KASPERSKY lab

Kaspersky Security для виртуальных сред 4.0 Легкий агент

Руководство администратора

Версия программы: 4.0

Уважаемый пользователь!

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

Внимание! Права на этот документ являются собственностью АО «Лаборатория Касперского» (далее также «Лаборатория Касперского») и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения «Лаборатории Касперского».

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, «Лаборатория Касперского» ответственности несет.

Дата редакции документа: 20.01.2017

© АО «Лаборатория Касперского», 2017.

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

Содержание

Об этом руководстве

Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент (далее «Kaspersky Security») адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security.

Руководство предназначено специалистам, которые имеют опыт работы с виртуальной инфраструктурой на платформе Microsoft® Windows Server® с установленной ролью Hyper-V® (далее также «Microsoft Windows Server (Hyper-V)»), Citrix XenServer, VMware ESXi™ или KVM (Kernel-based Virtual Machine) и системой удаленного централизованного управления программами «Лаборатории Касперского» Kaspersky Security Center. Для использования Kaspersky Security пользователю также нужно быть знакомым с операционными системами Microsoft Windows® и Linux® и владеть основными приемами работы в них.

В этом руководстве вы можете найти информацию о настройке и использовании Kaspersky Security.

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

В этом разделе

В этом документе

Этот документ содержит следующие разделы:

Источники информации о программе (см. стр. 14)

Этот раздел содержит описание источников информации о программе.

Kaspersky Security для виртуальных сред 4.0 Легкий агент (см. стр. 17)

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Security, перечень аппаратных и программных требований Kaspersky Security.

Архитектура программы (см. стр. 29)

Этот раздел содержит описание компонентов Kaspersky Security и их взаимодействия.

Лицензирование программы (см. стр. 39)

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

Запуск и остановка программы (см. стр. 75)

Этот раздел содержит информацию о том, как запустить программу и как завершить работу с ней.

Состояние защиты виртуальной машины (см. стр. 77)

Этот раздел содержит информацию об оценке состояния защиты виртуальной машины.

Концепция управления программой через Kaspersky Security Center (см. стр. 78)

Этот раздел содержит информацию об управлении программой через систему удаленного централизованного управления программами «Лаборатории Касперского» Kaspersky Security Center.

Постоянная защита и проверка виртуальной машины (см. стр. 79)

Этот раздел содержит информацию о том, как Kaspersky Security защищает и проверяет защищенную виртуальную машину.

Управление политиками (см. стр. 82)

Этот раздел содержит информацию о создании и настройке политик для программы Kaspersky Security для виртуальных сред 4.0 Легкий агент.

Управление задачами (см. стр. 121)

Этот раздел содержит информацию об управлении задачами для программы Kaspersky Security для виртуальных сред 4.0 Легкий агент, которые вы можете настраивать через Kaspersky Security Center.

Обновление баз и модулей программы (см. стр. 129)

Этот раздел содержит информацию об обновлении баз и модулей программы и инструкции о том, как настроить параметры обновления.

Настройка параметров Легкого агента для Linux через Kaspersky Security Center (см. стр. 141)

Этот раздел содержит информацию о настройке основных параметров защиты Легкого агента для Linux и параметров компонента Файловый Антивирус Легкого агента для Linux через Kaspersky Security Center.

Настройка параметров Легкого агента для Windows через Kaspersky Security Center (см. стр. 173)

Этот раздел содержит информацию о настройке некоторых параметров компонента Контроль запуска программ и компонента Контроль устройств Легкого агента для Windows через Kaspersky Security Center.

Технология лечения активного заражения (см. стр. 187)

Этот раздел содержит информацию о технологии лечения активного заражения, а также инструкцию о том, как включить использование технологии лечения активного заражения для серверных операционных систем Windows на защищенных виртуальных машинах.

Участие в Kaspersky Security Network (см. стр. 191)

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

Управление Легким агентом для Linux из командной строки (см. стр. 198)

Этот раздел содержит информацию об управлении компонентом Легкий агент для Linux с помощью команд из командной строки и настройке параметров команд.

Обращение в Службу технической поддержки (см. стр. 212)

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Глоссарий (см. стр. 225)

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

АО «Лаборатория Касперского» (см. стр. 231)

Этот раздел содержит информацию об АО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 233)

Этот раздел содержит информацию о стороннем коде.

Уведомления о товарных знаках (см. стр. 234)

Этот раздел содержит информацию о товарных знаках, которые используются в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.

Пример текста	Описание условного обозначения
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Тип задачи>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники для самостоятельного поиска информации

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

- страница Kaspersky Security на веб-сайте «Лаборатории Касперского»;
- страница программы на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 212).

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

Страница Kaspersky Security на веб-сайте «Лаборатории Касперского»

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

Страница Kaspersky Security в Базе знаний

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

На странице Kaspersky Security в Базе знаний (http://support.kaspersky.ru/ksv4) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

Электронная справка

В состав электронной справки программы входят файлы полной справки локального интерфейса программы и файлы контекстной справки.

В полной справке вы можете найти информацию о настройке и использовании программы.

В контекстной справке вы можете найти информацию об окнах локального интерфейса программы Kaspersky Security и окнах плагинов управления Kaspersky Security: перечень и описание параметров.

Документация

В состав документации к программе входят файлы руководств.

В руководстве по внедрению вы можете найти информацию для выполнения следующих задач:

- планирование установки Kaspersky Security (учитывая принципы работы Kaspersky Security и системные требования);
- подготовка к установке, установка и активация Kaspersky Security.

В руководстве администратора вы можете найти информацию о настройке и использовании Kaspersky Security.

В руководстве пользователя вы можете найти информацию о типовых задачах, которые пользователь может выполнять с помощью программы, с учетом имеющихся прав в программе Kaspersky Security.

Обсуждение программ «Лаборатории Касперского» на форуме

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

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

Kaspersky Security для виртуальных сред 4.0 Легкий агент

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Security, перечень аппаратных и программных требований Kaspersky Security.

В этом разделе

О Kaspersky Security для виртуальных сред 4.0 Легкий агент

Kaspersky Security для виртуальных сред 4.0 Легкий агент представляет собой интегрированное решение, обеспечивающее комплексную защиту виртуальных машин под управлением гипервизора Vmware ESXi, Citrix XenServer, Microsoft Windows Server с установленной ролью Hyper-V или KVM (Kernel-based Virtual Machine) от различных видов информационных угроз, сетевых и мошеннических атак.

Программа Kaspersky Security оптимизирована для обеспечения максимальной производительности виртуальных машин, которые вы хотите защищать.

Программа позволяет защищать виртуальные машины с настольными и серверными операционными системами.

Защита виртуальных машин

Каждый тип угроз обрабатывается отдельным компонентом программы. Компоненты можно включать и выключать независимо друг от друга, а также настраивать параметры их работы.

На виртуальную машину с гостевой настольной операционной системой Microsoft Windows® вы можете установить компоненты защиты и компоненты контроля. На виртуальную машину с гостевой серверной операционной системой Microsoft Windows компоненты контроля не устанавливаются.

На виртуальную машину с гостевой операционной системой Linux® вы можете установить компонент защиты Файловый Антивирус.

В дополнение к *постоянной защите*, реализуемой компонентами программы, рекомендуется периодически выполнять *проверку* виртуальных машин и их шаблонов на вирусы и другие вредоносные программы (см. раздел «О постоянной защите и проверке виртуальной машины» на стр. 79).

Чтобы поддерживать программу Kaspersky Security в актуальном состоянии, требуется *обновление* баз программы, используемых для обнаружения угроз (см. раздел «Обновление баз и модулей программы» на стр. 129).

К компонентам контроля относятся следующие компоненты программы:

- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.
- **Контроль активности программ**. Компонент регистрирует действия, совершаемые программами в операционной системе, установленной на защищенной виртуальной машине, и регулирует деятельность программ, исходя из того, к какой группе компонент 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 «Мои документы», файлы cookie, данные об активности пользователя), а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.
- **Контроль устройств**. Компонент позволяет установить гибкие ограничения доступа к устройствам, являющимся источниками информации (например, жесткие диски,

съемные диски, CD/DVD-диски), инструментами передачи информации (например, модемы), инструментами превращения информации в твердую копию (например, принтеры) или интерфейсам, с помощью которых устройства подключаются к защищенной виртуальной машине (например, USB, Bluetooth).

- **Веб-Контроль**. Компонент позволяет установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.

Работа компонентов контроля основана на правилах:

- Контроль запуска программ использует в своей работе правила контроля запуска программ.
- Контроль активности программ использует в своей работе правила контроля программ.
- Контроль устройств использует в своей работе правила доступа к устройствам и правила доступа к шинам подключения.
- Веб-Контроль использует в своей работе правила доступа к веб-ресурсам.

К компонентам защиты относятся следующие компоненты программы:

- **Файловый Антивирус**. Компонент позволяет избежать заражения файловой системы операционной системы защищенной виртуальной машины. Компонент запускается при старте Kaspersky Security, 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.
- **Мониторинг системы**. Компонент получает данные о действиях программ в операционной системе защищенной виртуальной машины и предоставляет эту информацию другим компонентам для более эффективной защиты.
- **Почтовый Антивирус**. Компонент проверяет входящие и исходящие сообщения электронной почты на вирусы и другие вредоносные программы.
- **Веб-Антивирус**. Компонент проверяет трафик, поступающий на защищенную виртуальную машину по протоколам HTTP и FTP, а также устанавливает принадлежность ссылок к вредоносным или фишинговым веб-адресам.

- **IM-Антивирус**. Компонент проверяет трафик, поступающий на защищенную виртуальную машину по протоколам IM-клиентов. Компонент обеспечивает безопасную работу со многими IM-клиентами.

- **Сетевой экран**. Компонент обеспечивает защиту персональных данных, хранящихся в операционной системе защищенной виртуальной машины пользователя, блокируя все возможные для операционной системы угрозы в то время, когда защищенная виртуальная машина подключена к интернету или к локальной сети. Компонент фильтрует всю сетевую активность согласно правилам двух типов: сетевым правилам программ и сетевым пакетным правилам.

- **Мониторинг сети**. Компонент предназначен для просмотра в режиме реального времени информации о сетевой активности защищенной виртуальной машины.

- **Защита от сетевых атак**. Компонент отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на защищенную виртуальную машину пользователя, Kaspersky Security блокирует сетевую активность атакующего компьютера.

Подробнее о работе компонентов контроля и компонентов защиты см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

Дополнительные функции программы

Kaspersky Security включает ряд дополнительных функций. Дополнительные функции предусмотрены для поддержки программы в актуальном состоянии, расширения возможностей использования программы, для оказания помощи в работе.

- **Резервное хранилище**. Если в ходе проверки операционной системы защищенной виртуальной машины на вирусы и другие вредоносные программы программа Kaspersky Security обнаруживает зараженный файл, она блокирует этот файл, удаляет его из папки исходного размещения, помещает его копию в *резервное хранилище* и пытается провести лечение файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности. Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. После этого вы можете восстановить файл из его вылеченной резервной копии в папку исходного размещения.

- **Обновление**. Kaspersky Security загружает обновленные базы и модули программы. Это обеспечивает актуальность защиты операционной системы защищенной виртуальной машины от новых вирусов и других вредоносных программ.

- **Отчеты**. В процессе работы программы для каждого компонента и задачи программы формируется отчет. Отчет содержит список событий, произошедших во время работы Kaspersky Security, 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**. С помощью уведомлений Kaspersky Security позволяет пользователю быть в курсе событий о текущем состоянии защиты операционной системы защищенной виртуальной машины. Программа может отображать уведомления на экране или отправлять по электронной почте.

- **Kaspersky Security Network**. Участие в Kaspersky Security Network позволяет повысить эффективность защиты операционной системы защищенной виртуальной машины за счет оперативного получения информации о репутации файлов, веб-ресурсов и программного обеспечения, полученной от пользователей во всем мире.

- **Лицензия**. Использование программы по коммерческой лицензии обеспечивает полнофункциональную работу программы, доступ к обновлению баз и модулей программы, получение подробной информации о программе, а также помощь специалистов Службы технической поддержки «Лаборатории Касперского».

- **Поддержка**. Все зарегистрированные пользователи Kaspersky Security могут обращаться за помощью к специалистам Службы технической поддержки. Вы можете отправить запрос через портал Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/faq/companyaccount_help) или получить консультацию наших сотрудников по телефону.

Управление программой

Настройка и управление работой программы осуществляется:

- удаленно через Kaspersky Security Center (см. раздел «Концепция управления программой через Kaspersky Security Center» на стр. 78);

- через командную строку для Легкого агента для Linux (см. раздел «Управление Легким агентом для Linux из командной строки» на стр. 198);
- через локальный интерфейс для Легкого агента для Windows (см. *Руководство пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*);
- через командную строку для Легкого агента для Windows (см. подробнее в Базе знаний (http://support.kaspersky.ru/13177)).

Что нового

В программе Kaspersky Security для виртуальных сред 4.0 Легкий агент появились следующие возможности:

- Реализован компонент Легкий агент для защиты виртуальных машин с операционной системой Linux (далее также «Легкий агент для Linux»). Компонент Легкий агент для Linux позволяет защищать объекты файловой системы, расположенные на локальных дисках защищенной виртуальной машины. Добавлена возможность создания задачи поиска вирусов и политики для Легкого агента для Linux в Kaspersky Security Center.
- Добавлена поддержка операционной системы Windows Server 2016 в качестве гостевой операционной системы защищенных виртуальных машин.
- Добавлена поддержка операционной системы Microsoft Windows Server 2016 с установленной ролью Hyper-V.
- Добавлена возможность использования для развертывания SVM сервера управления виртуальной инфраструктурой Microsoft System Center Virtual Machine Manager.
- SVM переведена под управление операционной системы CentOS 7.2 (64-разрядная).
- Расширен список программ и компаний-производителей программ, которые вы можете включить в область проверки и защиты или исключить из проверки и защиты в параметрах Легкого агента для Windows. Эти программы используются для администрирования и антивирусной защиты компьютерных сетей.

- Добавлена возможность отключения запуска локального интерфейса Легкого агента для Windows на защищенной виртуальной машине. Отключение запуска интерфейса позволяет уменьшить использование памяти, в том числе при работе на виртуальных машинах с серверной операционной системой в режимах с несколькими пользовательскими сессиями.
- В отчете об использовании ключей отображается информация о виртуальных машинах, для защиты которых используются ключи.

Комплект поставки

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

В комплект поставки входит следующее:

- файлы программы, в том числе образ SVM (виртуальная машина защиты) с установленной операционной системой CentOS 7.2;
- файлы документации к программе;
- Лицензионное соглашение, в котором указано, на каких условиях вы можете пользоваться программой.

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

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

Аппаратные и программные требования

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

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

В этом руководстве описана работа с версией Kaspersky Security Center 10 Service Pack 2.

Требования к виртуальной инфраструктуре

Для работы Kaspersky Security в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров:

- Microsoft Windows Server 2016 Hyper-V (в режиме полной установки или в режиме Server Core) со всеми доступными обновлениями;
- Microsoft Windows Server 2012 R2 Hyper-V (в режиме полной установки или в режиме Server Core) со всеми доступными обновлениями;
- Citrix XenServer 7;
- Citrix XenServer 6.5 Service Pack 1;
- VMware ESXi 6.5 с последними обновлениями;
- VMware ESXi 6.0 с последними обновлениями;
- VMware ESXi 5.5 с последними обновлениями;
- VMware ESXi 5.1 с последними обновлениями;
- KVM (Kernel-based Virtual Machine) на базе одной из следующих операционных систем:
  - Ubuntu Server 14.04 LTS;
  - Red Hat Enterprise Linux® Server 7 исправление 1;
  - CentOS 7.

Для развертывания и работы SVM (виртуальная машина защиты) под управлением гипервизора Vmware ESXi в виртуальной инфраструктуре должен быть установлен сервер VMware vCenter™ 5.1, VMware vCenter 5.5, VMware vCenter 6.0 или VMware vCenter 6.5 со всеми доступными обновлениями. Сервер Vmware vCenter – сервер управления виртуальной инфраструктурой, используется для развертывания SVM и предоставления SVM информации о виртуальной инфраструктуре.

Для развертывания SVM под управлением гипервизоров Microsoft Windows Server Hyper-V, Vmware ESXi и Citrix XenServer вы можете использовать сервер управления виртуальной инфраструктурой Microsoft SCVMM одной из следующих версий:

- Microsoft SCVMM 2012 R2 с последними обновлениями;
- Microsoft SCVMM 2016 с последними обновлениями.

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.

Требования к ресурсам SVM с установленным компонентом Сервер защиты Kaspersky Security

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

- 2 ГБ выделенной оперативной памяти;
- 30 ГБ выделенного свободного места на диске;
- виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Требования к виртуальной машине с установленным компонентом Легкий агент для Windows

Перед установкой компонента Легкий агент для Windows на виртуальной машине под управлением гипервизора Citrix XenServer должна быть установлена программа XenTools.

Перед установкой компонента Легкий агент для Windows на виртуальной машине под управлением гипервизора Vmware ESXi должен быть установлен пакет VMware™ Tools.

На виртуальной машине под управлением гипервизора Microsoft Windows Server (Hyper-V) должен быть установлен пакет служб интеграции (Integration Services).

Для установки и функционирования компонента Легкий агент для Windows на виртуальной машине должна быть установлена одна из следующих гостевых операционных систем:

- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-разрядная);
- Windows 8.1 Update 1 Pro / Enterprise (32 / 64-разрядная);

- Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 (32 / 64-разрядная);
- Windows Server 2008 Service Pack 2 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная);
- Windows Server 2008 R2 Service Pack 1 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная);
- Windows Server 2012 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная);
- Windows Server 2012 R2 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная);
- Windows Server 2016 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная).

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

- Citrix XenDesktop 7.9 или Citrix XenDesktop 7.11;
- Citrix Provisioning Services 7.9 или Citrix Provisioning Services 7.11;
- VMware Horizon™ View 7.

Требования к виртуальной машине с установленным компонентом Легкий агент для Linux

Программные требования для установки и функционирования компонента Легкий агент для Linux:

- интерпретатор языка Perl версии 5.0 или выше http://www.perl.org;
- установленная утилита which;
- установленные пакеты для компиляции программ (gcc, binutils, glibc, glibc-devel, make, ld), исходный код ядра операционной системы – для компиляции модулей Kaspersky Security;

- 32-разрядный пакет libc должен быть установлен на 64-разрядные версии гостевых серверных операционных систем Linux до установки Kaspersky Security;
- установленный пакет dmidecode.

Для установки и функционирования компонента Легкий агент для Linux на виртуальной машине должна быть установлена одна из следующих гостевых серверных операционных систем:

- Debian GNU / Linux 8.5 (32 / 64-разрядная);
- Ubuntu Server 14.04 LTS (32 / 64-разрядная);
- Ubuntu Server 16.04 LTS (64-разрядная);
- CentOS 6.8 (64-разрядная);
- CentOS 7.2 (64-разрядная);
- Red Hat Enterprise Linux Server 6.7 (64-разрядная);
- Red Hat Enterprise Linux Server 7.2 (64-разрядная);
- SUSE Linux Enterprise Server 12 Service Pack 1 (64-разрядная).

На виртуальную машину, где будет установлен Легкий агент для Linux, требуется установить компонент Агент администрирования версии 10.1.1-X, где 10.1.1-X – номер версии. Агент администрирования версии 10.1.1-X входит в комплект поставки программы Kaspersky Security для виртуальных сред 4.0 Легкий агент.

Программные и аппаратные требования для компонента Сервер интеграции

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

- Windows Server 2008 R2 Service Pack 1 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная);
- Windows Server 2012 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная);

- Windows Server 2012 R2 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная);
- Windows Server 2016 все редакции (в режиме полной установки или в режиме Server Core) (64-разрядная).

Для работы Сервера интеграции, Консоли управления Сервера интеграции и плагинов управления Kaspersky Security требуется платформа Microsoft .NET Framework 4.6. Платформа будет установлена автоматически в ходе установки Сервера интеграции, Консоли управления Сервера интеграции и плагинов управления Kaspersky Security.

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

- объем свободного места на диске – 40 МБ;
- объем оперативной памяти:
  - для работы Консоли управления Сервера интеграции – 50 МБ;
  - для работы Сервера интеграции, который обслуживает не более 30 гипервизоров и 2000–2500 защищенных виртуальных машин – 300 МБ. Объем оперативной памяти может изменяться в зависимости от размера виртуальной инфраструктуры.

Архитектура программы

Этот раздел содержит описание компонентов Kaspersky Security и их взаимодействия.

В этом разделе

Об архитектуре программы

Kaspersky Security для виртуальных сред 4.0 Легкий агент представляет собой интегрированное решение, обеспечивающее комплексную защиту виртуальных машин под управлением гипервизора Vmware ESXi, Microsoft Windows Server (Hyper-V), Citrix XenServer или KVM от вирусов и других вредоносных программ, а также от сетевых и мошеннических атак.

Компоненты программы

В состав программы входят следующие компоненты:

- *Сервер защиты Kaspersky Security* (далее также «Сервер защиты»).
- *Легкий агент Kaspersky Security* (далее также «Легкий агент»).
- *Сервер интеграции* (см. раздел «*О Сервере интеграции*» на стр. 37).

Сервер защиты поставляется в виде образа SVM (виртуальная машина защиты).

SVM (secure virtual machine, виртуальная машина защиты – виртуальная машина на гипервизоре, на которой установлен компонент Сервер защиты. SVM следует развернуть на каждом гипервизоре, виртуальные машины которого вы хотите защищать с помощью Kaspersky Security.

Развертывание SVM выполняется с помощью системы удаленного централизованного управления программами «Лаборатории Касперского» Kaspersky Security Center. Развертывание SVM вручную средствами гипервизора не поддерживается.

Легкий агент устанавливается на виртуальные машины с операционной системой Windows (в том числе на шаблоны виртуальных машин и на виртуальный диск, загружаемый с сервера Citrix PVS на виртуальные машины по сети) и на виртуальные машины с операционной системой Linux. *Защищенная виртуальная машина* – виртуальная машина, на которой установлен компонент программы Легкий агент. Легкий агент требуется установить на каждую виртуальную машину, которую вы хотите защищать с помощью Kaspersky Security. Компонент Легкий агент для Windows устанавливается локально на виртуальной машине или удаленно через Kaspersky Security Center или редактор управления групповыми политиками службы каталогов (Active Directory® Group Policies). Компонент Легкий агент для Linux устанавливается локально из командной строки или удаленно через Kaspersky Security Center.

Управление программой

Настройка и управление работой программы осуществляется:

- удаленно через Kaspersky Security Center (см. раздел «Концепция управления программой через Kaspersky Security Center» на стр. 78);
- через командную строку для Легкого агента для Linux (см. раздел «Управление Легким агентом для Linux из командной строки» на стр. 198);
- через локальный интерфейс для Легкого агента для Windows (см. подробнее в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

Взаимодействие программы Kaspersky Security с программой Kaspersky Security Center обеспечивает Агент администрирования, компонент Kaspersky Security Center. Агент администрирования включен в состав образа SVM Kaspersky Security. Если вы хотите управлять работой Легкого агента, установленного на защищенных виртуальных машинах, с помощью Kaspersky Security Center, вам требуется установить Агент администрирования на этих виртуальных машинах. Если Агент администрирования не установлен на защищенной виртуальной машине, управление работой Легкого агента на этой виртуальной машине осуществляется через локальный интерфейс Легкого агента для Windows или через командную строку Легкого агента для Linux.

Интерфейс для управления программой Kaspersky Security через Kaspersky Security Center обеспечивают плагины управления. Плагины управления Kaspersky Security входят в комплект поставки Kaspersky Security. Плагины управления Kaspersky Security должны быть установлены на том компьютере, на котором установлена Консоль администрирования Kaspersky Security Center.

Функции Сервера защиты

При запуске Легкий агент устанавливает и поддерживает соединение с Сервером защиты. По умолчанию Легкий агент подключается к Серверу защиты, установленному на SVM на том же гипервизоре, на котором работает защищенная виртуальная машина (см. раздел «О подключении Легкого агента к SVM» на стр. 34).

