище**.
5. Если вы хотите удалить одну или несколько резервных копий файлов из резервного хранилища, выполните следующие действия:
   a. В таблице на закладке **Резервное хранилище** выберите одну или несколько резервных копий, которые вы хотите удалить. Для выбора нескольких резервных копий используйте клавишу **CTRL**.
   b. Удалите резервные копии файлов одним из следующих способов:
      - Нажмите на кнопку **Удалить**.
      - По правой клавише мыши откройте контекстное меню и выберите пункт **Удалить**.

События, уведомления и отчеты

В процессе работы программы возникают различного рода события. Они могут иметь информационный характер или нести важную информацию. Например, с помощью события программа может уведомлять об успешно выполненном обновлении баз программы, а может фиксировать ошибку в работе некоторого компонента, которую требуется устранить.

Выделяют следующие уровни важности событий:

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

Список всех событий в работе Сервера администрирования, управляемых устройств и программ сохраняется в журнале событий Kaspersky Security Center и отображается в Консоли администрирования Kaspersky Security Center (см. раздел "Просмотр событий через Kaspersky Security Center" на стр. 423).

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

Вы можете настраивать параметры событий и уведомлений о событиях в политике для Сервера защиты и в политике для Легкого агента (см. раздел "Настройка общих параметров событий и уведомлений компонентов Kaspersky Security" на стр. 424), а также в локальном интерфейсе программы (см. раздел "Настройка событий и уведомлений Легкого агента для Windows" на стр. 425).

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

На основе событий, происходящих во время работы программы, программа формирует различные типы отчетов.

Отчеты о работе программы формируются как в Kaspersky Security Center, так и в локальном интерфейсе Легкого агента для Windows.

С помощью отчетов Kaspersky Security Center вы можете получить, например, сведения о зараженных файлах, изменении параметров защиты, использовании ключей и баз программы. Просматривать отчеты Kaspersky Security Center вы можете в Консоли администрирования Kaspersky Security Center. Подробную информацию о работе с отчетами Kaspersky Security Center см. в документации Kaspersky Security Center.

На защищенной виртуальной машине с компонентом Легкий агент для Windows в отчетах фиксируется информация о работе каждого функционального компонента программы, о выполнении каждой задачи проверки и задачи обновления, а также о работе Легкого агента в целом.

kaspersky

В этом разделе

Просмотр событий через Kaspersky Security Center

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

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

В списке отображаются события из выборки, которая в настоящий момент указана в раскрывающемся списке **Выборки событий**. События в списке не обновляются автоматически. Чтобы просмотреть последние события, обновите список по ссылке **Обновить**.

В Kaspersky Security Center вы можете выполнять следующие действия при просмотре событий:

- Выбирать выборку, события из которой должны отображаться в списке. Раскрывающийся список **Выборки событий** содержит предопределенные выборки (созданные по умолчанию), а также пользовательские выборки. Если пользователь не создавал собственные выборки, пользовательских выборок нет в списке.
- Добавлять или удалять графы из списка событий.
- Искать события в списке по ключевым словам.
- Просматривать подробную информацию о событии, выбранном в списке. Поле с подробной информацией о событии находится справа от списка событий.
- Создавать и настраивать выборки событий.
- Экспортировать и импортировать события выборки.
- Настраивать уведомления о событиях и экспорт событий в SIEM-систему.

Подробную информацию о работе с событиями см. в документации Kaspersky Security Center.

Настройка общих параметров событий и уведомлений компонентов Kaspersky Security

Настройка некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 525).

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

► *Чтобы настроить параметры событий и уведомлений о событиях, происходящих во время работы компонентов программы, выполните следующие действия:*

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

   Откроется окно **Свойства: <Название политики>**.
5. В окне свойств политики в списке слева выберите раздел **Настройка событий**.
6. В правой части окна выберите закладку с названием уровня важности событий, параметры которых вы хотите настроить:
   - **Предельный**.
   - **Отказ функционирования**.
   - **Предупреждение**.
   - **Информационное сообщение**.
7. Выберите типы событий, параметры которых вы хотите настроить:
   - Используйте клавиши **SHIFT** и **CTRL**, если вы хотите выбрать несколько типов событий.
   - Нажмите на кнопку **Выделить все**, если вы хотите выбрать все типы событий.
8. Нажмите на кнопку **Свойства**.
9. Откроется окно **Свойства <N событий>**, где N – количество выбранных типов событий.

10. В блоке **Регистрация событий** установите флажок **На Сервере администрирования в течение (сут)**. Программа будет отправлять на Сервер администрирования Kaspersky Security Center события выбранных вами типов.
11. В поле ввода укажите количество дней, в течение которых события должны храниться на Сервере администрирования. Kaspersky Security Center удаляет события по истечении заданного времени.
12. В блоке **Уведомления о событиях** выберите способ уведомления:
    - **Уведомлять по электронной почте**.
    - **Уведомлять по SMS**.
    - **Уведомлять запуском исполняемого файла или скрипта**.
    - **Уведомлять по SNMP**.
13. Нажмите на кнопку **OK** в окне **Свойства <N событий>**.
14. Нажмите на кнопку **OK** в окне свойств политики.

Настройка событий и уведомлений Легкого агента для Windows

Вы можете настроить следующие способы уведомления о событиях, возникающих во время работы Легкого агента для Windows:

- с помощью всплывающих уведомлений в области уведомлений панели задач Microsoft Windows;
- по электронной почте.

Способ уведомления настраивается для каждого типа событий.

Программа позволяет также сохранять информацию о событиях в журнал событий Microsoft Windows и / или использовать в отчетах программы.

Вы можете настраивать следующие параметры событий и уведомлений о событиях Легкого агента для Windows:

- сохранение событий Легкого агента для Windows (см. раздел "Настройка сохранения событий Легкого агента для Windows" на стр. 426);
- отображение уведомлений на экране (см. раздел "Настройка отображения уведомлений на экране" на стр. 427);
- уведомление о событиях по электронной почте (см. раздел "Настройка уведомлений о событиях по электронной почте" на стр. 428).

Работая с таблицей событий в локальном интерфейсе, вы можете выполнять следующие действия:

- использовать функцию поиска событий;
- сортировать события по возрастанию и убыванию;
- изменять набор граф, отображаемых в списке событий.

kaspersky

В этом разделе

Настройка сохранения событий Легкого агента для Windows

► *Чтобы настроить сохранение событий в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, в которую входят нужные виртуальные машины с компонентом Легкий агент для Windows.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.
6. В блоке **Уведомления** нажмите на кнопку **Настройка**.

   Откроется окно **Уведомления**.

   В левой части окна представлены компоненты и задачи программы. В правой части окна отображается список событий, сформированный для выбранного компонента или задачи.
7. В левой части окна выберите компонент или задачу, для которой вы хотите настроить сохранения событий.
8. Установите флажки напротив нужных типов событий в следующих графах:
   - **Сохранять в журнале программы**, если вы хотите сохранять события в отчетах программы (см. раздел "Работа с отчетами в локальном интерфейсе" на стр. 431).
   - **Сохранять в журнале событий Windows**, если вы хотите сохранять события в журнале событий Microsoft Windows.
9. Нажмите на кнопку **OK** в окне **Уведомления**.
10. Нажмите на кнопку **Применить**.

► *Чтобы настроить сохранение событий в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка отображения уведомлений на экране

► *Чтобы настроить отображение уведомлений на экране в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, в которую входят нужные виртуальные машины с компонентом Легкий агент для Windows.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.
6. В блоке **Уведомления** нажмите на кнопку **Настройка**.

   Откроется окно **Уведомления**.

   В левой части окна представлены компоненты и задачи программы. В правой части окна отображается список событий, сформированный для выбранного компонента или задачи.
7. В левой части окна выберите компонент или задачу, для которой вы хотите настроить отображение уведомлений на экране.
8. В графе **Уведомлять на экране** установите флажки напротив нужных типов событий.
9. Нажмите на кнопку **OK** в окне **Уведомления**.
10. Нажмите на кнопку **Применить**.

Информация о выбранных событиях будет отображаться на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.

► *Чтобы настроить отображение уведомлений на экране в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–9 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Информация о выбранных событиях будет отображаться на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.

Настройка уведомлений о событиях по электронной почте

► *Чтобы настроить уведомления о событиях по электронной почте в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, в которую входят нужные виртуальные машины с компонентом Легкий агент для Windows.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В окне свойств политики для Легкого агента для Windows в списке слева выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.
6. В блоке **Уведомления** нажмите на кнопку **Настройка**.

   Откроется окно **Уведомления**.

   В левой части окна представлены компоненты и задачи программы. В правой части окна отображается список событий, сформированный для выбранного компонента или задачи.
7. В левой части окна выберите компонент или задачу, для которой вы хотите настроить уведомления о событиях по электронной почте.
8. В графе **Уведомлять по почте** установите флажки напротив нужных типов событий.
9. Нажмите на кнопку **Настройка почтовых уведомлений** в нижней части окна.

   Откроется окно **Настройка почтовых уведомлений**.
10. Установите флажок **Отправлять уведомления о событиях**, чтобы включить отправку информации о событиях, отмеченных в графе **Уведомлять по почте**.
11. Укажите параметры отправки почтовых уведомлений.
12. Нажмите на кнопку **OK** в окне **Настройка почтовых уведомлений**.
13. Нажмите на кнопку **OK** в окне **Уведомления**.
14. Нажмите на кнопку **Применить**.

► *Чтобы настроить уведомления о событиях по электронной почте в локальном*

интерфейсе, выполните следующие действия:

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры локального интерфейса.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–13 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка параметров отчетов

Вы можете настраивать следующие параметры отчетов о работе Легкого агента:

- Максимальный срок хранения отчетов.

  По умолчанию максимальный срок хранения отчетов о событиях, фиксируемых программой, составляет 30 дней. По истечении этого времени программа автоматически удаляет наиболее старые записи из файла отчета. Вы можете отменить ограничение по времени или изменить максимальный срок хранения отчетов.

- Максимальный размер файла отчета.

  По умолчанию максимальный размер файла, содержащего отчет, составляет 1024 МБ. После достижения максимального размера файла отчета программа автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы не превышался максимальный размер. Вы можете отменить ограничение на размер файла отчета или изменить максимальный размер файла отчета.

Вы можете настраивать параметры отчетов о работе Легкого агента для Windows в свойствах политики для Легкого агента для Windows с помощью Консоли администрирования и в локальном интерфейсе Легкого агента для Windows.

► *Чтобы настроить параметры отчетов о работе Легкого агента для Windows в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные защищенные виртуальные машины.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику для Легкого агента для Windows и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
5. В списке слева выберите раздел **Отчеты и хранилища**.
6. Если вы хотите настроить срок хранения отчетов, в правой части окна в блоке **Параметры отчетов** выполните одно из следующих действий:

- Если вы хотите ограничить срок хранения отчетов, установите флажок **Хранить отчеты не более** и в поле справа от флажка укажите максимальный срок хранения отчетов.

  По умолчанию максимальный срок хранения отчетов составляет 30 дней.

- Если вы хотите отменить ограничение срока хранения отчетов, снимите флажок **Хранить отчеты не более**.

7. Если вы хотите настроить размер файла отчета, в правой части окна в блоке **Параметры отчетов** выполните одно из следующих действий:

   - Если вы хотите ограничить размер файла отчета, установите флажок **Максимальный размер файла** и в поле справа от флажка укажите максимальный размер файла отчета.

     По умолчанию максимальный размер файла отчета составляет 1024 МБ.

   - Если хотите отменить ограничение на размер файла отчета, снимите флажок **Максимальный размер файла**.

8. Нажмите на кнопку **Применить**.

► *Чтобы настроить параметры отчетов о работе Легкого агента в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Отчеты и хранилища**.

   Если параметры в локальном интерфейсе недоступны, это означает, что для всех защищенных виртуальных машин группы администрирования используются значения параметров, заданные политикой.

3. Выполните пункты 6–7 предыдущей инструкции.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с отчетами в локальном интерфейсе

В локальном интерфейсе Легкого агента для Windows вы можете сформировать отчеты следующих типов:

- Отчет "Системный аудит". Содержит информацию о событиях, возникающих в процессе вашего взаимодействия с программой, а также в ходе работы программы в целом и не относящихся к какому-либо отдельному компоненту или задаче программы.
- Отчет "Все компоненты защиты". Содержит информацию о событиях, возникающих в ходе работы следующих компонентов программы:
  - Файловый Антивирус.
  - Почтовый Антивирус.
  - Веб-Антивирус.
  - Мониторинг системы.
  - Сетевой экран.
  - Защита от сетевых атак.
- Отчет о работе компонента или задачи программы. Содержит информацию о событиях, возникающих в ходе работы выбранного компонента или задачи программы.

Данные в отчете представлены в виде таблицы, которая содержит список событий. Каждая строка таблицы содержит информацию об отдельном событии, атрибуты события находятся в графах таблицы. Некоторые графы являются составными и содержат вложенные графы с дополнительными атрибутами. События, зарегистрированные в работе разных компонентов или задач, имеют разный набор атрибутов.

По умолчанию события в отчетах отсортированы по возрастанию значений графы **Дата события**. Рядом с датой события в графе **Дата события** отображается также уровень важности события.

Предусмотрены следующие уровни важности событий в отчетах:

- **Информационные события**. Значок . События справочного характера, как правило, не содержащие важной информации.
- **Важные события**. Значок . События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе программы.
- **Критические события**. Значок . События критической важности и отказа функционирования программы, указывающие на проблемы в работе программы.

Вы можете выполнять следующие действия с данными отчетов:

- фильтровать список событий по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска определенного события;
- сортировать список событий по каждой графе;
- отображать и скрывать сгруппированные данные;
- изменять порядок и набор граф, отображаемых в отчете;
- просматривать выбранное событие в отдельном блоке (см. раздел "Просмотр отчетов" на стр. 432);
- сохранять сформированный отчет (см. раздел "Сохранение отчета в файл" на стр. 432) в текстовый

файл;

- удалять информацию из отчетов (см. раздел "Удаление информации из отчетов" на стр. 433) по компонентам и задачам программы, объединенным в группы.

Программа удаляет записи в файлах отчетов автоматически по истечении времени, заданного в параметрах программы, или по достижении максимального размера файла отчета. Вы можете отменить эти ограничения или установить другие значения параметров.

В этом разделе

Просмотр отчетов

► *Чтобы просмотреть отчеты в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**. По умолчанию на закладке **Отчеты** отображается отчет "Системный аудит".
3. Выполните одно из следующих действий:
   - Если вы хотите сформировать отчет "Все компоненты защиты", в левой части окна в списке компонентов и задач в разделе **Антивирусная защита** выберите пункт **Все компоненты защиты**.

     В правой части окна отобразится отчет "Все компоненты защиты", содержащий список событий о работе всех компонентов защиты программы.
   - Если вы хотите сформировать отчет о работе определенного компонента или задачи, в левой части окна в списке компонентов и задач выберите нужный компонент или задачу.

     В правой части окна отобразится отчет, содержащий список событий о работе выбранных компонента или задачи.

     По умолчанию события в отчете отсортированы по возрастанию значений графы **Дата события**.
4. Если требуется, воспользуйтесь функциями фильтрации, поиска и сортировки, чтобы найти нужное событие в отчете.
5. Если вы хотите посмотреть подробную информацию о событии отчета, представленную в отдельном блоке, выберите это событие в отчете.

   В нижней части окна отобразится блок, который содержит атрибуты этого события.

Сохранение отчета в файл

В локальном интерфейсе Легкого агента для Windows вы можете сохранить сформированный отчет в

файл текстового формата TXT или CSV.

Программа сохраняет событие в отчет в том виде, в каком событие отображается на экране, то есть с тем же составом и с той же последовательностью атрибутов события.

► *Чтобы сохранить отчет в файл в локальном интерфейсе, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**. По умолчанию на закладке **Отчеты** отображается отчет "Системный аудит".
3. Выполните одно из следующих действий:
   - Если вы хотите сформировать отчет "Все компоненты защиты", в левой части окна в списке компонентов и задач выберите пункт **Все компоненты защиты**.

     В правой части окна отобразится отчет "Все компоненты защиты", содержащий список событий о работе всех компонентов защиты.
   - Если вы хотите сформировать отчет о работе определенного компонента или задачи, в левой части окна в списке компонентов и задач выберите нужный компонент или задачу.

     В правой части окна отобразится отчет, содержащий список событий о работе выбранных компонента или задачи.
4. Если требуется, измените представление данных в отчете, используя следующие возможности:
   - фильтрация списка событий по значениям граф или по условиям сложного фильтра;
   - поиск событий;
   - изменение порядка и набора граф, отображаемых в отчете;
   - сортировка списка событий по каждой графе.
5. Нажмите на кнопку **Сохранить отчет**, расположенную в верхней правой части окна.

   Откроется контекстное меню.
6. В контекстном меню выберите нужную кодировку для сохранения файла отчета: **Сохранить в ANSI** или **Сохранить в Unicode**.

   Откроется стандартное окно Microsoft Windows **Сохранить как**.
7. В открывшемся окне **Сохранить как** укажите папку, в которую вы хотите сохранить файл отчета.
8. В поле **Имя файла** введите имя файла отчета.
9. В поле **Тип файла** выберите нужный формат файла отчета: TXT или CSV.
10. Нажмите на кнопку **Сохранить**.

Удаление информации из отчетов

Программа автоматически удаляет записи в файлах отчетов согласно значениям, заданным в параметрах

программы. Также вы можете удалить информацию из отчетов в локальном интерфейсе Легкого агента для Windows.

► *Чтобы удалить информацию из отчетов, выполните следующие действия:*

1. На защищенной виртуальной машине откройте окно настройки параметров программы (на стр. 121).
2. В левой части окна в блоке **Другие параметры** выберите раздел **Отчеты и хранилища**.
3. В правой части окна в блоке **Параметры отчетов** нажмите на кнопку **Удалить отчеты**.

   Откроется окно **Удаление информации из отчетов**.
4. Установите флажки для тех отчетов, из которых вы хотите удалить информацию:
   - **Все отчеты**.
   - **Общий отчет защиты**. Содержит информацию о работе следующих компонентов программы:
     - Файловый Антивирус.
     - Почтовый Антивирус.
     - Веб-Антивирус.
     - Сетевой экран.
     - Защита от сетевых атак.
   - **Отчет задач проверки**. Содержит информацию о выполненных задачах проверки:
     - Полная проверка.
     - Проверка важных областей.
     - Выборочная проверка.
   - **Отчет задач обновления**. Содержит информацию о выполненных задачах обновления.
   - **Отчет обработки правил Сетевого экрана**. Содержит информацию о работе Сетевого экрана.
   - **Отчет компонентов контроля**. Содержит информацию о работе следующих компонентов программы:
     - Контроль запуска программ.
     - Контроль активности программ.
     - Контроль устройств.
     - Веб-Контроль.
   - **Отчет Контроля целостности системы**. Содержит информацию о работе компонента Контроль целостности системы.
   - **Данные Мониторинга системы**. Содержит информацию о работе компонента Мониторинг системы.
5. Нажмите на кнопку **OK** в окне **Удаление информации из отчетов**.

Просмотр и изменение параметров Сервера интеграции

В Консоли Сервера интеграции вы можете посмотреть параметры Сервера интеграции (см. раздел «Просмотр параметров Сервера интеграции» на стр. 435), а также изменить следующие параметры:

- Пароли учетных записей Сервера интеграции (см. раздел "Изменение паролей учетных записей Сервера интеграции" на стр. 436):
  - учетной записи администратора Сервера интеграции;
  - учетной записи для подключения SVM к Серверу интеграции;
  - учетной записи для подключения Легких агентов к Серверу интеграции.

  Имена учетных записей недоступны для изменения.

- Имя и пароль учетной записи (см. раздел "Изменение и удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 437), которую Сервер интеграции использует для подключения к гипервизору или серверу управления виртуальной инфраструктурой.

Если требуется, вы можете удалить параметры подключения Сервера интеграции к виртуальной инфраструктуре (см. раздел "Изменение и удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 437).

В этом разделе

Просмотр параметров Сервера интеграции

► *Чтобы просмотреть параметры Сервера интеграции, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. 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 (см. раздел "О файлах трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 510), вы можете открыть для просмотра этот файл по ссылке **Посмотреть файл трассировки**. Файл трассировки открывается в текстовом редакторе Блокнот.

Изменение паролей учетных записей Сервера интеграции

Вы можете изменить пароли следующих учетных записей Сервера интеграции:

- учетной записи администратора Сервера интеграции;
- учетной записи для подключения SVM к Серверу интеграции;
- учетной записи для подключения Легких агентов к Серверу интеграции;
- учетной записи для взаимодействия с REST API Сервера интеграции.

Имена учетных записей недоступны для изменения.

► *Чтобы изменить пароли учетных записей Сервера интеграции, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Учетные записи Сервера интеграции**.
3. В таблице справа выберите имя учетной записи, пароль которой вы хотите изменить.
4. По ссылке **Изменить пароль учетной записи**, расположенной над таблицей, откройте окно **Пароль учетной записи** и 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.

5. Нажмите на кнопку **OK** в окне **Пароль учетной записи**.

Если вы изменили пароль учетной записи для подключения SVM к Серверу интеграции, вам нужно повторно настроить подключение SVM к Серверу интеграции (см. раздел "Настройка параметров подключения SVM к Серверу интеграции" на стр. 164) в политике для Сервера защиты.

Если в политике для Легкого агента настроено подключение Легких агентов к Серверу интеграции и вы изменили пароль учетной записи для подключения Легких агентов, вам нужно повторно настроить подключение Легких агентов к Серверу интеграции (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 165) в политике для Легкого агента для Windows и в политике для

Легкого агента для Linux.

Новые параметры учетной записи для подключения к Серверу интеграции передаются в политику при сохранении параметров политики.