Сервер защиты выполняет следующие функции:

- Идентифицирует Легкий агент, установленный на защищенной виртуальной машине.
- Получает информацию об актуальном состоянии виртуальной инфраструктуры и предоставляет ее Легкому агенту и программе Kaspersky Security Center.
- Проверяет файлы всех виртуальных машин, на которых установлен Легкий агент, на наличие вирусов и других вредоносных программ.
- Использует технологию SharedCache, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, уже проверенных на другой виртуальной машине. В ходе работы Kaspersky Security сохраняет в кеше на SVM информацию о проверенных файлах, чтобы не проверять их повторно. Если информация о файле, который нужно проверить, отсутствует в кеше на SVM, Kaspersky Security может использовать при проверке KSN. Службы KSN используются в работе программы, если вы приняли условия участия в программе Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network» на стр. 191).
- Загружает пакет обновлений из хранилища Сервера администрирования Kaspersky Security Center в папку на SVM и обновляет базы программы на SVM. Из папки на SVM на защищенную виртуальную машину загружаются обновления баз и модулей программы, необходимых для работы Легкого агента (см. раздел «Обновление баз и модулей программы» на стр. 129).
- Осуществляет работу с ключами и контроль лицензионных ограничений (см. раздел «Лицензирование программы» на стр. 39).

Варианты развертывания SVM

SVM требуется развернуть на тех гипервизорах в виртуальной инфраструктуре, виртуальные машины которых вы хотите защищать с помощью программы Kaspersky Security.

Гипервизоры VMware ESXi

Предусмотрены следующие варианты развертывания SVM на гипервизорах VMware ESXi:

- Развертывание на автономном гипервизоре VMware ESXi, подключенном к серверу VMware vCenter.
- Развертывание на гипервизорах VMware ESXi, входящих в состав кластера DRS или ресурсного пула.

  После развертывания SVM автоматически прикрепляется к гипервизору, то есть не мигрирует на другие гипервизоры Vmware ESXi в составе кластера DRS или ресурсного пула в соответствии с правилами миграции VMware DRS.

Гипервизоры Citrix XenServer

Предусмотрены следующие варианты развертывания SVM на гипервизорах Citrix XenServer:

- Развертывание на автономном гипервизоре Citrix XenServer.
- Развертывание на гипервизоре, входящем в состав пула гипервизоров Citrix XenServer.

  SVM можно развернуть в локальном хранилище гипервизора или в общем хранилище пула гипервизоров Citrix XenServer.

  SVM, развернутая в общем хранилище, после запуска работает на том гипервизоре в составе пула гипервизоров Citrix XenServer, который имеет наибольшее количество ресурсов и / или наименее загружен. Если на SVM добавлен ключ с ограничением по ядрам, при контроле лицензионных ограничений учитывается количество ядер процессоров на том гипервизоре, на котором работают SVM. При использовании схемы лицензирования по ядрам Сервер защиты может отправлять в Kaspersky Security Center событие с информацией о нарушении лицензионных ограничений. Вы можете игнорировать это событие.

Гипервизоры Microsoft Windows Server (Hyper-V)

Предусмотрены следующие варианты развертывания SVM на гипервизорах Microsoft Windows Server (Hyper-V):

- Развертывание на автономном гипервизоре Microsoft Windows Server (Hyper-V).
- Развертывание на гипервизорах Microsoft Windows Server (Hyper-V), входящих в состав кластера гипервизоров под управлением службы Windows Failover Clustering.

В ходе развертывания SVM на гипервизоре Microsoft Windows Server (Hyper-V) все файлы, необходимые для работы SVM, располагаются в отдельной папке. Этой папке присваивается такое же имя, как у SVM.

► *Чтобы развернуть SVM на кластере гипервизоров Microsoft Windows Server (Hyper-V), выполните следующие действия:*

1. Разверните SVM на каждом гипервизоре, входящем в состав кластера гипервизоров. Если вы хотите обеспечить «горячую» миграцию SVM между узлами кластера, разместите папку с файлами SVM на общем томе кластера (CSV).
2. С помощью консоли Failover Cluster Manager сделайте каждую SVM кластерной виртуальной машиной.
3. В свойствах кластерных ролей каждой SVM в поле **Possible Owners** укажите гипервизор, на котором должна работать SVM. Для этого вы можете использовать консоль Failover Cluster Manager или Microsoft System Center Virtual Machine Manager.

   Подробнее о работе с кластером гипервизоров Microsoft Windows Server (Hyper-V) см. в документации к виртуальной инфраструктуре.

Гипервизоры KVM

Предусмотрены следующие варианты развертывания SVM на гипервизорах KVM:

- Развертывание на автономном гипервизоре KVM.
- Развертывание на гипервизорах KVM, входящих в состав кластера гипервизоров.

  При развертывании SVM на гипервизорах KVM, входящих в состав HA кластера, требуется настроить привязку SVM к узлам кластера. См. подробнее в документации программного обеспечения, используемого для управления ресурсами кластера.

О подключении Легкого агента к SVM

Для функционирования компонента Легкий агент требуется подключение Легкого агента к SVM с установленным Сервером защиты.

Проверка файлов, которые требуется проверять в соответствии с параметрами защиты и в ходе выполнения запущенных задач проверки, выполняется на Сервере защиты. Легкий агент передает файлы на проверку Серверу защиты после подключения к SVM. Если Легкий агент не подключен ни к одной SVM, Сервер защиты не проверяет файлы этой виртуальной машины. Если в ходе выполнения запущенных задач проверки Легкий агент теряет подключение к SVM более чем на 5 минут, выполнение задач проверки приостанавливается, задачи завершаются с ошибкой.

Если Легкий агент не подключен ни к одной SVM более 5 минут, то статус защиты защищенной виртуальной машины в Kaspersky Security Center меняется на *Приостановлена*. Если вы хотите, чтобы в этом случае статус виртуальной машины в Kaspersky Security Center отображался как *Критический*, задайте условие присвоения статуса *Критический*: «Уровень постоянной защиты отличается от уровня, установленного администратором» со значением «Выполняется». Подробнее о настройке условий присвоения статусов см. в документации Kaspersky Security Center.

Чтобы выбрать SVM для подключения, Легкий агент должен получить информацию о SVM, работающих в сети (см. раздел «Об обнаружении SVM» на стр. 35). Легкий агент выбирает оптимальную для подключения SVM в соответствии с алгоритмом выбора SVM (см. раздел «Об алгоритме выбора SVM» на стр. 36).

В этом разделе

Об обнаружении SVM

Легкий агент может обнаруживать SVM, работающие в сети, одним из следующих способов:

- С помощью многоадресной рассылки (Multicast). SVM, для которых выбран этот способ предоставления информации, выполняют многоадресную рассылку информации о себе. Легкие агенты получают эту информацию и формируют список доступных для подключения SVM. Этот способ используется по умолчанию.

  Для использования этого способа предоставления информации необходимо разрешить в сети многоадресную рассылку.

- С помощью Сервера интеграции (см. раздел «О Сервере интеграции» на стр. 37). SVM передают информацию о себе на Сервер интеграции. Сервер интеграции формирует список доступных для подключения SVM и передает Легким агентам.

  Для использования этого способа предоставления информации вам нужно настроить подключение SVM и Легких агентов к Серверу интеграции.

- С использованием списка адресов SVM. Вы можете задать список SVM, к которым могут подключаться Легкие агенты.

Способ, который используют SVM для передачи информации о себе, вы можете указать в политике для Сервера защиты (см. раздел «Шаг 5. Настройка параметров обнаружения SVM» на стр. 90). SVM может передавать информацию о себе одновременно с помощью многоадресной рассылки и с помощью Сервера интеграции.

Способ, который используют Легкие агенты для Windows для обнаружения SVM, вы можете выбрать в политике для Легкого агента для Windows (см. раздел «Шаг 6. Настройка параметров обнаружения SVM» на стр. 102) или в локальном интерфейсе.

Способ, который используют Легкие агенты для Linux для обнаружения SVM, вы можете выбрать в политике для Легкого агента для Linux (см. раздел «Шаг 5. Настройка параметров обнаружения SVM» на стр. 114).

Для Легкого агента вы можете выбрать только один из трех возможных способов обнаружения SVM.

После получения информации о SVM и формирования списка SVM, доступных для подключения, Легкий агент выбирает SVM в соответствии с алгоритмом выбора SVM и подключается к ней (см. раздел «Об алгоритме выбора SVM» на стр. 36).

Вы можете получить информацию о SVM, к которой подключен Легкий агент:

- для Легкого агента для Windows – в локальном интерфейсе Легкого агента для Windows в окне **Поддержка**;
- для Легкого агента для Linux – с помощью команды svminfo (см. раздел «Просмотр информации о SVM» на стр. 200).

Об алгоритме выбора SVM

При выборе SVM для подключения Легкие агенты используют алгоритм выбора с учетом расположения SVM относительно гипервизора, на котором работает Легкий агент, и текущего количества Легких агентов, подключенных к SVM:

1. После установки и запуска на виртуальной машине Легкий агент подключается к SVM, развернутой на том же гипервизоре, на котором работает Легкий агент. Если на гипервизоре развернуто несколько SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов.
2. Если на том гипервизоре, где находится Легкий агент, SVM недоступна, Легкий агент выбирает из числа доступных, развернутых на других гипервизорах ту SVM, к которой подключено наименьшее количество Легких агентов, и подключается к ней.
3. После того как становится доступна SVM на том гипервизоре, на котором работает защищенная виртуальная машина, Легкий агент подключается к этой SVM.

Легкий агент не подключается к SVM, на которой не активирована программа (не добавлен ключ), если в виртуальной инфраструктуре есть SVM, на которых программа активирована. Если программа не активирована ни на одной SVM, Легкий агент подключается к одной из этих SVM в соответствии с алгоритмом выбора. После активации программы на одной или нескольких SVM Легкий агент подключается к одной из этих SVM в соответствии с алгоритмом выбора.

О Сервере интеграции

Сервер интеграции – это компонент программы Kaspersky Security, осуществляющий передачу информации от SVM с установленным Сервером защиты Легким агентам, установленным на защищенных виртуальных машинах. SVM передают на Сервер интеграции информацию, необходимую для подключения Легких агентов к SVM. Легкие агенты получают эту информацию от Сервера интеграции. Вы можете использовать Сервер интеграции для обнаружения SVM и получения информации о них Легкими агентами, если невозможно использование многоадресной рассылки (Multicast).

Если вы хотите использовать Сервер интеграции, вам требуется выполнить следующие действия:

1. Установить Сервер интеграции и Консоль управления Сервера интеграции.
2. Настроить параметры подключения SVM к Серверу интеграции. Настройка параметров подключения выполняется при создании политики для Сервера защиты (см. раздел «Шаг 5. Настройка параметров обнаружения SVM» на стр. 90) или в свойствах политики.
3. Настроить параметры подключения Легких агентов к Серверу интеграции.

   Настройка параметров подключения Легких агентов для Windows к Серверу интеграции выполняется в политике для Легкого агента для Windows (см. раздел «Шаг 6. Настройка параметров обнаружения SVM» на стр. 102) или в локальном интерфейсе Легкого агента для Windows.

   Настройка параметров подключения Легких агентов для Linux к Серверу интеграции выполняется в политике для Легкого агента для Linux (см. раздел «Шаг 5. Настройка параметров обнаружения SVM» на стр. 114).

SVM, для которых настроены параметры подключения к Серверу интеграции, передают информацию на Сервер интеграции каждые 5 минут.

SVM передают на Сервер интеграции следующую информацию:

- IP-адрес и номера портов для подключения к SVM;
- имя гипервизора, на котором работает SVM;

- информацию, на основании которой Легкий агент может определить, какая SVM развернута на том же гипервизоре, на котором работает Легкий агент;
- информацию о лицензии;
- среднее время нахождения запросов на проверку файлов в очереди.

Легкие агенты, для которых настроены параметры подключения к Серверу интеграции, пытаются подключиться к Серверу интеграции каждые 5 минут, если:

- у Легкого агента нет информации ни об одной SVM;
- последняя попытка подключения Легкого агента к Серверу интеграции была неудачной.

После того как Легкие агенты получили от Сервера интеграции информацию о SVM, интервал подключения Легкого агента к Серверу интеграции увеличивается до 30 минут.

Легкие агенты получают от Сервера интеграции список доступных для подключения SVM и информацию о них. С учетом полученной информации Легкие агенты выбирают SVM для подключения.

Во время работы Сервер интеграции сохраняет следующую информацию:

- информацию, необходимую для подключения к Серверу интеграции SVM, Легких агентов и Консоли управления Сервера интеграции;
- параметры, которые требуются для подключения Легких агентов к SVM.

Все данные хранятся в защищенном виде. Информация сохраняется на компьютере, на котором установлен Сервер интеграции, и не отправляется автоматически в «Лабораторию Касперского».

Вы можете настроить параметры Сервера интеграции в Консоли управления Сервера интеграции.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

В этом разделе

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО «Лаборатория Касперского», в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Security.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

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

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

Предусмотрены следующие типы лицензий:

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

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security 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.

Для Kaspersky Security предусмотрены следующие *схемы лицензирования:*

- Лицензирование по количеству виртуальных машин, защищаемых с помощью программы. Для этой схемы лицензирования используются серверные или настольные ключи (в зависимости от операционной системы защищаемых виртуальных машин). В соответствии с лицензионным ограничением программа используется для защиты определенного количества виртуальных машин, на которых установлен компонент Легкий агент.
- 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.

Для всех SVM и подключенных к ним защищенных виртуальных машин рекомендуется использовать только одну из двух предусмотренных схем лицензирования.

О Лицензионном сертификате

*Лицензионный сертифика*т – это документ, который передается вам вместе с файлом ключа или кодом активации.

> Если вы используете программу по подписке, Лицензионный сертификат не предоставляется.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- номер лицензии;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;

- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами «Лаборатории Касперского».

Вы можете добавить ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

После добавления ключей вы можете заменять их другими.

Ключ может быть заблокирован «Лабораторией Касперского», если условия Лицензионного соглашения нарушены. Если ключ заблокирован, вы можете обратиться в Службу технической поддержки или добавить другой ключ для работы программы.

Для Kaspersky Security используются ключи следующих типов:

- *Серверный ключ* – ключ программы для защиты виртуальных машин с серверной операционной системой.
- *Настольный ключ* – ключ программы для защиты виртуальных машин с настольной операционной системой.
- *Ключ с ограничением по ядрам* – ключ программы для защиты виртуальных машин независимо от установленной на них операционной системы. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин, работающих на гипервизорах, в которых используется определенное количество ядер физических процессоров.

Ключ может быть активным и дополнительным.

Активный ключ – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для пробной лицензии, ключ для коммерческой лицензии (коммерческий ключ) или ключ по подписке. На одну SVM не может быть добавлено больше одного активного ключа каждого типа (серверный ключ, настольный ключ, ключ с ограничением по ядрам). Если SVM используется в виртуальной инфраструктуре для защиты виртуальных машин и с серверной, и с настольной операционной системой, на нее добавляется два ключа: серверный и настольный.

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом.

Дополнительный ключ может быть добавлентолько при наличии активного ключа того же типа. Активный и дополнительный ключи должны соответствовать одному типу лицензии.

Ключ для пробной лицензии и ключ по подписке могут быть добавлены только в качестве активного ключа. Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве дополнительного ключа. Ключ для пробной лицензии не может заменить активный коммерческий ключ.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security или после заказа пробной версии Kaspersky Security.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации «Лаборатории Касперского».

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky

CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Способы получения технической поддержки» на стр. 212).

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет «Лаборатория Касперского». Файл ключа предназначен для добавления ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security или после заказа пробной версии Kaspersky Security.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации «Лаборатории Касперского».

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно обратиться в Службу технической поддержки (см. раздел «Способы получения технической поддержки» на стр. 212).

О подписке

Подписка на Kaspersky Security – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Вы можете оформить подписку на Kaspersky Security у поставщика услуг (например, у интернет-провайдера). Вы можете продлевать подписку или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security после окончания ограниченной подписки вам нужно продлить ее (см. раздел «Продление подписки» на стр. 60). Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка приостановлена, вам может предоставляться льготный период для продления подписки, в течение которого программа продолжает выполнять все свои функции. Наличие и длительность льготного периода определяет поставщик услуг.

Если подписка не продлена, по истечении льготного периода программа Kaspersky Security продолжает работу, но прекращает обновлять базы программы и использовать Kaspersky Security Network.

Чтобы использовать Kaspersky Security по подписке, вам нужно применить код активации, предоставленный поставщиком услуг. После применения кода активации в программу добавляется ключ по подписке – активный ключ, соответствующий лицензии на использование программы по подписке. Информация об этом ключе отображается в интерфейсе Kaspersky Security Center (см. раздел «Просмотр информации об используемых ключах» на стр. 61).

SVM, на которых программа используется по подписке, отправляют в Kaspersky Security Center события в случае изменения статуса подписки и изменения параметров подписки на стороне поставщика услуг. Если подписка истекла, статус SVM в Kaspersky Security Center изменяется на *Критический*.

Если вы хотите отказаться от подписки и продолжать использовать программу по коммерческой лицензии, вы можете заранее добавить в программу коммерческий ключ в качестве дополнительного ключа (см. раздел «Продление срока действия лицензии» на стр. 58). Этот ключ автоматически начнет использоваться в качестве активного ключа после окончания ограниченной подписки или после отказа от неограниченной подписки. Чтобы отказаться от подписки, вам нужно связаться с поставщиком услуг, у которого вы приобрели Kaspersky Security.

Ключ по подписке может быть добавлен только в качестве активного ключа. Нельзя добавить ключ по подписке в качестве дополнительного ключа.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security.

Об активации программы

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

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.

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

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

Вы можете добавить ключ в хранилище Kaspersky Security Center одним из следующих способов:

- с помощью файла ключа;
- с помощью кода активации.

Вы можете добавить ключ в хранилище ключей Kaspersky Security Center во время создания задачи активации программы или предварительно (см. раздел «Процедура активации программы» на стр. 50).

После активации программы на SVM компонент Сервер защиты передает сведения о лицензии компоненту Легкий агент, установленному на защищенных виртуальных машинах. Если статус 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 (см. раздел «Просмотр информации о лицензии» на стр. 201).

Информацию о ключах, добавленных на SVM, вы можете посмотреть в Консоли администрирования Kaspersky Security Center (см. раздел «Просмотр информации об используемых ключах» на стр. 61).

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:

- работают только компоненты Легкого агента Файловый Антивирус и Сетевой экран;
- 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.

Если на защищенную виртуальную машину с компонентом Легкий агент для Linux не переданы сведения о лицензии, Легкий агент для Linux функционирует в режиме ограниченной функциональности: обновление баз программы, необходимых для работы Легкого агента, выполняется только один раз.

Если в вашей инфраструктуре установлено несколько экземпляров программы Kaspersky Security под управлением нескольких Серверов администрирования Kaspersky Security Center, не связанных в иерархию, вы можете активировать разные экземпляры программы Kaspersky Security путем добавления одного и того же ключа. Ключ, ранее добавленный на SVM под управлением одного Сервера администрирования Kaspersky Security Center, можно добавить на SVM под управлением другого Сервера администрирования Kaspersky Security Center, если срок действия лицензии, связанной с ключом, не истек.

При контроле лицензионных ограничений учитывается общее количество единиц лицензирования, для которых используется ключ, на всех Серверах администрирования Kaspersky Security Center.

► *Чтобы использовать ранее добавленный ключ без нарушения лицензионных ограничений, выполните следующие действия:*

1. Удалите SVM, на которых программа активирована путем добавления этого ключа, на одном Сервере администрирования Kaspersky Security Center.

2. Создайте и выполните задачу активации программы на другом Сервере администрирования Kaspersky Security Center. Ключ, добавленный в хранилище ключей Kaspersky Security Center, вы можете предварительно экспортировать из одного Сервера администрирования Kaspersky Security Center на другой Сервер администрирования (см. подробнее в документации Kaspersky Security Center).

В этом разделе

Условия для активации программы с помощью кода активации

Для добавления ключа в хранилище ключей Kaspersky Security Center и активации программы с помощью кода активации требуется подключение к серверам активации «Лаборатории Касперского». Мастер добавления ключа в хранилище отправляет данные на серверы активации «Лаборатории Касперского», чтобы проверить введенный код активации. Подключение к серверам активации обеспечивает служба Activation Proxy. Если служба Activation Proxy отключена, добавление ключа в хранилище с помощью кода активации невозможно. Если доступ в интернет осуществляется через прокси-сервер, в свойствах Сервера администрирования Kaspersky Security Center должны быть настроены параметры прокси-сервера.

Подробнее о службе Activation Proxy и параметрах прокси-сервера см. в документации Kaspersky Security Center.

Особенности активации программы с помощью ключей разных типов

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

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

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

> Для защиты виртуальных машин с гостевой операционной системой Linux вы можете использовать только серверные ключи и ключи с ограничением по ядрам.

Если вы добавляете ключ с ограничением по ядрам, а ранее на SVM был добавлен настольный и / или серверный ключ, то в результате выполнения задачи активный и (при наличии) дополнительный настольный и / или серверный ключи удаляются. Вместо них добавляется в качестве активного ключ с ограничением по ядрам.

Если вы добавляете настольный или серверный ключ, а ранее на SVM был добавлен ключ с ограничением по ядрам, то в результате выполнения задачи активный и (при наличии) дополнительный ключи с ограничением по ядрам удаляются. Вместо них добавляется в качестве активного настольный или серверный ключ.

Если вы добавляете коммерческий ключ, а ранее на SVM был добавлен ключ по подписке, то ключ по подписке удаляется. Вместо него добавляется коммерческий ключ.

Если вы добавляете ключ по подписке, а ранее на SVM был добавлен один или несколько коммерческих ключей, то все активные и (при наличии) дополнительные коммерческие ключи удаляются. Вместо них добавляется один ключ по подписке.

Процедура активации программы

► *Чтобы активировать программу, выполните следующие действия:*

1. Создайте задачу активации программы для SVM, на которых вы хотите активировать программу (см. раздел «Создание задачи активации программы» на стр. 52).

   При создании задачи активации программы используется ключ из хранилища ключей Kaspersky Security Center. Вы можете добавить ключ в хранилище ключей Kaspersky Security Center предварительно (см. раздел «Добавление ключа в хранилище ключей Kaspersky Security Center» на стр. 51) или во время создания задачи активации программы.

2. Запустите задачу активации программы (см. раздел «Запуск и остановка задач в Kaspersky Security Center» на стр. 128).

Если вы добавляете активный ключ, задача активирует программу на тех SVM, где отсутствовал активный ключ, и заменит старый ключ на новый на тех SVM, где программа уже активирована:

- Если вы добавляете ключ с ограничением по ядрам, а ранее на SVM был добавлен настольный и / или серверный ключ, то в результате выполнения задачи активный и (при наличии) дополнительный настольный и / или серверный ключи удаляются. Вместо них добавляется в качестве активного ключ с ограничением по ядрам.

- Если вы добавляете настольный или серверный ключ, а ранее на SVM был добавлен ключ с ограничением по ядрам, то в результате выполнения задачи активный и (при наличии) дополнительный ключи с ограничением по ядрам удаляются. Вместо них добавляется в качестве активного настольный или серверный ключ.

- Если вы добавляете коммерческий ключ, а ранее на SVM был добавлен ключ по подписке, то в результате выполнения задачи ключ по подписке удаляется. Вместо него добавляется коммерческий ключ.

- Если вы добавляете ключ по подписке, а ранее на SVM был добавлен один или несколько коммерческих ключей, то в результате выполнения задачи активный и (при наличии) дополнительный коммерческие ключи удаляются. Вместо них добавляется один ключ по подписке.

Если на вашу SVM добавлены и серверный, и настольный ключ, сроком использования программы является наиболее длительный из двух сроков: срок использования программы с серверным ключом или срок использования программы с настольным ключом.