Изменение и удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре

Сервер интеграции получает информацию о защищаемой виртуальной инфраструктуре, необходимую для работы программы, от гипервизора или сервера управления виртуальной инфраструктурой. В разделе Консоли Сервера интеграции **Параметры подключения к инфраструктуре** отображается список всех гипервизоров и серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

В разделе Консоли Сервера интеграции **Параметры подключения к инфраструктуре** вы можете выполнить следующие действия:

- Изменить (см. раздел "Изменение параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 438) имя и пароль учетной записи, которая используется для подключения Сервера интеграции к гипервизору или серверу управления виртуальной инфраструктурой.
- В инфраструктуре VMware: включить или выключить использование VMware NSX Manager (см. раздел "Изменение параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 438) в работе Kaspersky Security, а также ввести или изменить параметры подключения Сервера интеграции к VMware NSX Manager.
- Удалить (см. раздел "Удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 440) гипервизор или сервер управления виртуальной инфраструктурой из списка гипервизоров и серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

Список гипервизоров и серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции, отображается в виде таблицы, каждая строка которой содержит следующие сведения:

- Тип и IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора или сервера управления виртуальной инфраструктурой.
- Статус подключения Сервера интеграции к виртуальной инфраструктуре.
- Для инфраструктуры VMware: IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX-V Manager или VMware NSX-T Manager, если включено использование VMware NSX Manager в работе Kaspersky Security. Если используется VMware NSX Manager, то Kaspersky Security может назначать теги безопасности (см. раздел "О тегах безопасности (Security Tags)" на стр. 163) (Security Tags) защищенным виртуальным машинам.

Если подключение Сервера интеграции к гипервизору или серверу управления виртуальной инфраструктурой не установлено, в таблице отображается сообщение об ошибке.

Сервер интеграции проверяет подлинность всех гипервизоров и серверов управления виртуальной инфраструктурой, которые отображаются в таблице, кроме гипервизора Microsoft Windows Server (Hyper-V). Для гипервизора Microsoft Windows Server (Hyper-V) проверка подлинности не выполняется.

Для проверки подлинности Сервер интеграции получает от каждого гипервизора или сервера управления виртуальной инфраструктурой SSL-сертификат или отпечаток открытого ключа и проверяет их. Если не удалось установить подлинность сертификата или открытого ключа, полученного от гипервизора или сервера управления виртуальной инфраструктурой, Сервер интеграции разрывает соединение с этим

гипервизором или сервером управления виртуальной инфраструктурой. В таблице отображается сообщение об ошибке.

Вы можете устранить эту ошибку одним из следующих способов:

- Подтвердить подлинность сертификата или открытого ключа, полученного от гипервизора или сервера управления виртуальной инфраструктурой. Для этого вам нужно перейти в список гипервизоров и серверов управления виртуальной инфраструктурой, который отображается в мастере управления SVM (см., например, шаг "Выбор гипервизоров для развертывания SVM (на стр. 67)" в процедуре развертывания SVM). Откроется окно **Проверка сертификата** или окно **Проверка отпечатка открытого ключа** (в зависимости от типа гипервизора или сервера управления виртуальной инфраструктурой), в котором вы можете подтвердить подлинность сертификата или подлинность открытого ключа.
- Если вы не считаете сертификат подлинным, вы можете заменить сертификат на новый.

Если включено использование VMware NSX Manager в работе Kaspersky Security, Сервер интеграции также проверяет сертификат VMware NSX Manager и отображает в таблице сообщение в случае обнаружения ошибки сертификата. Вы можете устранить ошибку сертификата VMware NSX Manager одним из следующих способов:

- Подтвердить подлинность сертификата. Чтобы посмотреть информацию о полученном сертификате, вам нужно перейти по ссылке **Подтверждение подлинности сертификата VMware NSX Manager**, которая отображается в сообщении об ошибке. Если сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и продолжить подключение к VMware NSX Manager. Для этого нажмите на кнопку **Считать сертификат подлинным** в окне **Проверка сертификата**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.
- Если вы не считаете сертификат подлинным, вы можете прервать подключение, нажав на кнопку **Отмена**, и заменить сертификат на новый.

В этом разделе

Изменение параметров подключения Сервера интеграции к виртуальной инфраструктуре

► *Чтобы изменить параметры подключения Сервера интеграции к виртуальной инфраструктуре, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Параметры подключения к инфраструктуре**.
3. В таблице выберите гипервизор или сервер управления виртуальной инфраструктурой, под управлением которого находятся гипервизоры, и перейдите по ссылке **Изменить**, расположенной

над таблицей. Откроется окно **Изменение параметров подключения к виртуальной инфраструктуре**.

4. Если вы хотите изменить учетную запись, которую Сервер интеграции использует для подключения к гипервизору или серверу управления виртуальной инфраструктурой, в верхней части окна укажите новые имя и пароль учетной записи.

   В целях повышения безопасности рекомендуется использовать учетную запись, которая обладает правами только на чтение (см. раздел "Учетные записи для установки и работы программы" на стр. 52).

5. Если в списке гипервизоров и серверов управления виртуальной инфраструктурой вы выбрали VMware vCenter Server, вы можете настроить использование VMware NSX Manager в работе программы Kaspersky Security.

   Чтобы включить использование VMware NSX Manager в работе программы Kaspersky Security, в нижней части окна **Изменение параметров подключения к виртуальной инфраструктуре** выполните следующие действия:

   a. Установите флажок **Использовать VMware NSX Manager**

   b. В раскрывающемся списке **Тип VMware NSX Manager** выберите один из следующих элементов:

      - **VMware NSX-V Manager** – если в вашей инфраструктуре установлен VMware NSX Manager из пакета VMware NSX Data Center for vSphere.
      - **VMware NSX-T Manager** – если в вашей инфраструктуре установлен VMware NSX Manager из пакета VMware NSX-T Data Center.

   c. Укажите следующие параметры подключения:

      - IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX Manager.

        Если в вашей виртуальной инфраструктуре VMware NSX-T Manager объединены в кластер, укажите виртуальный IP-адрес кластера. Предварительно вам нужно назначить кластеру виртуальный IP-адрес и сертификат (подробнее о настройке кластера VMware NSX-T Manager см. в документации VMware).
      - Имя и пароль учетной записи, которую Сервер интеграции должен использовать для подключения к VMware NSX Manager. Требуется учетная запись VMware NSX Manager, которой назначена роль Enterprise Administrator.

   Чтобы изменить параметры подключения Сервера интеграции к VMware NSX Manager, в нижней части окна **Изменение параметров подключения к виртуальной инфраструктуре** укажите тип VMware NSX Manager и новые имя и пароль учетной записи.

   Если вы изменили пароль учетной записи для подключения к VMware NSX-T Manager, то Сервер интеграции сможет подключиться к VMware NSX Manager не ранее, чем через 15 минут после сохранения новых параметров подключения.

   Чтобы выключить использование VMware NSX Manager в работе программы Kaspersky Security, снимите флажок **Использовать VMware NSX Manager**.

6. Нажмите на кнопку **OK** в окне **Изменение параметров подключения к виртуальной инфраструктуре**.

   Сервер интеграции выполняет следующие действия:

a. Проверяет подлинность каждого гипервизора или сервера управления виртуальной инфраструктурой, параметры которого вы изменили (кроме гипервизора Microsoft Windows Server (Hyper-V)). Для проверки подлинности Сервер интеграции получает SSL-сертификат или отпечаток открытого ключа от каждого гипервизора или сервера управления виртуальной инфраструктурой.

   Если сертификат, полученный от гипервизора или сервера управления виртуальной инфраструктурой, не является доверенным для Сервера интеграции или не соответствует ранее установленному сертификату, сообщение об ошибке отображается в списке гипервизоров и серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции (см. раздел "Изменение и удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 437).

b. Если вы включили использование VMware NSX Manager или изменили параметры подключения к VMware NSX Manager, Сервер интеграции проверяет подлинность VMware NSX Manager. Для проверки подлинности Сервер интеграции получает SSL-сертификат от VMware NSX Manager.

   Если сертификат, полученный от VMware NSX Manager, не является доверенным для Сервера интеграции или не соответствует ранее установленному сертификату, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. Если вы не считаете этот сертификат подлинным, нажмите на кнопку **Отмена**, чтобы прервать подключение, и замените сертификат на новый.

   Если сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и продолжить подключение к VMware NSX Manager. Для этого нажмите на кнопку **Считать сертификат подлинным** в окне **Проверка сертификата**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

Удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре

Если вы хотите, чтобы Сервер интеграции перестал получать информацию о виртуальной инфраструктуре от гипервизора или сервера управления виртуальной инфраструктурой, вы можете удалить этот гипервизор или сервер управления виртуальной инфраструктурой из списка гипервизоров и серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

Рекомендуется удалять из списка гипервизор или сервер управления виртуальной инфраструктурой, только если в инфраструктуре под управлением этого гипервизора или сервера управления виртуальной инфраструктурой не установлены компоненты программы Kaspersky Security.

► *Чтобы удалить параметры подключения Сервера интеграции к виртуальной инфраструктуре, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Параметры подключения к инфраструктуре**.
3. В таблице справа выберите гипервизор или сервер управления виртуальной инфраструктурой, под управлением которого находятся гипервизоры, и перейдите по ссылке **Удалить**, расположенной над таблицей.

4. Подтвердите удаление в открывшемся окне.

Если вы удалили гипервизор или сервер управления виртуальной инфраструктурой из этого списка, рекомендуется также удалить его из списка гипервизоров и серверов управления виртуальной инфраструктурой, который отображается в мастере управления SVM (см., например, шаг "Выбор SVM для удаления" в процедуре удаления SVM).

Проверка целостности компонентов программы

Компоненты программы Kaspersky Security содержат 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 файлов и модулей программы. Программа проверяет файлы и модули на наличие неавторизованных изменений или повреждений. Если файл или модуль программы имеет некорректную контрольную сумму, то он считается поврежденным.

Проверка целостности выполняется для файлов и модулей следующих компонентов программы:

- Mmc-плагинов управления Kaspersky Security.
- Сервера интеграции.
- Консоли Сервера интеграции.
- Сервера защиты.
- Легкого агента для Windows.
- Легкого агента для Linux.

Проверка целостности файлов и модулей компонентов программы выполняется с помощью утилиты проверки целостности integrity_check_tool. Утилита проверяет целостность файлов и модулей, перечисленных в специальных списках, которые называются *файлы манифеста.* Файл манифеста компонента программы содержит файлы и модули, целостность которых важна для корректной работы компонента. Целостность самих файлов манифеста также проверяется.

Во время проверки целостности файлов и модулей Легкого агента для Windows также проверяется наличие на виртуальной машине следующих функциональных компонентов Легкого агента:

- Файловый Антивирус;
- Почтовый Антивирус;
- Веб-Антивирус (только на виртуальных машинах с операционными системами для рабочих станций);
- Мониторинг системы;
- AMSI-защита (только на виртуальных машинах с операционными системами Windows 10, Windows Server 2016 и Windows Server 2019);
- Контроль запуска программ;
- Веб-Контроль (только на виртуальных машинах с операционными системами для рабочих станций);
- Контроль целостности системы (только на виртуальных машинах с операционными системами для серверов);
- Контроль активности программ (только на виртуальных машинах с операционными системами для рабочих станций);
- Интеграция с Kaspersky Endpoint Agent.

Проверка целостности файлов и модулей Легкого агента для Windows завершается с ошибкой, если указанные функциональные компоненты не установлены на виртуальной машине.

Расположение файлов манифеста и утилиты проверки целостности

- Mmc-плагин управления Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\ksvla5_2.svm.plg\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\ksvla5_2.svm.plg\integrity_check_tool.exe.
- Mmc-плагин управления Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\ksvla5_2.windows.plg\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\ksvla5_2.windows.plg\integrity_check_tool.exe.
- Mmc-плагин управления Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\ksvla5_2.linux.plg\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\ksvla5_2.linux.plg\integrity_check_tool.exe.
- Сервер защиты:
  - Комбинированный файл манифеста для Сервера защиты и Агента администрирования для Linux: /opt/kaspersky/la/bin/integrity_check.xml.
  - Файл манифеста для Сервера защиты: /opt/kaspersky/la/config/integrity.xml.
  - Файл манифеста для Агента администрирования для Linux: /opt/kaspersky/la/config/klnagent_integrity.xml.
  - Утилита проверки целостности для Сервера защиты и Агента администрирования для Linux: /opt/kaspersky/la/bin/integrity_check_tool.
- Сервер интеграции:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\integrity_check_tool.exe.
- Консоль Сервера интеграции:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA Console\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA Console\integrity_check_tool.exe.
- Легкий агент для Windows:
  - Файл манифеста в зависимости от операционной системы:

    - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\integrity_check.xml – для 64-разрядных операционных систем.
    - %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\integrity_check.xml – для 32-разрядных операционных систем.
  - Утилита проверки целостности в зависимости от операционной системы:
    - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\integrity_check_tool.exe – для 64-разрядных операционных систем.
    - %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Virtualization 5.2 Light Agent\integrity_check_tool.exe – для 32-разрядных операционных систем.
- Легкий агент для Linux:
  - Комбинированный файл манифеста для Легкого агента для Linux и Агента администрирования для Linux: /opt/kaspersky/lightagent/bin/integrity_check.xml.
  - Файл манифеста для Легкого агента для Linux: /opt/kaspersky/lightagent/config/integrity.xml.
  - Файл манифеста для Агента администрирования для Linux: /opt/kaspersky/lightagent/config/klnagent_integrity.xml.
  - Утилита проверки целостности для Легкого агента для Linux и Агента администрирования для Linux: /opt/kaspersky/lightagent/bin/integrity_check_tool.

Запуск утилиты проверки целостности компонентов программы

Для запуска утилиты проверки целостности на SVM и на виртуальной машине с установленным Легким агентом для Linux требуется учетная запись root. Для запуска утилиты проверки целостности остальных компонентов программы требуется учетная запись администратора.

► *Чтобы проверить целостность компонента программы, запустите утилиту из папки расположения утилиты для этого компонента, выполнив одну из следующих команд:*

- в операционной системе Windows:

  `integrity_check_tool.exe -v[|--verify] -m[|--manifest] <путь к файлу манифеста>`

- в операционной системе Linux:

  `integrity_check_tool -v[|--verify] -m[|--manifest] <путь к файлу манифеста>`

где `<путь к файлу манифеста>` – полный путь к файлу манифеста для компонента.

Вы можете запускать утилиту со следующими необязательными параметрами:

- `-V`, `--verbose` – дополнительно выводить информацию об успешно проверенных файлах и модулях. Если параметр не указан, выводится только результат выполнения проверки (succeeded / failed), информация об ошибках и общая статистика проверки.
- `-L`, `--log-file <файл>`, где <файл> – имя файла, в который записываются события, произошедшие во время проверки. По умолчанию события выводятся в стандартный поток stdout.
- `-l`, `--log-level <0-1000>`, где <0-1000> – уровень детализации событий. По умолчанию уровень детализации – 0.

Вы можете просмотреть описание всех доступных параметров утилиты проверки целостности в справке

параметров утилиты. Для этого запустите утилиту с параметром `-h [--help]`.

Результат выполнения проверки целостности компонентов программы

Результат проверки целостности компонента программы отображается в следующем виде:

- `SUCCEEDED` – целостность файлов и модулей подтверждена (код возврата `0`).
- `FAILED` – целостность файлов и модулей не подтверждена (код возврата отличен от `0`).

Использование программы в режиме multitenancy

При использовании программы в режиме multitenancy один экземпляр программы, установленный в инфраструктуре организации-провайдера (далее также "провайдера"), позволяет обеспечивать защиту изолированных виртуальных инфраструктур организаций-клиентов или изолированных подразделений одной организации (далее также "клиентов").

В программе Kaspersky Security реализована возможность автоматизировать процедуры развертывания и использования программы в режиме multitenancy средствами REST API Сервера интеграции (см. раздел "Использование REST API Сервера интеграции" на стр. 463).

Предусмотрены следующие сценарии использования программы Kaspersky Security в режиме multitenancy:

- Развертывание структуры защиты клиентов средствами REST API Сервера интеграции с использованием виртуальных Серверов администрирования Kaspersky Security Center и получение отчетов о защите клиентов (на стр. 459).
- Получение отчетов о защите клиентов без развертывания структуры защиты клиентов средствами REST API Сервера интеграции.

  Если структура защиты клиентов уже развернута в вашей инфраструктуре без использования REST API Сервера интеграции, вы можете регистрировать существующих клиентов и их виртуальные машины (см. раздел "Регистрация существующих клиентов и их виртуальных машин" на стр. 456) и получать отчеты о защите клиентов.

С помощью программы Kaspersky Security для виртуальных сред 5.2 Легкий агент вы можете продолжать управлять защитой клиентов, в виртуальной инфраструктуре которых установлены Легкие агенты версии Kaspersky Security для виртуальных сред 5.1 Легкий агент. Для включения и выключения защиты виртуальных машин с установленным Легким агентом версии 5.1 используются политики включения и выключения защиты (см. подробнее в справке Kaspersky Security для виртуальных сред 5.1 Легкий агент (https://support.kaspersky.com/KSVLA/5.1/ru-RU/199684.htm)). Для включения и выключения защиты виртуальных машин с установленным Легким агентом версии 5.2 политики включения и выключения защиты не требуются.

kaspersky

В этом разделе

Развертывание структуры защиты клиентов

Структура защиты клиентов, созданная с помощью REST API Сервера интеграции, основана на использовании виртуальных Серверов администрирования Kaspersky Security Center. Каждому клиенту предоставляется виртуальный Сервер администрирования и учетная запись, под которой администратор клиента будет подключаться к виртуальному Серверу администрирования.

Один Сервер администрирования Kaspersky Security Center может поддерживать до 500 виртуальных Серверов администрирования.

Виртуальные машины клиента с установленными Легкими агентами размещаются на виртуальном Сервере администрирования клиента.

Администратор клиента может выполнять следующие действия на своем виртуальном Сервере администрирования:

- Централизовано управлять защитой своих виртуальных машин с помощью политик для Легкого агента и групповых задач.
- Получать информацию о состоянии защиты своей инфраструктуры с помощью уведомлений о событиях и отчетов, доступных на виртуальном Сервере администрирования.
- Работать с копиями файлов, помещенными в резервные хранилища на всех виртуальных машинах этого клиента.

Подробнее о виртуальных Серверах администрирования см. в документации Kaspersky Security Center.

Администратор провайдера выполняет установку программы в своей инфраструктуре и обеспечивает работу Легких агентов и других компонентов программы:

- Настраивает параметры подключения Легких агентов, установленных на виртуальных машинах клиента, к SVM и к Серверу интеграции.
- Активирует программу и осуществляет контроль лицензионных ограничений.
- Выполняет обновление баз и модулей программы.

- Настраивает параметры работы Сервера защиты.

Также администратор провайдера может настраивать общие параметры защиты виртуальных машин клиентов.

Во время работы между компонентами программы Kaspersky Security, установленными в инфраструктуре провайдера и на виртуальных машинах клиента, а также программой Kaspersky Security Center осуществляется передача информации, которая может содержать персональные и конфиденциальные данные.

Перед тем, как создавать структуру защиты клиентов, вам нужно выполнить следующие действия:

1. Установить или обновить программу Kaspersky Security.

   В инфраструктуре провайдера должны быть установлены следующие компоненты:

   - Mmc-плагины Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции.
   - Сервер защиты.

2. Подготовить программу к работе:

   - Подготовить к работе Сервер защиты (см. раздел "Подготовка Сервера защиты к работе" на стр. 78).
   - В Консоли Сервера интеграции изменить заданный по умолчанию пароль учетной записи multitenancy (см. раздел "Изменение паролей учетных записей Сервера интеграции" на стр. 436). Учетная запись multitenancy создается автоматически в результате установки Сервера интеграции и требуется для взаимодействия с REST API Сервера интеграции.
   - В Консоли Сервера интеграции настроить параметры подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center (см. раздел "Настройка параметров подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 449). Эти параметры требуются для авторизации на Сервере администрирования Kaspersky Security Center при выполнении запросов к REST API Сервера интеграции.

Развертывание структуры защиты клиента состоит из следующих этапов:

1. Создание клиента и виртуального Сервера администрирования Kaspersky Security Center для клиента (см. раздел "Создание клиента и виртуального Сервера администрирования" на стр. 450).
2. Настройка расположения SVM, которые будут защищать виртуальные машины клиентов, b настройка параметров работы Сервера защиты (см. раздел "Настройка расположения SVM и параметров Сервера защиты" на стр. 452).
3. Настройка параметров обнаружения SVM Легкими агентами, установленными на виртуальных машинах клиентов, и настройка общих параметров работы Легких агентов (см. раздел "Настройка параметров обнаружения SVM Легкими агентами и общих параметров защиты клиентов" на стр. 453).
4. Установка Агента администрирования Kaspersky Security Center и Легкого агента на виртуальные машины клиента и перемещение виртуальных машин на виртуальный Сервер администрирования, настроенный для клиента (см. раздел "Установка Легкого агента на виртуальные машины клиента" на стр. 454).
5. Регистрация виртуальных машин клиента в базе данных Сервера интеграции (см. раздел "Регистрация виртуальных машин клиента" на стр. 455).

6. Активация клиента (на стр. 455).
7. Передача администратору клиента параметров для подключения к виртуальному Серверу администрирования Kaspersky Security Center:
   - адреса виртуального Сервера администрирования, настроенного для клиента;
   - параметров учетной записи администратора виртуального Сервера администрирования.

   Администратору клиента рекомендуется изменить пароль учетной записи, полученный от администратора провайдера.

Этапы развертывания структуры защиты клиентов могут быть автоматизированы средствами REST API Сервера интеграции (см. раздел "Использование REST API Сервера интеграции" на стр. 463) и OpenAPI™ Kaspersky Security Center.

В целях предотвращения несанкционированного доступа рекомендуется SVM и устройство, на котором установлены Сервер администрирования Kaspersky Security Center и Сервер интеграции, разместить в выделенной виртуальной сети и настроить маршрутизацию с трансляцией адресов (SNAT) из подсетей клиентов в эту подсеть.

В этом разделе

Настройка параметров подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center

Для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center во время выполнения запросов требуется учетная запись, которая обладает следующими правами в Kaspersky Security Center:

- Правами в функциональных областях Сервера администрирования:
  - Общий функционал → Базовая функциональность: Чтение, Изменение.
  - Общий функционал → Управление группами администрирования: Изменение.
  - Общий функционал → Права пользователей: Изменение списков управления доступом

объектов.

- Общий функционал → Виртуальные Серверы администрирования: Чтение, Изменение, Выполнение, Управление.

- Правами на чтение и на изменение в функциональных областях, к которым относятся параметры Легкого агента для Windows и Легкого агента для Linux.

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.

► *Чтобы настроить параметры подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Параметры подключения к Kaspersky Security Center**.
3. Укажите параметры подключения:
   - IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера администрирования Kaspersky Security Center.
   - Имя и пароль учетной записи, которая будет использоваться для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center.
4. Нажмите на кнопку **Сохранить**.

   Сервер интеграции выполняет попытку подключения, чтобы проверить указанные параметры подключения. Если SSL-сертификат, полученный от Сервера администрирования Kaspersky Security Center, не является доверенным для Сервера интеграции, открывается окно с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. Если полученный сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата, нажав на кнопку **Установить сертификат**. Полученный сертификат сохраняется в качестве доверенного для Сервера интеграции.

   После установки подключения Сервер интеграции сохраняет параметры подключения.

Создание клиента и виртуального Сервера администрирования

На этом этапе развертывания структуры защиты клиента выполняется добавление информации о клиенте в базу данных Сервера интеграции и создание виртуального Сервера администрирования для клиента. Процедуры автоматизированы средствами REST API Сервера интеграции (см. раздел "Создание клиента" на стр. 466).

Действия, выполняемые в результате запроса к REST API, зависят от типа клиента, который вы указываете при вызове метода REST API: развертывание структуры защиты клиентов доступно только для клиентов типа "полный".

В запросе к REST API нужно передать следующие сведения:

- Название клиента.
- Тип клиента: полный.
- Параметры учетной записи, которую будет использовать администратор клиента для подключения к виртуальному Серверу администрирования, настроенному для клиента. Во время выполнения процедуры автоматически будет создана учетная запись с правами главного администратора на виртуальном Сервере администрирования.

  Kaspersky Security Center проверяет уникальность имен учетных записей в пределах главного Сервера администрирования Kaspersky Security Center и всех его виртуальных Серверов администрирования. По умолчанию, если имя пользователя не уникально, создание учетной записи завершается с ошибкой. Если вы хотите использовать одинаковые имена учетных записей для виртуальных Серверов администрирования, вы можете отключить проверку уникальности имени внутреннего пользователя, см. подробнее в документации Kaspersky Security Center.

В результате выполнения процедуры выполняются следующие действия:

- В базе данных Сервера интеграции сохраняются данные о клиенте, клиенту присваивается уникальный идентификатор.
- Для каждого клиента создается виртуальный Сервер администрирования Kaspersky Security Center и учетная запись, под которой администратор клиента будет подключаться к виртуальному Серверу администрирования.
- При регистрации первого клиента в дереве консоли Kaspersky Security Center главного Сервера администрирования в папке **Управляемые устройства** создается папка с названием по умолчанию **Multitenancy KSV LA**. Вы можете изменить это название, если требуется.
- В папке **Multitenancy KSV LA** для каждого клиента создается структура папок и узлов следующего вида:

  папка **<Название клиента>**

  - узел **Серверы администрирования**
    - узел **Сервер администрирования <Название клиента>**
      - папки и группы администрирования, необходимые для управления защитой этого клиента, аналогично структуре папок и групп главного Сервера администрирования Kaspersky Security Center.
- В папке **Multitenancy KSV LA** → **<Название клиента>** создаются политики включения и выключения защиты виртуальных машин с установленным Легким агентом версии Kaspersky Security для виртуальных сред 5.1 Легкий агент.

Политики включения и выключения защиты применяются, только если в виртуальной инфраструктуре клиента установлены Легкие агенты версии Kaspersky Security для виртуальных сред 5.1 Легкий агент. Политики включения и выключения защиты используются для определения параметров обнаружения SVM и настройки общих параметров работы Легких агентов. Подробнее о политиках включения защиты см. в справке Kaspersky Security для виртуальных сред 5.1 Легкий агент (https://support.kaspersky.com/KSVLA/5.1/ru-RU/199684.htm).

Настройка расположения SVM и параметров Сервера защиты

На этом этапе развертывания структуры защиты клиента вы можете выполнить следующие действия:

1. Настроить расположение SVM, которые будут защищать виртуальные машины клиентов, в иерархии групп администрирования Kaspersky Security Center.
2. Настроить параметры работы Сервера защиты, установленного на этих SVM, с помощью политики для Сервера защиты.
3. Настроить общие параметры работы Легких агентов, которые будут установлены на виртуальных машинах клиентов, с помощью политик для Легкого агента.

Вы можете размещать SVM, которые будут защищать виртуальные машины клиентов, в любых папках и группах администрирования на главном Сервере администрирования Kaspersky Security Center.

Не рекомендуется размещать SVM и политику для Сервера защиты в папках и группах администрирования, к которым администратор клиента имеет доступ, то есть в папках и группах администрирования внутри узла **Сервер администрирования <Название клиента>**.

Если вы хотите, чтобы SVM защищала виртуальные машины только одного или нескольких клиентов, вам нужно ограничить доступ Легких агентов к SVM одним из следующих способов:

- С помощью механизма тегов для подключения. Теги нужно указать в политике для Сервера защиты и в политике для Легкого агента. Настроенные параметры рекомендуется закрыть "замком", чтобы запретить изменение этих параметров в локальных параметрах программы и в политиках вложенного уровня иерархии.
- Запретив сетевые подключения из подсети клиента в подсеть с SVM на TCP-порты 80, 9876, 9877, 11111, 11112.

Не рекомендуется настраивать теги для подключения в политиках для Легкого агента, расположенных в папках и группах администрирования, к которым администратор клиента имеет доступ, то есть в папках и группах администрирования внутри узла **Сервер администрирования <Название клиента>**.

В соответствии с порядком наследования политик Kaspersky Security Center на всех SVM в иерархии групп администрирования применяется политика по умолчанию для Сервера защиты, созданная в результате установки mmc-плагинов Kaspersky Security в папке **Управляемые устройства** на главном Сервере администрирования. Если вы хотите настроить особые параметры работы для SVM, которые будут защищать виртуальные машины клиентов, вам нужно создать политику для Сервера защиты в папке расположения SVM, которая защищает виртуальные машины клиентов.

Если вы хотите централизовано включить использование Kaspersky Security Network для защиты виртуальных машин клиентов, вам нужно убедиться, что обеспечивается законность обработки персональных данных клиентов (см. раздел "О предоставлении данных при использовании Kaspersky Security Network" на стр. 400).

Настройка параметров обнаружения SVM Легкими агентами и общих параметров защиты клиентов

На этом этапе развертывания структуры защиты клиента вам нужно создать политику для Легкого агента в одной из следующих папок:

- В папке **Multitenancy KSV LA** → **<Название клиента>**, если вы хотите настраивать общие параметры работы для всех Легких агентов, которые будут установлены на виртуальных машинах одного клиента. Политику в папке **Multitenancy KSV LA** → **<Название клиента>** нужно создать для каждого клиента.
- В папке **Multitenancy KSV LA**, если вы хотите настраивать общие параметры работы для всех Легких агентов, которые будут установлены на виртуальных машинах всех клиентов.

В политике для Легкого агента вам нужно настроить параметры работы Легкого агента следующим образом:

- Параметры подключения Легких агентов к SVM (см. раздел "Настройка параметров подключения Легких агентов к SVM" на стр. 168):
  - Вам нужно включить использование Сервера интеграции для обнаружения SVM в политике для Легкого агента (см. раздел "Настройка параметров обнаружения SVM" на стр. 168). Легкие агенты, установленные на виртуальных машинах клиентов типа "полный", должны использовать Сервер интеграции для обнаружения SVM, доступных для подключения.
  - Если вы хотите ограничить доступ Легких агентов к SVM с помощью механизма тегов для подключения, вы можете назначить теги для подключения Легким агентам (см. раздел "Назначение Легким агентам тегов для подключения" на стр. 170).

    Если вы используете программу по стандартной лицензии, использование тегов для подключения недоступно. Чтобы ограничить доступ Легких агентов к SVM, вы можете использовать настройки сети, например, вы можете запретить сетевые подключения из подсети клиента в подсеть с SVM по портам, используемым программой (см. раздел "Настройка портов, используемых программой" на стр. 35).

  Для остальных параметров подключения Легких агентов к SVM можно использовать значения по умолчанию.

  Все параметры подключения Легких агентов к SVM рекомендуется закрыть "замком", чтобы запретить изменение этих параметров в локальных параметрах программы и в политиках вложенного уровня иерархии.

- Если требуется, вы можете настроить общие параметры работы Легких агентов, которые будут установлены на виртуальных машинах клиентов.

  С помощью атрибута "замок" вы можете запретить или разрешить изменение параметров или

блоков параметров в локальных параметрах программы, в параметрах задач и в политиках вложенного уровня иерархии (для вложенных групп администрирования и подчиненных Серверов администрирования). Администраторы клиентов не могут настраивать параметры, которые закрыты "замком". Если "замки" открыты, то администратор клиента сможет самостоятельно настраивать работу компонентов Легкого агента.

Если в виртуальной инфраструктуре клиента установлены Легкие агенты и SVM версии Kaspersky Security для виртуальных сред 5.1 Легкий агент, для настройки общих параметров работы этих Легких агентов рекомендуется использовать политики включения защиты клиента, которые были автоматически созданы в папке **Multitenancy KSV LA** → **<Название клиента>**. Подробнее см. в справке Kaspersky Security для виртуальных сред 5.1 Легкий агент (https://support.kaspersky.com/KSVLA/5.1/ru-RU/199684.htm).

Не рекомендуется настраивать общие параметры работы Легких агентов в политиках, расположенных в папках и группах администрирования, к которым администратор клиента имеет доступ, то есть в папках и группах администрирования внутри узла **Сервер администрирования <Название клиента>**.

Установка Легкого агента на виртуальные машины клиента

На этом этапе развертывания структуры защиты клиента выполняются следующие действия:

- На виртуальные машины клиента устанавливается Агент администрирования Kaspersky Security Center, настроенный на подключение к виртуальному Серверу администрирования клиента.
- Виртуальные машины клиента перемещаются в папку **Управляемые устройства** виртуального Сервера администрирования, настроенного для клиента.
- На виртуальные машины клиента устанавливается Легкий агент для Windows или Легкий агент для Linux (см. раздел "Установка Легкого агента для Linux" на стр. 92).

Указанные действия могут быть выполнены как на стороне провайдера, так и на стороне клиента после предоставления администратору клиента параметров подключения к виртуальному Серверу администрирования.

Если установка выполняется на стороне провайдера

Вы можете автоматизировать установку программ на виртуальные машины клиентов и перемещение виртуальных машин в группы администрирования средствами OpenAPI Kaspersky Security Center. См. подробнее в Базе знаний (https://support.kaspersky.ru/15530).

Также вы можете использовать другие варианты установки:

- Удаленную установку программ на виртуальные машины с помощью мастера или задачи удаленной установки программы.

  Для установки на виртуальные машины с операционными системами Windows потребуется инсталляционный пакет Агента администрирования. Для каждого клиента вам нужно подготовить инсталляционный пакет Агента администрирования, в свойствах которого указаны параметры подключения к виртуальному Серверу администрирования, настроенному для этого клиента. В свойствах пакета или задачи удаленной установки вы можете указать группу администрирования, в которую должна попасть виртуальная машина после установки на ней Агента администрирования. Подробнее о настройке инсталляционного пакета см. в документации Kaspersky Security Center.

  Для установки на виртуальные машины с операционными системами Linux не требуется отдельный инсталляционный пакет Агента администрирования. Агент администрирования входит в

инсталляционный пакет Легкого агента для Linux. Вам нужно настроить параметры подключения Агента администрирования к виртуальному Серверу администрирования в свойствах инсталляционного пакета Легкого агента для Linux (см. раздел "Настройка параметров Агента администрирования в свойствах инсталляционного пакета Легкого агента для Linux" на стр. 101).

Инсталляционные пакеты, необходимые для установки Легкого агента для Windows, Легкого агента для Linux и Агента администрирования, размещаются на главном Сервере администрирования Kaspersky Security Center в папке **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**. Вы можете распространять инсталляционные пакеты на выбранные виртуальные Серверы администрирования с помощью задачи Сервера администрирования или автоматизировать распространение пакетов средствами OpenAPI Kaspersky Security Center. См. подробнее в Базе знаний (https://support.kaspersky.ru/15530).

- Развертывание виртуальных машин с операционными системами Windows из шаблона виртуальных машин.

  Вам нужно подготовить для каждого клиента шаблон виртуальных машин, на котором установлен Агент администрирования, настроенный на подключение к виртуальному Серверу администрирования клиента, и Легкий агент. Затем вы можете развернуть виртуальные машины для клиента из этого шаблона.

  > В ходе установки Агента администрирования на шаблон виртуальных машин рекомендуется включить оптимизацию параметров Агента администрирования для VDI.

Если установка выполняется на стороне клиента

При наличии подготовленных администратором провайдера инсталляционных пакетов или шаблона виртуальных машин установку Агента администрирования и Легкого агента на виртуальные машины клиента может выполнять администратор клиента.

Регистрация виртуальных машин клиента

На этом этапе развертывания структуры защиты клиента выполняется регистрация виртуальных машин клиента. Процедура автоматизирована средствами REST API Сервера интеграции (см. раздел "Регистрация виртуальных машин клиента" на стр. 470).

В запросе к REST API вам нужно передать идентификатор (BIOS ID) виртуальной машины и идентификатор клиента, которому принадлежит виртуальная машина.

В результате выполнения процедуры в базу данных Сервера интеграции добавляется информация о виртуальной машине и устанавливается связь между виртуальной машиной и клиентом.

Активация клиента

На этом этапе развертывания структуры защиты клиента выполняется процедура активации клиента. Клиенты регистрируются в базе данных Сервера интеграции со статусом "неактивный". Пока клиент имеет этот статус, Легкие агенты, установленные на виртуальных машинах клиента, не получают информацию об SVM, к которым доступно подключение, защита виртуальных машин клиента выключена. Чтобы начать защищать виртуальные машины клиента, вам нужно активировать клиента.

Процедура активации клиента автоматизирована средствами REST API Сервера интеграции (см. раздел "Активация клиента" на стр. 468).

В результате выполнения процедуры выполняются следующие действия:

- Статус клиента изменяется на "активный". Статус клиента сохраняется в базе данных Сервера интеграции. Вы можете получать информацию о статусе клиента средствами REST API Сервера интеграции или при просмотре списка клиентов в Консоли Сервера интеграции (см. раздел "Получение информации о клиентах" на стр. 458).
- Легкие агенты, установленные на виртуальных машинах клиента, получают от Сервера интеграции список SVM, доступных для подключения. Легкие агенты выбирают оптимальную для подключения SVM в соответствии с настроенными параметрами подключения к SVM, защита виртуальных машин клиента включается.
- Изменяется состояние политик включения и выключения защиты виртуальных машин с установленным Легким агентом версии Kaspersky Security для виртуальных сред 5.1 Легкий агент.

  Политики включения и выключения защиты применяются, только если в виртуальной инфраструктуре клиента установлены Легкие агенты версии Kaspersky Security для виртуальных сред 5.1 Легкий агент. Подробнее см. в справке Kaspersky Security для виртуальных сред 5.1 Легкий агент (https://support.kaspersky.com/KSVLA/5.1/ru-RU/199684.htm).

Регистрация существующих клиентов и их виртуальных машин

Если структура защиты клиентов настроена без использования REST API Сервера интеграции, для получения отчетов о защите клиентов вам нужно добавить информацию о клиентах и их виртуальных машинах в базу данных Сервера интеграции.

Регистрация существующего клиента и его виртуальных машин в базе данных Сервера интеграции состоит из следующих этапов:

1. Создание клиента в базе данных Сервера интеграции.

   Процедура создания клиентов автоматизирована средствами REST API Сервера интеграции (см. раздел "Создание клиента" на стр. 466).

   Действия, выполняемые в результате запроса к REST API, зависят от типа клиента, который вы указываете при вызове метода REST API. Чтобы внести данные о клиенте в базу данных Сервера интеграции без создания структуры защиты клиента, вам нужно указать тип клиента "упрощенный".

   В запросе к REST API вам нужно передать следующие сведения:

   - Название клиента.
   - Тип клиента: упрощенный.

   В результате выполнения процедуры в базе данных Сервера интеграции сохраняются данные о клиенте; клиенту присваивается идентификатор.

2. Регистрация виртуальных машин клиента в базе данных Сервера интеграции.

   Процедура регистрации виртуальных машин автоматизирована средствами REST API Сервера интеграции (см. раздел "Регистрация виртуальных машин клиента" на стр. 470).

   В запросе к REST API нужно передать идентификатор (BIOS ID) каждой виртуальной машины и идентификатор клиента, которому принадлежат виртуальные машины.

В результате выполнения процедуры в базе данных Сервера интеграции сохраняются данные о виртуальных машинах клиента.

3. Активация клиента.

   Процедура активации клиента автоматизирована средствами REST API Сервера интеграции (см. раздел "Активация клиента" на стр. 468).

   После активации статус клиента сохраняется в базе данных Сервера интеграции. Вы можете получать информацию о статусе клиента средствами REST API Сервера интеграции или при просмотре списка клиентов в Консоли Сервера интеграции (см. раздел "Получение информации о клиентах" на стр. 458).

   В случае клиента типа "упрощенный" статус ("активный" или "неактивный") не влияет на состояние защиты виртуальных машин клиента.

Включение и выключение защиты клиентов

Клиенты, зарегистрированные в базе данных Сервера интеграции, могут находиться в статусе "активный" или "неактивный". По умолчанию статус клиента "неактивный".

Для клиентов типа «полный» статус клиента определяет состояние защиты виртуальных машин клиента:

- Если клиент имеет статус "активный", Сервер интеграции передает Легким агентам, установленным на виртуальных машинах клиента, список SVM, доступных для подключения. Легкие агенты выбирают оптимальную для подключения SVM в соответствии с настроенными параметрами подключения к SVM, и подключаются к ней. Защита виртуальных машин клиента включена.
- Если клиент имеет статус "неактивный", Сервер интеграции передает Легким агентам, установленным на виртуальных машинах клиента, адрес несуществующей SVM. Это означает, что Легкие агенты не смогут подключиться ни к одной SVM. Защита виртуальных машин клиента выключена.

Чтобы включить защиту виртуальных машин клиента типа "полный", вам нужно активировать клиента. Если вы хотите выключить защиту виртуальных машин клиента типа "полный" (приостановить предоставление услуг защиты клиенту), вы можете деактивировать клиента.

После деактивации клиента на Сервере администрирования Kaspersky Security Center регистрируются события от Легких агентов, установленных на виртуальных машинах клиента: однократно регистрируется событие об отсутствии доступных для подключения SVM и каждые 2 часа регистрируются события о том, что невозможно выполнить задачу обновления на защищенной виртуальной машине.

Чтобы избежать несанкционированного использования программы, после деактивации клиента рекомендуется запретить сетевые подключения из подсети деактивированного клиента в подсеть с SVM на TCP-порты 80, 9876, 9877, 11111, 11112.

Для клиента типа "упрощенный" статус не влияет на состояние защиты виртуальных машин.

Процедуры активации (см. раздел "Активация клиента" на стр. 468) и деактивации (см. раздел "Деактивация клиента" на стр. 469) клиентов автоматизированы средствами REST API Сервера интеграции.

Получение информации о клиентах

В программе реализованы следующие способы получения информации о клиентах:

- просмотр списка клиентов в Консоли Сервера интеграции;
- получение списка клиентов (см. раздел "Получение списка клиентов" на стр. 465), списка виртуальных машин клиента (см. раздел "Получение списка виртуальных машин клиента" на стр. 466) и информации о клиенте (см. раздел "Получение информации о клиенте" на стр. 464) средствами REST API Сервера интеграции.

► *Чтобы посмотреть список клиентов в Консоли Сервера интеграции, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Список клиентов**.

В рабочей области справа откроется список всех клиентов, зарегистрированных в базе данных Сервера интеграции. Список представлен в виде таблицы.

В списке отображается следующая информация о каждом клиенте:

- **Статус** – статус клиента в базе данных Сервера интеграции. Статус обозначается значком:
  - ✔ – клиент находится в статусе "активный".
  - ✖ – клиент находится в статусе "неактивный".

  Для клиентов типа "полный" статус определяет состояние защиты виртуальных машин клиента:
  - если клиент имеет статус "активный", защита виртуальных машин клиента включена;
  - если клиент имеет статус "неактивный", защита виртуальных машин клиента выключена.

  Для клиентов типа "упрощенный" статус не влияет на состояние защиты виртуальных машин.
- **Сведения о клиенте и его виртуальных машинах**:
  - название клиента;
  - тип клиента: **Полный** или **Упрощенный**;
  - идентификатор клиента;
  - для клиента типа "полный": идентификатор виртуального Сервера администрирования, настроенного для клиента;
  - список идентификаторов (BIOS ID) или имен виртуальных машин клиента.
- **Учетная запись администратора** – имя учетной записи, под которой администратор клиента типа "полный" подключается к виртуальному Серверу администрирования, настроенному для клиента. В списке отображается имя учетной записи, указанное при создании клиента, даже если впоследствии имя было изменено.

Вы можете обновлять список клиентов с помощью ссылки **Обновить**, расположенной над таблицей.

Получение отчетов о защите клиентов

Виртуальная машина считается защищенной, когда установленный на ней Легкий агент подключен к SVM. Каждая SVM может собирать данные о периодах времени, когда Легкие агенты были подключены к SVM, и передавать эти данные в базу данных Сервера интеграции. На основе этой информации средствами REST API Сервера интеграции можно получать отчеты о защите виртуальных машин клиентов.

С помощью отчета о защите клиентов вы можете получать информацию обо всех защищаемых виртуальных машинах клиента с указанием всех периодов времени, когда каждая виртуальная машина находилась под защитой программы. Также с помощью отчета вы можете получать информацию о защите всех виртуальных машин, которые подключались к SVM за указанный отчетный период, в том числе виртуальных машин, которые не принадлежат ни одному клиенту.

Получение отчетов о защите клиентов состоит из следующих этапов:

1. Включение функции передачи данных для отчетов (на стр. 459) в базу данных Сервера интеграции.
2. Формирование отчета (см. раздел "Формирование отчета о защите клиентов" на стр. 460). Отчет формируется в виде файла формата CSV во временной папке.
3. Выгрузка отчета (см. раздел "Выгрузка отчета о защите клиентов" на стр. 461). Сформированный отчет может быть выгружен целиком или по частям для интеграции в систему отчетов провайдера.

В этом разделе

Включение функции передачи данных для отчетов

По умолчанию функция передачи данных для отчетов выключена на Сервере интеграции. Если вы хотите получать отчеты о защите клиентов, вам нужно включить функцию получения данных для отчетов в конфигурационном файле Сервера интеграции: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\viislaservice.exe.config.

► *Чтобы включить функцию получения данных для отчетов, выполните следующие действия:*

1. Откройте на редактирование конфигурационный файл viislaservice.exe.config.
2. Установите для параметра `EnableTenantsProtectionReports` значение `true` и сохраните файл.
3. Перезапустите Сервер интеграции.

Сервер интеграции будет получать от каждой SVM данные о периодах подключения Легких агентов к SVM.