Если количество защищаемых виртуальных машин или количество ядер процессоров, используемых в виртуальной инфраструктуре, превышает количество, указанное в Лицензионном сертификате, Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center событие с информацией о нарушении лицензионных ограничений (см. в документации Kaspersky Security Center).

В этом разделе

Добавление ключа в хранилище ключей Kaspersky Security Center

► *Чтобы добавить ключ в хранилище ключей Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли в папке **Дополнительно** / **Управление программами** выберите вложенную папку **Лицензии на ПО Лаборатории Касперского**.
3. По ссылке **Добавить ключ** в рабочей области запустите мастер добавления ключа в хранилище.
4. В окне мастера **Выбор способа добавления ключа** выберите способ добавления ключа в хранилище:
   - Нажмите на кнопку **Ввести код активации**, если вы хотите добавить ключ с помощью кода активации.
   - Нажмите на кнопку **Указать файл ключа**, если вы хотите добавить ключ с помощью файла ключа.

5. На следующем шаге мастера, в зависимости от выбранного вами способа добавления ключа, выполните одно из следующих действий:

   - Введите код активации.
   - Укажите путь к файлу ключа. Для этого нажмите на кнопку **Выбрать** и в открывшемся окне выберите файл с расширением key.

6. Снимите флажок **Автоматически распространять ключ на управляемые компьютеры**. Перейдите к следующему шагу мастера.

7. Завершите работу мастера добавления ключа в хранилище.

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

Ключи, добавленные в хранилище ключей Kaspersky Security Center, вы можете использовать при создании задачи активации программы на SVM (см. раздел «Создание задачи активации программы» на стр. 52).

Создание задачи активации программы

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

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Выполните одно из следующих действий:

   - Если вы хотите создать задачу активации программы для всех SVM, входящих в состав выбранной группы администрирования, в дереве консоли папке **Управляемые компьютеры** выберите папку с названием этой группы администрирования. В рабочей области выберите закладку **Задачи**. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.

- Если вы хотите создать задачу активации программы для одной или нескольких SVM, запустите мастер создания задачи одним из следующих способов:
  - Откройте папку **Задачи** дерева консоли. Нажмите на кнопку **Создать задачу**.
  - В дереве консоли в папке **Дополнительно** / **Управление программами** выберите вложенную папку **Лицензии на ПО Лаборатории Касперского**. Нажмите на кнопку **Распространить ключ на управляемые компьютеры**.

3. Следуйте указаниям мастера создания задачи.

В этом разделе

Шаг 1. Выбор программы и типа задачи

Если вы запустили мастер создания задачи из папки **Управляемые компьютеры** или из папки **Задачи**, на этом шаге укажите программу, для которой создается задача, и тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты** выберите **Активация программы**.

Если вы запустили мастер создания задачи из папки **Лицензии на ПО Лаборатории Касперского**, на этом шаге укажите программу, для которой создается задача: **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты**.

Перейдите к следующему шагу мастера создания задачи.

Шаг 2. Добавление ключа

На этом шаге выберите ключ изхранилища ключей Kaspersky Security Center.

Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно (см. раздел «Добавление ключа в хранилище ключей Kaspersky Security Center» на стр. 51), нажмите на кнопку **Добавить**. В открывшемся окне **Хранилище ключей Kaspersky Security Center** выберите ключ и нажмите на кнопку **ОК**.

► *Чтобы добавить ключ в хранилище ключей Kaspersky Security Center, выполните следующие действия:*

1. Нажмите на кнопку **Добавить**.

   Откроется окно **Хранилище ключей Kaspersky Security Center**.

2. Нажмите на кнопку **Добавить**, расположенную в нижней части окна. Запустится мастер добавления ключа в хранилище ключей Kaspersky Security Center.

3. Следуйте указаниям мастера, чтобы добавить ключ в хранилище ключей (см. раздел «Добавление ключа в хранилище ключей Kaspersky Security Center» на стр. 51).

4. Завершите работу мастера добавления ключа в хранилище.

После завершения работы мастера выберите добавленный ключ в окне **Хранилище ключей Kaspersky Security Center** и нажмите на кнопку **ОК**.

Если вы хотите использовать выбранный ключ как дополнительный, установите флажок **Использовать ключ в качестве дополнительного**.

Флажок недоступен, если вы добавляете ключ по подписке. Невозможно добавить ключ по подписке в качестве дополнительного ключа.

После того как вы выбрали ключ, в нижней части окна отобразится следующая информация:

- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Тип лицензии** – пробная, коммерческая или коммерческая (подписка).

- **Срок действия лицензии** – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа. Например, 365 дней. Если вы используете программу по неограниченной подписке, в поле отображается <*Недоступно*>.

- **Действует до** – дата окончания срока использования программы, активированной путем добавления этого ключа. Если вы используете программу по неограниченной подписке, в поле отображается <*Неограниченно*>.

- **Льготный период** – количество дней после приостановки подписки, в течение которых программа продолжает выполнять все свои функции. Поле отображается, если вы используете программу по подписке, и поставщик услуг, у которого вы зарегистрировали подписку, предоставляет льготный период для продления подписки.

- **Ограничение** – в зависимости от типа ключа:

  - для серверного ключа – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, для которых включена защита;

  - для настольного ключа – максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой, для которых включена защита;

  - для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

Перейдите к следующему шагу мастера создания задачи.

Шаг 3. Выбор SVM

Этот шаг доступен, если вы запустили мастер создания задачи из папки **Задачи** или из папки **Лицензии на ПО Лаборатории Касперского**.

Укажите способ выбора SVM, для которых вы создаете задачу:

- Нажмите на кнопку **Выбрать компьютеры, обнаруженные в сети Сервером администрирования**, если вы хотите выбрать SVM из списка виртуальных машин,

обнаруженных Сервером администрирования при опросе локальной сети организации.

- Нажмите на кнопку **Задать адреса компьютеров вручную или импортировать из списка**, если вы хотите задать адреса SVM вручную или импортировать список SVM из файла. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

  Если вы импортируете список адресов SVM из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- Нажмите на кнопку **Компьютеры из заданной выборки компьютеров**, если вы хотите создать задачу для выборки SVM по предопределенному критерию.

В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

- В списке обнаруженных виртуальных машин укажите SVM, на которых вы хотите активировать программу. Для этого установите флажок в списке слева от названия SVM.
- Нажмите на кнопку **Добавить** или **Добавить IP-интервал** и вручную задайте адреса SVM.
- Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
- Нажмите на кнопку **Выбрать** и в открывшемся окне укажите название выборки, содержащей SVM, на которых вы хотите активировать программу.

Перейдите к следующему шагу мастера создания задачи.

Шаг 4. Определение параметров расписания запуска задачи

На этом шаге настройте режим запуска задачи активации программы:

- **Запуск по расписанию**. В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Запускать пропущенные задачи**. Если требуется, чтобы программа запускала пропущенную задачу сразу после появления SVM в сети, установите этот флажок.

  Если флажок снят, для режима **Вручную** запуск задачи производится только на видимых в сети SVM.

- **Автоматически определять интервал для распределения запуска задачи**. По умолчанию запуск задачи на SVM распределяется в течение определенного периода времени. Этот период рассчитывается автоматически, в зависимости от количества SVM, на которые распространяется задача:

  - 0–200 SVM – запуск задачи не распределяется;
  - 200–500 SVM – запуск задачи распределяется в течение 5 минут;
  - 500–1000 SVM – запуск задачи распределяется в течение 10 минут;
  - 1000–2000 SVM – запуск задачи распределяется в течение 15 минут;
  - 2000–5000 SVM – запуск задачи распределяется в течение 20 минут;
  - 5000–10000 SVM – запуск задачи распределяется в течение 30 минут;
  - 10000–20000 SVM – запуск задачи распределяется в течение 1 часа;
  - 20000–50000 SVM – запуск задачи распределяется в течение 2 часов;
  - более 50000 SVM – запуск задачи распределяется в течение 3 часов.

Если не требуется распределять запуск задачи в течение автоматически рассчитываемого периода, снимите флажок **Автоматически определять интервал для распределения запуска задачи**. По умолчанию флажок установлен.

- **Распределять запуск задачи случайным образом в интервале (мин.)**. Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента запуска вручную, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае после запуска вручную задача запустится в случайное время в рамках указанного периода. Флажок доступен для изменения, если не установлен флажок **Автоматически определять интервал для распределения запуска задачи**.

Перейдите к следующему шагу мастера создания задачи.

Шаг 5. Определение названия задачи

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

Перейдите к следующему шагу мастера создания задачи.

Шаг 6. Завершение создания задачи

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Завершите работу мастера. Созданная задача активации программы отобразится в списке задач для выбранной группы администрирования на закладке **Задачи** или в папке **Задачи**.

Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска задачи, то задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу активации программы вручную (см. раздел «Запуск и остановка задач в Kaspersky Security Center» на стр. 128).

Продление срока действия лицензии

Когда срок действия лицензии подходит к концу, вы можете его продлить, добавив дополнительный ключ. Это позволит избежать ограничения функциональности программы

в период после истечения срока действия лицензии и до активации программы по новой лицензии.

Для добавления дополнительного ключа на SVM используется задача активации программы.

Тип дополнительного ключа должен соответствовать типу ранее добавленного активного ключа.

Если вы используете схему лицензирования по количеству защищаемых виртуальных машин, тип дополнительного ключа должен соответствовать гостевой операционной системе виртуальных машин: для виртуальных машин с серверной операционной системой предназначен дополнительный серверный ключ, для виртуальных машин с настольной операционной системой – дополнительный настольный ключ.

Если SVM используется в виртуальной инфраструктуре для защиты виртуальных машин и с серверной, и с настольной гостевой операционной системой, для каждого типа операционной системы рекомендуется добавить соответствующий дополнительный ключ.

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

► *Чтобы продлить срок действия лицензии, выполните следующие действия:*

1. Создайте задачу активации программы для SVM, на которые вы хотите добавить дополнительный ключ (см. раздел «Создание задачи активации программы» на стр. 52).

   При создании задачи активации программы используется ключ из хранилища ключей Kaspersky Security Center. Вы можете добавить ключ в хранилище ключей Kaspersky Security Center предварительно (см. раздел «Добавление ключа в хранилище ключей Kaspersky Security Center» на стр. 51) или во время создания задачи активации программы.

2. Установите флажок **Использовать ключ в качестве дополнительного** на шаге 2 мастера создания задачи (см. раздел «Шаг 2. Добавление ключа» на стр. 54).

3. Запустите задачу активации программы (см. раздел «Запуск и остановка задач в Kaspersky Security Center» на стр. 128).

   В результате выполнения задачи дополнительный ключ добавляется на те SVM, на которые уже добавлен активный ключ. Дополнительный ключ автоматически начнет использоваться в качестве активного ключа по истечении срока действия лицензии на Kaspersky Security.

Если для активации программы вы применяете код активации, по истечении срока действия лицензии программа автоматически подключается к серверам активации «Лаборатории Касперского» для замены активного ключа с истекшим сроком годности. Если автоматическое подключение программы к серверам активации «Лаборатории Касперского» завершается с ошибкой, требуется вручную запустить задачу активации программы, чтобы продлить срок действия лицензии на использование Kaspersky Security.

Задача активации программы завершается с ошибкой и дополнительный ключ не добавляется, если выполняется одно из следующих условий:

- активный ключ отсутствует на SVM;
- тип добавляемого дополнительного ключа не соответствует типу ранее добавленного активного ключа.

Если на SVM добавлены активный и дополнительный ключи и вы заменяете активный ключ, Kaspersky Security проверяет дату окончания срока годности дополнительного ключа. Если срок годности дополнительного ключа истекает ранее продленного срока действия лицензии, Kaspersky Security автоматически удаляет дополнительный ключ. В этом случае после добавления активного ключа вы можете добавить другой дополнительный ключ.

Продление подписки

Во время использования программы по подписке Kaspersky Security обращается к серверам активации «Лаборатории Касперского» через определенные промежутки времени вплоть до даты окончания подписки.

Если вы используете программу по неограниченной подписке, Kaspersky Security в фоновом режиме проверяет наличие нового ключа на серверах активации «Лаборатории Касперского» и, в случае его наличия, добавляет новый ключ вместо предыдущего ключа. Таким образом неограниченная подписка на Kaspersky Security продлевается без вашего участия.

Если подписка истекла, Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию об этом и прекращает попытки автоматического продления подписки. Kaspersky Security прекращает обновлять базы программы и использовать Kaspersky Security Network.

Вы можете продлить подписку, связавшись с поставщиком услуг, у которого вы приобрели Kaspersky Security.

После продления подписки вам требуется повторно запустить задачу активации программы, которую вы создали для активации программы по подписке.

Просмотр информации об используемых ключах

Информацию об используемых ключах вы можете просмотреть:

- в папке **Дополнительно** / **Управление программами** дерева консоли, во вложенной папке **Лицензии на ПО Лаборатории Касперского**;
- в свойствах программы, установленной на SVM;
- в свойствах задачи активации программы;
- в отчете об использовании ключей.

В этом разделе

Просмотр информации о ключе в папке Лицензии на ПО Лаборатории Касперского

► *Чтобы просмотреть информацию о ключе в папке Лицензии на ПО Лаборатории Касперского, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Дополнительно** / **Управление программами** дерева консоли выберите папку **Лицензии на ПО Лаборатории Касперского**.

   В рабочей области отобразится список ключей, добавленных в хранилище ключей Kaspersky Security Center.

3. В списке ключей выберите ключ, информацию о котором хотите просмотреть.

   Справа от списка ключей отобразится следующая информация о ключе:

   - **Ключ** – уникальная буквенно-цифровая последовательность.
   - **Тип лицензии** – тип лицензии: пробная, коммерческая или коммерческая (подписка).
   - **Программа** – название программы, которая активирована путем добавления этого ключа, и информация о лицензии.
   - **Срок действия** – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа. Например, 365 дней. Если вы используете программу по подписке, в поле отображается <*Недоступно*>.
   - **Дата окончания срока годности** – дата окончания срока годности ключа. Активировать программу путем добавления этого ключа и использовать эту программу можно только до истечения этого срока.
   - **Дата окончания срока действия лицензии** – дата окончания срока использования программы, активированной путем добавления этого ключа. Если ключ в разное время был добавлен на несколько SVM, в этом поле указана дата для той SVM, на которой срок использования программы оканчивается раньше остальных. Если вы используете программу по неограниченной подписке, в поле отображается <*Неограниченная*>.
   - **Ограничение** – в зависимости от типа ключа:
     - для серверного ключа – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, для которых включена защита;
     - для настольного ключа – максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой, для которых включена защита;

- для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

- **Компьютеров, на которых является активным** – в зависимости от типа ключа:
  - для серверного или настольного ключа – количество защищенных виртуальных машин, для которых ключ используется в качестве активного;
  - для ключа с ограничением по ядрам – количество SVM, на которые ключ добавлен в качестве активного.
- **Компьютеров, на которых является дополнительным** – количество SVM, на которые ключ добавлен в качестве дополнительного.
- **Служебная информация** – в этом поле отображается служебная информация, связанная с ключом и лицензией.

Если вы выбрали в списке ключ по подписке, то справа от списка ключей также отображается следующая информация:

- **Льготный период** – количество дней после приостановки подписки, в течение которых программа продолжает выполнять все свои функции.
- **Веб-адрес провайдера** – веб-адрес поставщика услуг, у которого зарегистрирована подписка.
- **Состояние подписки** – текущий статус подписки (*активна*, *приостановлена*, *остановлена*, *отменена*).
- **Причина состояния подписки** – причина перехода подписки в текущее состояние.

> Сведения о подписке отображаются также в окне свойств ключа по подписке в разделе **О подписке**. Окно свойств ключа открывается по ссылке **Открыть окно свойств ключа**, расположенной справа от списка ключей.

Если на вашу SVM добавлены и серверный, и настольный ключ, в папке **Лицензии на ПО Лаборатории Касперского** Kaspersky Security Center отображает информацию об этих ключах, а также следующую информацию о комбинации серверного ключа и настольного ключа:

- Уникальная буквенно-цифровая последовательность – комбинация серверного ключа и настольного ключа. Вы можете использовать комбинацию серверного и настольного ключа для поиска информации о SVM, на которую добавлены эти ключи (см. подробнее в документации Kaspersky Security Center).

- **Срок действия** – наиболее длительный из двух сроков использования программы: срок использования программы с серверным ключом или срок использования программы с настольным ключом.

- **Дата окончания срока годности** – наиболее поздняя из двух дат окончания срока годности ключа: дата окончания срока годности серверного ключа или дата окончания срока годности настольного ключа.

- **Дата окончания срока действия лицензии** – наиболее поздняя из двух дат: дата окончания использования программы с серверным ключом или дата окончания использования программы с настольным ключом.

- **Ограничение** – сумма следующих значений: максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой и максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, которые вы можете защищать с помощью программы.

- **Компьютеров, на которых является активным** – количество SVM, на которые ключ добавлен в качестве активного.

- **Льготный период** – наиболее длительный из двух льготный периодов: льготный период, соответствующий серверному ключу, или льготный период, соответствующий настольному ключу.

- **Состояние подписки** – в поле указывается статус *активна*, если подписка, соответствующая хотя бы одному из ключей (серверному или настольному), находится в статусе *активна*. Если обе подписки не активны, в поле указывается лучший статус (например, если одна подписка имеет статус *приостановлена*, а вторая – статус *отменена*, то в поле указывается статус *приостановлена*).

Просмотр информации о ключе в свойствах программы

► *Чтобы просмотреть информацию о ключе в свойствах программы, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите посмотреть информацию о ключе.

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

4. В списке выберите SVM, для которой вы хотите посмотреть информацию о ключе.

5. Откройте окно свойств SVM одним из следующих способов:

   - Двойным щелчком мыши.

   - По правой клавише мыши откройте контекстное меню и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Имя SVM>**.

6. В списке слева выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на этой SVM.

7. Выберите **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты** и откройте окно параметров программы одним из следующих способов:

   - По правой клавише мыши откройте контекстное меню и выберите пункт **Свойства**.

   - Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты**.

8. В списке слева выберите раздел **Ключи**.

В правой части окна отобразится информация о ключе, добавленном на SVM. В блоке **Активный ключ** отображается информация об активном ключе, в блоке **Дополнительный ключ** отображается информация о дополнительном ключе. Если дополнительный ключ не добавлен, в блоке **Дополнительный ключ** отображается строка *<Не добавлен>*.

В блоке **Активный ключ** отображается следующая информация о ключе:

- Уникальная буквенно-цифровая последовательность (ключ).
- **Тип лицензии** – пробная, коммерческая или коммерческая (подписка).
- **Дата активации** – дата активации программы путем добавления этого ключа.
- **Дата окончания срока действия лицензии** – дата окончания срока использования программы, активированной путем добавления этого ключа. Если вы используете программу по неограниченной подписке, в поле отображается *<Неограниченная>*.
- **Срок действия** – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа. Например, 365 дней. Если вы используете программу по подписке, в поле отображается *<Недоступно>.*
- **Ограничение** – в зависимости от типа ключа:
  - для серверного ключа – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, для которых включена защита;
  - для настольного ключа – максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой, для которых включена защита;
  - для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

В блоке **Дополнительный ключ** отображается следующая информация о ключе:

- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Тип лицензии** – тип лицензии: коммерческая.

- **Срок действия** – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа. Например, 365 дней.
- **Ограничение** – в зависимости от типа ключа:
  - для серверного ключа – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, для которых включена защита;
  - для настольного ключа – максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой, для которых включена защита;
  - для ключа с ограничением по ядрам – максимальное количество ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

Если на вашу SVM добавлены и серверный, и настольный ключ, в окне свойств программы Kaspersky Security Center отображает следующую информацию о комбинации серверного ключа и настольного ключа:

- Уникальная буквенно-цифровая последовательность – комбинация серверного ключа и настольного ключа. Вы можете использовать комбинацию серверного и настольного ключа для поиска информации о SVM, на которую добавлены эти ключи (см. подробнее в документации Kaspersky Security Center).
- **Дата окончания срока действия лицензии** – наиболее поздняя из двух дат: дата окончания использования программы с серверным ключом или дата окончания использования программы с настольным ключом.
- **Срок действия** – наиболее длительный из двух сроков использования программы: срок использования программы с серверным ключом или срок использования программы с настольным ключом.
- **Ограничение** – сумма следующих значений: максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой и максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, которые вы можете защищать с помощью программы.

Просмотр информации о ключе в свойствах задачи активации программы

► *Чтобы просмотреть информацию о ключе в свойствах задачи активации программы, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Выполните одно из следующих действий:

   - В папке **Управляемые компьютеры** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите посмотреть свойства задачи активации программы. В рабочей области выберите закладку **Задачи**.

   - Выберите папку **Задачи** дерева консоли, если вы хотите посмотреть свойства задачи активации программы, созданной для одной или нескольких SVM.

3. В списке задач выберите задачу, свойства которой вы хотите посмотреть, и выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню и выберите пункт **Свойства**.

   - Откройте окно свойств задачи по ссылке **Изменить параметры задачи**. Ссылка находится справа от списка задач.

   Откроется окно **Свойства: <Название задачи>**.

4. В списке слева выберите раздел **Добавление ключа**.

   В правой части окна отобразится информация о ключе, добавляемом на SVM с помощью этой задачи:

   - **Ключ** – уникальная буквенно-цифровая последовательность.

   - **Тип лицензии** – пробная, коммерческая или коммерческая (подписка).

   - **Срок действия лицензии** – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа. Например, 365 дней. Если вы используете программу по неограниченной подписке, в поле отображается <*Недоступно*>.

- **Действует до** – дата окончания срока использования программы, активированной путем добавления этого ключа. Если ключ в разное время был добавлен на несколько SVM, в этом поле указана дата для той SVM, на которой срок использования программы оканчивается раньше остальных. Если вы используете программу по неограниченной подписке, в поле отображается <*Неограниченно*>.

- **Льготный период** – количество дней после приостановки подписки, в течение которых программа продолжает выполнять все свои функции. Поле отображается, если вы используете программу по подписке, и поставщик услуг, у которого вы зарегистрировали подписку, предоставляет льготный период для продления подписки.

- **Ограничение** – в зависимости от типа ключа:

  - для серверного ключа – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, для которых включена защита;

  - для настольного ключа – максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой, для которых включена защита;

  - для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

Просмотр отчета об использовании ключей

► *Чтобы просмотреть отчет об использовании ключей, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В рабочей области узла **Сервер администрирования** перейдите на закладку **Отчеты** и выберите шаблон отчета «Отчет об использовании ключей».

   В рабочей области отобразится отчет, сформированный по шаблону «Отчет об использовании ключей».

На диаграмме в верхней части окна для каждого ключа отображаются следующие сведения об использовании ключа:

- количество единиц лицензирования, для которых ключ уже используется;
- количество единиц лицензирования, для которых ключ может использоваться в соответствии с лицензионным ограничением;
- количество единиц лицензирования, на которое превышено лицензионное ограничение при использовании ключа.

Отчет об использовании ключей состоит из двух таблиц:

- таблица сводной информации содержит сведения об используемых ключах;
- таблица детальной информации содержит сведения о SVM, на которые добавлены ключи, или о защищенных виртуальных машинах, для которых используется ключ.

Вы можете настроить состав полей, отображаемых в каждой таблице. О добавлении и удалении полей в таблицах отчета см. в документации Kaspersky Security Center.

Таблица сводной информации содержит следующие сведения об используемых ключах:

- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Используется всего в качестве активного** – в зависимости от типа ключа:
  - для серверного и настольного ключа – количество защищенных виртуальных машин, для которых ключ используется в качестве активного;
  - для ключа с ограничением по ядрам – количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.
- **Используется всего в качестве дополнительного** – количество SVM, на которые ключ добавлен в качестве дополнительного.
- **Ограничение** – в зависимости от типа ключа:
  - для серверного ключа – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, для которых включена защита;
  - для настольного ключа – максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой, для которых включена защита;

- для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

- **Дата окончания срока действия лицензии** – дата окончания срока использования программы, активированной путем добавления этого ключа. Если вы используете программу по неограниченной подписке, в поле отображается <*Неограниченная*>.