Если функция получения данных включена, но подключение SVM к Серверу интеграции отсутствует, пакеты данных помещаются в очередь на отправку. После достижения максимального числа пакетов в очереди более старые пакеты данных удаляются. Параметры отправки данных задаются в конфигурационном файле /etc/opt/kaspersky/agents_monitor/agents_monitor.conf на SVM. Вы можете настраивать максимальный размер очереди пакетов на отправку с помощью параметра `max_queue_size`.

Полученные данные сохраняются в базе данных Сервера интеграции. Срок хранения данных для отчетов по умолчанию составляет 460 дней. Вы можете настраивать это значение с помощью параметра `TenantsProtectionPeriodsRecordsLifetimeDays` в конфигурационном файле Сервера интеграции viislaservice.exe.config.

Размер базы данных Сервера интеграции увеличивается пропорционально числу защищаемых виртуальных машин клиентов.

Формирование отчета о защите клиентов

Процедура формирования отчета автоматизирована средствами REST API Сервера интеграции (см. раздел "Формирование отчета" на стр. 473).

В запросе к REST API вы можете передавать следующие параметры формирования отчета:

- идентификатор клиента, о защите которого вы хотите получить отчет;
- дата и время начала периода, за который вы хотите получить отчет;
- дата и время окончания периода, за который вы хотите получить отчет.

Если в запросе не указан идентификатор клиента, отчет будет включать в себя данные обо всех виртуальных машинах, которые находились под защитой в указанный период. В том числе, о виртуальных машинах, которые не принадлежат клиентам.

Если в запросе не указан период формирования отчета, в отчет войдут данные с самой ранней из дат, зафиксированных в базе данных Сервера интеграции, и до текущего момента.

Для получения достоверной информации в отчетах при формировании отчетного периода рекомендуется следовать правилам:

- задавать отчетный период с точностью до дня;
- устанавливать окончание отчетного периода не менее чем через 60 минут от текущего момента.

В результате выполнения процедуры формирования отчета возвращается идентификатор отчета. Отчет формируется в защищенной служебной папке %ProgramData%\Kaspersky Lab\VIISLA\protectionPeriodsReports и хранится по умолчанию 24 часа с момента формирования. Чтобы получить отчет, вам нужно использовать идентификатор отчета в запросе к REST API для выгрузки отчета (см. раздел "Выгрузка отчета о защите клиентов" на стр. 461).

Вы можете настроить срок хранения отчета с помощью параметра `TenantsProtectionReportsLifetimeHours` в конфигурационном файле Сервера интеграции: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\viislaservice.exe.config.

Данные в отчете представлены построчно. В каждой строке содержится информация об одном периоде защиты виртуальной машины в следующем формате:

```
{идентификатор клиента};{название клиента};{идентификатор виртуальной машины};{имя виртуальной машины};{дата и время включения защиты};{дата и время выключения защиты}
```

где:

- `{идентификатор клиента}` – идентификатор клиента, которому принадлежит виртуальная машина. Если виртуальная машина не принадлежит ни одному клиенту, в поле ничего не указывается.
- `{название клиента}` – название клиента, заданное при создании клиента. Если виртуальная машина не принадлежит ни одному клиенту, в поле ничего не указывается.
- `{идентификатор виртуальной машины}` – идентификатор виртуальной машины, которая находилась под защитой программы.
- `{имя виртуальной машины}` – имя виртуальной машины, которая находилась под защитой программы.
- `{дата и время включения защиты}` – дата и время начала периода защиты виртуальной машины.
- `{дата и время выключения защиты}` – дата и время окончания периода защиты виртуальной машины.

Если в течение отчетного периода виртуальная машина находилась под защитой программы несколько раз (защита включалась и выключалась), то в отчете отображается каждый период защиты виртуальной машины.

Выгрузка отчета о защите клиентов

Процедура выгрузки отчета автоматизирована средствами REST API Сервера интеграции (см. раздел "Выгрузка отчета" на стр. 474).

В запросе к REST API вам нужно передать идентификатор отчета, полученный на предыдущем этапе (см. раздел "Формирование отчета о защите клиентов" на стр. 460), и формат отображения данных: CSV.

Другие форматы отображения данных не поддерживаются.

Вы можете выгружать данные отчета полностью или получить частичные данные.

Вы можете интегрировать данные, полученные в результате выполнения запроса, в вашу систему отчетов.

Удаление виртуальных машин из защищаемой инфраструктуры

Для удаления виртуальной машины из защищаемой инфраструктуры клиента типа "полный" вам нужно

выполнить следующие действия:

1. Отменить регистрацию виртуальной машины в базе данных Сервера интеграции. Процедура отмены регистрации автоматизирована средствами REST API Сервера интеграции (см. раздел "Отмена регистрации виртуальной машины" на стр. 471).

   В результате выполнения процедуры информация о виртуальной машине клиента удаляется из базы данных Сервера интеграции.

2. Удалить на виртуальной машине Легкий агент для Windows или Легкий агент для Linux и агент администрирования Kaspersky Security Center.

   Вы можете выполнить эти действия вручную в интерфейсе Kaspersky Security Center или автоматизировать удаление средствами OpenAPI Kaspersky Security Center. См. подробнее в Базе знаний (https://support.kaspersky.ru/15530).

3. Удалить виртуальную машину из списка управляемых устройств клиента. Вы можете переместить виртуальную машину в папку **Нераспределенные устройства** главного Сервера администрирования Kaspersky Security Center или удалить виртуальную машину из Kaspersky Security Center.

   Вы можете выполнить эти действия вручную в интерфейсе Kaspersky Security Center или автоматизировать удаление виртуальных машин из списка управляемых устройств средствами OpenAPI Kaspersky Security Center. См. подробнее в Базе знаний (https://support.kaspersky.ru/15530).

Если виртуальная машина удалена из защищаемой инфраструктуры клиента типа "упрощенный", вам нужно отменить регистрацию виртуальной машины в базе данных Сервера интеграции (см. раздел "Отмена регистрации виртуальной машины" на стр. 471).

Удаление клиентов

Если вы хотите прекратить предоставление услуг клиенту типа "полный", вам нужно удалить клиента. Для этого нужно выполнить следующие действия:

1. Удалить на виртуальных машинах клиента Легкий агент для Windows, Легкий агент для Linux и агент администрирования Kaspersky Security Center.

   Вы можете выполнить эти действия вручную в интерфейсе Kaspersky Security Center или автоматизировать удаление средствами OpenAPI Kaspersky Security Center. См. подробнее в Базе знаний (https://support.kaspersky.ru/15530).

2. Удалить клиента из базы данных Сервера интеграции, а также удалить структуру защиты клиента. Процедура удаления автоматизирована средствами REST API Сервера интеграции (см. раздел "Удаление клиента" на стр. 472). При вызове метода REST API вам нужно указать параметр `removeTenantArtifacts=true`.

   В результате выполнения процедуры автоматически выполняются следующие действия:

   - Удаляется информация о клиенте и виртуальных машинах клиента из базы данных Сервера интеграции.
   - Удаляется структура защиты клиента в Kaspersky Security Center: виртуальный Сервер администрирования и учетная запись для подключения к нему, папка **Multitenancy KSV LA** → **<Название клиента>** и ее содержимое (вложенные папки и группы администрирования, политики и задачи, инсталляционные пакеты).
   - Если других клиентов нет, также удаляется папка **Multitenancy KSV LA**.

Если прекращено предоставление услуг защиты клиенту типа "упрощенный", вам нужно удалить клиента из базы данных Сервера интеграции (см. раздел "Удаление клиента" на стр. 472).

Использование REST API Сервера интеграции

Взаимодействие с REST API Сервера интеграции основано на запросах и ответах и осуществляется по протоколу HTTPS под учетной записью multitenancy.

Параметры учетной записи передаются при вызове каждого метода в заголовке запроса Authorization в виде строки `{имя пользователя}:{пароль}`, закодированной методом Base64. Используется аутентификация типа Basic.

Адрес запроса к REST API Сервера интеграции состоит из следующих частей:

```
https://{адрес Сервера интеграции}:{порт Сервера
интеграции}/{метод}?{параметры}
```

где:

- `{адрес Сервера интеграции}` – IP-адрес или полное доменное имя (FQDN) Сервера интеграции.
- `{порт Сервера интеграции}` – порт для подключения к Серверу интеграции (по умолчанию 7271).
- `{метод}` – метод, который нужно вызвать.
- `{параметры}` – параметры метода, если есть.

Для обработки запросов, которые требуют много времени и выполняются асинхронно, используются задачи (см. раздел "Методы для работы с задачами" на стр. 475) (*tasks*). Задача создается как промежуточный результат выполнения запроса.

В этом разделе

Методы для работы с клиентами

Средствами REST API Сервера интеграции вы можете выполнять следующие действия при работе с клиентами и виртуальными машинами клиентов:

- получать информацию о клиенте;
- получать список клиентов;
- получать список виртуальных машин клиентов;
- создавать нового клиента и структуру защиты для него или регистрировать существующего клиента;

- удалять клиента;
- активировать и деактивировать клиента;
- регистрировать виртуальные машины клиента и отменять их регистрацию.

Набор действий, выполняемых в результате некоторых запросов к REST API, зависит от признака *тип клиента*, который вы указываете при добавлении информации о клиенте в базу данных Сервера интеграции. Развертывание и удаление структуры защиты клиентов средствами REST API Сервера интеграции доступно для клиентов типа "полный". Для клиентов типа "упрощенный" автоматизируется только функция получения отчетов.

В этом разделе

Получение информации о клиенте

Позволяет получить информацию о клиенте из базы данных Сервера интеграции.

Метод:

```
GET /api/2.0/virtualization/tenants/{идентификатор клиента}
```

где:

`{идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции (обязательный параметр).

В случае успешного выполнения запроса REST API возвращает сведения о клиенте в следующем виде:

```
<tenant id="{идентификатор}" created="{дата и время}" updated="{дата и
время}">
   <name>{название}</name>
   <description>{описание}</description>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
   <!-- Информация в секции vKsc доступна только для клиента типа "полный" -->
      <vKsc id="{идентификатор}">
         <user>
            <name>{администратор}</name>
         </user>
      </vKsc>
```

```
    <status>{статус}</status>
    <type>{тип клиента}</type>
  </tenant>
```

где:

- `tenant id="{идентификатор}"` – идентификатор клиента в базе данных Сервера интеграции.
- `created="{дата и время}"` – дата и время регистрации клиента в базе данных Сервера интеграции в формате YYYY-MM-DDThh:mm:ss.
- `updated="{дата и время}"` – дата и время обновления сведений о клиенте в базе данных в формате YYYY-MM-DDThh:mm:ss.
- `{название}` – название клиента, указанное при создании клиента.
- `{описание}` – описание клиента.
- `{дополнительные сведения}` – дополнительная информация о клиенте, внесенная в базу данных Сервера интеграции.
- `vKsc id="{идентификатор}"` – идентификатор, назначенный виртуальному Серверу администрирования клиента в Kaspersky Security Center.
- `{администратор}` – имя администратора виртуального Сервера администрирования клиента.
- `{статус}` – текущий статус клиента: "активный" (`Active`) или "неактивный" (`Inactive`).
- `{тип клиента}` – тип клиента: "полный" (`Complete`) или "упрощенный" (`Simple`).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращаются сведения о клиенте.
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.

Получение списка клиентов

Позволяет получить список всех клиентов, сведения о которых содержатся в базе данных Сервера интеграции, и сведения о каждом клиенте.

Метод:

```
GET /api/2.0/virtualization/tenants
```

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращаются в виде списка сведения (см. раздел "Получение информации о клиенте" на стр. 464) обо всех клиентах.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Получение списка виртуальных машин клиента

Позволяет получить список всех зарегистрированных виртуальных машин клиента.

Метод:

```
GET /api/2.0/virtualization/tenants/{идентификатор клиента}/vms
```

где:

`{идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции (обязательный параметр).

В случае успешного выполнения запроса REST API возвращает список виртуальных машин и сведения о каждой виртуальной машине клиента в следующем виде:

```
<vm id="{идентификатор в базе}" biosId={идентификатор BIOS ID} created="{дата
и время}" updated="{дата и время}">
   <name>{имя}</name>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
</vm>
```

где:

- `{идентификатор в базе}` – идентификатор, назначенный виртуальной машине в базе данных Сервера интеграции.
- `{идентификатор BIOS ID}` – идентификатор виртуальной машины (BIOS ID) в формате UUID.
- `created="{дата и время}"` – дата и время регистрации виртуальной машины в базе данных Сервера интеграции в формате YYYY-MM-DDThh:mm:ss.
- `updated="{дата и время}"` – дата и время обновления сведений о виртуально машине в базе данных в формате YYYY-MM-DDThh:mm:ss.
- `{имя}` – имя виртуальной машины.
- `{дополнительные сведения}` – дополнительная информация о виртуальной машине, внесенная в базу данных Сервера интеграции.

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращается список виртуальных машин клиента.
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.

Создание клиента

В зависимости от типа клиента, который вы указываете при вызове метода REST API, позволяет выполнить следующие действия:

- Для клиента типа "полный":
  - Добавить сведения о клиенте в базу данных Сервера интеграции.
  - Создать структуру защиты клиента в Kaspersky Security Center (виртуальный Сервер администрирования, учетную запись для подключения к нему, структуру папок и групп

администрирования).

- Создать в папке **Multitenancy KSV LA** → **<Название клиента>** политики включения и выключения защиты виртуальных машин с установленным Легким агентом версии Kaspersky Security для виртуальных сред 5.1 Легкий агент.

  Политики включения и выключения защиты применяются, только если в виртуальной инфраструктуре клиента установлены Легкие агенты Kaspersky Security . Подробнее см. в справке Kaspersky Security для виртуальных сред 5.1 Легкий агент (https://support.kaspersky.com/KSVLA/5.1/ru-RU/199684.htm).

- Добавить сведения о виртуальном Сервере администрирования клиента в базу данных Сервера интеграции.

- Для клиента типа "упрощенный": добавить сведения о клиенте в базу данных Сервера интеграции.

Метод:

```
POST /api/2.0/virtualization/tenants
```

В теле запроса вам нужно указать следующие параметры:

```
<tenant>
   <name>{название}</name>
   <description>{описание}</description>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
   <preferredViisAddress>{IP-адрес}</preferredViisAddress>
   <type>{тип клиента}</type>
   <!-- Данные в секции vKsc указываются только для клиента типа "полный" -->
      <vKsc>
         <user>
            <name>{имя администратора}</name>
            <password>{пароль администратора}</password>
         </user>
      </vKsc>
</tenant>
```

где:

- `{название}` – название клиента (обязательный параметр).
- `{описание}` – описание клиента (необязательный параметр).
- `{дополнительные сведения}` – дополнительная информация о клиенте (необязательный параметр).
- `{IP-адрес}` – IP-адрес Сервера интеграции, к которому должны подключаться Легкие агенты, установленные на виртуальных машинах клиента (необязательный параметр). Указанный адрес используется по умолчанию при создании политики для Легкого агента. Если параметр не указан, в политике используется IP-адрес Сервера интеграции из запроса к REST API.
- `{тип клиента}` – тип клиента: "полный" (`Complete`) или "упрощенный" (`Simple`) (обязательный параметр).
- `{имя администратора}` – имя учетной записи администратора для подключения к виртуальному Серверу администрирования клиента (обязательный параметр при создании клиента типа

"полный"). Учетная запись будет создана автоматически во время выполнения процедуры.

- `{пароль администратора}` – пароль учетной записи администратора, закодированный методом Base64 (обязательный параметр при создании клиента типа "полный").

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **CreateTenant**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 475) вы можете следить за ходом выполнения процедуры создания клиента. После завершения задачи в поле **result** содержится информация о клиенте, в том числе идентификатор созданного клиента, или сведения об ошибке. В случае ошибки на любом из шагов выполнения процедуры выполняется откат всех внесенных изменений.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **CreateTenant**.
- `400 (Bad request) VIRMT_MandatoryParameterIsNotSpecified` – в теле запроса не указан один из обязательных параметров, например название клиента.
- `400 (Bad request) VIRMT_InvalidTenantType` – в теле запроса указан неверный тип клиента, указанный тип не существует.
- `400 (Bad request) VIRMT_VKscCredentialsNotSpecified` – не указаны имя или пароль учетной записи администратора виртуального Сервера администрирования Kaspersky Security Center (при создании клиента типа "полный").
- `400 (Bad request) VIRMT_InvalidViisAddressFormat` – неверный формат IP-адреса Сервера интеграции.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Возможные коды ошибок в задаче:

- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.
- `VIRMT_TenantGroupAlreadyExists` – папка с названием, соответствующим указанному названию клиента, уже существует в Kaspersky Security Center.
- `VIRMT_TenantWithSpecifiedNameAlreadyExists` – клиент с указанным названием уже существует в базе данных Сервера интеграции.
- `VIRMT_PasswordNotComplyPolicy` – не удалось создать учетную запись администратора виртуального Сервера администрирования Kaspersky Security Center: указанный пароль не удовлетворяет требованиям к паролям в Kaspersky Security Center.
- `VIRMT_UserWithSpecifiedNameAlreadyExists` – не удалось создать учетную запись администратора виртуального Сервера администрирования Kaspersky Security Center: пользователь с таким именем уже существует в Kaspersky Security Center.

Активация клиента

В зависимости от типа клиента позволяет выполнить следующие действия:

- Для клиента типа "полный":
  - Изменить статус клиента на "активный".
  - Изменить состояние политик включения защиты виртуальных машин с установленным Легким агентом версии Kaspersky Security для виртуальных сред 5.1 Легкий агент.

> Политики включения защиты применяются, только если в виртуальной инфраструктуре клиента установлены Легкие агенты Kaspersky Security . Если политики включения защиты клиента отсутствуют, они будут автоматически созданы. Подробнее см. в справке Kaspersky Security для виртуальных сред 5.1 Легкий агент (https://support.kaspersky.com/KSVLA/5.1/ru-RU/199684.htm).

- Для клиента типа "упрощенный": только изменить статус клиента на "активный".

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор клиента}/activate
```

где:

`{идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции (обязательный параметр).

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **ChangeTenantActivation**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 475) вы можете следить за ходом выполнения процедуры изменения статуса клиента. После завершения задачи в поле **result** содержится подтверждение изменения статуса клиента (`true`) или сведения об ошибке.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **ChangeTenantActivation**.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Коды ошибок в задаче:

- `VIRMT_TenantWithSpecifiedIdNotFound` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.
- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.

Деактивация клиента

В зависимости от типа клиента позволяет выполнить следующие действия:

- Для клиента типа "полный":
  - Изменить статус клиента на "неактивный".
  - Изменить состояние политик выключения защиты виртуальных машин с установленным Легким агентом версии Kaspersky Security для виртуальных сред 5.1 Легкий агент.

    > Политики выключения защиты применяются, только если в виртуальной инфраструктуре клиента установлены Легкие агенты Kaspersky Security . Если политики выключения защиты клиента отсутствуют, они будут автоматически созданы. Подробнее см. в справке Kaspersky Security для виртуальных сред 5.1 Легкий агент (https://support.kaspersky.com/KSVLA/5.1/ru-RU/199684.htm).

- Для клиента типа "упрощенный": только изменить статус клиента на "неактивный".

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор клиента}/deactivate
```

где:

`{идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции (обязательный параметр).

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **ChangeTenantActivation**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 475) вы можете следить за ходом выполнения процедуры изменения статуса клиента. После завершения задачи в поле **result** содержится подтверждение изменения статуса клиента (`true`) или сведения об ошибке.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **ChangeTenantActivation**.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Коды ошибок в задаче:

- `VIRMT_TenantWithSpecifiedIdNotFound` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.
- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.

Регистрация виртуальных машин клиента

Позволяет добавить информацию о виртуальных машинах клиентов в базу данных Сервера интеграции.

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор клиента}/vms/register
```

где:

`{идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции (обязательный параметр).

В теле запроса нужно указать следующие параметры:

```
<vm biosId="{идентификатор BIOS ID}">
   <name>{имя}</name>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
</vm>
```

где:

- `{идентификатор BIOS ID}` – уникальный идентификатор (BIOS ID) виртуальной машины (обязательный параметр).
- `{имя}` – имя виртуальной машины (необязательный параметр).
- `{дополнительные сведения}` – дополнительная информация о виртуальной машине (необязательный параметр).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно (информация о виртуальной машине добавлена в базу данных Сервера интеграции).
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.
- `409 (Conflict) VIRMT_VmWithSpecifiedBiosIdAlreadyExists` – виртуальная машина с указанным идентификатором уже зарегистрирована в базе данных Сервера интеграции.

Отмена регистрации виртуальной машины

Позволяет удалить информацию о виртуальной машине клиента из базы данных Сервера интеграции.

> Отмена регистрации не приводит к выключению защиты на виртуальной машине клиента. Вы можете выключить защиту на виртуальной машине клиента типа "полный", выполнив все этапы процедуры удаления виртуальных машин из защищаемой инфраструктуры (см. раздел "Удаление виртуальных машин из защищаемой инфраструктуры" на стр. 461).

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор
клиента}/vms/unregister?biosId={идентификатор}
```

или

```
POST /api/2.0/virtualization/tenants/{идентификатор
клиента}/vms/unregister?vmId={идентификатор}
```

где:

- `{идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции (обязательный параметр).
- `biosId={идентификатор}` – идентификатор виртуальной машины (BIOS ID) в формате UUID (обязательный параметр).
- `vmId={идентификатор}` – идентификатор виртуальной машины в базе данных Сервера интеграции в формате UUID (обязательный параметр).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно (информация о виртуальной машине удалена из базы данных Сервера интеграции).
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.
- `404 (Not Found) VIRMT_VmWithSpecifiedIdNotFound` – виртуальная машина с указанным идентификатором не найдена в базе данных Сервера интеграции.

Удаление клиента

В зависимости от типа клиента и заданных параметров, позволяет выполнить следующие действия:

- Для клиента типа "полный":
  - Удалить информацию о клиенте и виртуальных машинах клиента из базы данных Сервера интеграции.
  - Удалить структуру защиты клиента в Kaspersky Security Center (виртуальный Сервер администрирования, учетную запись для подключения к нему, структуру папок и групп администрирования, политики, задачи и инсталляционные пакеты). Если других клиентов нет, также удаляется папка **Multitenancy KSV LA**.
  - Удалить сведения о виртуальном Сервере администрирования клиента из базы данных Сервера интеграции.

  Вызов метода удаления клиента не приводит к выключению защиты на виртуальных машинах клиента. Чтобы выключить защиту, вам нужно выполнить все этапы процедуры удаления клиента (см. раздел "Удаление клиентов" на стр. 462), в том числе удалить на виртуальных машинах Легкий агент для Windows, Легкий агент для Linux и Агент администрирования Kaspersky Security Center. Если вы хотите приостановить защиту виртуальных машин клиента типа "полный", вы можете использовать метод деактивации клиента (см. раздел "Деактивация клиента" на стр. 469).

- Для клиента типа "упрощенный": удалить клиента из базы данных Сервера интеграции.

Метод:

```
DELETE /api/2.0/virtualization/tenants/{идентификатор
клиента}?removeTenantArtifacts={true|false}
```

где:

- `{идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции (обязательный параметр).
- `removeTenantArtifacts={true|false}` – необязательный параметр, определяющий необходимость удаления структуры защиты клиента при удалении клиента из базы данных Сервера интеграции. Возможные значения:
  - `true` – при удалении клиента будут также выполнены следующие действия:
    - удален виртуальный Сервера администрирования клиента;
    - удалена учетная запись администратора виртуального Сервера администрирования клиента;
    - удалена папка **Multitenancy KSV LA** → **<Название клиента>** и ее содержимое;
    - если других клиентов нет, удалена папка **Multitenancy KSV LA**.
  - `false` – выполняется только удаление клиента из базы данных Сервера интеграции, структура защиты клиента не удаляется.

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **DeleteTenant**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 475) вы можете следить за ходом выполнения процедуры удаления клиента. После завершения задачи в поле **result** содержится

информация об удаленном клиенте или сведения об ошибке.

В случае ошибки на любом из шагов выполнения процедуры выполняется откат всех внесенных изменений.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа DeleteTenant.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Коды ошибок в задаче:

- `VIRMT_TenantWithSpecifiedIdNotFound` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.
- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.

Методы для работы с отчетами

Средствами REST API Сервера интеграции вы можете выполнять следующие действия при работе с отчетами о защите клиентов:

- формировать отчет;
- выгружать отчет.

В этом разделе

Формирование отчета

Позволяет сформировать отчет на основе данных, переданных в базу данных Сервера интеграции, с учетом заданных параметров отчета. Вы можете указать клиента, о защите которого нужно сформировать отчет, и период, данные за который вы хотите получить.

В заголовке запроса `Accept` нужно передать формат вывода данных в виде `Accept:application/csv`.

Метод:

```
POST /api/2.0/virtualization/reports/tenants?tenantId={идентификатор клиента}&from={дата и время}&to={дата и время}
```

где:

- `tenantId={идентификатор клиента}` – идентификатор клиента в базе данных Сервера интеграции. Если клиент указан, в отчет попадают только сведения о периодах защиты виртуальных машин этого клиента. Если клиент не указан, отчет будет включать в себя данные обо всех виртуальных машинах, которые находились под защитой в указанный период.
- `from={дата и время}` – дата и время начала отчетного периода в формате YYYY-MM-DDThh:mm:ss. Если не задано, то используется дата самой ранней записи в базе данных

Сервера интеграции.

- `to={дата и время}` – дата и время окончания отчетного периода в формате YYYY-MM-DDThh:mm:ss. Если не задано, то используется текущая дата.

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **CreateTenantReport**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 475) вы можете следить за ходом выполнения процедуры формирования отчета. После завершения задачи в поле **result** содержится идентификатор отчета или сведения об ошибке.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **CreateTenantReport**.
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found)` – клиент с указанным идентификатором не найден в базе данных Сервера интеграции.

Выгрузка отчета

Позволяет выгрузить отчет, сформированный ранее.

В заголовке запроса `Accept` нужно передать формат вывода данных в виде `Accept: application/csv`.

Поддерживается выгрузка отчета по частям. Вы можете указать диапазон данных в заголовке запроса `Range`, например:

```
Range: bytes=0-1023
```

В ответ на запрос с таким заголовком REST API возвращает результат `206 (Partial content)` и первый килобайт данных. В ответе присутствуют заголовки `Content-Range` и `Content-Length`.

Например:

```
Content-Range: bytes=0-1023/123456
Content-Length: 1024
```

Метод:

```
GET /api/2.0/virtualization/reports/tenants/{идентификатор отчета}
```

где:

`{идентификатор отчета}` – идентификатор отчета, полученный в результате успешного завершения задачи **CreateTenantReport** (обязательный параметр).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращаются данные отчета в формате, указанном в заголовке `Accept`.
- `206 (Partial content)` – запрос выполнен успешно. В ответе возвращается часть отчета, заданная заголовком `Range`.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

- `404 (Not Found)` – отчет с указанным идентификатором не найден.
- `415 (Unsupported Media Type)` – неподдерживаемый формат запрашиваемых данных (в заголовке запроса `Accept` передан неверный формат).

Методы для работы с задачами

Задачи используются для обработки запросов, которые требуют много времени и выполняются асинхронно. С помощью состояний задачи вы можете следить за ходом выполнения действий, заданных в запросе.

Задача может находиться в одном из следующих состояний:

- **Created** – задача создана, но не запущена.
- **Starting** – задача находится в процессе запуска.
- **Running** – задача выполняется. Для задачи в этом состоянии указывается прогресс (**progress**) выполнения в процентах.
- **Completed** – задача успешно завершена. Для задачи в этом состоянии указывается результат выполнения (**result**). Результат содержит зависимые от задачи данные, например идентификатор нового клиента после выполнения задачи **CreateTenant**.
- **Stopping** – задача подготавливается к завершению. Если вы прекратили выполнение задачи, она может находиться в этом состоянии, прежде чем перейти в состояние **Cancelled**.
- **Failed** – задача завершилась с ошибкой. Для задачи в этом состоянии указывается расширенная информация об ошибке (**error**).
- **Cancelled** – выполнение задачи прекращено пользователем или системой. Для задачи в этом состоянии указывается расширенная информация об ошибке (**error**).
- **Queued** – задача поставлена в очередь и ожидает начала выполнения.

Средствами REST API Сервера интеграции вы можете выполнять следующие действия с задачами:

- получать список задач;
- получать сведения об указанной задаче;
- отменять выполнение указанной задачи.

В этом разделе

Получение информации о задаче

Позволяет получить информацию о задаче по ее идентификатору.

Метод:

```
GET /api/2.0/virtualization/tasks/{идентификатор}
```

где:

`{идентификатор}` – идентификатор задачи (обязательный параметр).

В случае успешного выполнения запроса REST API возвращает сведения о задаче в следующем виде:

```
<task id="{идентификатор}" created="{дата и время}" stateChanged="{дата и время}" changed="{дата и время}">
   <state>{состояние}</state>
   <type>{тип}</type>
   <stage>{этап}</stage>
   <progress>{процент выполнения}</progress>
   <result>{результат}</result>
   <!-- Если задача завершилась с ошибкой вместо результата отображается сообщение об ошибке. -->
   <error>{сообщение об ошибке}</error>
</task>
```

где:

- `{идентификатор}` – идентификатор задачи.
- `created="{дата и время}"` – время создания задачи в формате YYYY-MM-DDThh:mm:ss.
- `stateChanged="{дата и время}"` – время изменения состояния задачи в формате YYYY-MM-DDThh:mm:ss.
- `changed="{дата и время}"` – время изменения задачи в формате YYYY-MM-DDThh:mm:ss.
- `{состояние}` – состояние (см. раздел "Методы для работы с задачами" на стр. 475) задачи.
- `{тип}` – тип задачи. Например:
  - `CreateTenant` – задача, которая используется в процедуре создания клиента (см. раздел "Создание клиента" на стр. 466).
  - `ChangeTenantActivation` – задача, которая используется в процедурах активации (см. раздел "Активация клиента" на стр. 468) и деактивации (см. раздел "Деактивация клиента" на стр. 469) клиента.
  - `DeleteTenant` – задача, которая используется в процедуре удаления клиента (см. раздел "Удаление клиента" на стр. 472).
  - `CreateTenantReport` – задача, которая используется в процедуре формирования отчета (см. раздел "Формирование отчета" на стр. 473) о защите клиентов.
- `{название}` – название задачи.
- `{этап}` – этап выполнения задачи.
- `{процент выполнения}` – ход выполнения задачи в процентах.
- `{результат}` – результат выполнения задачи, например, информация о созданном клиенте или идентификатор отчета.
- `{сообщение об ошибке}` – если в ходе выполнения задачи произошла ошибка, отображается сообщение об ошибке.

Коды возврата:

- `200 (OK)` – запрос выполнен успешно.
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found)` – задача с указанным идентификатором не найдена в базе данных Сервера интеграции.

Получение списка задач

Позволяет получить список всех существующих задач и информацию о каждой задаче (см. раздел "Получение информации о задаче" на стр. 475) из списка.

Метод:

```
GET /api/2.0/virtualization/tasks?createdFrom={дата и
время}&state={статус}&type={тип}
```

где:

- `createdFrom={дата и время}` – дата и время в формате YYYY-MM-DDThh:mm:ss (необязательный параметр). Если параметр задан, в списке отображаются задачи, которые созданы не раньше указанных даты и времени.
- `state={состояние}` – состояние задачи (необязательный параметр). Если параметр задан, в списке отображаются только задачи в указанном состоянии (см. раздел "Методы для работы с задачами" на стр. 475).
- `type={тип}` – тип (см. раздел "Получение информации о задаче" на стр. 475) задачи (необязательный параметр). Если параметр задан, в списке отображаются только задачи указанного типа.

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращается список задач.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Отмена выполнения задачи

Позволяет прекращать выполнение запущенных задач. Некоторые задачи не могут быть завершены немедленно. В этом случае возвращается код `202 (Accepted)` и состояние задачи изменяется на **Stopping**.

Метод:

```
POST /api/2.0/virtualization/tasks/{идентификатор}/cancel
```

где:

`{идентификатор}` – идентификатор задачи (обязательный параметр).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно (выполнение задачи отменено).
- `202 (Accepted)` – запрос принят к исполнению (состояние задачи изменяется на **Stopping**).

- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found)` – задача с указанным идентификатором не найдена.
- `405 (Method Not Allowed)` – для дочерних задач: отменить дочернюю задачу можно, только отменив родительскую задачу.
- `409 (Conflict)` – задача уже находится в одном из состояний: **Cancelled**, **Failed**, **Stopped**.

Управление Легким агентом для Linux из командной строки

Предусмотрены следующие команды для управления из командной строки компонентом Легкий агент для Linux, установленным на виртуальной машине:

- delete (см. раздел "Удаление файлов из резервного хранилища" на стр. 492) – удаляет файл из резервного хранилища;
- export (см. раздел "Экспорт и импорт параметров Легкого агента для Linux из командной строки" на стр. 415) – экспортирует в конфигурационный файл параметры Легкого агента для Linux;
- import (см. раздел "Экспорт и импорт параметров Легкого агента для Linux из командной строки" на стр. 415) – импортирует из конфигурационного файла параметры Легкого агента для Linux;
- license (см. раздел "Просмотр информации о лицензии" на стр. 480) – выводит информацию о лицензии на SVM;
- list (см. раздел "Просмотр списка файлов в резервном хранилище" на стр. 492) – выводит список файлов резервного хранилища;
- productinfo (см. раздел "Просмотр информации о программе" на стр. 481) – выводит информацию о программе;
- restore (см. раздел "Восстановление файлов из резервного хранилища" на стр. 492) – восстанавливает файл из резервного хранилища;
- scan (см. раздел "Проверка виртуальной машины" на стр. 486) – запускает антивирусную проверку виртуальной машины;
- statistics (см. раздел "Просмотр статистики выполнения задачи" на стр. 484) – выводит статистику о работе задачи;
- status (см. раздел "Просмотр состояния задачи" на стр. 483) – выводит информацию о текущем состоянии задачи;
- start (см. раздел "Запуск и остановка задачи" на стр. 482) – запускает задачу;
- stop (см. раздел "Запуск и остановка задачи" на стр. 482) – останавливает выполнение задачи;
- svminfo (см. раздел "Просмотр информации об SVM" на стр. 482) – выводит информацию об SVM, к которой подключена защищенная виртуальная машина;
- traces (см. раздел "Файлы трассировки Легкого агента для Linux" на стр. 517) – включает или выключает создание файлов трассировки на защищенной виртуальной машине;
- update (см. раздел "Обновление баз" на стр. 490) – запускает задачу обновления баз с дополнительными параметрами;
- viisinfo (см. раздел "Просмотр информации о Сервере интеграции" на стр. 482) – выводит информацию о Сервере интеграции, к которому подключена защищенная виртуальная машина.

Команда help выводит справку обо всех командах.

Синтаксис команды:

```
lightagent help [<command>]
```

где `<command>` – название команды, справку о которой вы хотите получить.

Перед выполнением команд убедитесь, что служба lightagent запущена на защищенной виртуальной машине.

В этом разделе

Просмотр информации о лицензии

Команда license выводит информацию о лицензии, по которой активирована программа.

► *Чтобы просмотреть информацию о лицензии, по которой активирована программа, выполните следующую команду:*

```
lightagent license
```

Команда выводит следующую информацию:

- `License source` – IP-адрес SVM или полное доменной имя (FQDN) SVM, к которой подключен Легкий агент для Linux.
- `Key` – ключ, добавленный на SVM.
- `License type` – тип лицензии и `<количество единиц лицензирования>` (`<server(s)>` или `<core(s)>`). Возможные значения:
  - `Commercial` – коммерческая.
  - `Trial` – пробная.
  - `Beta` – на бета-тестирование.
  - `Subscription` – подписка.
- `Expiration date` – дата окончания срока действия лицензии (в формате YYYY-MM-DDThh:mm:ss).

- `Days till expiration` – количество дней до окончания срока действия лицензии.

Параметры:

- `<количество единиц лицензирования> <server(s)>` – максимальное количество одновременно запущенных виртуальных машин с операционными системами для серверов, для которых включена защита;
- `<количество единиц лицензирования> <core(s)>` – максимальное количество одновременно используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

Просмотр информации о программе

Команда productinfo выводит информацию о программе.

► *Чтобы просмотреть информацию о программе, выполните следующую команду:*

```
lightagent productinfo
```

Команда выводит следующую информацию:

- `Product version` – версия установленной программы Kaspersky Security.
- `Product installation date` – дата и время установки программы (в формате YYYY-MM-DDThh:mm:ss).
- `Update information` – информация об обновлении баз:
  - `Bases timestamp` – дата и время выпуска обновления антивирусных баз.
  - `Last successful update date` – дата и время последнего успешного обновления антивирусных баз программы (в формате YYYY-MM-DDThh:mm:ss).
- `Installed patches` – информация об установленных обновлениях модулей программы:
  - `id` – идентификатор обновления модулей программы;
  - `description` – описание обновления модулей программы.
- `KSN information` – информация об использовании KSN:
  - `Use KSN to check files and web addresses` – использовать KSN для проверки файлов и веб-адресов. Возможные значения: `Yes`, `No`.
  - `Use extended KSN` – использовать расширенный KSN. Возможные значения: `Yes`, `No`.
  - `KSN type` – тип KSN. Возможные значения:
    - `Global KSN` – Глобальный KSN.
    - `Private KSN` – Локальный KSN.

Просмотр информации об SVM

Способ, который используют Легкие агенты для обнаружения SVM, настраивается администратором в политике для Легкого агента для Linux.

Вы можете получить информацию об SVM, к которой подключен Легкий агент, с помощью команды svminfo.

► *Чтобы просмотреть информацию об SVM, к которой подключен Легкий агент, выполните следующую команду:*

```
lightagent svminfo
```

Команда выводит следующую информацию:

- `Current SVM` – IP-адрес SVM, к которой подключен Легкий агент, или полное доменное имя (FQDN) SVM. Если SVM, к которой подключен Легкий агент, локальная, то в скобках рядом с IP-адресом или полным доменным именем SVM указано `local`. Если SVM, к которой подключен Легкий агент, не является локальной, то в скобках указано `not local`.
- `Discovery method` – способ получения информации об SVM. Возможные значения:
  - `VIIS` – с помощью Сервера интеграции.
  - `List` – с использованием списка адресов SVM.
- `List of known SVMs` – список SVM, к которым могут подключаться Легкие агенты. Эта информация отображается, только если в качестве `Discovery method` указан способ `List`.

Просмотр информации о Сервере интеграции

Команда viisinfo выводит информацию о Сервере интеграции, к которому подключен Легкий агент.

► *Чтобы просмотреть информацию о Сервере интеграции, к которому подключен Легкий агент, выполните следующую команду:*

```
lightagent viisinfo
```

Команда выводит следующую информацию:

- `Viis address` – IP-адрес или полное доменное имя (FQDN) Сервера интеграции, к которому подключен Легкий агент, и порт Сервера интеграции.
- `Status` – статус подключения Легкого агента к Серверу интеграции. Возможные значения:
  - `Connected` – Легкий агент подключен к Серверу интеграции.
  - `No connection` – подключение к Серверу интеграции отсутствует.

Запуск и остановка задачи

Запуск и остановка задач пользователем предусмотрены для задач следующих типов:

- задача постоянной защиты;
- задача обновления баз.

► *Чтобы запустить задачу, выполните следующую команду:*

```
lightagent start <тип задачи>
```

где `<тип задачи>` – тип задачи, которую вы хотите запустить.

Если вы не укажете тип задачи, программа выведет список всех задач, для которых возможен запуск этой команды. Возможные значения:

- `File_Monitoring` – задача постоянной защиты.
- `Updater` – задача обновления баз.

Также вы можете использовать для запуска задачи обновления команду запуска задачи обновления баз с дополнительными параметрами (см. раздел "Обновление баз" на стр. 490).

► *Чтобы остановить задачу, выполните следующую команду:*

```
lightagent stop <тип задачи>
```

где `<тип задачи>` – тип задачи, которую вы хотите запустить.

Если вы не укажете тип задачи, программа выведет список всех задач, для которых возможен запуск этой команды. Возможные значения:

- `File_Monitoring` – задача постоянной защиты.
- `Updater` – задача обновления баз.

Просмотр состояния задачи

Одним из аспектов управления задачами является просмотр текущего состояния задач.

Просмотр текущего состояния доступен для задач следующих типов:

- задача постоянной защиты;
- задача выборочной проверки;
- задача обновления баз.

► *Чтобы просмотреть состояние задачи, выполните следующую команду:*

```
lightagent status <тип задачи>
```

где `<тип задачи>` – тип задачи, состояние которой вы хотите просмотреть.

Если вы не укажете тип задачи, программа выведет список всех задач, для которых возможен запуск этой команды. Возможные значения:

- `File_Monitoring` – задача постоянной защиты.
- `Scan_Objects` – задача выборочной проверки.
- `Updater` – задача обновления баз.

Команда выводит одно из следующих состояний задачи:

- `Starting` – запускается.
- `Running` – выполняется.
- `Pausing` – приостанавливается.
- `Paused` – приостановлена.
- `Resuming` – возобновляется.
- `Stopping` – останавливается.
- `Stopped` – остановлена.
- `Database update is expected` – ожидается обновление баз. Это состояние отображается после установки программы. Базы будут обновлены после подключения Легкого агента для Linux к SVM. Для подключения Легкого агента к SVM требуется указать способ обнаружения SVM.
- `Stop reason` – причина завершения выполнения задачи. Возможные значения:
  - `Unknown` – неизвестно.
  - `NeverRun` – задача ни разу не была запущена.
  - `Completed` – задача успешно выполнена.
  - `Canceled` – задача остановлена пользователем.
  - `Failed` – задача остановилась из-за внутренней ошибки.

Просмотр статистики выполнения задачи

Просмотр статистики выполнения доступен для задач следующих типов:

- задача выборочной проверки;
- задача обновления баз.

► *Чтобы просмотреть статистику выполнения задачи, выполните следующую команду:*

```
lightagent statistics <тип задачи>
```

где `<тип задачи>` – тип задачи, статистику о выполнении которой вы хотите получить.

Если вы не укажете тип задачи, программа выведет список всех задач, для которых возможен запуск этой команды. Возможные значения:

- `Scan_Objects` – задача выборочной проверки.
- `Updater` – задача обновления баз.

Команда выводит следующую информацию о задаче выборочной проверки:

- `Current time` – текущее время.
- `Time Start` – время запуска задачи.
- `Time Finish` – время завершения выполнения задачи.
- `Completion` – процент выполнения задачи.
- `Stop reason` – причина завершения выполнения задачи. Возможные значения:
  - `Unknown` – неизвестно.
  - `NeverRun` – задача ни разу не была запущена.
  - `Completed` – задача успешно выполнена.
  - `Canceled` – задача остановлена пользователем.
  - `Failed` – задача остановилась из-за внутренней ошибки.
- `Processed objects` – количество обработанных файлов.
- `Total detected` – количество зараженных файлов.
- `Threats detected` – количество типов обнаруженных вредоносных программ.
- `Untreated` – количество необработанных файлов.
- `Disinfected` – количество вылеченных файлов.
- `Deleted` – количество удаленных файлов.
- `Skipped` – количество пропущенных файлов.
- `Archived` – количество архивов.
- `Packed` – количество упакованных файлов.
- `Password protected` – количество файлов, защищенных паролем.
- `Corrupted` – количество поврежденных файлов.
- `Errors` – количество ошибок при проверке.
- `Last object` – последний проверенный файл.

Команда выводит следующую информацию о задаче обновления баз:

- `Current time` – текущее время.
- `Time Start` – время запуска задачи.
- `Time Finish` – время завершения выполнения задачи.
- `Completion` – процент выполнения задачи.
- `Stop reason` – причина завершения выполнения задачи. Возможные значения:
  - `Unknown` – неизвестно.
  - `NeverRun` – задача ни разу не была запущена.

  - `Completed` – задача успешно выполнена.
  - `Canceled` – задача остановлена пользователем.
  - `Failed` – задача остановилась из-за внутренней ошибки.
- `Total downloaded size` – общий объем загруженных обновлений (в байтах).
- `Speed` – скорость загрузки обновлений (байт/сек.).

Проверка виртуальной машины

На защищенных виртуальных машинах с установленным компонентом Легкий агент для Linux предусмотрены следующие задачи, которыми вы можете управлять с помощью командной строки:

- *Полная проверка* – тщательная проверка операционной системы защищенной виртуальной машины, включая системную память, объекты автозапуска, загрузочные секторы, а также все жесткие, съемные и сетевые диски.
- *Выборочная проверка* – проверка на защищенной виртуальной машине объектов, выбранных пользователем.