- **Дата окончания срока годности** – дата окончания срока годности ключа. Активировать программу путем добавления этого ключа и использовать эту программу можно только до истечения этого срока.

- **Дополнительные свойства** – дополнительные свойства ключа.

- **Используется всего в качестве активного для рабочих станций** – количество защищенных виртуальных машин с настольной операционной системой, для которых ключ используется в качестве активного.

- **Используется всего в качестве активного для серверов** – количество защищенных виртуальных машин с серверной операционной системой, для которых ключ используется в качестве активного.

- **Служебная информация** – служебная информация, связанная с ключом и лицензией.

  В строке ниже находится следующая сводная информация:

  - **Ключей** – общее количество используемых ключей.

  - **Ключей, используемых более чем на 90%** – общее количество ключей, которые используются более чем на 90% процентов от лицензионного ограничения. В зависимости от типа ключа в ограничении указывается максимальное количество одновременно запущенных виртуальных машин с серверной или настольной операционной системой, для которых включена защита, или максимальное количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM. Например, в ограничении указано 100 виртуальных машин. Ключ используется на двух SVM, из которых первая защищает 42 виртуальных машины, а вторая – 53 виртуальных машины. Следовательно, этот ключ используется на 95% и включен в число ключей, указанное в этом поле.

- **Ключей с превышенным ограничением** – общее количество ключей, для которых превышено ограничение на количество одновременно запущенных виртуальных машин с серверной или настольной операционной системой или на количество используемых ядер физических процессоров на всех гипервизорах (в зависимости от типа ключа).

В таблице детальной информации в зависимости от типа ключа отображаются сведения о SVM, на которую добавлен ключ (для ключа с ограничением по ядрам), или сведения о защищенной виртуальной машине, для которой используется ключ (для серверного или настольного ключа):

- **Виртуальный сервер** – имя виртуального Сервера администрирования, под управлением которого находится SVM или защищенная виртуальная машина.
- **Группа** – группа администрирования, в которую входит SVM или защищенная виртуальная машина.
- **Клиентский компьютер** – имя SVM или защищенной виртуальной машины.
- **Программа** – название компонента Kaspersky Security, установленного на SVM или на защищенной виртуальной машине.
- **Номер версии** – номер версии программы.
- **Активный ключ** – ключ, который добавлен в качестве активного.
- **Дополнительный ключ** – ключ, который добавлен в качестве дополнительного.
- **Дата окончания срока действия лицензии** – дата окончания использования программы с этим ключом. Если вы используете программу по неограниченной подписке, в поле отображается <*Неограниченная*>.
- **Дата окончания срока годности** – дата окончания срока годности ключа. Активировать программу путем добавления этого ключа и использовать эту программу можно только до истечения этого срока.
- **IP-адрес** – IP-адрес SVM или защищенной виртуальной машины, на которую добавлен ключ.
- **Видим в сети** – дата и время, когда SVM или защищенная виртуальная машина была видна в локальной сети организации последний раз.

- **Последнее соединение с Сервером администрирования** – дата и время последнего соединения SVM или защищенной виртуальной машины с Сервером администрирования Kaspersky Security Center.

- **Домен** – домен, к которому относится SVM или защищенная виртуальная машина.

- **Доменное имя**, **NetBIOS-имя** – имя SVM или защищенной виртуальной машины.

- **DNS-домен** – DNS-домен, к которому относится SVM или защищенная виртуальная машина (указывается, только если имя SVM или защищенной виртуальной машины содержит название DNS-домена).

- **Использовано** – в зависимости от типа активного ключа:

  - для серверного и настольного ключа – количество защищенных виртуальных машин с настольной и серверной операционной системой;

  - для ключа с ограничением по ядрам – количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

- **Использовано для рабочих станций** – для настольного ключа: количество защищенных виртуальных машин с настольной операционной системой.

- **Использовано для серверов** – для серверного ключа: количество защищенных виртуальных машин с серверной операционной системой.

Если на SVM добавлены и серверный, и настольный ключ, в отчете об использовании ключей Kaspersky Security Center отображает информацию об этих ключах, а также следующую информацию о комбинации серверного ключа и настольного ключа:

- **Ключ**, **Активный ключ**, **Дополнительный ключ** – уникальная комбинация серверного ключа и настольного ключа. Вы можете использовать комбинацию серверного и настольного ключа для поиска информации о SVM, на которую добавлены эти ключи (см. подробнее в документации Kaspersky Security Center).

- **Дата окончания срока действия лицензии** – наиболее поздняя из двух дат: дата окончания использования программы с серверным ключом или дата окончания использования программы с настольным ключом.

- **Дата окончания срока годности** – наиболее поздняя из двух дат окончания срока годности ключа: дата окончания срока годности серверного ключа или дата окончания срока годности настольного ключа.

- **Ограничение** – сумма следующих значений: максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой и максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, которые вы можете защищать с помощью программы.

- **Ограничение для рабочих станций** – максимальное количество одновременно запущенных виртуальных машин с настольной операционной системой, которое вы можете защищать с помощью программы.

- **Ограничение для серверов** – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, которое вы можете защищать с помощью программы.

Запуск и остановка программы

Компонент Сервер защиты Kaspersky Security 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 и модулей 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 (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=850)).

Компонент Легкий агент по умолчанию запускается автоматически при запуске операционной системы на защищенной виртуальной машине.

Для Легкого агента для Windows вы можете включить или выключить автоматический запуск программы в локальном интерфейсе (см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

Компонент Сервер интеграции запускается автоматически при запуске операционной системы на компьютере, где установлен Сервер интеграции.

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. 46).

Задачи Kaspersky Security запускаются в соответствии со своим расписанием.

Компоненты Сервер защиты и Легкий агент останавливаются автоматически при завершении работы операционной системы на SVM и защищенной виртуальной машине. Вы можете вручную завершить работу компонентов Сервер защиты и Легкий агент на виртуальных машинах, запустить программу, а также приостановить и возобновить защиту и контроль защищенных виртуальных машин средствами Kaspersky Security Center (см. в документации Kaspersky Security Center).

Остановить и запустить Легкий агент для Windows вы можете также через локальный интерфейс Легкого агента (подробнее см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

Остановить и запустить 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 запустить задачи вручную (см. раздел «Запуск и остановка задачи обновления» на стр. 206).

Компонент Сервер интеграции останавливается автоматически при завершении работы операционной системы на компьютере, где установлен Сервер интеграции.

Состояние защиты виртуальной машины

Виртуальная машина с установленным компонентом Легкий агент в Kaspersky Security Center является аналогом клиентского компьютера.

Информация о состоянии защиты клиентского компьютера в Kaspersky Security Center отображается с помощью статуса клиентского компьютера.

При обнаружении угрозы статус защищенной виртуальной машины изменяется на *Критический* или *Предупреждение*. Если Легкий агент не смог подключиться ни к одной SVM, статус защищенной виртуальной машины изменяется на *Не включена защита*. Подробно о статусах клиентского компьютера см. в документации Kaspersky Security Center.

Информация о работе каждого компонента Kaspersky Security, о выполнении задач, а также о работе программы в целом фиксируется в отчетах.

Сведения о состоянии защиты каждой виртуальной машины с установленным компонентом Легкий агент вы также можете посмотреть в локальном интерфейсе Легкого агента для Windows (см. *Руководство пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*) или с помощью команд из командной строки Легкого агента для Linux (см. стр. 200).

Концепция управления 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 проверки;
  - управлять ключами для программы;
- обновлять базы и модули программы;
- формировать отчеты о событиях, которые произошли во время работы программы;
- удалять программу из виртуальной инфраструктуры.

Управление работой программы Kaspersky Security через Kaspersky Security Center осуществляется при помощи политик и задач:

- *Политики* определяют параметры защиты виртуальных машин и параметры работы компонентов Легкий агент и Сервер защиты (см. раздел «О политиках для Kaspersky Security» на стр. 82).
- *Задачи* реализуют такие функции программы, как активация программы, проверка виртуальных машин, обновление баз и модулей программы (см. раздел «О задачах для Kaspersky Security» на стр. 121).

При помощи 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.

Постоянная защита и проверка виртуальной машины

Этот раздел содержит информацию о том, как Kaspersky Security защищает и проверяет защищенную виртуальную машину.

В этом разделе

О постоянной защите и проверке виртуальной машины

Постоянная защита автоматически включается вместе с программой Kaspersky Security при старте защищенной виртуальной машины и продолжает работать непрерывно. 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), Kaspersky Security перехватывает обращение к этому файлу.

В дополнение к постоянной защите требуется регулярно выполнять *проверку* защищенной виртуальной машины 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.

На виртуальной машине с установленным компонентом Легкий агент для Linux из проверки и защиты исключаются объекты файловой системы /dev, /sys и /proc.

Kaspersky Security проверяет файл на наличие угроз, используя антивирусные базы (см. раздел «Об обновлении баз и модулей программы» на стр. 129). Если Kaspersky Security обнаруживает в файле вредоносный код, Kaspersky Security выполняет над ним выбранные вами действия, например, пытается вылечить файл или удаляет его.

Программа, обратившаяся к файлу, может работать с ним только в случае, если этот файл не заражен или успешно вылечен.

Kaspersky Security перед выполнением действия блокирует доступ к файлу вне зависимости от выбранного действия.

Особенности проверки символических и жестких ссылок

Kaspersky Security позволяет проверять символические и жесткие ссылки на файлы.

Проверка символических ссылок

Задача постоянной защиты проверяет файл, обращение к которому происходит по символической ссылке, только если этот файл входит в область защиты задачи постоянной защиты.

Если файл, обращение к которому происходит по символической ссылке, не входит в область защиты задачи 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.

Управление политиками

Этот раздел содержит информацию о создании и настройке политик для программы Kaspersky Security для виртуальных сред 4.0 Легкий агент. Подробнее о политиках см. в документации Kaspersky Security Center.

В этом разделе

О политиках для Kaspersky Security

Для управления параметрами программы Kaspersky Security для виртуальных сред 4.0 Легкий агент используются следующие политики Kaspersky Security Center:

- **Политика для Сервера защиты**. Политика применяется на всех SVM, входящих в группу администрирования, для которой настроена политика.

  Параметры политики для Сервера защиты включают в себя:

  - общие параметры защиты виртуальных машин и параметры событий (см. в документации Kaspersky Security Center);

  - параметры использования Kaspersky Security Network (KSN) в работе программы (см. раздел «Участие в Kaspersky Security Network» на стр. 191);

- параметры обновления модулей Легкого агента для Windows в ходе обновления баз программы (см. раздел «Включение и выключение обновления модулей Легкого агента для Windows» на стр. 132);

- параметры обнаружения SVM, то есть параметры предоставления Легким агентам информации о SVM (см. раздел «Шаг 5. Настройка параметров обнаружения SVM» на стр. 90);

- дополнительные параметры работы SVM (см. раздел «Отображение параметров политик» на стр. 85).

- **Политика для Легкого агента для Windows**. 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.

  Параметры политики для Легкого агента для Windows включают в себя:

  - общие параметры защиты виртуальных машин и параметры событий (см. в документации Kaspersky Security Center);

  - основные параметры антивирусной защиты;

  - параметры работы компонентов контроля и защиты;

  - параметры обнаружения SVM, работающих в сети, и получения информации о них;

  - дополнительные параметры работы программы (параметры самозащиты, режимы работы, параметры отчетов и хранилища данных, параметры интерфейса).

  Пользователь может изменять параметры, определенные в политике для Легкого агента для Windows, локально на каждой защищенной виртуальной машине через интерфейс программы, если это не запрещено политикой (см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

- **Политика для Легкого агента для Linux**. 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.

  Параметры политики для Легкого агента для Linux включают в себя:

  - общие параметры защиты виртуальных машин и параметры событий (см. в документации Kaspersky Security Center);
  - основные параметры антивирусной защиты;
  - параметры работы компонента Файловый Антивирус;
  - параметры обнаружения SVM, работающих в сети, и получения информации о них;
  - параметры резервного хранилища.

Возможность изменять параметр программы локально на защищенной виртуальной машине определяется статусом «замка» у параметра в политике:

- 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.

Вы можете выполнять следующие действия над политикой:

- создавать политику;
- изменять параметры политики;
- удалять политику;
- изменять состояние политики.

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

Отображение параметров политик

По умолчанию в мастере создания политики для Сервера защиты и в свойствах политики для Сервера защиты не отображаются дополнительные параметры работы SVM (см. раздел «Шаг 6. Настройка дополнительных параметров работы SVM» на стр. 91).

Если вы хотите настраивать эти параметры с помощью политики, вам требуется предварительно создать ключ AdvancedUI типа 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\3.4.0.0\Settings\ (для 32-разрядной операционной системы);
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\SVM\3.4.0.0\Settings\ (для 64-разрядной операционной системы).

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 компьютеры** дерева консоли выберите папку с названием группы администрирования, для SVM которой вы хотите создать политику.

   На закладке **Компьютеры** 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 **Создать политику**, чтобы запустить мастер создания политики.
5. Следуйте указаниям мастера создания политики.

В этом разделе

Шаг 1. Определение названия групповой политики для программы

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

Перейдите к следующему шагу мастера создания политики.

Шаг 2. Выбор программы для создания групповой политики

На этом шаге в списке **Название программы** выберите **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты**.

Перейдите к следующему шагу мастера создания политики.

Шаг 3. Настройка параметров KSN

На этом шаге вам предлагается принять участие в программе Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network» на стр. 191).

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

В зависимости от расположения инфраструктуры различают:

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

Участие в Kaspersky Security Network добровольное. Перед принятием решения об участии в Kaspersky Security Network внимательно ознакомьтесь с Положением о Kaspersky Security Network или с Положением о Kaspersky Private Security Network, в зависимости от того, какой тип KSN использует Kaspersky Security. Чтобы ознакомиться с Положением, нажмите на кнопку **Положение о KSN**.

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

► *Чтобы настроить параметры использования KSN в работе программы, выполните следующие действия:*

1. Установите флажок **Принимаю условия Положения и участвую в KSN**.

   Установка флажка **Принимаю условия Положения и участвую в KSN** означает, что вы согласны с условиями участия в программе Kaspersky Security Network, изложенными в Положении о Kaspersky Security Network.

2. Если вы хотите, чтобы программа Kaspersky Security использовала KSN при проверке файлов, установите флажок **Использовать для проверки файлов и категоризации**.

   Флажок включает / выключает использование служб KSN в работе следующих компонентов Легкого агента и задач:

   - Контроль запуска программ.
   - Контроль активности программ.
   - Файловый Антивирус.
   - Мониторинг системы.
   - Задачи проверки.

   Если флажок установлен, то в ходе работы перечисленных компонентов Легкого агента и задач программа Kaspersky Security получает от служб KSN сведения о категории и репутации проверяемых файлов.

   Если флажок снят, то Kaspersky Security не получает от служб KSN сведения о репутации и категории файлов.

   Флажок доступен, если установлен флажок **Принимаю условия Положения и участвую в KSN**.

3. Если вы хотите, чтобы программа Kaspersky Security использовала KSN для проверки веб-адресов, установите флажок **Использовать для проверки веб-адресов**.

   Флажок включает / выключает использование служб KSN в работе следующих компонентов Легкого агента для Windows:

   - Веб-Антивирус.
   - Веб-Контроль.
   - IM-Антивирус.

   Если флажок установлен, то в ходе работы перечисленных компонентов Легкого агента для Windows программа Kaspersky Security получает от служб KSN сведения о репутации проверяемых веб-адресов.

   Если флажок снят, то Kaspersky Security не получает от служб KSN сведения о репутации веб-адресов.

   Флажок доступен, если установлен флажок **Принимаю условия Положения и участвую в KSN**.

4. Если вы хотите запретить или разрешить изменение параметров KSN в политиках вложенного уровня иерархии (для вложенных групп администрирования), нажмите на значок «замок» слева от флажка **Принимаю условия Положения и участвую в KSN**.

Перейдите к следующему шагу мастера создания политики.

Шаг 4. Настройка параметров обновления

На этом шаге вы можете настроить обновление модулей программы (модулей компонента Легкий агент для Windows) в ходе обновления баз программы на защищенной виртуальной машине. По умолчанию программа Kaspersky Security не включает обновления модулей программы в пакет обновлений.

Если вы хотите включить обновление модулей Легкого агента для Windows, установите флажок **Обновлять модули программы**.

Перейдите к следующему шагу мастера создания политики.

Шаг 5. Настройка параметров обнаружения SVM

На этом шаге укажите, каким способом SVM будут передавать информацию о себе Легким агентам.

- **Использовать многоадресную рассылку (Multicast)**.

  Если флажок установлен, то SVM передают Легким агентам информацию о себе с помощью многоадресной рассылки (Multicast).

  Если флажок снят, многоадресная рассылка не используется.

  По умолчанию флажок установлен.

- **Использовать Сервер интеграции**.

  Если флажок установлен, то SVM передают на Сервер интеграции информацию, необходимую для подключения к ним Легких агентов. Если вы хотите использовать Сервер интеграции, вам требуется указать параметры подключения SVM к Серверу интеграции.

  Если флажок снят, информация об SVM не передается на Сервер интеграции.

  По умолчанию флажок установлен.

Если установлен флажок **Использовать Сервер интеграции**, укажите параметры подключения SVM к Серверу интеграции.

► *Чтобы указать параметры подключения SVM к Серверу интеграции, выполните следующие действия:*

1. 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) Сервера интеграции.

2. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.

3. Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен, или ваша учетная запись не входит в 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.

   При переходе к следующему шагу мастера выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, переход к следующему шагу невозможен. Проверьте введенные параметры подключения. Информация об ошибках подключения к Серверу интеграции записывается в журнал работы Сервера интеграции (см. раздел «О журналах Сервера интеграции» на стр. 224).

Если вы сняли оба флажка **Использовать многоадресную рассылку (Multicast)** и **Использовать Сервер интеграции**, вам нужно указать список адресов SVM, к которым могут подключаться Легкие агенты, в политике для Легкого агента для Windows (см. раздел «Шаг 6. Настройка параметров обнаружения SVM» на стр. 102) и в политике для Легкого агента для Linux (см. раздел «Шаг 5. Настройка параметров обнаружения SVM» на стр. 114).

Перейдите к следующему шагу мастера.

Шаг 6. Настройка дополнительных параметров работы SVM

Этот шаг доступен, если вы включили отображение дополнительных параметров политики для Сервера защиты в реестре операционной системы (см. раздел «Отображение параметров политик» на стр. 85).

На этом шаге укажите 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 пользователь запустил вручную. Для SVM такие задачи проверки являются высокоприоритетными.

  По умолчанию одновременно выполняется пять высокоприоритетных задач проверки.

Перейдите к следующему шагу мастера.

Шаг 7. Создание групповой политики для программы

Завершите работу мастера создания политики.

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

При следующем подключении SVM к Серверу администрирования Kaspersky Security Center передаст информацию программе Kaspersky Security, политика распространится на 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 вы выбрали вариант **Неактивная политика**, созданная политика не применяется на SVM.

Настройка отображения параметров контроля в Консоли администрирования

По умолчанию в мастере создания политики для Легкого агента и всвойствах политики для Легкого агента неотображаются параметры работы компонентов контроля Легкого агента:

- Контроль запуска программ.
- Контроль активности программ.
- Контроль устройств.
- Веб-Контроль.

О работе компонентов контроля Легкого агента см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

Если вы хотите настраивать параметры работы компонентов контроля Легкого агента с помощью политики для Легкого агента, вам требуется предварительно настроить отображение параметров контроля в интерфейсе Консоли администрирования Kaspersky Security Center.

► *Чтобы настроить отображение параметров контроля в Консоли администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите Сервер администрирования и откройте окно **Настройка интерфейса** одним из следующих способов:
   - с помощью пункта контекстного меню **Вид** → **Настройка интерфейса**;
   - по ссылке **Настроить функциональность, отображаемую в пользовательском интерфейсе**, расположеннй в рабочей области в блоке **Сервер администрирования**.
3. В окне **Настройка интерфейса** установите флажок **Отображать параметры контроля рабочего места**.
4. Нажмите на кнопку **ОК**, чтобы закрыть окно.

Изменения вступят в силу после перезапуска Консоли администрирования Kaspersky Security Center.

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 компьютеры** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите создать политику.

   На закладке **Компьютеры** 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 **Создать политику**, чтобы запустить мастер создания политики.
5. Следуйте указаниям мастера создания политики.

В этом разделе

Шаг 1. Определение названия групповой политики для программы

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

Перейдите к следующему шагу мастера создания политики.

Шаг 2. Выбор программы для создания групповой политики

На этом шаге в списке **Название программы** выберите **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows**.

Перейдите к следующему шагу мастера создания политики.

Шаг 3. Импорт параметров Легкого агента

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 в формате CFG, который вы можете создать в локальном интерфейсе Легкого агента (см. подробнее в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

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**.

На следующих шагах мастера создания политики вы можете изменить значения параметров, перенесенных из конфигурационного файла.

Перейдите к следующему шагу мастера создания политики.

Шаг 4. Настройка параметров контроля

> Этот шаг доступен, если в параметрах интерфейса Консоли администрирования Kaspersky Security Center включено отображение параметров контроля (см. раздел «Настройка отображения параметров контроля в Консоли администрирования» на стр. 93).

На этом шаге вы можете настроить параметры контроля виртуальных машин. В окне мастера отображается список компонентов контроля Легкого агента.

Вы можете выполнить следующие действия:

- включить или отключить компоненты контроля;
- настроить параметры каждого компонента контроля;
- запретить или разрешить изменение параметров каждого компонента контроля через локальный интерфейс Легкого агента. 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 указаны в политике.

► *Чтобы включить или отключить компоненты контроля, выполните следующие действия:*

- Если вы хотите включить компонент контроля, установите флажок слева от названия компонента в списке.
- Если вы хотите отключить компонент контроля, снимите флажок слева от названия компонента в списке.

По умолчанию включены все компоненты контроля.

► *Чтобы настроить параметры компонента контроля, выполните следующие действия:*

1. Выберите компонент контроля в списке и нажмите на кнопку **Изменить**, расположенную над списком компонентов контроля.

   Откроется окно **Настройка: <Название компонента>**.

2. Настройте параметры работы выбранного компонента контроля. Эти параметры Kaspersky Security использует на защищенных виртуальных машинах после применения политики.

   Подробную информацию о настройке параметров каждого компонента контроля см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

3. Нажмите на кнопку **ОК** в окне **Настройка: <Название компонента>**, чтобы сохранить изменения и закрыть окно настройки.

► *Чтобы запретить или разрешить изменение параметров компонента контроля в локальном интерфейсе Легкого агента, выполните одно из следующих действий:*

- Если вы хотите запретить изменение параметров в локальном интерфейсе Легкого агента, выполните следующие действия:
  - Выберите компонент контроля в списке и нажмите на кнопку **Закрыть**. Кнопка расположена над списком компонентов контроля.
  - Нажмите на значок «замок» слева от названия компонента контроля.

- Если вы хотите разрешить изменение параметров в локальном интерфейсе Легкого агента, выполните следующие действия:

  - Выберите компонент контроля в списке и нажмите на кнопку **Открыть**. Кнопка расположена над списком компонентов контроля.

  - Нажмите на значок «замок» слева от названия компонента контроля.

Перейдите к следующему шагу мастера создания политики.

Шаг 5. Настройка параметров защиты

На этом шаге вы можете настроить параметры защиты виртуальных машин. В окне мастера отображается список компонентов защиты Легкого агента для Windows.

Вы можете выполнить следующие действия:

- Настроить основные параметры защиты, в том числе включить технологию лечения активного заражения.

- Включить или отключить компоненты защиты.

- Настроить параметры каждого компонента защиты.

- Запретить или разрешить изменение параметров каждого компонента защиты через локальный интерфейс Легкого агента для Windows.

  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 указаны в политике.

► *Чтобы настроить основные параметры защиты, выполните следующие действия:*

1. Выберите в списке компонентов раздел **Основные параметры защиты**.

2. Нажмите на кнопку **Изменить**, расположенную над списком компонентов защиты.

   Откроется окно **Настройка: Управление защитой**.

3. Установите флажок **Запускать Kaspersky Security для виртуальных сред 4.0 Легкий агент при включении виртуальной машины**, если вы хотите, чтобы программа Kaspersky Security запускалась после загрузки операционной системы и защищала виртуальную машину в течение всего сеанса работы.

4. Установите флажок **Применять технологию лечения активного заражения**, если вы хотите использовать специальную технологию лечения активного заражения для виртуальных машин с серверной операционной системой (см. раздел «Включение и выключение технологии лечения активного заражения для серверных операционных систем» на стр. 189).

   Если Легкий агент работает на временной виртуальной машине, технология лечения активного заражения не используется. В случае активного заражения 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.

   По умолчанию технология лечения активного заражения для виртуальных машин с серверной операционной системой выключена. Для лечения активного заражения на файловом сервере требуется запустить групповую задачу поиска вирусов (см. раздел «Управление задачами» на стр. 121). После окончания процедуры лечения активного заражения выполняется перезагрузка виртуальной машины.

   Включение и выключение технологии лечения активного заражения для виртуальных машин с настольной операционной системой выполняется в локальном интерфейсе Легкого агента. Подробнее о технологии лечения активного заражения см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

5. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка** и в открывшемся окне **Объекты для обнаружения** установите флажки для типов объектов, которые должна обнаруживать программа Kaspersky Security (подробнее см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

   Обратите внимание, что обнаруженные объекты могут быть удалены программой.

6. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка** и в открывшемся окне **Доверенная зона** настройте список исключений из защиты Kaspersky Security (см. раздел «Настройка исключений из защиты через Kaspersky Security Center» на стр. 155). Эти параметры Kaspersky Security Center переносит на защищенные виртуальные машины при применении политики.

   > Если на вашей виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из защиты, добавив ее в исключения.

7. В блоке **Контролируемые порты** настройте режим контроля сетевых портов, в котором Файловый Антивирус, Почтовый Антивирус и Веб-Антивирус проверяют входящие и исходящие потоки данных. Подробнее о контроле сетевого трафика см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

8. Нажмите на кнопку **ОК** в окне **Настройка: Управление защитой**, чтобы сохранить изменения и закрыть окно настройки.

Настроенные параметры Kaspersky Security Center переносит на защищенные виртуальные машины при применении политики.

► *Чтобы включить или отключить компоненты защиты, выполните следующие действия:*

- Если вы хотите включить компонент защиты, установите флажок слева от названия компонента в списке.
- Если вы хотите отключить компонент защиты, снимите флажок слева от названия компонента в списке.

По умолчанию все компоненты защиты включены.

► *Чтобы настроить параметры компонента защиты, выполните следующие действия:*

1. Выберите компонент защиты в списке и нажмите на кнопку **Изменить**, расположенную над списком компонентов защиты.

   Откроется окно **Настройка: <Название компонента>**.

2. Настройте параметры работы выбранного компонента защиты. Эти параметры Kaspersky Security использует на защищенных виртуальных машинах после применения политики.

   Подробную информацию о настройке параметров каждого компонента защиты см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

3. Нажмите на кнопку **ОК** в окне **Настройка: <Название компонента>**, чтобы сохранить изменения и закрыть окно настройки.

► *Чтобы запретить или разрешить изменение параметров компонента защиты в локальном интерфейсе Легкого агента, выполните одно из следующих действий:*

- Если вы хотите запретить изменение параметров в локальном интерфейсе Легкого агента, выполните одно из следующих действий:

  - Выберите компонент защиты в списке и нажмите на кнопку **Закрыть**. Кнопка расположена над списком компонентов защиты.

  - Нажмите на значок «замок» слева от названия компонента защиты.

- Если вы хотите разрешить изменение параметров в локальном интерфейсе Легкого агента, выполните одно из следующих действий:

  - Выберите компонент защиты в списке и нажмите на кнопку **Открыть**. Кнопка расположена над списком компонентов защиты.

  - Нажмите на значок «замок» слева от названия компонента защиты.

Перейдите к следующему шагу мастера создания политики.

Шаг 6. Настройка параметров обнаружения SVM

На этом шаге выберите способ, который Легкие агенты используют для обнаружения SVM, работающих в сети, и получения информации о них:

- **Использовать многоадресную рассылку (Multicast)**.

  Если выбран этот вариант, компонент Легкий агент получает информацию об SVM с помощью многоадресной рассылки (Multicast).

  Этот вариант выбран по умолчанию.

- **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 требуется указать параметры подключения Легких агентов к Серверу интеграции.

- **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 Сервер интеграции**, укажите параметры подключения Легких агентов к Серверу интеграции.

► *Чтобы указать параметры подключения Легких агентов к Серверу интеграции, выполните следующие действия:*

1. 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) Сервера интеграции.

2. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.

3. Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен, или ваша учетная запись не входит в 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.

   При переходе к следующему шагу мастера выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, переход к следующему шагу невозможен. Проверьте введенные параметры подключения. Информация об ошибках подключения к Серверу интеграции записывается в журнал работы Сервера интеграции (см. раздел «О журналах Сервера интеграции» на стр. 224).

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную**, сформируйте список SVM.

► *Чтобы сформировать список SVM, выполните следующие действия:*

1. Нажмите на кнопку **Добавить**, расположенную над списком адресов SVM.

   Откроется окно **Адреса SVM**.

2. 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.

3. Нажмите на кнопку **ОК** 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.

4. 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.

Перейдите к следующему шагу мастера.

Шаг 7. Настройка доверенной зоны

На этом шаге вы можете сформировать доверенную зону.

Доверенная зона – это сформированный администратором системы список файлов, папок, объектов и программ, которые Kaspersky Security не контролирует в процессе работы. Подробнее о доверенной зоне см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

Список окна **Исключения** содержит названия программ или названия компаний-производителей программ, которые вы можете включить в доверенную зону или исключить из доверенной зоны. Перечисленные программы используются для администрирования и антивирусной защиты компьютерных сетей. Вы можете настроить параметры доверенной зоны в свойствах политики для Легкого агента для Windows или в параметрах Легкого агента в локальном интерфейсе программы (см. *Руководство пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows)*.

► *Чтобы настроить доверенную зону, выполните следующие действия:*

1. Выберите в списке название нужной программы или компании-производителя программ.

2. Выполните одно из следующих действий:

   - если вы хотите включить программу или программы компании-производителя в доверенную зону, установите флажок слева от названия программы или компании-производителя;

   - если вы хотите исключить программу или программу компании-производителя из доверенной зоны, снимите флажок слева от названия программы или компании-производителя.

> Если установлены флажки **Citrix EdgeSite**, **Citrix Profile Manager**, **Citrix Provisioning Services**, **Citrix XenApp** и **Citrix XenDesktop**, то файлы, папки и процессы, рекомендованные для этих программ, включаются в доверенную зону, а исполняемые файлы этих программ автоматически добавляются в список доверенных программ. Исключения применяются для настольных и серверных операционных систем. Полный список рекомендованных исключений вы можете посмотреть на веб-сайте Citrix http://blogs.citrix.com/2013/09/22/citrix-consolidated-list-of-antivirus-exclusions/. Флажки **Citrix EdgeSite**, **Citrix Profile Manager**, **Citrix Provisioning Services**, **Citrix XenApp** и **Citrix XenDesktop** установлены по умолчанию для улучшения производительности этих программ.

Помимо программ, указанных в списке, в доверенную зону по умолчанию включаются программы, рекомендованные для настольных и серверных операционных систем.

Если вы хотите исключить из доверенной зоны программы, рекомендованные для настольных операционных систем, снимите флажок **Создать рекомендованные исключения для настольных операционных систем**.

Если вы хотите исключить из доверенной зоны программы, рекомендованные для серверных операционных систем, снимите флажок **Создать рекомендованные исключения для серверных операционных систем**.

Перейдите к следующему шагу мастера создания политики.

Шаг 8. Настройка интерфейса Легкого агента

На этом шаге вы можете выполнить следующие действия:

- Настроить параметры взаимодействия локального интерфейса Легкого агента с пользователем.
- Настроить параметры уведомлений о событиях, происходящих во время работы Легкого агента.
- Настроить отображение информации о поддержке пользователя в локальном интерфейсе Легкого агента.
- Запретить или разрешить изменение параметров интерфейса, параметров уведомлений и параметров отображения информации о поддержке через локальный интерфейс Легкого агента.

  Если изменение параметров через локальный интерфейс запрещено, Kaspersky Security использует на всех защищенных виртуальных машинах параметры, заданные политикой. Если изменение параметров через локальный интерфейс разрешено, Kaspersky Security использует локальные значения параметров работы программы, а не те, которые указаны в политике.

Чтобы обеспечить возможность работы программы Kaspersky Security на виртуальной машине, на которой используется технология Citrix XenApp, требуется снять флажок **Запускать локальный интерфейс программы**.

Если вы используете Легкий агент на временных виртуальных машинах, для повышения производительности виртуальной инфраструктуры рекомендуется снять флажок **Запускать локальный интерфейс программы**.

► *Чтобы настроить параметры уведомлений о событиях, происходящих во время работы Легкого агента, выполните следующие действия:*

1. Нажмите на кнопку **Настройка** в блоке **Уведомления**.

   Откроется окно **Уведомления**.

2. Настройте использование уведомлений о событиях и запись информации о событиях в журнал программы и журнал событий Windows. Подробнее о настройке уведомлений см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

3. Нажмите на кнопку **ОК** в окне **Уведомления**, чтобы сохранить изменения и закрыть окно.

► *Чтобы настроить отображение информации о поддержке пользователя в локальном интерфейсе Легкого агента, выполните следующие действия:*

1. Нажмите на кнопку **Настройка** в блоке **Поддержка пользователей**.

   Откроется окно **Информация о поддержке**.

2. Сформируйте список ссылок на веб-ресурсы, который будет отображаться в локальном интерфейсе Легкого агента. Для добавления, изменения, удаления и перемещения ссылок в списке используйте кнопки, расположенные над списком.

3. Нажмите на кнопку **ОК** в окне **Информация о поддержке**, чтобы сохранить изменения и закрыть окно.

► *Чтобы запретить или разрешить изменение параметров интерфейса, параметров уведомлений и параметров отображения информации о поддержке пользователя через локальный интерфейс Легкого агента,*

нажмите на значок «замок» слева от нужного блока параметров.

Перейдите к следующему шагу мастера создания политики.

Шаг 9. Защита доступа к функциям и параметрам Легкого агента

На этом шаге вы можете настроить защиту доступа ко всем или отдельным функциям и параметрам Легкого агента с помощью пароля. Если защита доступа включена, для доступа к функциям и параметрам Легкого агента на защищенной виртуальной машине пользователь должен ввести имя пользователя и пароль. По умолчанию защита доступа отключена.

► *Чтобы включить защиту доступа к функциям и параметрам Легкого агента, выполните следующие действия:*

1. Установите флажок **Включить защиту паролем**.
2. Введите имя пользователя в поле **Имя пользователя**.
3. Введите пароль в полях **Пароль** и **Подтверждение пароля**.
4. Нажмите на кнопку **Настройка**, чтобы выбрать операции с Легким агентом, которые должны быть защищены паролем.

   Откроется окно **Параметры защиты паролем**.
5. В открывшемся окне укажите операции с Легким агентом, для выполнения которых пользователь должен ввести пароль:

   - все операции (кроме уведомлений об опасности);
   - изменение параметров работы программы;
   - завершение работы программы;
   - включение компонентов защиты;
   - включение компонентов контроля;
   - выключение компонентов защиты и остановка задач проверки;
   - выключение компонентов контроля;
   - выключение политики Kaspersky Security Center;
   - удаление / изменение / восстановление программы;
   - просмотр отчетов.

   По умолчанию паролем защищаются все операции с Легким агентом.

Перейдите к следующему шагу мастера создания политики.

Шаг 10. Создание групповой политики для программы

Завершите работу мастера создания политики.

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

При следующем подключении виртуальной машины к Серверу администрирования Kaspersky Security Center передаст информацию программе Kaspersky Security, политика распространится на защищенные виртуальные машины. 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 вы выбрали вариант **Неактивная политика**, созданная политика не применяется на защищенных виртуальных машинах.

Если сведения о лицензии не переданы на защищенную виртуальную машину, компонент Легкий агент функционирует в режиме ограниченной функциональности (см. раздел «Об активации программы» на стр. 46).

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 компьютеры** дерева консоли выберите папку с названием группы администрирования, для защищенных виртуальных машин которой вы хотите создать политику.

На закладке **Компьютеры** 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 **Создать политику**, чтобы запустить мастер создания политики.
5. Следуйте указаниям мастера создания политики.

В этом разделе

Шаг 1. Определение названия групповой политики для программы

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

Перейдите к следующему шагу мастера создания политики.

Шаг 2. Выбор программы для создания групповой политики

На этом шаге в списке **Название программы** выберите **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Linux**.

Перейдите к следующему шагу мастера создания политики.

Шаг 3. Импорт параметров Легкого агента

На этом шаге вы можете перенести в создаваемую политику параметры Легкого агента для Linux, сохраненные ранее в конфигурационный файл в формате CFG.

Для этого 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**.

На следующих шагах мастера создания политики вы можете изменить значения параметров, перенесенных из конфигурационного файла.

Перейдите к следующему шагу мастера создания политики.

Шаг 4. Настройка параметров защиты

На этом шаге вы можете настроить параметры защиты виртуальных машин. В окне мастера отображается список компонентов защиты Легкого агента для Linux.

Вы можете выполнить следующие действия:

- Настроить основные параметры защиты, в том числе включить технологию лечения активного заражения.
- Включить или отключить компонент Файловый Антивирус.
- Настроить параметры компонента Файловый Антивирус.
- Запретить или разрешить изменение параметров в политиках вложенного уровня иерархии.

  Если в политике для параметра установлен «замок», переопределить значение будет невозможно (подробнее см. в документации Kaspersky Security Center).

► *Чтобы настроить основные параметры защиты, выполните следующие действия:*

1. Выберите в списке компонентов раздел **Основные параметры защиты**.

   Откроется окно **Настройка: Управление защитой**.

2. Установите флажок **Запускать Kaspersky Security для виртуальных сред 4.0 Легкий агент при включении виртуальной машины**, если вы хотите, чтобы программа Kaspersky Security запускалась после загрузки операционной системы и защищала виртуальную машину в течение всего сеанса работы.

3. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка** и в открывшемся окне **Доверенная зона** настройте список исключений из защиты Kaspersky Security (см. раздел «Настройка исключений из защиты через Kaspersky Security Center» на стр. 155). Эти параметры Kaspersky Security Center переносит на защищенные виртуальные машины при применении политики.

   Помимо добавленных на этом шаге исключений из защиты исключены объекты файловой системы /dev, /sys и /proc.

   > Если на вашей виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из защиты, добавив ее в исключения.

4. Нажмите на кнопку **ОК** в окне **Настройка: Управление защитой**, чтобы сохранить изменения и закрыть окно настройки.

► *Чтобы включить или отключить компонент Файловый Антивирус, выполните следующие действия:*

- Если вы хотите включить работу компонента Файловый Антивирус, установите флажок слева от названия компонента в списке.

- Если вы хотите отключить работу компонента Файловый Антивирус, снимите флажок слева от названия компонента в списке.

► *Чтобы настроить параметры Файлового Антивируса, выполните следующие действия:*

1. Выберите компонент Файловый Антивирус в списке и нажмите на кнопку **Изменить**, расположенную над списком компонентов защиты.

   Откроется окно **Настройка: Файловый Антивирус**.

2. Настройте параметры работы Файлового Антивируса (см. раздел «Настройка Файлового Антивируса через Kaspersky Security Center» на стр. 141). Эти параметры Kaspersky Security использует на защищенных виртуальных машинах после применения политики.

3. Нажмите на кнопку **ОК** в окне **Настройка: Файловый Антивирус**, чтобы сохранить изменения и закрыть окно настройки.

► *Чтобы запретить или разрешить наследование параметров политики, выполните одно из следующих действий:*

- Если вы хотите запретить изменение параметров политики, выполните одно из следующих действий:
  - Выберите компонент защиты в списке и нажмите на кнопку **Закрыть**, расположенную над списком компонентов защиты.
  - Нажмите на значок «замок» слева от названия компонента защиты.
- Если вы хотите разрешить изменение параметров политики, выполните одно из следующих действий:
  - Выберите компонент защиты в списке и нажмите на кнопку **Открыть**, расположенную над списком компонентов защиты.
  - Нажмите на значок «замок» слева от названия компонента защиты.

Перейдите к следующему шагу мастера создания политики.

Шаг 5. Настройка параметров обнаружения SVM

На этом шаге выберите способ, который Легкие агенты используют для обнаружения SVM, работающих в сети, и получения информации о них:

- **Использовать многоадресную рассылку (Multicast)**.

  Если выбран этот вариант, компонент Легкий агент получает информацию об SVM с помощью многоадресной рассылки (Multicast).

  Этот вариант выбран по умолчанию.

- **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 требуется указать параметры подключения Легких агентов к Серверу интеграции.

- **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 Сервер интеграции**, укажите параметры подключения Легких агентов к Серверу интеграции.

► *Чтобы указать параметры подключения Легких агентов к Серверу интеграции, выполните следующие действия:*

1. 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) Сервера интеграции.

2. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.

3. Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен, или ваша учетная запись не входит в 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.

   При переходе к следующему шагу мастера выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, переход к следующему шагу невозможен. Проверьте введенные параметры подключения. Информация об ошибках подключения к Серверу интеграции записывается в журнал работы Сервера интеграции (см. раздел «О журналах Сервера интеграции» на стр.224).

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную**, сформируйте список SVM.

► *Чтобы сформировать список SVM, выполните следующие действия:*

1. Нажмите на кнопку **Добавить**, расположенную над списком адресов SVM.

   Откроется окно **Адреса SVM**.

2. 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.

3. Нажмите на кнопку **ОК** 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.

4. 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.

Перейдите к следующему шагу мастера.

Шаг 6. Создание групповой политики для программы

Завершите работу мастера создания политики.

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

При следующем подключении виртуальной машины к Серверу администрирования Kaspersky Security Center передаст информацию программе Kaspersky Security, политика распространится на защищенные виртуальные машины. 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 вы выбрали вариант **Неактивная политика**, созданная политика не применяется на защищенных виртуальных машинах.

Если сведения о лицензии не переданы на защищенную виртуальную машину, компонент Легкий агент функционирует в режиме ограниченной функциональности (см. раздел «Об активации программы» на стр. 46).

Изменение параметров политик

Этот раздел содержит сведения об изменении параметров политики Сервера защиты и политик для Легкого агента.

В этом разделе

Изменение параметров политики для Сервера защиты

► *Чтобы изменить параметры политики для Сервера защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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 **Изменить параметры политики**. Ссылка **Изменить параметры политики** находится справа от списка политик в блоке с параметрами политики.
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.

5. Измените параметры политики.

   Если вы хотите настроить дополнительные параметры работы SVM, вам требуется включить отображение дополнительных параметров политики для Сервера защиты в реестре операционной системы (см. раздел «Отображение параметров политик» на стр. 85).

   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 **ОК** в окне **Свойства: <Название политики>**.

Изменение параметров политики для Легкого агента для Windows

► *Чтобы изменить параметры политики для Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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 **Изменить параметры политики**. Ссылка **Изменить параметры политики** находится 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.

Параметры контроля отображаются в свойствах политики для Легкого агента для Windows, если в параметрах интерфейса Консоли администрирования Kaspersky Security Center включено отображение параметров контроля (см. раздел «Настройка отображения параметров контроля в Консоли администрирования» на стр. 93).

В разделе **Основные параметры защиты** вы можете включить или отключить технологию лечения активного заражения для защищенных виртуальных машин с серверной операционной системой (см. раздел «Включение и выключение технологии лечения активного заражения для серверных операционных систем» на стр. 189).

О настройке параметров защиты и параметров работы Легкого агента для Windows см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

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 **ОК** в окне **Свойства: <Название политики>**.

Изменение параметров политики для Легкого агента для Linux

► *Чтобы изменить параметры политики для Легкого агента для Linux, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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 **Изменить параметры политики**. Ссылка **Изменить параметры политики** находится 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 (см. раздел «Настройка параметров Легкого агента для Linux через Kaspersky Security Center» на стр. 141).

   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 **ОК** в окне **Свойства: <Название политики>**.

Управление задачами

Этот раздел содержит информацию об управлении задачами для программы Kaspersky Security для виртуальных сред 4.0 Легкий агент.

В этом разделе

О задачах для Kaspersky Security

Вы можете управлять работой программы Kaspersky Security для виртуальных сред 4.0 Легкий агент с помощью задач как локально на защищенных виртуальных машинах (через интерфейс Легкого агента для Windows или с помощью командной строки в случае Легкого агента для Linux), так и централизованно, через Kaspersky Security Center.

Вы можете выполнять следующие действия над задачами:

- запускать и останавливать задачи;
- создавать и удалять задачи;
- изменять параметры задач;
- просматривать результаты выполнения задач.

Управление задачами через Kaspersky Security Center

Через Kaspersky Security Center вы можете настраивать следующие задачи:

- Задачи, которые выполняются на SVM:
  - **Активация программы**. Kaspersky Security Center добавляет на SVM ключ для активации программы или для продления срока действия лицензии (см. в *Руководстве по внедрению Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

- **Обновление баз** (см. раздел «**Создание задачи обновления на Сервере защиты**» на стр. 134). Компонент Сервер защиты автоматически загружает пакет обновлений баз и модулей программы и устанавливает обновления на SVM.

- **Откат обновления** (см. раздел «**Создание задачи отката обновления на Сервере защиты**» на стр. 139). Компонент Сервер защиты откатывает последнее обновление баз и модулей программы на SVM.

- Задачи, которые выполняются на защищенных виртуальных машинах с установленным компонентом Легкий агент для Windows:

  - **Инвентаризация** (см. раздел «**Создание задач, выполняемых на защищенных виртуальных машинах**» на стр. 125). В процессе выполнения задачи Kaspersky Security выполняет поиск информации обо всех исполняемых файлах программ, хранящихся на защищенных виртуальных машинах.

  - **Поиск вирусов** (см. раздел «**Создание задач, выполняемых на защищенных виртуальных машинах**» на стр. 125). В процессе выполнения задачи Kaspersky Security проверяет области защищенной виртуальной машины, указанные в параметрах задачи, на вирусы и другие вредоносные программы.

  - **Изменение состава компонентов программы**. В процессе выполнения задачи Kaspersky Security устанавливает или удаляет компоненты Легкого агента на защищенных виртуальных машинах (см. в *Руководстве по внедрению Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

- Задачу **Поиск вирусов**, которая выполняется на защищенных виртуальных машинах с установленным компонентом Легкий агент для Linux (см. раздел «Создание задач, выполняемых на защищенных виртуальных машинах» на стр. 125). В процессе выполнения задачи Kaspersky Security проверяет области защищенной виртуальной машины, указанные в параметрах задачи, на вирусы и другие вредоносные программы.

Для работы с программой Kaspersky Security для виртуальных сред 4.0 Легкий агент вы можете создавать задачи следующих типов:

- *Групповая задача* – задача, которая выполняется на клиентских компьютерах выбранной группы администрирования. Применительно к программе Kaspersky Security групповые задачи выполняются на SVM или защищенных виртуальных машинах, входящих в группы администрирования.

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

Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию обо всех событиях, произошедших во время выполнения задач. Вы можете посмотреть информацию о ходе и результатах выполнения задач в Консоли администрирования Kaspersky Security Center одним из следующих способов:

- В окне **Результаты выполнения задачи**. Окно открывается по ссылке **Посмотреть результаты**, расположенной справа от списка задач, который отображается в папке **Задачи** дерева консоли Kaspersky Security Center или на закладке **Задачи** в рабочей области группы администрирования.

- В списке событий, которые SVM отправляют на Сервер администрирования Kaspersky Security Center. Список событий отображается на закладке **События** в рабочей области узла **Сервер администрирования**.