Вы можете выполнить следующие действия для запуска и настройки параметров задач проверки из командной строки:

- Запустить задачу полной проверки (см. раздел "Полная проверка" на стр. 487) всех объектов файловой системы защищенной виртуальной машины.
- Запустить задачу выборочной проверки (см. раздел "Выборочная проверка" на стр. 487), указав область проверки задачи.
- Настроить проверку составных файлов (см. раздел "Проверка составных файлов" на стр. 488).
- Указать действие (см. раздел "Выбор действий над зараженными файлами" на стр. 488), которое программа выполняет при обнаружении зараженного файла.
- Настроить использование технологии проверки iChecker (см. раздел "Использование технологии iChecker при проверке" на стр. 489).
- Настроить дополнительные параметры задач проверки (см. раздел "Настройка дополнительных параметров задачи проверки" на стр. 490).

Обратите внимание на особенности проверки жестких и символических ссылок (см. раздел "Особенности проверки символических и жестких ссылок" на стр. 383).

kaspersky

В этом разделе

Полная проверка

Вы можете запустить *полную проверку* всех объектов файловой системы защищенной виртуальной машины, включая системную память, объекты автозапуска, загрузочные секторы, а также все жесткие, съемные и сетевые диски.

Из проверки исключаются объекты файловой системы /dev, /sys, /proc и /.snapshots.

► *Чтобы запустить задачу полной проверки, выполните следующую команду:*

```
lightagent scan
```

Вы также можете запустить задачу проверки с дополнительными параметрами (см. раздел "Настройка дополнительных параметров задачи проверки" на стр. 490), которые позволяют сохранять в файл события, возникающие при выполнении задачи, или использовать для выполнения задачи параметры конфигурационного файла.

Выборочная проверка

Вы можете запустить задачу выборочной проверки защищенной виртуальной машины, указав список файлов и объектов для проверки, имена файлов (или путей к ним) или шаблоны имен файлов (или путей к ним).

Из проверки исключаются объекты файловой системы /dev, /sys, /proc и /.snapshots.

► *Чтобы запустить задачу выборочной проверки, выполните следующую команду:*

```
lightagent scan [<путь к файлу или папке>][<путь к файлу или
папке>...][--boot][--memory][--startup][--@:<filelist.lst>]
```

где:

- `<путь к файлу или папке>` – путь к файлу или папке, которые вы хотите проверить на вирусы и

другие вредоносные программы. Вы можете использовать маски для указания пути к файлу или папке. Если вы не укажете пути к файлам или папкам, программа проверит все объекты файловой системы защищенной виртуальной машины.

- `boot` – проверять загрузочные секторы.
- `memory` – проверять системную память.
- `startup` – проверять объекты автозапуска.
- `@:<filelist.lst>` – проверять файлы, указанные в списке. В текстовом файле укажите с новой строки файлы и папки, которые вы хотите проверить на вирусы и другие вредоносные программы.

Вы также можете запустить задачу проверки с дополнительными параметрами (см. раздел "Настройка дополнительных параметров задачи проверки" на стр. 490), которые позволяют сохранять в файл события, возникающие при выполнении задачи, или использовать для выполнения задачи параметры конфигурационного файла.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

Кроме того, вы можете сократить время проверки составных файлов, задав следующие ограничения:

- на длительность проверки составных файлов: программа прекратит проверку составного файла по истечении указанного времени;
- на максимальный размер проверяемого составного файла: программа не будет распаковывать и проверять составные файлы, размеры которых превышают указанное значение.

► *Чтобы настроить проверку составных файлов, выполните следующую команду:*

```
lightagent scan [--e:a] [--e:b] [--e:<seconds>] [--es:<size>]
```

где:

- `--e:a` – не проверять архивы.
- `--e:b` – не проверять почтовые базы и файлы почтовых форматов.
- `--e:<seconds>` – не проверять составные файлы, если их проверка длится дольше указанного времени. Укажите максимальное время проверки файла в секундах.
- `--es:<size>` – не проверять составные файлы, если их размер превышает указанное значение. Укажите максимальный размер проверяемого составного файла в мегабайтах.

Выбор действий над зараженными файлами

Вы можете задать действия, которые программа Kaspersky Security будет выполнять при обнаружении зараженных файлов.

► *Чтобы задать действия над зараженными файлами, выполните следующую команду:*

```
lightagent scan [<путь к файлу или папке>] [--i<0-4>]
```

где:

- `<путь к файлу или папке>` – путь к файлу или папке, которые вы хотите проверить на вирусы и другие вредоносные программы. Если вы не укажете пути к файлам или папкам, программа проверит все объекты файловой системы защищенной виртуальной машины.
- `i0` – при обнаружении зараженных файлов выполнять действие *Информировать*. Если указан этот параметр, то при обнаружении зараженных файлов программа Kaspersky Security информирует вас об этом.
- `i1` – при обнаружении зараженных файлов выполнять действие *Лечить*. Если указан этот параметр, программа Kaspersky Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, программа оставляет файлы неизменными.
- `i2` – при обнаружении зараженных файлов выполнять действие *Лечить. Удалять, если лечение невозможно. Пропускать составные файлы, если лечение и удаление невозможны*. Если указан этот параметр, программа Kaspersky Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, программа удаляет их. Если зараженный файл является частью составного файла и его невозможно удалить, программа оставляет такой файл неизменным.
- `i3` – при обнаружении зараженных файлов выполнять действие *Лечить. Удалять, если лечение невозможно*. Если указан этот параметр, программа Kaspersky Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, программа удаляет их. Если зараженный файл является частью составного файла и его невозможно удалить, программа удаляет весь составной файл целиком. Это действие выполняется по умолчанию.
- `i4` – при обнаружении зараженных файлов выполнять действие *Удалять*. Если указан этот параметр, программа Kaspersky Security автоматически удаляет зараженный файл, предварительно создав его резервную копию. Если зараженный файл, являющийся частью составного файла, невозможно удалить, программа удаляет весь составной файл целиком.

Использование технологии iChecker при проверке

Вы можете включить использование технологии iChecker при проверке защищенной виртуальной машины. Технология iChecker позволяет увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз программы, дату предыдущей проверки файла, а также изменение параметров проверки. По умолчанию использование технологии iChecker при проверке защищенной виртуальной машины включено.

► *Чтобы выключить использование технологии iChecker, выполните следующую команду:*

```
lightagent scan --iChecker:off
```

► *Чтобы включить использование технологии iChecker, выполните следующую команду:*

```
lightagent scan --iChecker:on
```

Настройка дополнительных параметров задачи проверки

Вы можете запустить задачу проверки с дополнительными параметрами, которые позволяют сохранять в файл события, возникающие при выполнении задачи, или использовать для выполнения задачи параметры конфигурационного файла.

► *Чтобы настроить дополнительные параметры проверки, выполните следующую команду:*

```
lightagent scan [--R[A]:<путь к файлу отчета>][--C:<путь к конфигурационному файлу>]
```

где:

- `R:<путь к файлу отчета>` – сохранять в файле отчета только важные события, возникающие во время выполнения задачи проверки. Укажите полный путь к файлу для сохранения событий. Программа создаст этот файл и отобразит в нем события.
- `RA:<путь к файлу отчета>` – сохранять в файле отчета все события, возникающие во время выполнения задачи проверки. Укажите полный путь к файлу для сохранения событий. Программа создаст этот файл и отобразит в нем события.
- `C:<путь к конфигурационному файлу>` – при проверке использовать параметры, указанные в конфигурационном файле. Укажите полный путь к конфигурационному файлу.

Примеры:

► *Запустить задачу проверки, при проверке использовать параметры из конфигурационного файла config:*

```
lightagent scan --C:/temp/config
```

► *Пример конфигурационного файла с параметрами, которые задают проверку файла example и сохранение информации о событиях, возникших во время выполнения задачи, в файле report.log:*

```
./example --RA:/tmp/report.log
```

Обновление баз

Кроме стандартной команды запуска задач с помощью команды start (см. раздел "Запуск и остановка задачи" на стр. 482), вы можете использовать команду запуска задачи обновления с дополнительными параметрами. Эти параметры позволяют сохранять в файл события, возникающие при выполнении задачи обновления, или использовать для выполнения задачи обновления параметры конфигурационного файла.

► *Чтобы запустить задачу обновления баз, выполните следующую команду:*

```
lightagent update [--R[A]:<путь к файлу отчета>] [--C:<путь к конфигурационному файлу>]
```

где:

- `R:<путь к файлу отчета>` – сохранять в файле отчета только важные события, возникающие во время выполнения задачи обновления. Укажите полный путь к файлу для сохранения событий. Программа создаст этот файл и отобразит в нем события.
- `RA:<путь к файлу отчета>` – сохранять в файле отчета все события, возникающие во время выполнения задачи обновления. Укажите полный путь к файлу для сохранения событий. Программа создаст этот файл и отобразит в нем события.
- `C:<путь к конфигурационному файлу>` – при обновлении использовать параметры, указанные в конфигурационном файле. Укажите полный путь к конфигурационному файлу.

Пример:

► *Запустить задачу обновления баз и сохранить информацию о событиях, возникших во время выполнения задачи, в файле update.txt:*

```
lightagent update --RA:/usr/local/update.txt
```

Команда выводит в файл отчета следующую информацию:

- `Update source` – сетевой адрес папки на SVM, в которой хранятся базы программы.
- `Completion` – процент выполнения задачи.
- `Update status` – результат выполнения задачи. Возможные значения:
  - `Succeed` – задача успешно выполнена.
  - `Failed` – задача не выполнена из-за внутренней ошибки.

Работа с резервным хранилищем

Вы можете выполнить следующие действия в резервном хранилище через командную строку Легкого агента для Linux:

- просмотреть список резервных копий файлов (см. раздел "Просмотр списка файлов в резервном хранилище" на стр. 492);
- восстановить файлы из резервных копий (см. раздел "Восстановление файлов из резервного хранилища" на стр. 492) в папки их исходного размещения;
- удалить резервные копии файлов (см. раздел "Удаление файлов из резервного хранилища" на стр. 492) из резервного хранилища.

В этом разделе

Просмотр списка файлов в резервном хранилище

► *Чтобы просмотреть список файлов в резервном хранилище, выполните следующую команду:*

```
lightagent list backup
```

Команда выводит список файлов в резервном хранилище, содержащий следующую информацию о файлах:

- дата и время помещения файла в резервное хранилище (в формате YYYY-MM-DDThh:mm:ss);
- числовой идентификатор файла в резервном хранилище;
- путь к папке исходного размещения файла, в которую он может быть восстановлен (см. раздел "Восстановление файлов из резервного хранилища" на стр. 492).

Восстановление файлов из резервного хранилища

Вы можете восстановить файл из его резервной копии в папку исходного размещения.

Восстановление зараженных файлов из резервного хранилища может привести к заражению виртуальной машины.

► *Чтобы восстановить файл из резервного хранилища, выполните следующую команду:*

```
lightagent restore <идентификатор файла> [--replace]
```

где:

- `<идентификатор файла>` – числовой идентификатор файла в резервном хранилище, который вы можете узнать с помощью команды list (см. раздел "Просмотр списка файлов в резервном хранилище" на стр. 492);
- `replace` – перезаписать файл с указанным идентификатором восстановленным файлом, если он находится в той же папке.

Программа восстановит файл в папку исходного размещения.

Удаление файлов из резервного хранилища

► *Чтобы удалить файл из резервного хранилища, выполните следующую команду:*

```
lightagent delete <идентификатор файла>
```

где:

`<идентификатор файла>` – числовой идентификатор файла в резервном хранилище, который вы можете узнать с помощью команды list (см. раздел "Просмотр списка файлов в резервном хранилище" на стр. 492).

Управление Легким агентом для Windows из командной строки

Предусмотрены следующие команды для управления из командной строки компонентом Легкий агент для Windows, установленным на виртуальной машине:

- EXIT – завершает работу Легкого агента для Windows;
- EXPORT – экспортирует в файл параметры Легкого агента для Windows;
- IMPORT – импортирует из файла параметры Легкого агента для Windows;
- LICENSE – выводит информацию о лицензии на SVM;
- RESTORE – восстанавливает файл из резервного хранилища;
- SCAN – запускает антивирусную проверку виртуальной машины;
- START – запускает задачу;
- STATISTICS – выводит статистику выполнения задачи;
- STATUS – выводит информацию о текущем состоянии задачи;
- STOP – останавливает выполнение задачи;
- SVMINFO – выводит информацию об SVM, к которой подключена защищенная виртуальная машина;
- TRACES – включает или выключает создание файлов трассировки на защищенной виртуальной машине;
- UPDATE – обновляет базы и модули программы.

Команда `HELP` выводит справку о командах.

kaspersky

В этом разделе

Команда EXIT

Синтаксис команды:

```
EXIT /login:<login> /password:<password>
```

Параметры:

- `/login` – имя пользователя;
- `/password` – пароль.

Примеры:

```
avp.com EXIT /login:<login> /password:<password>
```

Команда EXPORT

Синтаксис команды:

```
EXPORT <filename>
```

где `<filename>` – имя файла, в который должны быть экспортированы параметры.

Используйте расширение txt для файлов в текстовом формате.

Примеры:

- `avp.com EXPORT settings.dat` – экспорт в конфигурационный файл
- `avp.com EXPORT settings.txt` – экспорт в текстовый файл

Команда IMPORT

Синтаксис команды:

```
IMPORT <filename> /login:<login> /password:<password>
```

Параметры:

- `<filename>` – файл, в который должны быть импортированы параметры (поддерживаются только бинарные файлы);
- `/login` – имя пользователя;
- `/password` – пароль.

Примеры:

```
avp.com IMPORT settings.dat
```

Команда LICENSE

Синтаксис команды:

```
LICENSE /check
```

где `/check` – показать информацию о лицензии, по которой активирована программа.

Команда RESTORE

Синтаксис команды:

```
RESTORE [/REPLACE] <filename>
```

Параметры:

- `/REPLACE` – переписать существующий файл;
- `<filename>` – имя восстанавливаемого файла.

Примеры:

```
avp.com RESTORE /REPLACE C:\eicar.com
```

Команда SCAN

Синтаксис команды:

```
SCAN [<files>] [/ALL][/MEMORY][/STARTUP][/MAIL][/REMDRIVES]
[/FIXDRIVES][/NETDRIVES][/@:<filelist.lst>]
[/i<0-4>] [/e:a|s|b|<filemask>|<seconds>]
[/R[A]:<report_file>] [/C:<settings_file>]
```

Параметры:

- `<files>` – список файлов и папок через пробелы (длинные пути требуется заключать в кавычки);
- `/ALL` – проверять все объекты файловой системы защищенной виртуальной машины;
- `/MEMORY` – проверять память защищенной виртуальной машины;
- `/STARTUP` – проверять объекты автозапуска;
- `/MAIL` – проверять почтовые ящики;
- `/REMDRIVES` – проверять съемные диски;
- `/FIXDRIVES` – проверять жесткие диски;
- `/NETDRIVES` – проверять сетевые диски;
- `/@:<filelist.lst>` – проверять файлы, перечисленные в списке;
- `/i0` – информировать;
- `/i1` – лечить и пропускать, если лечение невозможно;
- `/i2` – лечить и удалять, если лечение невозможно (при этом программа не удаляет файлы из контейнеров, но удаляет контейнеры с исполняемым расширением);
- `/i3` – лечить и удалять, если лечение невозможно (при этом программа удаляет контейнеры, если удаление объекта из контейнера невозможно);
- `/i4` – удалять (в том числе удалять контейнеры, если удаление объекта из контейнера невозможно);
- `/i8` (по умолчанию) – спрашивать пользователя немедленно;
- `/i9` – спрашивать пользователя после завершения задачи;
- `/fe` – быстрый режим проверки (по расширению);
- `/fi` – интеллектуальный режим проверки (по формату);
- `/fa` (по умолчанию) – проверять все файлы;
- `/e:a` – не проверять архивы;
- `/e:b` – не проверять почтовые базы и текст сообщений электронной почты;
- `/e:<filemask>` – не проверять файлы по маске;
- `/e:<seconds>` – не проверять составные файлы, если их проверка длится дольше указанного

количества <секунд>;

- /es:<size> – не проверять файлы размером более указанного количества <мегабайт>;
- /iSwift=<on|off> – включить или выключить технологию iSwift;
- /C:<settings_file> – указать конфигурационный файл;
- /R:<report_file> – сохранять в файле отчета только критические события;
- /RA:<report_file> – сохранять в файле отчета все события.

Примеры:

- avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" C:\Downloads\test.exe
- avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log

Команда START

Синтаксис команды:

START <Profile> [/login:<login>] [/password:<password>] [/R[A]:<report_file>]

Параметры:

- <Profile> – название профиля;
- /login – имя пользователя;
- /password – пароль;
- /R:<report_file> – сохранять в отчет только критические события;
- /RA:<report_file> – сохранять в отчет все события.

Доступные профили:

- File_Monitoring (FM) – Файловый Антивирус;
- Group_Scan – групповая задача проверки;
- Mail_Monitoring (EM) – Почтовый Антивирус;
- Scan_IdleScan – проверка в режиме простоя защищенной виртуальной машины;
- Scan_My_Computer – задача полной проверки;
- Scan_Objects – задача выборочной проверки;
- Scan_Qscan – задача проверки объектов автозапуска;
- Scan_Startup (STARTUP) – задача проверки важных областей;
- SW2 – Мониторинг системы;
- Updater – задача обновления баз;
- Web_Monitoring (WM) – Веб-Антивирус;
- AmsiTask (Amsi) – AMSI-защита.

Вы можете получить список названий доступных профилей с помощью команды: `avp.com HELP START`.

Примеры:

```
avp.com START Scan_Objects
```

Команда STATISTICS

Применение:

```
STATISTICS <Profile>
```

где `<Profile>` – название профиля.

Доступные профили:

- Scan_Objects – задача выборочной проверки;
- Updater – задача обновления баз.

Команда STATUS

Синтаксис команды:

```
STATUS [Profile]
```

где `<Profile>` – название профиля.

Доступные профили:

- File_Monitoring (FM) – Файловый Антивирус;
- Group_Scan – групповая задача проверки;
- Mail_Monitoring (EM) – Почтовый Антивирус;
- Scan_IdleScan – проверка в режиме простоя защищенной виртуальной машины;
- Scan_My_Computer – задача полной проверки;
- Scan_Objects – задача выборочной проверки;
- Scan_Qscan – задача проверки объектов автозапуска;
- Scan_Startup (STARTUP) – задача проверки важных областей;
- SW2 – Мониторинг системы;
- Updater – задача обновления баз;
- Web_Monitoring (WM) – Веб-Антивирус;
- AmsiTask (Amsi) – AMSI-защита.

Вы можете получить список названий доступных профилей с помощью команды: `avp.com HELP STATUS`.

Команда STOP

Синтаксис команды:

```
STOP <Profile> /login:<login> /password:<password>
```

Параметры:

- `<Profile>` – название профиля;
- `/login` – имя пользователя;
- `/password` – пароль.

Доступные профили:

- File_Monitoring (FM) – Файловый Антивирус;
- Group_Scan – групповая задача проверки;
- Mail_Monitoring (EM) – Почтовый Антивирус;
- Scan_IdleScan – проверка в режиме простоя защищенной виртуальной машины;
- Scan_My_Computer – задача полной проверки;
- Scan_Objects – задача выборочной проверки;
- Scan_Qscan – задача проверки объектов автозапуска;
- Scan_Startup (STARTUP) – задача проверки важных областей;
- SW2 – Мониторинг системы;
- Updater – задача обновления баз;
- Web_Monitoring (WM) – Веб-Антивирус;
- AmsiTask (Amsi) – AMSI-защита.

Вы можете получить список названий доступных профилей с помощью команды: `avp.com HELP STOP`.

Команда SVMINFO

Синтаксис команды:

```
SVMINFO
```

Команда TRACES

Синтаксис команды:

```
TRACES on|off|clear|copyto <UNC path>
```

Параметры:

- `on` – включить трассировку;

- off – выключить трассировку;
- clear – удалить все файлы трассировки;
- copyto <UNC path> – сохранить файл трассировки в указанной папке.

Примеры:

- avp.com TRACES off
- avp.com TRACES on
- avp.com TRACES clear
- avp.com TRACES copyto C:\Traces

Команда UPDATE

Синтаксис команды:

```
UPDATE [source] [/R[A]:<report_file>] [/C:<settings_file>] [/APP on|off]
```

Параметры:

- source – путь к локальной папке источника обновлений;
- /R:<report_file> – сохранять в файле отчета только критические события;
- /RA:<report_file> – сохранять в файле отчета все события;
- /C:<settings_file> – указать конфигурационный файл;
- /APP <on|off> – включить или выключить загрузку автопатчей.

Примеры:

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать срочные пакеты обновлений программного обеспечения, устраняющие уязвимости и ошибки. Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского".

Для сохранения бинарной целостности сертифицированной программы запрещается устанавливать обновления программных модулей, не прошедшие инспекционный контроль. Прошедшие инспекционный контроль обновления программных модулей необходимо получать путем обращения в техническую поддержку АО "Лаборатория Касперского" по телефонам: +7 (495) 663-81-47, 8-800-700-88-11 или из регулярно обновляемых статей об актуальных версиях сертифицированных программ на сайте разработчика-изготовителя (http://support.kaspersky.ru/general/certificates). Информацию об обновлениях следует проверять не реже, чем один раз в месяц.

Программы должны периодически (один раз в полгода) подвергаться анализу уязвимостей: компания, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с сайта разработчика-изготовителя (https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 503).

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

"Лаборатория Касперского" предоставляет поддержку этой программы в течение ее жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону (http://support.kaspersky.ru/b2b).
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (http://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Получение информации для Службы технической поддержки

Получение файлов данных

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас прислать следующие файлы:

- файлы системной статистики SVM;
- файлы дампа Сервера защиты и Легких агентов (см. раздел "О файлах дампа Сервера защиты и Легкого агента" на стр. 506);

- файлы трассировки мастера установки компонентов программы (см. раздел "О файлах трассировки мастера установки компонентов Kaspersky Security" на стр. 509);
- файлы трассировки Сервера интеграции и Консоли Сервера интеграции (см. раздел "О файлах трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 510);
- файлы трассировки SVM, Легкого агента и плагинов управления Kaspersky Security (см. раздел "О файлах трассировки SVM, Легкого агента и плагинов управления Kaspersky Security" на стр. 513).

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Security на момент создания файла дампа.

Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

Изменение параметров программы

Специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на защищенной виртуальной машине, подробные отчеты о работе компонентов программы.