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

Управление задачами через локальный интерфейс Легкого агента для Windows

Помимо задач, которые вы можете настраивать через Kaspersky Security Center, для управления программой Kaspersky Security для виртуальных сред 4.0 Легкий агент используются задачи, которые вы можете настраивать через локальный интерфейс Легкого агента для Windows на защищенной виртуальной машине.

Для управления программой через локальный интерфейс Легкого агента для Windows вы можете использовать следующие задачи:

- *Полная проверка*. Kaspersky Security выполняет тщательную проверку операционной системы защищенной виртуальной машины, включая системную память, загружаемые при старте объекты, резервное хранилище операционной системы, а также все жесткие и съемные диски.
- *Выборочная проверка*. Kaspersky Security проверяет на защищенной виртуальной машине объекты, выбранные пользователем.
- *Проверка важных областей*. Kaspersky Security проверяет объекты, загрузка которых осуществляется при старте операционной системы защищенной виртуальной машины (загрузочные секторы и объекты автозапуска), системную память и объекты заражения руткитами.
- *Обновление*. Kaspersky Security загружает с SVM пакет обновлений баз и модулей программы и устанавливает обновления на защищенную виртуальную машину.

Подробнее об этих задачах см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

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 «*Запуск задачи проверки*» на стр. 202). Kaspersky Security выполняет тщательную проверку операционной системы защищенной виртуальной машины, включая системную память, загружаемые при старте объекты, резервное хранилище операционной системы, а также все жесткие и съемные диски.
- *Выборочная проверка* (см. раздел «*Запуск задачи проверки*» на стр. 202). Kaspersky Security проверяет на защищенной виртуальной машине объекты, выбранные пользователем.
- *Обновление* (см. раздел «*Запуск и остановка задачи обновления*» на стр. 206). Kaspersky Security загружает с SVM пакет обновлений антивирусных баз и устанавливает обновления на защищенную виртуальную машину.

Создание задач, выполняемых на защищенных виртуальных машинах

► *Чтобы создать задачу поиска вирусов для Легкого агента для Linux, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Выполните одно из следующих действий:

   - Выберите папку **Управляемые компьютеры** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.

   - В папке **Управляемые компьютеры** 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**.

   - Откройте папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин.

3. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.

4. Выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Linux** выберите **Поиск вирусов**. Перейдите к следующему шагу мастера.

5. В окне **Область проверки** сформируйте список объектов, которые проверяет Kaspersky Security. Перейдите к следующему шагу мастера создания задачи.

6. В окне **Действие Kaspersky Security для виртуальных сред 4.0 Легкий агент** выберите действие, которое программа Kaspersky Security выполняет, если в результате проверки обнаруживает зараженные файлы. Перейдите к следующему шагу мастера.

7. Далее следуйте указаниям мастера создания задачи.

► *Чтобы создать задачу поиска вирусов для Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые компьютеры** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые компьютеры** 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**.
   - Откройте папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин.
3. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.
4. Выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows** выберите **Поиск вирусов**. Перейдите к следующему шагу мастера.
5. В окне **Область проверки** сформируйте список объектов, которые проверяет Kaspersky Security (подробнее см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*). Перейдите к следующему шагу мастера создания задачи.
6. В окне **Действие Kaspersky Security для виртуальных сред 4.0 Легкий агент** выберите действие, которое программа Kaspersky Security выполняет, если в результате проверки обнаруживает зараженные файлы (подробнее см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).
7. Установите флажок **Выполнять лечение активного заражения немедленно**, если вы хотите, чтобы программа выполняла процедуру лечения активного заражения (см. раздел «О технологии лечения активного заражения» на стр. 187) сразу после его обнаружения в процессе выполнения групповой задачи поиска вирусов и перезагружала виртуальную машину после лечения активного заражения без запроса подтверждения у пользователя.

8. Установите флажок **Приостанавливать проверку по расписанию, если экранная заставка не включена и защищенная виртуальная машина разблокирована**, если вы хотите, чтобы программа приостанавливала запуск задачи проверки, если ресурсы виртуальной машины заняты. Перейдите к следующему шагу мастера.

9. Далее следуйте указаниям мастера создания задачи.

► *Чтобы создать задачу инвентаризации для Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Выполните одно из следующих действий:

   - Выберите папку **Управляемые компьютеры** дерева консоли, если вы хотите создать задачу для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.

   - В папке **Управляемые компьютеры** 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**.

   - Откройте папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких виртуальных машин.

3. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.

4. Выберите тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows** выберите **Инвентаризация**. Перейдите к следующему шагу мастера.

5. В окне **Область инвентаризации** сформируйте список объектов для инвентаризации. Перейдите к следующему шагу мастера создания задачи.

6. Установите флажок **Приостанавливать проверку по расписанию, если экранная заставка не включена и защищенная виртуальная машина разблокирована**, если вы хотите, чтобы программа приостанавливала запуск задачи инвентаризации, если ресурсы виртуальной машины заняты.

7. Далее следуйте указаниям мастера создания задачи.

Более подробно работа с задачами описана в документации Kaspersky Security Center.

Запуск и остановка задач в Kaspersky Security Center

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые компьютеры** дерева консоли, если вы хотите запустить или остановить задачу, созданную для виртуальных машин, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые компьютеры** дерева консоли выберите папку с названием группы администрирования, если вы хотите запустить или остановить задачу для виртуальных машин, входящих в состав этой папки. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли, если вы хотите запустить или остановить задачу, созданную для одной или нескольких виртуальных машин.
3. В списке задач выберите задачу, которую вы хотите запустить или остановить.
4. Если вы хотите запустить задачу, выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Запустить**.
   - Нажмите на кнопку **Запустить**, расположенную справа от списка задач.
5. Если вы хотите остановить задачу, выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Остановить**.
   - Нажмите на кнопку **Остановить**, расположенную справа от списка задач.

Обновление баз и модулей программы

Этот раздел содержит информацию об обновлении баз и модулей программы и инструкции о том, как настроить параметры обновления.

В этом разделе

Об обновлении баз и модулей программы

Обновление баз и модулей 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 Kaspersky Security.

Если базы программы давно не обновлялись, сообщение об этом появляется в окне **События** свойств SVM.

Чтобы программа Kaspersky Security своевременно обнаруживала угрозы, вам нужно регулярно обновлять базы и модули программы.

Обновления баз и модулей программы могут изменить некоторые параметры Kaspersky Security, например, параметры эвристического анализа, повышающие эффективность защиты и проверки.

Для обновления баз и модулей программы требуется действующая лицензия на использование программы.

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы для программ «Лаборатории Касперского». Источником обновлений для Kaspersky Security для виртуальных сред 4.0 Легкий агент является хранилище Сервера администрирования Kaspersky Security Center.

Обновление баз и модулей программы Kaspersky Security 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. Для этого вам требуется включить в пакет обновлений обновления модулей Легкого агента для Windows (см. раздел «Включение и выключение обновления модулей Легкого агента для Windows» на стр. 132).

   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 и модулей программы» на стр. 133).

   Чтобы успешно загрузить пакет обновлений из хранилища Сервера администрирования, SVM должна иметь доступ к Серверу администрирования Kaspersky Security Center.

Если базы и модули 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 и модулей программы устанавливаются из папки на SVM:

   - После загрузки пакета обновлений компонент Сервер защиты автоматически устанавливает на SVM обновления баз, необходимых для работы Сервера защиты (антивирусных баз).

   - Компонент Легкий агент проверяет наличие пакета обновлений в папке на той SVM, к которой он подключен. При наличии пакета обновлений Легкий агент устанавливает на защищенной виртуальной машине обновления баз, необходимых для работы Легкого агента, и обновления модулей Легкого агента для Windows (если обновления модулей включены в состав пакета обновлений). Обновление баз и модулей 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 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 (см. подробнее в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

     На защищенной виртуальной машине с установленным компонентом Легкий агент для Linux пользователь может вручную запустить задачу обновления из командной строки (см. раздел «Запуск и остановка задачи обновления» на стр. 206).

     Чтобы обеспечить актуальность защиты временных виртуальных машин, рекомендуется регулярно обновлять базы и модули Легкого агента на шаблоне виртуальных машин, из которого созданы временные защищенные виртуальные машины (см. раздел «Обновление баз и модулей Легкого агента для Windows на шаблоне виртуальных машин» на стр. 136).

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.

Для обновления баз и модулей Легкого агента для Windows на защищенной виртуальной машине должны быть выполнены следующие условия:

- В свойствах сетевой карты на защищенной виртуальной машине установлены:
  - протокол Интернета (TCP/IP) (Internet Protocol (TCP/IP));
  - клиент для сетей Microsoft (Client for Microsoft Networks).
- На защищенной виртуальной машине запущена служба «Рабочая станция» (Workstation).
- На SVM разрешено прохождение сетевого трафика через порт 445 по протоколу TCP.

Включение и выключение обновления модулей Легкого агента для Windows

Включение и выключение обновления модулей Легкого агента для Windows выполняется в параметрах политики для Сервера защиты. Если обновление модулей Легкого агента для Windows включено, Kaspersky Security включает обновления модулей Легкого агента для Windows в пакет обновлений.

► *Чтобы включить или выключить обновление модулей Легкого агента для Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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**. Ссылка **Изменить параметры политики** находится 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. В окне свойств политики для Сервера защиты в списке слева выберите раздел **Параметры обновления**.

   В правой части окна отобразятся параметры обновления.

6. Выполните одно из следующих действий:

   - Установите флажок **Обновлять модули программы**, если вы хотите включить обновление модулей Легкого агента для Windows.

   - Снимите флажок **Обновлять модули программы**, если вы хотите выключить обновление модулей Легкого агента для Windows.

7. Нажмите на кнопку **ОК**.

Автоматическое получение пакета обновлений баз и модулей программы

Kaspersky Security Center позволяет автоматически загружать пакеты обновлений баз и модулей 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 и модулей программы на SVM, входящие в выбранную группу администрирования, в соответствии с настроенным расписанием.

► *Чтобы настроить автоматическое получение пакета обновлений баз и модулей 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. Создайте задачу обновления на Сервере защиты для SVM, на которых вы хотите обновлять базы и модули программы (см. раздел «Создание задачи обновления на Сервере защиты» на стр. 134).

Создание задачи обновления на Сервере защиты

► *Чтобы создать задачу обновления на Сервере защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Выполните одно из следующих действий:

   - Выберите папку **Управляемые компьютеры** дерева консоли, если вы хотите создать задачу обновления для SVM, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.

   - В папке **Управляемые компьютеры** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу обновления 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.

3. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите для программы **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты** в качестве типа задачи **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. 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-интервал** и задайте адреса SVM вручную.
   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
   - Нажмите на кнопку **Выбрать** 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 **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. В поле **Имя** введите имя 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 в любой момент запустить или остановить задачу вручную (см. раздел «Запуск и остановка задач в Kaspersky Security Center» на стр. 128).

Обновление баз и модулей Легкого агента для Windows на шаблоне виртуальных машин

Шаблон виртуальных машин на гипервизоре Microsoft Windows Server (Hyper-V) или Citrix XenServer

► *Чтобы обновить базы и модули Легкого агента на шаблоне виртуальных машин, выполните следующие действия:*

1. Включите на гипервизоре защищенную виртуальную машину, являющуюся шаблоном временных защищенных виртуальных машин.

2. По умолчанию Легкий агент, установленный на защищенной виртуальной машине, запускается автоматически при запуске операционной системы. Если вы отключили автоматический запуск программы, запустите Легкий агент на защищенной виртуальной машине.

3. Обновите базы и модули Легкого агента вручную или дождитесь запуска задачи обновления баз и модулей Легкого агента по расписанию (см. подробнее в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

4. Создайте заново временные защищенные виртуальные машины из обновленного шаблона. Подробнее см. в документации к виртуальной инфраструктуре.

Чтобы автоматизировать обновление баз и модулей Легкого агента на шаблонах виртуальных машин, вы можете использовать такие средства, как Microsoft Virtual Machine Servicing Tool (для шаблонов на гипервизоре Microsoft Windows Server (Hyper-V)), Citrix PowerShell SDK и Citrix Provisioning Services (для шаблонов, созданных на базе Citrix XenDesktop).

Шаблон виртуальных машин на базе Vmware Horizon View

► *Чтобы обновить базы и модули Легкого агента на шаблоне виртуальных машин (linked clones), выполните следующие действия:*

1. Включите защищенную виртуальную машину, на базе снимка с которой был создан пул временных защищенных виртуальных машин.

2. По умолчанию Легкий агент, установленный на защищенной виртуальной машине, запускается автоматически при запуске операционной системы. Если вы отключили автоматический запуск программы, запустите Легкий агент на защищенной виртуальной машине и убедитесь, что Легкий агент подключился к SVM.

3. Обновите базы и модули Легкого агента вручную или дождитесь запуска задачи обновления баз и модулей Легкого агента по расписанию (см. подробнее в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

4. После завершения обновления выключите защищенную виртуальную машину и создайте новый снимок этой виртуальной машины.

5. Выполните пересоздание пула временных защищенных виртуальных машин на базе созданного снимка. Подробнее см. раздел Update Linked-Clone Desktops документа VMware Horizon View Administration.

Чтобы автоматизировать обновление баз и модулей Легкого агента на виртуальных машинах под управлением VMware Horizon View, вы можете использовать скриптовый язык VMware vSphere™ PowerCLI™ для создания скрипта автоматического обновления снимка защищенной виртуальной машины и пересоздания пула временных защищенных виртуальных машин при помощи конструкций Get-Snapshot и Update-AutomaticLinkedClonePool.

Откат последнего обновления баз и модулей программы

После первого обновления баз и модулей программы становится доступна функция отката к предыдущему набору баз и модулей программы.

Каждый раз, когда на SVM запускается обновление, Kaspersky Security создает резервную копию используемых баз и модулей программы и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущего набора баз и модулей программы при необходимости. 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 и модулей программы Kaspersky Security выполняется в следующем порядке:

1. Откат последнего обновления баз и модулей программы на SVM. Вы можете откатить последнее обновление баз и модулей 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 и модулей программы на защищенных виртуальных машинах. После отката обновления баз и модулей 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 (см. подробнее в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

   На защищенной виртуальной машине с установленным компонентом Легкий агент для Linux пользователь может вручную запустить задачу обновления из командной строки (см. раздел «Запуск задачи обновления с дополнительными параметрами» на стр. 207).

► *Чтобы откатить последнее обновление баз и модулей программы на SVM, выполните следующие действия:*

1. Создайте задачу отката обновления на Сервере защиты для SVM, на которых вы хотите откатить обновление баз и модулей программы (см. раздел «Создание задачи отката обновления на Сервере защиты» на стр. 139).
2. Запустите задачу отката обновления на Сервере защиты (см. раздел «Запуск и остановка задач в Kaspersky Security Center» на стр. 128).

Создание задачи отката обновления на Сервере защиты

► *Чтобы создать задачу отката обновления на Сервере защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые компьютеры** дерева консоли, если вы хотите создать задачу отката обновления для SVM, входящих во все группы администрирования. В рабочей области выберите закладку **Задачи**.
   - В папке **Управляемые компьютеры** дерева консоли выберите папку с названием группы администрирования, если вы хотите создать задачу отката обновления для всех SVM, входящих в состав этой группы. В рабочей области выберите закладку **Задачи**.
   - Откройте папку **Задачи** дерева консоли, если вы хотите создать задачу отката обновления для одной или нескольких SVM.
3. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.
4. На первом шаге мастера выберите для программы **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты** в качестве типа задачи **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. 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-интервал** и задайте адреса SVM вручную.
- Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
- Нажмите на кнопку **Выбрать** 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.

Настройка параметров Легкого агента для Linux через Kaspersky Security Center

Этот раздел содержит информацию о настройке основных параметров защиты и проверки Легкого агента для Linux через Kaspersky Security Center.

В этом разделе

Настройка Файлового Антивируса через Kaspersky Security Center

Файловый Антивирус позволяет избежать заражения файловой системы защищенной виртуальной машины. По умолчанию Файловый Антивирус запускается при старте Kaspersky Security, 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 технологию iChecker. Если при проверке в файле не обнаружены вирусы или другие вредоносные программы, Kaspersky Security разрешает доступ к этому файлу.

Если в результате проверки Файловый Антивирус обнаруживает угрозу в файле, 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.

Вы можете выполнить следующие действия для настройки работы Файлового Антивируса:

- Изменить уровень безопасности файлов.

  Вы можете выбрать один из предустановленных уровней безопасности файлов или настроить параметры уровня безопасности файлов самостоятельно. После того как вы изменили параметры уровня безопасности файлов, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности файлов.

- Изменить действие, которое Файловый Антивирус выполняет при обнаружении зараженного файла.

- Сформировать область защиты Файлового Антивируса.

  Вы можете расширить или сузить область защиты, добавив или удалив объекты, которые проверяет Файловый Антивирус.

- Настроить использование эвристического анализа.

  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.

  Чтобы повысить эффективность 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.

- Настроить проверку составных файлов.

- Изменить режим проверки файлов.

- Настроить использование технологии проверки 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 Kaspersky Security, дату предыдущей проверки файла, а также изменение параметров проверки.

В этом разделе

Включение и выключение Файлового Антивируса

По умолчанию Файловый Антивирус включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Файловый Антивирус при необходимости.

► *Чтобы включить или выключить Файловый Антивирус, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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>** одним из следующих способов:
   - Двойным щелчком мыши.

- По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
- По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

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 Файловый Антивирус.
   - Снимите флажок **Файловый Антивирус**, если вы хотите выключить 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*. 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 компьютеры** 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>** одним из следующих способов:

   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
   - По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

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 при помощи 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 компьютеры** 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>** одним из следующих способов:

   - Двойным щелчком мыши.

   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.

   - По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

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:

   - **Выбирать действие автоматически**.

     Этот вариант выбран по умолчанию. При обнаружении угрозы программа выполняет действие **Лечить. Удалять, если лечение невозможно**.

   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.

   - **Выполнять действие: Лечить**.

- **Выполнять действие: Удалять**.
- **Выполнять действие: Блокировать**.

> 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.

► *Чтобы сформировать область защиты Файлового Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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>** одним из следующих способов:
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
   - По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

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 наиболее подвержены заражению.
   - Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, наиболее подверженными заражению.

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. В окне **Выбор объекта** 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, 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.

11. При необходимости 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 компьютеры** 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>** одним из следующих способов:

   - Двойным щелчком мыши.

   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.

   - По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

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, установочные пакеты, 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 не хотите, чтобы Файловый Антивирус пропускал файлы по истечении заданного времени, снимите флажок **Пропускать файлы, если их проверка длится более**.

   - 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.

10. В блоке **Ограничение по размеру** выполните одно из следующих действий:

    - 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.

    - Если вы хотите, чтобы Файловый Антивирус распаковывал 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**.

      > 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**.

Настройка использования эвристического анализа в работе Файлового Антивируса

► *Чтобы настроить использование эвристического анализа в работе Файлового Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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>** одним из следующих способов:
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
   - По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
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 при помощи 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**.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором Файловый Антивирус начинает проверять файлы. По умолчанию Kaspersky Security 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, Kaspersky Security 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 компьютеры** 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>** одним из следующих способов:

   - Двойным щелчком мыши.

   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.

   - По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

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**.

Настройка использования технологии iChecker в работе Файлового Антивируса

► *Чтобы настроить использование технологии iChecker в работе Файлового Антивируса, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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>** одним из следующих способов:

   - Двойным щелчком мыши.

- По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
- По ссылке **Изменить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

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**.

Настройка исключений из защиты через Kaspersky Security Center

Вы можете формировать список объектов, которые программа Kaspersky Security не контролирует в процессе работы, то есть набор исключений из защиты и проверки.

Исключение – это совокупность условий, описывающих объект. Если объект удовлетворяет этим условиям, Kaspersky Security не проверяет этот объект на вирусы и другие вредоносные программы.

Вы можете исключать из защиты и проверки объекты следующих типов:

- файлы определенного формата;
- файлы по маске;
- папки;
- объекты по классификации Вирусной энциклопедии «Лаборатории Касперского».

Помимо добавленных вами исключений из защиты и проверки исключены объекты файловой системы /dev, /sys и /proc.

Некоторые легальные программы могут быть использованы злоумышленниками для нанесения вреда вашей защищенной виртуальной машине или вашим данным. Такие программы сами по себе не имеют вредоносных функций, но 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 Kaspersky Security такие программы могут быть заблокированы. Чтобы избежать блокирования, вы можете настроить исключения из защиты программой Kaspersky Security для используемых вами программ. Для этого нужно добавить в исключения название объекта или маску названия объекта по классификации Вирусной энциклопедии «Лаборатории Касперского».

Если на вашей виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из защиты, добавив ее в исключения.

Вы можете выполнить следующие действия для настройки исключений:

- Создать новое исключение (см. раздел «Создание исключения» на стр. 158).

  Вы можете создать новое исключение, при применении которого Kaspersky Security не проверяет указанные файлы или папки и / или объекты с указанным именем.

- Приостановить использование исключения (см. раздел «Запуск и остановка использования исключения» на стр. 159).

  Вы можете временно приостановить использование исключения, не удаляя его из списка исключений.

- Изменить параметры существующего исключения (см. раздел «Изменение исключения» на стр. 160).

  После того как вы создали новое исключение, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Удалить исключение (см. раздел «Удаление исключения» на стр. 161).

  Вы можете удалить исключение, если вы не хотите, чтобы программа Kaspersky Security применяла это исключение во время проверки защищенной виртуальной машины.

В этом разделе

Создание исключения

► *Чтобы создать исключение, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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.
5. По правой кнопке мыши откройте контекстное меню политики для Легкого агента для Linux и выберите пункт **Свойства**.

   Откроется окно свойств политики для Легкого агента для Linux.
6. В окне свойств политики для Легкого агента для Linux выберите раздел **Основные параметры защиты**.

   В правой части окна отобразятся основные параметры защиты.
7. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.
8. Нажмите на кнопку **Добавить**.

   Откроется окно **Исключение**.
9. Если вы хотите исключить из защиты 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 название файла или папки или маску названия файла.

   c. Нажмите на кнопку **ОК** в окне **Название файла или папки**.

      Ссылка на добавленный файл или папку появится в блоке **Описание исключения** окна **Исключения**.

10. Если вы хотите исключить из защиты 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» на веб-сайте www.securelist.ru.

    c. Нажмите на кнопку **ОК** в окне **Название объекта**.

11. При необходимости в поле **Комментарий** введите краткий комментарий к создаваемому исключению.

12. Нажмите на кнопку **ОК** 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 **ОК** в окне **Доверенная зона**.

14. Нажмите на кнопку **Применить**.

Запуск и остановка использования исключения

► *Чтобы запустить или остановить использование исключения, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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.
5. По правой кнопке мыши откройте контекстное меню политики для Легкого агента для Linux и выберите пункт **Свойства**.

   Откроется окно свойств политики для Легкого агента для Linux.
6. В окне свойств политики для Легкого агента для Linux выберите раздел **Основные параметры защиты**.

   В правой части окна отобразятся основные параметры защиты.
7. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.
8. В списке исключений выберите нужное исключение.
9. Выполните одно из следующих действий:
   - Установите флажок рядом с названием исключения, если вы хотите использовать это исключение.
   - Снимите флажок рядом с названием исключения, если вы хотите временно приостановить использование этого исключения.
10. Нажмите на кнопку **ОК** в окне **Доверенная зона**.
11. Нажмите на кнопку **Применить**.

Изменение исключения

► *Чтобы изменить исключение, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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.

5. По правой кнопке мыши откройте контекстное меню политики для Легкого агента для Linux и выберите пункт **Свойства**.

   Откроется окно свойств политики для Легкого агента для Linux.

6. В окне свойств политики для Легкого агента для Linux выберите раздел **Основные параметры защиты**.

   В правой части окна отобразятся основные параметры защиты.

7. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.

8. В списке исключений выберите нужное исключение.

9. Нажмите на кнопку **Изменить**.

   Откроется окно **Исключение**.

10. Измените параметры исключения.

11. Нажмите на кнопку **ОК** в окне **Исключение**.

    В блоке **Описание исключения** отобразятся измененные параметры этого исключения.

12. Нажмите на кнопку **ОК** в окне **Доверенная зона**.

13. Нажмите на кнопку **Применить**.

Удаление исключения

► *Чтобы удалить исключение, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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.

5. По правой кнопке мыши откройте контекстное меню политики для Легкого агента для Linux и выберите пункт **Свойства**.

   Откроется окно свойств политики для Легкого агента для Linux.

6. В окне свойств политики для Легкого агента для Linux выберите раздел **Основные параметры защиты**.

   В правой части окна отобразятся основные параметры защиты.

7. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.

8. В списке исключений выберите нужное исключение.

9. Нажмите на кнопку **Удалить**.

   Удаленное исключение исчезнет из списка исключений закладки **Исключения** окна **Доверенная зона**.

10. Нажмите на кнопку **ОК** в окне **Доверенная зона**.

11. Нажмите на кнопку **Применить**.

Настройка параметров задачи поиска вирусов для Легкого агента для Linux

Для настройки параметров задач поиска вирусов вы можете выполнить следующие действия:

- Изменить уровень безопасности.

  Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

- Изменить действие, которое Kaspersky Security выполняет при обнаружении зараженного файла.

- Сформировать область проверки.

Вы можете расширить или сузить область проверки, добавив или удалив объекты, которые проверяет программа.

- Настроить проверку составных файлов.
- Настроить использование эвристического анализа.

  Во время своей работы Kaspersky Security использует сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Security сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов «Лаборатории Касперского», сигнатурный анализ всегда включен.

  Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Security анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

- Настроить использование технологии проверки iChecker.

  Вы можете включить использование технологии iChecker, которая 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.

В этом разделе

Изменение уровня безопасности

Для выполнения задач проверки Kaspersky Security применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности*. 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 компьютеры** 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>** 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.
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 при помощи 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 компьютеры** 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>** 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.

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:

   - **Выбирать действие автоматически**.

     Этот вариант выбран по умолчанию. При обнаружении угрозы программа выполняет действие **Лечить. Удалять, если лечение невозможно**.

   - **Выполнять действие: Лечить. Удалять, если лечение невозможно.**
   - **Выполнять действие: Лечить.**
   - **Выполнять действие: Удалять.**
   - **Выполнять действие: Информировать.**

   При удалении или лечении копии файлов сохраняются в резервном хранилище.

7. Нажмите на кнопку **Применить**.

Формирование области проверки

Областью проверки называется местоположение файлов, которые программа проверяет во время выполнения задачи проверки.

► *Чтобы сформировать область проверки, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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>** 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.

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. В окне **Выбор объекта** 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**.

- Если вы хотите изменить путь к объекту, укажите другой путь к объекту в поле **Объект** и нажмите на кнопку **OK**.
- Если вы хотите удалить объект, нажмите на кнопку **Да** в окне подтверждения удаления.

9. При необходимости 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 ним. Объект остается в списке проверяемых объектов, но не проверяется во время выполнения задачи проверки.
11. Нажмите на кнопку **OK** 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 компьютеры** 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>** 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.

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: архивы, установочные пакеты, 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 времени** выполните одно из следующих действий:

   - Если вы не хотите, чтобы программа пропускала файлы по истечении заданного времени, снимите флажок **Пропускать файлы, если их проверка длится более**.
   - 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.

10. 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**.

  > 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**.

Настройка использования эвристического анализа

► *Чтобы настроить использование эвристического анализа, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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>** 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.

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 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**.

8. Нажмите на кнопку **OK** в окне **Поиск вирусов**.

9. Нажмите на кнопку **Применить**.

Настройка использования технологии iChecker

► *Чтобы настроить использование технологии iChecker, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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>** 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.

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 проверки.
   - Снимите флажок **Технология iChecker**, если вы не хотите использовать эту технологию во время проверки.

8. Нажмите на кнопку **OK** в окне **Поиск вирусов**.

9. Нажмите на кнопку **Применить**.

Настройка параметров Легкого агента для Windows через Kaspersky Security Center

Настройка параметров Легкого агента для Windows осуществляется локально на защищенной виртуальной машине через интерфейс Легкого агента для Windows (см. *Руководство пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

Этот раздел содержит информацию о настройке некоторых параметров компонента Контроль запуска программ и компонента Контроль устройств Легкого агента для Windows через Kaspersky Security Center.

В этом разделе

Настройка Контроля запуска программ через Kaspersky Security Center

Компонент Легкого агента Контроль запуска программ отслеживает попытки запуска программ на виртуальной машине и регулирует запуск программ с помощью *правил контроля запуска программ* (подробная информация о правилах контроля запуска программ приведена в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

Компонент Контроль запуска программ доступен, если программа Kaspersky Security установлена на виртуальной машине с настольной операционной системой Windows. Этот компонент недоступен, если программа Kaspersky Security установлена на виртуальной машине с серверной операционной системой Windows.

Запуск программ, параметры которых не удовлетворяют ни одному из правил контроля запуска программ, регулируется созданным по умолчанию правилом «Разрешить все». Правило «Разрешить все» разрешает любым пользователям запускать любые программы. Все попытки запуска программ на виртуальной машине фиксируются в отчетах.

Компонент Легкого агента Контроль запуска программ может работать в двух режимах:

- *Черный список*. Режим, при котором Контроль запуска программ разрешает всем пользователям запуск любых программ на защищенной виртуальной машине, кроме тех, которые указаны в запрещающих правилах контроля запуска программ.

  Этот режим работы Контроля запуска программ настроен по умолчанию. Разрешение на запуск всех программ основано на правиле контроля запуска программ «Разрешено все», созданном по умолчанию.

- *Белый список*. Режим, при котором Контроль запуска программ запрещает всем пользователям запуск любых программ на защищенной виртуальной машине, кроме тех, которые указаны в разрешающих правилах контроля запуска программ. Таким образом, если разрешающие 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.

Настройка Контроля запуска программ для работы в этих режимах возможна как в локальном интерфейсе Легкого агента, так и на стороне Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Легкого агента и необходимые для:

- Создания категорий программ (см. раздел «Этап 2. Создание категорий программ» на стр. 177). Правила контроля запуска программ на стороне Kaspersky Security Center основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Легкого агента.
- Получения информации о программах, которые установлены на защищенных виртуальных машинах локальной сети организации (см. раздел «Этап 1. Получение информации о программах, которые установлены на защищенных виртуальных машинах» на стр. 176).
- Анализа работы Контроля запуска программ после изменения режима (см. раздел «Этап 4. Тестирование разрешающих правил контроля запуска программ» на стр. 179).

Поэтому настройку режима работы компонента Контроль запуска программ рекомендуется выполнять на стороне Kaspersky Security Center.

В этом разделе

Переход из режима «Черный список» к режиму «Белый список»

Этот раздел содержит информацию о переходе из режима работы Контроля запуска программ «Черный список» в режим «Белый список» и рекомендации по оптимальному использованию функциональности Контроля запуска программ.

В этом разделе

Этап 1. Получение информации о программах, которые установлены на защищенных виртуальных машинах

На этом этапе требуется получить представление о программах, используемых на защищенных виртуальных машинах в локальной сети организации. Для этого рекомендуется получить информацию о:

- Производителях, версиях и локализациях программ, установленных на защищенных виртуальных машинах.
- Регулярности обновлений программ.
- Политиках использования программ, принятых в организации. Это могут быть политики безопасности или административные политики.
- Расположении хранилищ установочных пакетов программ.

Чтобы получить информацию о программах, которые используются на защищенных виртуальных машинах в локальной сети организации, вы можете использовать данные, представленные в папках **Реестр программ** и **Исполняемые файлы**. Папки **Реестр программ** и **Исполняемые файлы** входят в состав папки **Управление программами** дерева консоли Kaspersky Security Center (подробнее см. в документации Kaspersky Security Center).

Папка **Реестр программ** содержит список программ, которые обнаружил на защищенных виртуальных машинах установленный на них Агент администрирования.

Папка **Исполняемые файлы** содержит список исполняемых файлов, которые когда-либо запускались на защищенных виртуальных машинах или были обнаружены в процессе работы задачи инвентаризации Kaspersky Security.

В окне свойств выбранной программы в папке **Реестр программ** или **Исполняемые файлы**, 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.

Этап 2. Создание категорий программ

На этом этапе требуется создать категории программ, на основе которых можно создать правила контроля запуска программ.

Рекомендуется создать категорию «Программы для работы», которая включает в себя стандартный набор программ, используемых в организации. Если различные группы пользователей используют различные наборы программ для работы, вы можете создать отдельную категорию программ для каждой группы пользователей.

► *Чтобы создать категорию программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Откройте папку **Управление программами** → **Категории программ** дерева консоли.
3. Запустите мастер создания пользовательской категории по ссылке **Создать категорию** в рабочей области.
4. Следуйте указаниям мастера создания пользовательской категории.

Этап 3. Создание разрешающих правил контроля запуска программ

На этом этапе требуется создать правила контроля запуска программ, которые разрешают пользователям локальной сети организации запускать на защищенных виртуальных машинах программы, принадлежащие к категориям, созданным на предыдущем этапе.

► *Чтобы создать разрешающее правило контроля запуска программ выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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.

5. По правой кнопке мыши откройте контекстное меню политики для Легкого агента для Windows и выберите пункт **Свойства**.

   Откроется окно свойств политики для Легкого агента для Windows.

6. В окне свойств политики для Легкого агента для Windows выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

7. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило контроля запуска программ**.

8. Из раскрывающегося списка **Категория** выберите созданную на предыдущем этапе категорию программ, на основе которой вы хотите создать разрешающее правило.

9. Задайте список пользователей и / или групп пользователей, которым разрешено запускать программы, принадлежащие к выбранной категории. Для этого в поле **Пользователи и / или группы, получающие разрешение** введите имена пользователей и / или групп пользователей вручную или нажмите на кнопку **Выбрать**. Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**. В этом окне вы можете выбрать пользователей и / или группы пользователей.

10. Список пользователей, которым запрещено запускать программы, принадлежащие к выбранной категории, оставьте пустым.

11. 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.

12. Нажмите на кнопку **ОК**.

13. Нажмите на кнопку **Применить** в разделе **Контроль запуска программ** окна свойств политики для Легкого агента для Windows.

Этап 4. Тестирование разрешающих правил контроля запуска программ

На этом этапе требуется выполнить следующие действия:

1. Изменить статус работы созданных разрешающих правил контроля запуска программ на *Тест* (см. раздел «*Изменение статуса правила контроля запуска программ*» на стр. 180).

2. Проанализировать работу тестовых разрешающих правил контроля запуска программ.

   Для анализа работы тестовых правил контроля запуска программ требуется изучить события о работе компонента Легкого агента Контроль запуска программ, приходящие в Kaspersky Security Center. Если разрешен запуск всех программ, которые вы имели в виду при формировании категорий программ, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами категорий программ и правил контроля запуска программ.

► *Чтобы в хранилище событий Kaspersky Security Center просмотреть события о работе компонента Легкого агента Контроль запуска программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В рабочей области узла **Сервер администрирования** выберите закладку **События** и на ней выберите нужную выборку событий: **Информационные события** или **Критические события** для просмотра событий о разрешенных или запрещенных запусках программ соответственно. В списке отображаются все события выбранного уровня важности, переданные в Kaspersky Security Center за период, указанный в свойствах Сервера администрирования.

3. Для просмотра информации о событии откройте окно свойств события одним из следующих способов:

   - Дважды нажмите левой клавишей мыши по событию.
   - По правой клавише мыши откройте контекстное меню события и выберите пункт **Свойства**.
   - По ссылке **Открыть окно свойств события** справа от списка событий.

Этап 5. Переход к режиму «Белый список»

На этом этапе требуется выполнить следующие действия:

- Включить созданные вами правила контроля запуска программ. Для этого требуется изменить статус работы правил с *Тест* на *Вкл*.
- Включить созданные по умолчанию правила «Доверенные программы обновления» и «Операционная система и ее компоненты». Для этого требуется изменить статус работы правил с *Выкл* на *Вкл*.
- Выключить созданное по умолчанию правило «Разрешить все». Для этого требуется изменить статус работы правил с *Вкл* на *Выкл*.

Подробная информация о статусах правил контроля запуска программ приведена в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*.

Изменение статуса 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 компьютеры** 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.
5. По правой кнопке мыши откройте контекстное меню политики для Легкого агента для Windows и выберите пункт **Свойства**.

   Откроется окно свойство политики для Легкого агента для Windows.
6. В окне свойств политики для Легкого агента для Windows выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
7. Выберите правило контроля запуска программ, статус работы которого вы хотите изменить.
8. В графе **Статус** выполните одно из следующих действий:
   - Если вы хотите включить использование правила, выберите значение *Вкл*.
   - Если вы хотите выключить использование правила, выберите значение *Выкл*.
   - Если вы хотите, чтобы правило работало в тестовом режиме, выберите значение *Тест*.
9. Нажмите на кнопку **Применить**.

Настройка Контроля устройств через Kaspersky Security Center

Контроль устройств обеспечивает безопасность конфиденциальных данных путем ограничения доступа пользователей к устройствам, установленным или подключенным к защищенной виртуальной машине, с помощью *правил доступа к устройствам* и *правил доступа к шинам подключения* (подробная информация об этих правилах приведена в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

Кроме того, вы можете настроить список доверенных устройств. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

> Компонент Контроль устройств доступен, если программа Kaspersky Security установлена на виртуальной машине с настольной операционной системой Windows. Этот компонент недоступен, если программа Kaspersky Security установлена на виртуальной машине с серверной операционной системой Windows.

Настройка компонента Контроль устройств возможна как в локальном интерфейсе Легкого агента, так и на стороне Kaspersky Security Center.

Однако Kaspersky Security Center дополнительно предоставляет следующие инструменты, недоступные в локальном интерфейсе Легкого агента для Windows:

- Добавление устройств в список доверенных по их модели или идентификатору (на стр. 182).
- Добавление устройств в список доверенных по маске их идентификатора (на стр. 184).

> Если устройство добавлено в список доверенных устройств, а для устройств этого типа создано правило доступа, запрещающее или ограничивающее доступ, то при принятии решения о доступе к устройству наличие устройства в списке доверенных устройств имеет более высокий приоритет, чем правило доступа.

В этом разделе

Добавление устройств в список доверенных по их модели или идентификатору

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей «Все»).

Добавление устройств в список доверенных по их модели или по их идентификатору возможно только на стороне Kaspersky Security Center.

► *Чтобы добавить устройства в список доверенных по их модели или идентификатору, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите сформировать список доверенных устройств.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
   - Перейдите по ссылке **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Контроль устройств**.
7. В правой части окна выберите закладку **Доверенные устройства**.
8. Нажмите на кнопку **Добавить**.

   Откроется контекстное меню кнопки.
9. В контекстном меню кнопки **Добавить** выполните одно из следующих действий:
   - Выберите пункт **Устройства по идентификатору**, если вы хотите добавить в список доверенные устройства, для которых известны их уникальные идентификаторы.
   - Выберите пункт **Устройства по модели**, если вы хотите добавить в список доверенные устройства, для которых известны VID (идентификатор производителя) и PID (идентификатор продукта).

10. В открывшемся окне в раскрывающемся списке **Тип устройств** выберите тип устройств для вывода в таблице ниже.

11. Нажмите на кнопку **Обновить**.

    В таблице отобразится список устройств, для которых известны их идентификаторы и / или модели и которые отнесены к типу, указанному в раскрывающемся списке **Тип устройств**.

12. Установите флажки напротив названий устройств, которых вы хотите добавить в список доверенных устройств.

13. Нажмите на кнопку **Выбрать**.

    Откроется окно **Выбор пользователей или групп**.

14. В окне **Выбор пользователей или групп** задайте пользователей и / или группы пользователей, для которых Kaspersky Security распознает выбранные устройства как доверенные.

    Имена пользователей и / или групп пользователей, заданных в окне **Выбор пользователей или групп**, отобразятся в поле **Разрешать пользователям и / или группам пользователей**.

15. Нажмите на кнопку **ОК**.

    В таблице на закладке **Доверенные устройства** отобразятся строки с параметрами добавленных доверенных устройств.

16. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Добавление устройств в список доверенных по маске их идентификатора

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей «Все»).

Добавление устройств в список доверенных по маске их идентификатора возможно только на стороне Kaspersky Security Center.

► *Чтобы добавить устройства в список доверенных по маске их идентификатора, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите сформировать список доверенных устройств.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
   - Перейдите по ссылке **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Контроль устройств**.
7. В правой части окна выберите закладку **Доверенные устройства**.
8. Нажмите на кнопку **Добавить**.

   Откроется контекстное меню кнопки.
9. В контекстном меню кнопки **Добавить** выберите пункт **Устройства по маске идентификатора**.

   Откроется окно **Добавление доверенных устройств по маске идентификатора**.
10. В окне **Добавление доверенных устройств по маске идентификатора** в поле **Маска** введите маску для идентификаторов устройств.

11. Нажмите на кнопку **Выбрать**.

    Откроется окно **Выбор пользователей или групп**.

12. В окне **Выбор пользователей или групп** задайте пользователей и / или группы пользователей, для которых Kaspersky Security распознает устройства, модели или идентификаторы которых удовлетворяют заданной маске, как доверенные.

    Имена пользователей и / или групп пользователей, заданных в окне **Выбор пользователей или групп**, отобразятся в поле **Разрешать пользователям и / или группам пользователей**.

13. Нажмите на кнопку **ОК**.

    В таблице на закладке **Доверенные устройства** окна параметров компонента **Контроль устройств** появится строка с параметрами правила добавления устройств в список доверенных по маске их идентификаторов.

14. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Технология лечения активного заражения

Этот раздел содержит информацию о технологии лечения активного заражения, а также инструкцию о том, как включить использование технологии лечения активного заражения для серверных операционных систем Windows на защищенных виртуальных машинах.

В этом разделе

О технологии лечения активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность в операционной системе Windows, 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. Технология лечения активного заражения требует значительных ресурсов операционной системы Windows, что может замедлить работу других программ.

После окончания процедуры лечения активного заражения на виртуальной машине с настольной операционной системой Windows программа Kaspersky Security запрашивает разрешение на перезагрузку виртуальной машины. После перезагрузки виртуальной машины Kaspersky Security удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку виртуальной машины.

Запрос перезагрузки на виртуальной машине с серверной операционной системой Windows невозможен из-за особенностей программы Kaspersky Security для серверных операционных систем. Незапланированная перезагрузка серверной операционной системы может повлечь за собой проблемы, связанные с временным отказом доступа к данным серверной операционной системы или потерей несохраненных данных. Перезагрузку серверной операционной системы рекомендуется выполнять строго по расписанию. Поэтому по умолчанию технология лечения активного заражения на защищенной виртуальной машине с серверной операционной системой Windows выключена.

В случае обнаружения активного заражения на защищенной виртуальной машине с серверной операционной системой Windows в Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на защищенной виртуальной машине с серверной операционной системой Windows требуется включить технологию лечения активного заражения для серверных операционных систем (см. раздел «Включение и выключение технологии лечения активного заражения для серверных операционных систем» на стр. 189) и запустить групповую задачу поиска вирусов в удобное для пользователей серверной операционной системы время.

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.

Включение и выключение технологии лечения активного заражения для серверных операционных систем

► *Чтобы включить / выключить технологию лечения активного заражения для серверных операционных систем Windows, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** 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.

5. По правой кнопке мыши откройте контекстное меню политики для Легкого агента и выберите пункт **Свойства**.

   Откроется окно свойство политики для Легкого агента.

6. В окне свойств политики для Легкого агента выберите раздел **Основные параметры защиты**.

7. В правой части окна выполните одно из следующих действий:

   - Установите флажок **Применять технологию лечения активного заражения**, если вы хотите включить технологию лечения активного заражения.

   - Снимите флажок **Применять технологию лечения активного заражения**, если вы хотите выключить технологию лечения активного заражения.

8. Нажмите на кнопку **ОК** в окне свойств политики, чтобы сохранить внесенные изменения. Окно свойств политики закроется.

9. В рабочей области выберите закладку **Задачи**.

10. В списке задач выберите задачу **Поиск вирусов**.

11. По правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**.

    Откроется окно **Свойства: Поиск вирусов**.

12. В окне **Свойства: Поиск вирусов** выберите раздел **Параметры**.

    В правой части окна отобразятся параметры групповой задачи поиска вирусов.

13. В блоке параметров **Действие при обнаружении угрозы** выполните одно из следующих действий:

    - Установите флажок **Выполнять лечение активного заражения немедленно**, если вы хотите включить технологию лечения активного заражения.

    - Снимите флажок **Выполнять лечение активного заражения немедленно**, если вы хотите выключить технологию лечения активного заражения.

14. Нажмите на кнопку **ОК** в окне **Свойства: Поиск вирусов**, чтобы сохранить внесенные изменения.

Участие в Kaspersky Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

В этом разделе

Об участии в Kaspersky Security Network

Чтобы повысить эффективность защиты виртуальных машин, Kaspersky Security использует данные, полученные от пользователей 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 программы Kaspersky Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры различают:

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

Информация о том, какой тип KSN использует программа Kaspersky Security, отображается в свойствах политики для Сервера защиты (см. раздел «Настройка использования Kaspersky Security Network» на стр. 195) и в локальном интерфейсе Легкого агента для Windows (см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

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

Чтобы продолжить использовать Локальный KSN после изменения ключа, требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с KSN невозможен.

Если вы участвуете в Kaspersky Security Network и используете Глобальный KSN, определенная информация, полученная в результате работы Kaspersky Security на виртуальной машине пользователя, автоматически отправляется в «Лабораторию Касперского» (см. раздел «О предоставлении данных» на стр. 193).

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

Участие в Kaspersky Security Network является добровольным. Решение об участии в Kaspersky Security Network принимается при создании политики для Сервера защиты, его можно изменить в любой момент (см. раздел «Настройка использования Kaspersky Security Network» на стр. 195).

О предоставлении данных

Принимая условия участия в Kaspersky Security Network, вы соглашаетесь передавать в «Лабораторию Касперского» в автоматическом режиме следующие сведения:

- Информацию об установке и лицензировании установленной версии программы Kaspersky Security, включая версию программы, информацию о файлах загружаемых модулей и версии используемых баз программы.
- Информацию об установленном на виртуальных машинах аппаратном и программном обеспечении, в том числе версию операционной системы, установленные пакеты обновлений, загруженные объекты.
- Информацию о состоянии антивирусной защиты виртуальных машин, включая версии используемых антивирусных баз, данные статистик обновлений и соединений с серверами «Лаборатории Касперского».
- Информацию обо всех вредоносных объектах и действиях (в том числе название детектируемого объекта, MD5-хеш, дата и время обнаружения, веб-адрес, по которому он был загружен, названия и размер зараженных файлов и пути к ним, IP-адрес атакующего компьютера и номер порта, на который была направлена сетевая атака, перечень активностей вредоносной программы, вредоносные веб-адреса), а также информацию о ваших решениях и решениях программы в отношении этих объектов и действий.
- Информацию о загружаемых вами файлах (веб-адрес, IP-адрес, с которого выполнена загрузка, атрибуты, размер файла, информация о процессе, загрузившем файл).
- Информацию о запускаемых на виртуальных машинах программах и их модулях (размер, атрибуты, дата создания, информация заголовка PE, имена файлов и их модулей, упаковщики).
- Информацию об обнаруженных на виртуальных машинах уязвимостях, включая идентификатор уязвимости в базе уязвимостей, класс опасности уязвимости и статус обнаружения.

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

Параметры, определяющие состав данных, отправляемых в «Лабораторию Касперского», и получателя данных, хранятся в конфигурационных файлах на защищенной виртуальной машине. Безопасность конфигурационных файлов на защищенной виртуальной машине обеспечивает механизм самозащиты (см. подробнее в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*). 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.