Во время проведения работ по диагностике специалисты Службы технической поддержки могут попросить вас в отладочных целях изменить параметры программы:

- активировать функциональность получения расширенной диагностической информации;
- запустить утилиты поддержки, входящие в комплект поставки программы;
- изменить параметры хранения диагностической информации;
- включить режим отладки для Сервера интеграции;
- настроить перехват сетевого трафика и сохранение сетевого трафика в файле;
- выполнить более тонкую настройку работы функциональных компонентов программы, Легких агентов, Сервера защиты, Сервера интеграции, Консоли Сервера интеграции и плагинов управления, недоступную через описанные в этой справке средства управления работой программы (Kaspersky Security Center, локальный интерфейс, командную строку).

Специалисты Службы технической поддержки сообщат вам всю необходимую для выполнения перечисленных действий информацию: описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты, а также состав отправляемых в отладочных целях данных.

Расширенная диагностическая информация сохраняется на вашей виртуальной машине. Автоматическая пересылка данных в "Лабораторию Касперского" не выполняется.

Настоятельно рекомендуется выполнять перечисленные выше действия только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в документации к программе или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты виртуальной машины, а также к нарушению доступности и целостности обрабатываемой информации.

Выключение функции отката изменений

Для анализа ошибки, произошедшей в ходе развертывания SVM, может потребоваться выключить функцию

отката внесенных изменений.

► *Чтобы выключить функцию отката, выполните следующие действия:*

1. На компьютере, на котором установлена Консоль администрирования Kaspersky Security Center, откройте для изменения в текстовом редакторе файл %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA Console\Kaspersky.VIISConsole.UI.exe.config.

   Изменение файла требуется выполнять от имени администратора.

2. В секции `<appSettings></appSettings>` измените строку `<!--<add key="disableRollback" value="1" />-->` следующим образом:

   ```
   <add key="disableRollback" value="1" />
   ```

3. Сохраните и закройте файл Kaspersky.VIISConsole.UI.exe.config.

Получение информации об SVM, подключенных к Серверу интеграции

Специалисты Службы технической поддержки могут попросить вас предоставить информацию об SVM, которые подключены к Серверу интеграции. Вы можете просмотреть список всех SVM, подключенных к Серверу интеграции (см. раздел "Просмотр списка SVM, подключенных к Серверу интеграции" на стр. 105), в Консоли Сервера интеграции.

Диагностика работы программы

Для диагностики работы программы может потребоваться включить отладочный режим работы Сервера интеграции. Для включения отладочного режима работы используются специальные параметры конфигурационного файла. Более подробную информацию вы можете получить у специалистов Службы технической поддержки.

Для диагностики работы Сервера интеграции специалисты Службы технической поддержки могут попросить вас использовать диагностическую утилиту viis_console, входящую в комплект поставки программы. Более подробную информацию вы можете получить у специалистов Службы технической поддержки.

В этом разделе

О файлах дампа Сервера защиты и Легкого агента

Файл дампа содержит информацию о рабочей памяти процессов Kaspersky Security на момент создания

файла дампа.

Файл дампа может также содержать персональные данные. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

О файлах дампа Сервера защиты

По умолчанию файлы дампа Сервера защиты не создаются. Вы можете включать и выключать запись дампов.

► *Чтобы включить запись дампов Сервера защиты:*

1. Создайте файл etc/opt/kaspersky/la/dumps_enabled.
2. Перезапустите службу scanserver, выполнив команду `systemctl restart la-scanserver`.

Все созданные файлы дампа по умолчанию располагаются в директории /var/opt/kaspersky/la/dumps. Имя каждого файла *.dmp содержит дату и время создания файла, идентификатор процесса (PID) и номер дампа в сессии.

Вы можете изменять параметры записи дампов в конфигурационном файле ScanServer.conf (раздел [dumps]).

Для доступа к файлам дампа требуется пароль учетной записи root на SVM, заданный при установке Сервера защиты. Если вы изменили директорию хранения файлов дампа по умолчанию, то Kaspersky Security не контролирует доступ к файлам дампов. Если файловая система, в которой расположена указанная директория, поддерживает соответствующее управление доступом, для доступа к файлам дампов требуются права учетной записи root.
Автоматическая отправка файлов дампа Сервера защиты в "Лабораторию Касперского" не выполняется. Файлы дампа автоматически удаляются при удалении программы.

► *Чтобы выключить запись дампов Сервера защиты:*

1. Удалите файл etc/opt/kaspersky/la/dumps_enabled.
2. Перезапустите службу scanserver, выполнив команду `systemctl restart la-scanserver`.

О файлах дампа Легкого агента для Windows

Файлы дампа Легкого агента для Windows *.dmp создаются автоматически при сбое программы и сохраняются в папке %ProgramData%\Kaspersky Lab.

Сохраненные файлы дампа могут содержать конфиденциальные данные. Файлы сохраняются в доступном для чтения виде, доступ к файлам не ограничивается. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампа.

Автоматическая отправка файлов дампа Легкого агента для Windows в "Лабораторию Касперского" не выполняется. Файлы дампа автоматически удаляются при удалении программы.

О файлах дампа Легкого агента для Linux

По умолчанию файлы дампа Легкого агента для Linux не создаются. Вы можете включать и выключать запись дампов.

► *Чтобы включить запись дампов Легкого агента для Linux:*

1. Создайте файл /etc/opt/kaspersky/lightagent/dumps_enabled.
2. Перезапустите службу lightagent, выполнив одну из следующих команд:
   - `systemctl restart lightagent` – для систем с поддержкой systemd;
   - `/etc/init.d/lightagent restart` – для систем с поддержкой SysV init.

Все созданные файлы дампа по умолчанию располагаются в директории /var/opt/kaspersky/lightagent/dumps. Имя каждого файла *.dmp содержит дату и время создания файла, идентификатор процесса (PID) и номер дампа в сессии.

Вы можете изменять параметры записи дампов в конфигурационном файле LightAgent.conf (раздел [dumps]).

Если вы изменили директорию для записи файлов дампа по умолчанию, файлы дампа не будут автоматически удаляться при удалении Легкого агента для Linux. Вы можете удалить файлы вручную.

Для доступа к файлам дампа требуются права учетной записи root. Если вы изменили директорию хранения файлов дампа по умолчанию, то Kaspersky Security не контролирует доступ к файлам дампов. Если файловая система, в которой расположена указанная директория, поддерживает соответствующее управление доступом, для доступа к файлам дампов требуются права учетной записи root.
Автоматическая отправка файлов дампа Легкого агента для Linux в "Лабораторию Касперского" не выполняется. Файлы дампа автоматически удаляются при удалении программы, если вы не изменяли директорию хранения файлов дампа по умолчанию.

► *Чтобы выключить запись дампов Легкого агента для Linux:*

1. Удалите файл /etc/opt/kaspersky/lightagent/dumps_enabled.
2. Перезапустите службу lightagent, выполнив одну из следующих команд:
   - `systemctl restart lightagent` – для систем с поддержкой systemd;
   - `/etc/init.d/lightagent restart` – для систем с поддержкой SysV init.

О файлах трассировки мастера установки компонентов Kaspersky Security

Информация о ходе и результатах работы мастера установки компонентов Kaspersky Security записывается в файлы трассировки. Если установка, обновление или удаление mmc-плагинов, Сервера интеграции и Консоли Сервера интеграции 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 был запущен мастер.

Если вы выполняли установку компонентов Kaspersky Security, распаковку дистрибутивов Легкого агента или загрузку образов SVM, файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_<номер версии>_Light_Agent_BundleInitialInstall_logs_<дата и время>.zip, где:

- <номер версии> – номер установленной версии программы Kaspersky Security;
- <дата и время> – дата и время завершения установки.

Если вы выполняли обновление компонентов Kaspersky Security, файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_<номер версии>_Light_Agent_BundleMajorUpgrade_logs_<дата и время>.zip, где:

- <номер версии> – номер установленной версии программы Kaspersky Security;
- <дата и время> – дата и время завершения обновления.

Если вы выполняли удаление компонентов Kaspersky Security, файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_<номер версии>_Light_Agent_BundleUninstall_logs_<дата и время>.zip, где:

- <номер версии> – номер установленной версии программы Kaspersky Security;
- <дата и время> – дата и время завершения удаления.

Файлы трассировки мастера установки компонентов Kaspersky Security содержат следующую информацию:

- диагностическую информацию о процессе установки, обновления, удаления компонентов Kaspersky Security или распаковки дистрибутивов Легкого агента;
- 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;
- путь к папке распаковки дистрибутивов Легкого агента.

Файлы трассировки мастера установки компонентов Kaspersky Security хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов трассировки мастера установки компонентов Kaspersky Security в "Лабораторию Касперского" не выполняется.

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\VIISLA\logs\service.log – файл трассировки Сервера интеграции;
- %ProgramData%\Kaspersky Lab\VIISLA Console\logs\console.log – файл трассировки Консоли Сервера интеграции.

Файлы трассировки создаются только после включения записи информации о работе 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 следующих конфигурационных файлов:

- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\Nlog.config – для файла трассировки Сервера интеграции.
- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA 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 защищенных виртуальных машин, а также IP-адрес компьютера, на котором установлена Консоль администрирования Kaspersky Security Center и mmc-плагины 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) гипервизоров или серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

- Если программа используется в режиме multitenancy:
  - названия и идентификаторы клиентов, зарегистрированных в базе данных Сервера интеграции;
  - имена учетных записей администраторов виртуальных Серверов администрирования Kaspersky Security Center;
  - идентификаторы и IP-адреса виртуальных машин клиентов.

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) гипервизоров или серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.
- Если программа используется в режиме multitenancy, названия клиентов, зарегистрированных в базе данных Сервера интеграции.

Вы можете использовать файлы трассировки Сервера интеграции и Консоли Сервера интеграции при обращении в Службу технической поддержки. Информация, записанная в файлы трассировки, может потребоваться для анализа и выяснения причин возникновения ошибок в работе Сервера интеграции.

Файлы трассировки Сервера интеграции и Консоли Сервера интеграции хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов трассировки Сервера интеграции и Консоли Сервера интеграции в "Лабораторию Касперского" не выполняется.

О журнале работы мастера управления SVM

Во время развертывания SVM и во время изменения конфигурации SVM мастер управления SVM сохраняет в журнал работы мастера всю информацию, указанную вами на каждом шаге мастера.

Вы можете использовать журнал работы мастера при обращении в Службу технической поддержки в случае, если развертывание или изменение конфигурации SVM завершилось с ошибкой. Сведения, записанные в журнал работы мастера, не отправляются автоматически в "Лабораторию Касперского".

Журнал работы мастера сохраняется в файле %LOCALAPPDATA%\Kaspersky Lab\Kaspersky VIISLA Console\logs\KasperskyDeployWizard_<дата и время создания файла>.log на компьютере, где был запущен мастер.

Информация в файле перезаписывается при каждом запуске мастера. Чтобы использовать информацию журнала работы мастера в дальнейшем, нужно сохранить файл в место постоянного хранения.

Во время развертывания SVM в журнале работы мастера сохраняется следующая информация:

- выбранное действие (развертывание SVM);
- тип гипервизора или сервера управления виртуальной инфраструктурой;
- адрес гипервизора или адрес сервера управления виртуальной инфраструктурой;
- версия гипервизора или версия сервера управления виртуальной инфраструктурой;
- имя гипервизора, версия установленной на гипервизоре операционной системы, количество виртуальных машин на гипервизоре;
- имя учетной записи, которая используется для подключения мастера управления SVM к гипервизору или к серверу управления виртуальной инфраструктурой;
- имя учетной записи, которая используется для подключения Сервера интеграции к гипервизору или к серверу управления виртуальной инфраструктурой;
- версия образа SVM;
- версии ранее развернутых SVM;
- статус издателя образа SVM;
- путь к файлу образа SVM и информация об образе SVM (производитель, описание, размер виртуального диска);
- статус проверки образа SVM;
- список всех гипервизоров VMware ESXi под управлением одного сервера VMware vCenter Server, их состояние, статусы защиты и права учетной записи, которая используется для подключения к серверу VMware vCenter Server (только при установке на гипервизор VMware ESXi);
- список и версии гипервизоров VMware ESXi, выбранных для развертывания SVM (только при установке на гипервизор VMware ESXi);
- разрешено ли параллельное развертывание SVM на нескольких гипервизорах и количество параллельных сессий (только при установке на гипервизор VMware ESXi);
- параметры SVM на каждом из выбранных гипервизоров (имя, хранилище, имя сети);
- идентификатор VLAN (только при установке на гипервизор Microsoft Windows Server (Hyper-V));
- способ выделения места на диске;
- параметры подключения SVM к Серверу администрирования Kaspersky Security Center (IP-адрес,

порт, SSL-порт);

- разрешен ли доступ для учетной записи root к SVM через SSH;
- тип аутентификации Сервера интеграции на гипервизоре Microsoft Windows Server (Hyper-V): локальная, доменная;
- сетевые параметры SVM: IP-адрес, IP-адрес основного сетевого шлюза, IP-адреса основного и альтернативного DNS-серверов, маска подсети.

Во время изменения конфигурации SVM в журнале работы мастера сохраняется следующая информация:

- выбранное действие (изменение конфигурации SVM);
- IP-адреса или полные доменные имена (FQDN) гипервизоров, на которых выполняется изменение конфигурации SVM;
- IP-адреса или полные доменные имена SVM, на которых выполняется изменение конфигурации;
- сведения о том, будут ли в результате изменения конфигурации изменены:
  - параметры учетных записей для подключения к SVM (пароль конфигурирования, пароль учетной записи root, возможность подключения к SVM с использованием учетной записи root через SSH);
  - список виртуальных сетей, которые использует SVM;
  - сетевые параметры SVM (IP-адрес, IP-адрес основного сетевого шлюза, IP-адреса основного и альтернативного DNS-серверов, маска подсети).

О файлах трассировки SVM, Легкого агента и плагинов управления Kaspersky Security

Файлы трассировки SVM, Легкого агента и плагинов управления Kaspersky Security могут содержать следующие общие данные:

- время события;
- номер потока выполнения;
- название компонента 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.

В этом разделе

Файлы трассировки SVM

Во время работы на SVM могут создаваться следующие файлы трассировки:

- Файл трассировки Сервера защиты ScanServer.log. Имя файла содержит дату и время создания файла. Помимо общих данных (см. раздел "О файлах трассировки SVM, Легкого агента и плагинов управления Kaspersky Security" на стр. 513) этот файл может содержать следующую информацию:
  - персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам на защищенных виртуальных машинах;
  - имя учетной записи для входа в операционную систему, если имя учетной записи является частью имени файла;
  - адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта;
  - параметры подключения SVM к Серверу интеграции;
  - информацию о подключении Легких агентов к SVM: уникальный идентификатор SVM, уникальный идентификатор и сведения об операционной системе виртуальной машины, на которой установлен Легкий агент, периоды времени, в течение которых Легкий агент был подключен к SVM.
- Файл трассировки boot_config.log. В этот файл записываются результаты выполнения команд скрипта первого запуска SVM.
- Файл трассировки wdserver.log. В этот файл записывается информация о событиях, возникающих во время работы службы watchlog (wdserver). Файл содержит общие данные.
- Файл трассировки Агента администрирования Kaspersky Security Center. В этот файл записывается информация о событиях, возникающих при работе модуля связи с Kaspersky Security Center. Файл содержит общие данные.

Файлы трассировки boot_config.log и wdserver.log создаются автоматически.

Файл трассировки ScanServer.log вы можете создать с помощью конфигурационного файла ScanServer.conf, который расположен в директории /etc/opt/kaspersky/la/ на SVM. Для создания файла трассировки Агента администрирования используется специальный скрипт.

За подробной информацией о том, как создать и настроить файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки SVM расположены в директории /var/log/kaspersky/la/.

Файл трассировки ScanServer.log вы также можете создать в политике для Сервера защиты.

► *Чтобы создать файл трассировки ScanServer.log в политике для Сервера защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Включите отображение дополнительных параметров политики для Сервера защиты в реестре операционной системы (см. раздел "Настройка отображения дополнительных параметров политики для Сервера защиты" на стр. 124).
3. В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите создать файл трассировки.
4. В рабочей области выберите закладку **Политики**.

5. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
6. В списке слева выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры работы SVM.
7. В раскрывающемся списке **Уровень трассировки** выберите уровень трассировки.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки.
8. Нажмите на кнопку **Применить**, чтобы запустить процесс трассировки.

Файлы трассировки SVM хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского"

Автоматическая отправка файлов трассировки SVM в "Лабораторию Касперского" не выполняется. Файлы трассировки автоматически удаляются при удалении программы.

Файлы трассировки Легкого агента для Windows

Во время работы Легкого агента для Windows на виртуальной машине могут создаваться следующие файлы трассировки:

- Файлы трассировки SRV.log и GUI.log. Имя каждого файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). Помимо общих данных (см. раздел "О файлах трассировки SVM, Легкого агента и плагинов управления Kaspersky Security" на стр. 513) эти файлы могут содержать следующую информацию:
  - Персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам на защищенной виртуальной машине.
  - Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке веб-трафика. Трафик записывается в файлы трассировки только из компонента Мониторинг сети.
  - Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
  - Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.
  - Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
  - Веб-сайты, которые вы посещаете, а также ссылки с этих веб-сайтов. Эти данные записываются в файлы трассировки, когда программа проверяет веб-сайты.
- Файл трассировки SRV.exception.log. Имя файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о необработанных исключениях.
- Файл трассировки dumpwriter.log. Имя файла содержит номер версии программы, дату и время

создания файла и идентификатор процесса (PID). В этот файл записывается служебная информация, необходимая для устранения неполадок, возникающих при записи файла дампа. Файл содержит общие данные.

- Файл трассировки AVPCon.log. Имя файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих при работе модуля связи с Kaspersky Security Center. Файл содержит общие данные.
- Файл трассировки плагина Почтового Антивируса MCOU.log. Имя файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). Этот файл, помимо общих данных, может содержать части сообщений, в том числе адреса электронной почты.
- Файл трассировки ALL.log. Имя файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях командной строки. Файл содержит общие данные.
- Файлы трассировки задачи изменения состава компонентов Легкого агента (modify_watcher.base.log, modify_install.log, Setup.log). Имена файлов modify_watcher.base.log и modify_install.log содержат номер версии программы, дату и время создания файла и идентификатор процесса (PID). В файлы записывается информация о выполнении задачи изменения состава компонентов и о событиях, возникающих при выполнении задачи. Помимо общих данных файлы могут содержать персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам на защищенных виртуальных машинах.
- Файл трассировки COMAV.log. Имя файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). Помимо общих данных (см. раздел "О файлах трассировки SVM, Легкого агента и плагинов управления Kaspersky Security" на стр. 513) файл содержит информацию о результатах проверок, выполненных по AMSI-запросу от сторонних программ (см. раздел "AMSI-защита" на стр. 221).

По умолчанию файлы трассировки Легкого агента для Windows не создаются. Вы можете создать все файлы трассировки Легкого агента для Windows одним из следующих способов:

- в локальном интерфейсе Легкого агента для Windows;
- из командной строки (см. раздел "Управление Легким агентом для Windows из командной строки" на стр. 493) для Легкого агента для Windows;
- с помощью ключей реестра (см. подробнее в Базе знаний (http://support.kaspersky.ru/14061)).

Все созданные файлы трассировки, кроме файла трассировки задачи изменения состава компонентов Setup.log, расположены в папке %ProgramData%\Kaspersky Lab. Файл трассировки задачи изменения состава компонентов Setup.log расположен в папке установки программы во вложенной папке Setup.

Чтобы получить доступ к файлам в папке %ProgramData%\Kaspersky Lab, включите отображение скрытых файлов и папок.

► *Чтобы создать файлы трассировки в локальном интерфейсе Легкого агента для Windows, выполните следующие действия:*

1. Запустите процесс трассировки. Для этого выполните следующие действия:
   a. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).
   b. По ссылке **Поддержка**, расположенной в нижней части главного окна программы, откройте окно

Поддержка.

c. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

Откроется окно **Информация для поддержки**.

d. В окне **Информация для поддержки** установите флажок **Включить трассировку**.

e. В раскрывающемся списке **Уровень** выберите уровень трассировки.

Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Если указания от специалиста Службы технической поддержки отсутствуют, рекомендуется устанавливать уровень трассировки **Обычный (500)**.

f. Нажмите на кнопку **ОК**.

2. Воспроизведите ситуацию, при которой у вас возникает проблема.
3. Остановите процесс трассировки. Для этого выполните следующие действия:

a. На защищенной виртуальной машине откройте главное окно программы (на стр. 120).

b. По ссылке **Поддержка**, расположенной в нижней части главного окна программы, откройте окно **Поддержка**.

c. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

Откроется окно **Информация для поддержки**.

d. В окне **Информация для поддержки** снимите флажок **Включить трассировку**.

e. Нажмите на кнопку **ОК**.

Файлы трассировки Легкого агента для Windows хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов трассировки Легкого агента для Windows в "Лабораторию Касперского" не выполняется. Файлы трассировки автоматически удаляются при удалении программы, если вы не изменяли папку хранения файлов трассировки по умолчанию.

Файлы трассировки Легкого агента для Linux

Во время работы Легкого агента для Linux на виртуальной машине могут создаваться следующие файлы трассировки:

- Файл трассировки LightAgent.log. Имя файла содержит дату и время создания файла. Помимо общих данных (см. раздел "О файлах трассировки SVM, Легкого агента и плагинов управления Kaspersky Security" на стр. 513) этот файл может содержать следующую информацию:
  - персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам на защищенной виртуальной машине;
  - имя учетной записи для входа в операционную систему Linux, если имя учетной записи является частью имени файла;

  - адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- Файл трассировки avp-cli.log. В этот файл записывается информация о событиях командной строки. Файл содержит общие данные.
- Файл трассировки install.log. В этот файл записывается вывод результатов выполнения команд, формирующих необходимые параметры для подготовки запуска Легкого агента для Linux. Файл содержит общие данные.
- Файл трассировки wdserver.log. В этот файл записывается информация о событиях, возникающих во время работы службы watchlog (wdserver). Файл содержит общие данные.
- Файл трассировки autopatch.log. В этот файл записывается информация о процессе поиска подходящего обновления модулей программы и об установке обновления модулей программы. Файл содержит общие данные.
- Файл трассировки Агента администрирования Kaspersky Security Center. В этот файл записывается информация о событиях, возникающих при работе модуля связи с Kaspersky Security Center. Файл содержит общие данные.

Файлы трассировки wdserver.log, autopatch.log и install.log создаются автоматически.

Файлы трассировки avp-cli.log и LightAgent.log вы можете создать с помощью конфигурационных файлов LightAgent.conf и avp-cli.conf, которые расположены в директории /etc/opt/kaspersky/lightagent/ на защищенной виртуальной машине. Для создания файла трассировки Агента администрирования используется специальный скрипт.

За подробной информацией о том, как создать и настроить файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки Легкого агента для Linux по умолчанию расположены в директории /var/log/kaspersky/lightagent/.

Файл трассировки LightAgent.log вы также можете создать, запустив процесс трассировки из командной строки на защищенной виртуальной машине.

► *Чтобы создать файл трассировки LightAgent.log из командной строки, выполните следующие действия:*

1. Запустите процесс трассировки, выполнив команду

   ```
   lightagent traces on [<уровень трассировки>]
   ```

   где <уровень трассировки> – уровень детализации отладочной информации. Возможны следующие значения: 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000. Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Этот параметр необязательный. Если вы не укажете значение уровня трассировки, программа создаст файл трассировки с уровнем детализации по умолчанию – 500.
2. Воспроизведите ситуацию, при которой у вас возникает проблема.
3. Остановите процесс трассировки, выполнив команду

   ```
   lightagent traces off
   ```

   Файл трассировки LightAgent.log по умолчанию создается в директории /var/log/kaspersky/lightagent/. Если вы хотите сохранить файл в другую директорию, выполните команду

   ```
   lightagent traces --copyto <путь к файлу трассировки> [--overwrite]
   ```

где:

- copyto <путь к файлу трассировки> – сохранить файл трассировки в указанной директории. Укажите полный путь к директории, в которую вы хотите сохранить файл трассировки.
- overwrite – если в указанной директории находится файл трассировки с таким именем, перезаписать этот файл сохраняемым файлом трассировки.

Если файл трассировки LightAgent.log расположен в директории по умолчанию (/var/log/kaspersky/lightagent), вы можете удалить его с помощью команды

```
lightagent traces --clear
```

Файлы трассировки Легкого агента для Linux хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов трассировки Легкого агента для Linux в "Лабораторию Касперского" не выполняется. Файлы трассировки автоматически удаляются при удалении программы, если вы не изменяли директорию хранения файлов трассировки по умолчанию.

Файлы трассировки mmc-плагинов Kaspersky Security

Во время работы программы на компьютере, где установлен Сервер администрирования Kaspersky Security Center, могут создаваться следующие файлы трассировки mmc-плагинов Kaspersky Security:

- KSVLA_AdminGUI.log – файл трассировки mmc-плагина управления Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows. Имя файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы плагина, в частности, о работе политики для Легкого агента для Windows и задач.
- KSVLALIN_AdminGUI.log – файл трассировки mmc-плагина управления Kaspersky Security для виртуальных сред 5.2 Легкий агент для Linux. Имя файла содержит номер версии программы, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы плагина, в частности, о работе политики для Легкого агента для Linux и задач.
- Файл трассировки mmc-плагина управления Kaspersky Security для виртуальных сред 5.2 Легкий агент – Сервер защиты. Имя файла задается пользователем, к заданному имени добавляются имя пользователя и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы плагина, в частности, о работе политики для Сервера защиты и задач.

Помимо общих данных (см. раздел «О файлах трассировки SVM, Легкого агента и плагинов управления Kaspersky Security» на стр. 513) эти файлы могут содержать следующую информацию:

- персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам;
- имя учетной записи для входа в операционную систему, если имя учетной записи является частью

имени файла.

По умолчанию файлы трассировки mmc-плагинов Kaspersky Security не создаются. Вы можете создать все файлы трассировки mmc-плагинов с помощью ключей реестра. За подробной информацией о том, как создать файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки mmc-плагинов расположены в папке, указанной пользователем во время настройки ключей реестра.

Файлы трассировки mmc-плагинов Kaspersky Security хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов трассировки mmc-плагинов Kaspersky Security в "Лабораторию Касперского" не выполняется. Файлы трассировки автоматически удаляются при удалении программы.

О журнале работы мастера управления SVM

Во время развертывания SVM и во время изменения конфигурации SVM мастер управления SVM сохраняет в журнал работы мастера всю информацию, указанную вами на каждом шаге мастера.

Вы можете использовать журнал работы мастера при обращении в Службу технической поддержки в случае, если развертывание или изменение конфигурации SVM завершилось с ошибкой. Сведения, записанные в журнал работы мастера, не отправляются автоматически в "Лабораторию Касперского".

Журнал работы мастера сохраняется в файле %LOCALAPPDATA%\Kaspersky Lab\Kaspersky VIISLA Console\logs\KasperskyDeployWizard_<дата и время создания файла>.log на компьютере, где был запущен мастер.

Информация в файле перезаписывается при каждом запуске мастера. Чтобы использовать информацию журнала работы мастера в дальнейшем, нужно сохранить файл в место постоянного хранения.

Во время развертывания SVM в журнале работы мастера сохраняется следующая информация:

- выбранное действие (развертывание SVM);
- тип гипервизора или сервера управления виртуальной инфраструктурой;
- адрес гипервизора или адрес сервера управления виртуальной инфраструктурой;
- версия гипервизора или версия сервера управления виртуальной инфраструктурой;
- имя гипервизора, версия установленной на гипервизоре операционной системы, количество виртуальных машин на гипервизоре;
- имя учетной записи, которая используется для подключения мастера управления SVM к

гипервизору или к серверу управления виртуальной инфраструктурой;

- имя учетной записи, которая используется для подключения Сервера интеграции к гипервизору или к серверу управления виртуальной инфраструктурой;
- версия образа SVM;
- версии ранее развернутых SVM;
- статус издателя образа SVM;
- путь к файлу образа SVM и информация об образе SVM (производитель, описание, размер виртуального диска);
- статус проверки образа SVM;
- список всех гипервизоров VMware ESXi под управлением одного сервера VMware vCenter Server, их состояние, статусы защиты и права учетной записи, которая используется для подключения к серверу VMware vCenter Server (только при установке на гипервизор VMware ESXi);
- список и версии гипервизоров VMware ESXi, выбранных для развертывания SVM (только при установке на гипервизор VMware ESXi);
- разрешено ли параллельное развертывание SVM на нескольких гипервизорах и количество параллельных сессий (только при установке на гипервизор VMware ESXi);
- параметры SVM на каждом из выбранных гипервизоров (имя, хранилище, имя сети);
- идентификатор VLAN (только при установке на гипервизор Microsoft Windows Server (Hyper-V));
- способ выделения места на диске;
- параметры подключения SVM к Серверу администрирования Kaspersky Security Center (IP-адрес, порт, SSL-порт);
- разрешен ли доступ для учетной записи root к SVM через SSH;
- тип аутентификации Сервера интеграции на гипервизоре Microsoft Windows Server (Hyper-V): локальная, доменная;
- сетевые параметры SVM: IP-адрес, IP-адрес основного сетевого шлюза, IP-адреса основного и альтернативного DNS-серверов, маска подсети.

Во время изменения конфигурации SVM в журнале работы мастера сохраняется следующая информация:

- выбранное действие (изменение конфигурации SVM);
- IP-адреса или полные доменные имена (FQDN) гипервизоров, на которых выполняется изменение конфигурации SVM;
- IP-адреса или полные доменные имена SVM, на которых выполняется изменение конфигурации;
- сведения о том, будут ли в результате изменения конфигурации изменены:
  - параметры учетных записей для подключения к SVM (пароль конфигурирования, пароль учетной записи root, возможность подключения к SVM с использованием учетной записи root через SSH);
  - список виртуальных сетей, которые использует SVM;
  - сетевые параметры SVM (IP-адрес, IP-адрес основного сетевого шлюза, IP-адреса основного и альтернативного DNS-серверов, маска подсети).

Использование утилит и скриптов 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:

- ai_config – утилита, позволяющая преобразовать параметры SVM из формата базы данных конфигурации SVM в текстовый файл и обратно;
- cleanUpdateShare.sh – скрипт, предназначенный для удаления старых баз Легких агентов с SVM;
- configure.sh – скрипт, предназначенный для управления SVM, просмотра и изменения параметров конфигурации SVM; используется мастером управления SVM для изменения конфигурации SVM под учетной записью klconfig;
- dump_ods_scan_queue и dump_ods_scan_queue.sh – утилиты, позволяющие посмотреть текущую очередь задач проверки;
- eventlog_client и eventlog_client.sh – утилиты, позволяющие формировать события для отправки в Kaspersky Security Center;
- firewall.sh – скрипт, позволяющий открыть порты для подключения к Агенту администрирования;
- first_boot.sh – скрипт, позволяющий изменить параметры конфигурации SVM при первой загрузке SVM;
- get_used_mem.sh – скрипт, позволяющий посмотреть статистику использования памяти;
- kvp_read – утилита, позволяющая посмотреть общие данные гипервизора в хранилище Hyper-V KVP Exchange;
- la-kvm-guest – скрипт в формате init.d, предназначенный для управления службой KVM guest;
- la-scanserver – скрипт в формате init.d, предназначенный для управления службой scanserver;
- managenet.sh – скрипт, предназначенный для управления сетевыми интерфейсами;
- on_product_install.sh – скрипт, позволяющий применить временную конфигурацию SVM во время развертывания SVM;
- sfw – утилита, позволяющая управлять брандмауэром netfilter операционной системы Linux;
- show_inventory и show_inventory.sh – утилиты, позволяющие посмотреть информацию о дереве виртуальной инфраструктуры, полученную SVM от Сервера интеграции;
- show_virt_info и show_virt_info.sh – утилиты, позволяющие посмотреть информацию о виртуальной машине (например, версию BIOS, информацию о гипервизоре);
- storage_util – утилита, предназначенная для управления хранилищем данных, которые используются при обновлении баз программы;
- viis_console и viis_console.sh – утилиты для подключения и управления Сервером интеграции, позволяющие подключиться к Серверу интеграции, получить информацию о Сервере интеграции и соединении утилит с Сервером интеграции, управлять списком гипервизоров и серверов управления виртуальной инфраструктурой, управлять информацией об SVM, которую SVM передают на Сервер интеграции, получать информацию о дереве виртуальной инфраструктуры, получать статистику о работе утилит;
- patch_detector.pl – скрипт, позволяющий искать обновление модулей программы в указанной папке и запускать утилиту KSV Patch Installer для установки обновления;
- patch_installer.pl – скрипт, позволяющий установить обновление модулей программы из файла

tar.gz;

- patch_list.pl – скрипт, позволяющий сформировать список установленных на SVM обновлений модулей программы в формате XML;
- patch_rollback.pl – скрипт, позволяющий откатить последнее установленное обновление модулей программы.

Соответствие терминов

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

Таблица 3. Соответствие терминов

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

Приложение. Значения параметров программы в сертифицированном состоянии

Этот раздел содержит перечень параметров программы, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии.

Если вы меняете какие-либо из перечисленных параметров с их значений в сертифицированном состоянии на другие значения, вы выводите программу из сертифицированного состояния.

Таблица 4. Параметры и их значения для программы в сертифицированном состоянии

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Политика для Сервера защиты – **Настройка событий**	**Регистрация событий**: **Хранить в базе данных Сервера администрирования в течение (сут)**	Флажок установлен, значение не ниже установленного по умолчанию.
Политика для Сервера защиты – **Параметры Kaspersky Security Network**	**Использовать KSN для проверки файлов и веб-адресов**	Флажок снят. Допускается устанавливать флажок только при использовании Локального KSN.
Политика для Сервера защиты – **Параметры обновления**	**Обновлять модули программы**	Флажок снят.
Политика для Сервера защиты – **Параметры SNMP-мониторинга**	**Включить SNMP-мониторинг состояния SVM**	Флажок снят.
Политика для Легкого агента для Windows – **Настройка событий**	**Регистрация событий**: **Хранить в базе данных Сервера администрирования в течение (сут)**	Флажок установлен, значение не ниже установленного по умолчанию.
Политика для Легкого агента для Windows – **Основные параметры защиты**	**Запускать Kaspersky Security для виртуальных сред 5.2 Легкий агент при включении виртуальной машины**	Флажок установлен.
Политика для Легкого агента для Windows – **Основные параметры защиты**	**Объекты для обнаружения**: • **Вредоносные утилиты** • **Упакованные файлы** • **Многократно упакованные файлы**	Флажки установлены.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Политика для Легкого агента для Windows – **Основные параметры защиты**	**Доверенная зона**: • **Исключения** (таблица) • **Доверенные программы** (таблица)	Значения по умолчанию.
Политика для Легкого агента для Windows – параметры Файлового Антивируса	**Файловый Антивирус**	Флажок установлен.
Политика для Легкого агента для Windows– параметры Файлового Антивируса	**Уровень безопасности**	**Рекомендуемый**
Политика для Легкого агента для Windows – параметры Файлового Антивируса	**Действие при обнаружении угрозы**	Одно из следующих значений: • **Выбирать действие автоматически**. • **Лечить. Удалять, если лечение невозможно**.
Политика для Легкого агента для Windows – параметры AMSI-защиты	Параметры компонента AMSI-защита.	Значения в соответствии с вашей корпоративной политикой безопасности.
Политика для Легкого агента для Windows – параметры Почтового Антивируса	**Почтовый Антивирус**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Почтового Антивируса	**Уровень безопасности**	**Рекомендуемый**
Политика для Легкого агента для Windows – параметры Почтового Антивируса	**Действие при обнаружении угрозы**	Одно из следующих значений: • **Выбирать действие автоматически**. • **Лечить. Удалять, если лечение невозможно**.
Политика для Легкого агента для Windows – параметры Веб-Антивируса	**Веб-Антивирус**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Веб-Антивируса	**Уровень безопасности**	**Рекомендуемый**
Политика для Легкого агента для Windows – параметры Веб-Антивируса	**Действие при обнаружении угрозы**	Одно из следующих значений: • **Выбирать действие автоматически**. • **Запрещать загрузку**.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Политика для Легкого агента для Windows – параметры Мониторинга системы	**Мониторинг системы**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Мониторинга системы	**Включить защиту от эксплойтов**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Мониторинга системы	**Хранить историю активности программ для базы BSS**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Мониторинга системы	**Не контролировать активность программ, имеющих цифровую подпись**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Мониторинга системы	**Выполнять откат действий вредоносных программ при лечении**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Мониторинга системы	**При обнаружении вредоносной активности программы**	Одно из следующих значений: • **Выбирать действие автоматически**. • **Завершать работу вредоносной программы**.
Политика для Легкого агента для Windows – параметры Контроля активности программ	**Контроль активности программ**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Контроля активности программ	Параметры правил Контроля активности программ (см. раздел "Работа с правилами контроля программ" на стр. 293).	Значения в соответствии с вашей корпоративной политикой безопасности.
Политика для Легкого агента для Windows – параметры Веб-Контроля	**Веб-Контроль**	Флажок установлен.
Политика для Легкого агента для Windows – параметры Веб-Контроля	Параметры компонента Веб-Контроль (на стр. 306)	Значения в соответствии с вашей корпоративной политикой безопасности.
Политика для Легкого агента для Windows – **Дополнительные параметры**	**Включить самозащиту**	Флажок установлен.
Политика для Легкого агента для Windows – **Дополнительные параметры**	**Выключить внешнее управление системной службой**	Флажок установлен.
Политика для Легкого агента для Windows – **Дополнительные параметры**	**Разрешить управление групповыми задачами**	Флажок снят.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Политика для Легкого агента для Windows – **Отчеты и хранилища**	**Хранить отчеты не более**	Флажок установлен, значение не ниже установленного по умолчанию (30 дней).
Политика для Легкого агента для Windows – **Отчеты и хранилища**	**Максимальный размер файла**	Флажок установлен, значение не ниже установленного по умолчанию (1024 МБ).
Политика для Легкого агента для Windows – **Отчеты и хранилища**	**Информировать Сервер администрирования – О файлах резервного хранилища**	Флажок установлен.
Политика для Легкого агента для Windows – **Отчеты и хранилища**	**Информировать Сервер администрирования – О необработанных файлах**	Флажок установлен.
Политика для Легкого агента для Windows – **Интерфейс**	**Запускать локальный интерфейс программы**	Флажок установлен.
Политика для Легкого агента для Windows – **Интерфейс**	**Отображать локальный интерфейс программы**	Флажок установлен.
Политика для Легкого агента для Windows – **Интерфейс**	**Включить защиту паролем**	Флажок установлен.
Политика для Легкого агента для Windows – **Интерфейс**	Параметры защиты паролем.	Выбран вариант **Все операции (кроме уведомлений об опасности)**.
Политика для Легкого агента для Windows – **Интерфейс**	Параметры уведомлений о событиях (окно **Уведомления**).	Флажки напротив названий событий, значения не ниже установленных по умолчанию. Флажок **Сохранять в журнале программы** установлен для всех событий.
Политика для Легкого агента для Windows – **Managed Detection and Response**	**Managed Detection and Response**	Флажок снят. Допускается устанавливать флажок только при использовании Локального KSN.
Политика для Легкого агента для Linux – **Настройка событий**	**Регистрация событий**: **Хранить в базе данных Сервера администрирования в течение (сут)**	Флажок установлен, значение не ниже установленного по умолчанию.
Политика для Легкого агента для Linux – **Основные параметры защиты**	**Объекты для обнаружения**: • **Вредоносные утилиты** • **Упакованные файлы** • **Многократно упакованные файлы**	Флажки установлены.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Политика для Легкого агента для Linux – **Основные параметры защиты**	**Доверенная зона**: **Исключения** (таблица)	Значения по умолчанию.
Политика для Легкого агента для Linux – параметры Файлового Антивируса	**Файловый Антивирус**	Флажок установлен.
Политика для Легкого агента для Linux – параметры Файлового Антивируса	**Уровень безопасности**	**Рекомендуемый**
Политика для Легкого агента для Linux – параметры Файлового Антивируса	**Действие при обнаружении угрозы**	Одно из следующих значений: • **Удалять**. • **Лечить. Удалять, если лечение невозможно**.
Политика для Легкого агента для Linux – **Отчеты и хранилища**	**Информировать Сервер администрирования**: **О файлах резервного хранилища**	Флажок установлен.
Задача Обновление баз для Сервера защиты – **Уведомление**	**Сохранять информацию о результатах**: **На сервере администрирования в течении (сут)**	Флажок установлен, значение не ниже установленного по умолчанию (7 дней).
Задача Обновление баз для Сервера защиты – **Уведомление**	**Сохранять все события**	Выбран этот вариант.
Задача Обновление баз для Сервера защиты – **Расписание**	**Запуск по расписанию**	**При загрузке обновлений в хранилище**
Задача Обновление баз для Сервера защиты – **Исключения из области действия задачи**	Таблица исключений.	е заданы.
Задача Обновление для Легкого агента для Windows	**Режим запуска**	**Автоматически**
Задача Поиск вирусов для Легкого агента для Windows Задача Выборочная проверка для Легкого агента для Windows Задача Полная проверка для Легкого агента для Windows Задача Поиск вирусов для Легкого агента для Linux	**Уровень безопасности**	**Рекомендуемый**

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Задача Поиск вирусов для Легкого агента для Windows Задача Выборочная проверка для Легкого агента для Windows Задача Полная проверка для Легкого агента для Windows Задача Проверка важных областей для Легкого агента для Windows Задача Поиск вирусов для Легкого агента для Linux	**Действие при обнаружении угрозы**	Одно из следующих значений: • **Выбирать действие автоматически**. • **Лечить. Удалять, если лечение невозможно**. • **Удалять**.
Задача Поиск вирусов для Легкого агента для Windows – **Уведомление** Задача Поиск вирусов для Легкого агента для Linux – **Уведомление**	**Сохранять информацию о результатах**: **На Сервере администрирования в течение (дней)**	Флажок установлен, значение не ниже установленного по умолчанию (7 дней).
Задача Полная проверка для Легкого агента для Windows	**Область проверки**	Список областей не меньше, чем заданный по умолчанию: • Системная память. • Объекты автозапуска. • Загрузочные секторы. • Системное резервное хранилище. • Все жесткие диски. • Все съемные диски.
Задача Проверка важных областей для Легкого агента для Windows	**Уровень безопасности**	**Высокий**
Задача Проверка важных областей для Легкого агента для Windows	**Область проверки**	Список областей не меньше, чем заданный по умолчанию: • Системная память. • Объекты автозапуска. • Загрузочные секторы.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Задача Изменение состава компонентов Легкого агента для Windows	**Компоненты для установки на ОС для серверов**: • Ядро программы и задачи проверки. • Файловый Антивирус. • Почтовый Антивирус. • Мониторинг системы. • AMSI-защита. • Контроль запуска программ. • Контроль целостности системы. • Интеграция с Kaspersky Endpoint Agent.	Флажки установлены.
Задача Изменение состава компонентов Легкого агента для Windows	**Компоненты для установки на ОС для серверов**: • Сетевой экран. • Защита от сетевых атак.	Флажки сняты.
Задача Изменение состава компонентов Легкого агента для Windows	**Компоненты для установки на ОС для рабочих станций**: • Ядро программы и задачи проверки. • Файловый Антивирус. • Почтовый Антивирус. • Веб-Антивирус. • Мониторинг системы. • AMSI-защита. • Контроль запуска программ. • Веб-Контроль. • Контроль активности программ. • Интеграция с Kaspersky Endpoint Agent.	Флажки установлены.
Задача Изменение состава компонентов Легкого агента для Windows	**Компоненты для установки на ОС для рабочих станций**: • Сетевой экран. • Защита от сетевых атак. • Контроль устройств.	Флажки сняты.

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 (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.

Adobe, Acrobat, Flash – товарные знаки или зарегистрированные в Соединенных Штатах Америки и / или в других странах товарные знаки Adobe Systems Incorporated.

Citrix, Citrix Hypervisor, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktops, XenApp, XenDesktop и XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

HUAWEI, FusionCompute и FusionSphere являются зарегистрированными товарными знаками Huawei Technologies Co., Ltd в Китае и других странах.

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

Microsoft, Active Directory, Hyper-V, Outlook, PowerShell, Windows, Windows Server и Windows Store – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla, Firefox – товарные знаки Mozilla Foundation.

Oracle, Java – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

CentOS – товарный знак компании Red Hat, Inc.

Red Hat, Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

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

OpenAPI – товарный знак компании The Linux Foundation.

VMware, VMware ESXi, VMware Horizon, VMware NSX, VMware NSX Manager, VMware Tools, VMware vCenter Server и VMware vSphere – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.