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

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

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

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

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

Настройка использования Kaspersky Security Network

Настройка использования служб Kaspersky Security Network выполняется в параметрах политики для Сервера защиты. Если в активной политике группы администрирования использование служб Kaspersky Security Network включено, 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 служб Kaspersky Security Network включено, не активна, службы KSN не используются в работе программы Kaspersky Security.

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

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** 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 и выберите пункт **Свойства**.

5. В списке слева выберите раздел **Параметры KSN**.

6. Выполните одно из следующих действий:

   - Установите флажок **Принимаю условия Положения и участвую в KSN**, если вы хотите включить использование служб Kaspersky Security Network.

   - Снимите флажок **Принимаю условия Положения и участвую в KSN**, если вы хотите выключить использование служб Kaspersky Security Network.

   Установка флажка **Принимаю условия Положения и участвую в KSN** означает, что вы согласны с условиями участия в программе Kaspersky Security Network, изложенными в Положении о Kaspersky Security Network.

7. Если вы установили флажок **Принимаю условия Положения и участвую в KSN**, укажите параметры использования служб Kaspersky Security Network в работе программы:

   - **Использовать для проверки файлов и категоризации**.

     Флажок включает / выключает использование служб KSN в работе следующих компонентов Легкого агента и задач:

     - Контроль запуска программ.
     - Контроль активности программ.
     - Файловый Антивирус.
     - Мониторинг системы.
     - Задачи проверки.

     Если флажок установлен, то в ходе работы перечисленных компонентов Легкого агента и задач программа Kaspersky Security получает от служб KSN сведения о категории и репутации проверяемых файлов.

     Если флажок снят, то Kaspersky Security не получает от служб KSN сведения о репутации и категории файлов.

     Флажок доступен, если установлен флажок **Принимаю условия Положения и участвую в KSN**.

- **Использовать для проверки веб-адресов**.

  Флажок включает / выключает использование служб KSN в работе следующих компонентов Легкого агента для Windows:

  - Веб-Антивирус.
  - Веб-Контроль.
  - IM-Антивирус.

  Если флажок установлен, то в ходе работы перечисленных компонентов Легкого агента для Windows программа Kaspersky Security получает от служб KSN сведения о репутации проверяемых веб-адресов.

  Если флажок снят, то Kaspersky Security не получает от служб KSN сведения о репутации веб-адресов.

  Флажок доступен, если установлен флажок **Принимаю условия Положения и участвую в KSN**.

8. Если вы хотите запретить или разрешить изменение параметров KSN в политиках вложенного уровня иерархии (для вложенных групп администрирования), нажмите на значок «замок» слева от флажка **Принимаю условия Положения и участвую в KSN**.

9. Нажмите на кнопку **ОК**.

Управление Легким агентом для Linux из командной строки

Этот раздел содержит информацию об управлении компонентом Легкий агент для Linux с помощью команд из командной строки и настройке параметров команд.

Управление Легким агентом для Linux через командную строку также описано в Базе знаний (http://support.kaspersky.ru/13170).

В этом разделе

Вывод справки о командах Kaspersky Security

Команда help выводит справку о командах управления программой Kaspersky Security.

Синтаксис команды

```
/opt/kaspersky/lightagent/bin/avp-cli help [command]
```

где:

command – название команды управления, справку о которой вы хотите получить.

Возможные значения:

- license – команда, которая выводит информацию о лицензии на SVM;
- list – команда, которая выводит список файлов резервного хранилища;
- restore – команда, которая восстанавливает файл из резервного хранилища;
- scan – команда, которая запускает антивирусную проверку виртуальной машины;
- statistics – команда, которая выводит статистику о работе задачи обновления;
- status – команда, которая выводит информацию о текущем состоянии задачи обновления;
- start – команда, которая запускает задачу обновления баз;
- stop – команда, которая останавливает выполнение задачи обновления баз;
- svminfo – команда, которая выводит информацию о SVM, к которым подключена защищенная виртуальная машина;
- trace – команда, которая включает или выключает создание файлов трассировки на защищенной виртуальной машине;
- update – команда, которая запускает задачу обновления баз с дополнительными параметрами.

Перед выполнением команд убедитесь, что служба lightagent запущена на защищенной виртуальной машине.

Просмотр информации о состоянии защиты виртуальной машины

Вы можете узнать о состоянии защищенной виртуальной машины с установленным компонентом Легкий агент для Linux помощью следующих команд:

- команда svminfo (см. раздел «Просмотр информации о SVM» на стр. 200) позволяет получить информацию о SVM, к которой подключен Легкий агент для Linux, и о способах получения информации о SVM;
- команда license (см. раздел «Просмотр информации о лицензии» на стр. 201) позволяет получить информацию о лицензии, по которой программа активирована на SVM;
- команда status (см. раздел «Просмотр состояния задачи обновления» на стр. 208) позволяет получить информацию о текущем состоянии задачи обновления;
- команда statistics (см. раздел «Просмотр статистики работы задачи обновления» на стр. 208) позволяет получить информацию о статистике работы задачи обновления (проценте выполнения задачи, объеме загруженных обновлений и другую информацию);
- команда update (см. раздел «Запуск задачи обновления с дополнительными параметрами» на стр. 207) позволяет запускать задачу обновления баз и сохранять в файле отчета информацию о событиях, возникающих во время выполнения задачи обновления (проценте выполнения задачи, результате выполнения задачи и других событиях).

Просмотр информации о SVM

По умолчанию Легкие агенты обнаруживают SVM, работающие в сети, с помощью многоадресной рассылки (Multicast). При необходимости можно настроить другие способы обнаружения SVM (см. раздел «Об обнаружении SVM» на стр. 35). Способ, который используют Легкие агенты для обнаружения SVM, настраивается администратором в политике для Легкого агента для Linux (см. раздел «Шаг 5. Настройка параметров обнаружения SVM» на стр. 114).

Вы можете получить информацию о SVM, к которой подключен Легкий агент, с помощью команды svminfo.

► *Чтобы просмотреть информацию о 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 имя SVM в формате FQDN.
- Discovery method – способ получения информации о SVM. Возможные значения:
  - Multicast – с помощью многоадресной рассылки (Multicast);
  - 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 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, к которой подключен Легкий агент для Linux, или имя SVM в формате FQDN;
- Key – ключ, добавленный на SVM;

- License type – тип лицензии (коммерческая, пробная, на бета-тестирование, подписка) для количество <server(s)> или <core(s)>;
- Expiration date – дата окончания срока действия лицензии (в формате YYYY-MM-DDTHH:MM:SS);
- Days till expiration – количество дней до окончания срока действия лицензии;

где:

server(s) – максимальное количество одновременно запущенных виртуальных машин с серверной операционной системой, для которых включена защита;

core(s) – максимальное количество одновременно используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

Запуск задачи проверки

Вы можете запустить задачу *выборочной проверки* защищенной виртуальной машины, указав список файлов для проверки, имена файлов (или путей к ним) или шаблоны имен файлов (или путей к ним) с помощью масок. Также вы можете запустить *полную проверку* всех объектов файловой системы защищенной виртуальной машины.

> Из проверки исключены объекты файловой системы /dev, /sys и /proc.

Вы можете запустить задачу проверки с дополнительными параметрами. Эти параметры позволяют сохранять в файл события, возникающие при выполнении задачи, или использовать для выполнения задачи параметры конфигурационного файла.

► *Чтобы запустить задачу проверки, выполните следующую команду:*

```
lightagent scan [<путь к файлу или папке>] [<путь к файлу или папке>...]
[--@:<filelist.lst>] [--R[A]:<путь к файлу отчета>]\

[--C:<путь к конфигурационному файлу>]
```

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.
- @:<filelist.lst> – список файлов для проверки. В текстовом файле укажите с новой строки файлы и папки, которые вы хотите проверить на вирусы и другие вредоносные программы.
- 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.

Обратите внимание на особенности проверки жестких и символических ссылок (см. раздел «Особенности проверки символических и жестких ссылок» на стр. 80).

Выбор действий над зараженными файлами

Вы можете задать следующие действия, которые программа Kaspersky Security будет выполнять при обнаружении зараженных файлов:

- Информировать (i0). При обнаружении зараженных файлов Kaspersky Security информирует вас об этом.
- Лечить (i1). Kaspersky Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, программа оставляет файлы неизменными.

- Лечить. Удалять, если лечение невозможно. Пропускать составные файлы, если лечение и удаление невозможны (i2). 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.
- Лечить. Удалять, если лечение невозможно (i3). 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.
- Удалять (i4). 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.

► *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, которую 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.
- i1 – при обнаружении зараженных файлов выполнять действие Лечить.
- i2 – при обнаружении зараженных файлов выполнять действие Лечить. Удалять, если лечение невозможно. Пропускать составные файлы, если лечение и удаление невозможны.
- i3 – при обнаружении зараженных файлов выполнять действие Лечить. Удалять, если лечение невозможно. Это действие выполняется по умолчанию.
- i4 – при обнаружении зараженных файлов выполнять действие Удалять.

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.

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 отключить использование технологии iChecker, выполните следующую команду:*

```
lightagent scan --iChecker:off
```

► *Чтобы включить использование технологии iChecker, выполните следующую команду:*

```
lightagent scan --iChecker:on
```

Запуск и остановка задачи обновления

► *Чтобы запустить задачу обновления, выполните следующую команду:*

```
lightagent start Updater
```

Для запуска задачи обновления баз с дополнительными параметрами используйте команду update (см. раздел «Запуск задачи обновления с дополнительными параметрами» на стр. 207).

► *Чтобы остановить задачу обновления, выполните следующую команду:*

```
lightagent stop Updater
```

Запуск задачи обновления с дополнительными параметрами

Кроме стандартной команды запуска задачи обновления start (см. раздел «Запуск и остановка задачи обновления» на стр. 206), вы можете использовать команду запуска задачи обновления с дополнительными параметрами. Эти параметры позволяют сохранять в файл события, возникающие при выполнении задачи, или использовать для выполнения задачи параметры конфигурационного файла.

► *Чтобы запустить задачу обновления, 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 и сохранить информацию обо всех 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.

Просмотр состояния задачи обновления

Вы можете просмотреть текущее состояние задачи обновления.

► *Чтобы просмотреть состояние задачи обновления, выполните следующую команду:*

```
lightagent status Updater
```

Команда выводит одно из следующих состояний задачи обновления:

- Running – выполняется;
- Starting – запускается;
- NeverStarted – не была запущена;
- Stopped – остановлена;
- Stopping – останавливается.

Просмотр статистики работы задачи обновления

► *Чтобы просмотреть статистику работы задачи обновления, выполните следующую команду:*

```
lightagent statictics Updater
```

Команда выводит следующую информацию о задаче обновления:

- Current time – текущее время.
- Time Start – время запуска задачи.
- Time Finish – время завершения выполнения задачи.
- Completion – процент выполнения задачи.
- 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/с).

Резервное хранилище

Этот раздел содержит инструкции о том, как работать с резервным хранилищем.

В этом разделе

О резервном хранилище

Резервное хранилище – это список резервных копий зараженных файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Если в файле обнаружен вредоносный код, Kaspersky Security блокирует файл, удаляет его из папки исходного размещения, затем помещает его копию в резервное хранилище и пытается провести лечение файла.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете восстановить файл из его резервной копии (см. раздел «Восстановление файлов из резервного хранилища» на стр. 211).

Просмотр списка файлов в резервном хранилище

► *Чтобы просмотреть список файлов в резервном хранилище, выполните следующую команду:*

```
lightagent list backup
```

Команда выводит следующую информацию о файлах в резервном хранилище:

- дата и время помещения файла в резервное хранилище (в формате YYYY-MM-DDTHH:MM:SS);
- идентификатор файла;
- путь, по которому файл обнаружен и по которому файл будет восстановлен (см. раздел «Восстановление файлов из резервного хранилища» на стр. 211).

Восстановление файлов из резервного хранилища

Восстановление зараженных файлов из резервного хранилища может привести к заражению виртуальной машины.

► *Чтобы восстановить файл из резервного хранилища, выполните следующую команду:*

```
lightagent restore [--replace] <идентификатор файла>
```

где:

- <идентификатор файла> – числовой идентификатор файла в резервном хранилище;
- replace – перезаписать файл с указанным идентификатором восстановленным файлом, если он находится в той же папке.

Программа восстановит файл в папку исходного размещения.

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 (см. раздел «Источники информации о программе» на стр. 14), 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.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (http://support.kaspersky.ru/b2b);
- отправить запрос в Службу технической поддержки «Лаборатории Касперского» с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы «Лаборатории Касперского». Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами «Лаборатории Касперского» с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами «Лаборатории Касперского» и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в «Лабораторию Касперского», а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/faq/companyaccount_help).

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 трассировки SVM и защищенной виртуальной машины;
- файлы дампа SVM и защищенной виртуальной машины;

Файлы дампа сохраняются на виртуальной машине в доступном для чтения виде. Рекомендуется обеспечить защиту информации, которая хранится на виртуальной машине, от несанкционированного доступа до ее передачи в «Лабораторию Касперского». За подробной информацией о том, как создать файл дампа, вы можете обратиться к специалистам Службы технической поддержки.

Изменение параметров программы

Кроме того, 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;
- выполнить более тонкую настройку работы отдельных компонентов Легкого агента, недоступную через стандартные средства пользовательского интерфейса;
- изменить параметры хранения диагностической информации;
- включить режим отладки для Сервера интеграции;
- настроить перехват сетевого трафика и сохранение сетевого трафика в файле.

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.

Получение информации о SVM, подключенных к Серверу интеграции

Специалисты Службы технической поддержки могут попросить вас предоставить информацию о SVM, подключенных к Серверу интеграции.

► *Чтобы получить информацию о SVM, подключенных к Серверу интеграции, выполните следующие действия:*

1. На компьютере, на котором установлена Консоль администрирования Kaspersky Security Center, создайте строковый параметр SVMPlugin и установите для него значение 1 в следующей ветке реестра операционной системы:
   - HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\VIIS\Console\Public\ (для 32-разрядной операционной системы);
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\VIIS\Console\Public\ (для 64-разрядной операционной системы).
2. Запустите Консоль управления Сервера интеграции (см. в *Руководстве по внедрению Kaspersky Security для виртуальных сред 4.0 Легкий агент*).
3. Откройте раздел **Список подключенных SVM**.

   В правой части окна отобразятся параметры SVM, подключенных к Серверу интеграции.

О составе файлов трассировки

Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

Вы можете просмотреть данные, записанные в файлы трассировки. Для консультации по просмотру данных вам нужно обратиться в Службу технической поддержки «Лаборатории Касперского».

Все файлы трассировки содержат следующие общие данные:

- время события;
- номер потока выполнения;
- компонент программы, в результате работы которого произошло событие;
- степень важности события (информационное, предупреждение, критическое, ошибка);
- описание события выполнения команды компонента программы и результата выполнения этой команды.

Состав файлов трассировки SVM

Содержание файла трассировки ScanServer.log

В файл трассировки ScanServer.log, помимо общих данных (см. раздел «О составе файлов трассировки» на стр. 216), может записываться следующая информация:

- Персональные данные, в том числе фамилия, 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.

Содержание файла трассировки Агента администрирования

Файл трассировки Агента администрирования, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файла трассировки boot_config.log

Файл трассировки boot_config.log, помимо общих данных, содержит информацию о первом запуске после развертывания SVM или изменения конфигурации SVM.

Содержание файла трассировки wdserver.log

Файл трассировки wdserver.log, помимо общих данных, содержит информацию о событиях, возникающих во время работы службы watchdog.

Состав файлов трассировки Легкого агента для Windows

Содержание файлов трассировки SRV.log и GUI.log

В файлы трассировки SRV.log и GUI.log, помимо общих данных (см. раздел «О составе файлов трассировки» на стр. 216), может записываться следующая информация:

- Персональные данные, в том числе фамилия, 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 интернет-трафика. Трафик записывается в файлы трассировки только из исполняемого файла компонента Мониторинг сети trafmon2.ppl.
- 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.

Содержание файлов трассировки Dumpwriter.log, AVPCon.dll.log

Файл трассировки Dumpwriter.log, помимо общих данных, содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи файла дампа.

Файл трассировки AVPCon.dll.log, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файла трассировки плагина Почтового Антивируса

Файл трассировки плагина Почтового Антивируса mcou.OUTLOOK.EXE, помимо общих данных, может содержать части сообщений, в том числе адреса электронной почты.

Содержание файла трассировки ALL.log

Файл трассировки ALL.log, помимо общих данных, содержит информацию о событиях командной строки.

Состав файлов трассировки Легкого агента для Linux

Содержание файла трассировки LightAgent.log

В файл трассировки LightAgent.log, помимо общих данных (см. раздел «О составе файлов трассировки» на стр. 216), может записываться следующая информация:

- Персональные данные, в том числе фамилия, 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.

Содержание файла трассировки Агента администрирования

Файл трассировки Агента администрирования, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файла трассировки avp-cli.log

Файл трассировки avp-cli.log, помимо общих данных, содержит информацию о событиях командной строки.

Содержание файла трассировки install.log

Файл трассировки install.log, помимо общих данных, содержит вывод результатов выполнения команд, формирующих необходимые параметры для подготовки запуска Легкого агента для Linux.

Содержание файла трассировки wdserver.log

Файл трассировки wdserver.log, помимо общих данных, содержит информацию о событиях, возникающих во время работы службы watchdog.

Работа с файлами трассировки SVM

Вы можете создать файл трассировки SVM и настроить уровень детализации отладочной информации с помощью конфигурационного файла программы ScanServer.conf, расположенного на SVM. За подробной информацией о том, как создать и настроить файл трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Файлы трассировки сохраняются на SVM в доступном для чтения виде. Пользователь несет ответственность за обеспечение безопасности информации и, в частности, за контроль и ограничение доступа к информации, которая хранится на SVM, до ее передачи в «Лабораторию Касперского».

Для анализа ошибки, произошедшей в ходе развертывания или изменения конфигурации SVM, может потребоваться отключить функцию отката внесенных изменений. Для этого нужно изменить файл Kaspersky.Virtualization.Wizard.exe.config. Файл расположен на компьютере, на котором установлена Консоль администрирования Kaspersky Security Center.

► *Чтобы отключить функцию отката, выполните следующие действия:*

1. На компьютере, на котором установлена Консоль администрирования Kaspersky Security Center, откройте для изменения в текстовом редакторе файл Kaspersky.Virtualization.Wizard.exe.config. Файл расположен в следующей папке в зависимости от установленной операционной системы:

   - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\la.plg\DeployWizard\ (для 64-разрядной операционной системы);
   - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\la.plg\DeployWizard\ (для 32-разрядной операционной системы).

   Изменение файла требуется выполнять от имени администратора.

2. В секции `<appSettings></appSettings>` измените строку

   `<add key=" disableRollback" value="false" />` следующим образом:

   `<add key=" disableRollback" value="true" />`

3. Сохраните и закройте файл Kaspersky.Virtualization.Wizard.exe.config.

Работа с файлами трассировки на Легком агенте для Windows

Вы можете создать файл трассировки на защищенной виртуальной машине с компонентом Легкий агент для Windows с помощью программы Kaspersky Security.

► *Чтобы создать файлы трассировки на защищенной виртуальной машине с компонентом Легкий агент для Windows, выполните следующие действия:*

1. На защищенной виртуальной машине откройте главное окно программы Kaspersky Security (см. *Руководство пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

2. По ссылке **Поддержка**, расположенной в нижней части главного окна программы, откройте окно **Поддержка**.

3. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

   Откроется окно **Информация для поддержки**.

4. 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)**.

5. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.

6. Воспроизведите ситуацию, при которой у вас возникает проблема.

7. Чтобы остановить процесс трассировки, нажмите на кнопку **Выключить**.

Программа создаст файлы трассировки с уникальным именем KSVLA.<номер версии>_<дата и время создания_GMT>_<PID>.<тип файла трассировки>.log.enc1 в папке %ProgramData%\Kaspersky Lab.

Файлы трассировки сохраняются на защищенной виртуальной машине с компонентом Легкий агент для Windows в измененном и недоступном для чтения виде в течение всего времени использования программы и безвозвратно удаляются при удалении программы.

Кроме того, вы можете получить файл трассировки защищенной виртуальной машины с компонентом Легкий агент для Windows с помощью ключей реестра. См. описание на странице программы в Базе знаний (http://support.kaspersky.ru/13174).

Работа с файлами трассировки на Легком агенте для Linux

На защищенной виртуальной машине с компонентом Легкий агент для Linux вы можете создавать, сохранять и удалять файлы трассировки.

► *Чтобы создать файл трассировки на защищенной виртуальной машине с компонентом Легкий агент для Linux, выполните следующие команду:*

```
lightagent trace 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 будет создавать файлы трассировки с уровнем детализации по умолчанию – 500.

Программа создаст файл трассировки с уникальным именем LightAgent.<дата и время создания>.log в папке /var/log/kaspersky/lightagent. Вы можете сохранить созданный файл трассировки в другую папку на защищенной виртуальной машине.

Файлы трассировки хранятся на защищенной виртуальной машине с компонентом Легкий агент для Linux в доступном для чтения виде и безвозвратно удаляются при удалении программы. Пользователь несет ответственность за обеспечение безопасности информации и, в частности, за контроль и ограничение доступа к информации, которая хранится на защищенной виртуальной машине, до ее передачи в «Лабораторию Касперского».

► *Чтобы сохранить файл трассировки на защищенной виртуальной машине с компонентом Легкий агент для Linux, выполните следующую команду:*

```
lightagent trace --copyto <путь к файлу трассировки> [--overwrite]
```

где:

- copyto <путь к файлу трассировки> – сохранить файл трассировки в указанной папке. Укажите полный путь к папке, в которую вы хотите сохранить файл трассировки.
- overwrite – если в указанной папке находится файл трассировки с таким именем, перезаписать этот файл сохраняемым файлом трассировки.

► *Чтобы отключить создание файла трассировки на защищенной виртуальной машине с компонентом Легкий агент для Linux, выполните следующую команду:*

```
lightagent trace off
```

► *Чтобы удалить файлы трассировки с защищенной виртуальной машины с компонентом Легкий агент для Linux, выполните следующую команду:*

```
lightagent trace --clear
```

Программа удалит файлы трассировки из папки /var/log/kaspersky/lightagent.

О журналах Сервера интеграции

Информация о работе Сервера интеграции и Консоли управления Сервера интеграции записывается в следующие журналы:

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

Журнал работы Сервера интеграции вы можете открыть для просмотра по ссылке **Посмотреть журнал работы** в разделе **Параметры Сервера интеграции** Консоли управления Сервера интеграции.

Сведения, записанные в журналы Сервера интеграции, не отправляются автоматически в «Лабораторию Касперского». Вы можете использовать журналы при обращении в Службу технической поддержки. Информация, записанная в файлах журналов, может потребоваться для анализа и выяснения причин возникновения ошибок в работе Сервера интеграции.

Журналы хранятся в незашифрованном виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа.

Вы можете изменить уровень детализации информации в журналах Сервера интеграции с помощью конфигурационного файла. За подробной информацией вы можете обратиться к специалистам Службы технической поддержки.

Глоссарий

K

Kaspersky CompanyAccount

Портал, предназначенный для отправки электронных запросов в «Лабораторию Касперского» и отслеживания их обработки специалистами «Лаборатории Касперского».

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ «Лаборатории Касперского» получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network «Лаборатории Касперского» со своей стороны.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» орепутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ «Лаборатории Касперского» на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

S

SVM

Secure virtual machine, виртуальная машина защиты. Виртуальная машина на гипервизоре, на которой установлен компонент Сервер защиты Kaspersky Security.

А

Активация программы

Процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Б

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами «Лаборатории Касперского» как фишинговые. База регулярно обновляется и входит в поставку программы «Лаборатории Касперского».

Базы программы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска баз. Базы программы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

Д

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

З

Защищенная виртуальная машина

Виртуальная машина, на которой установлен компонент Легкий агент.

И

Источник обновлений

Ресурс, содержащий обновления баз и модулей программы для программ «Лаборатории Касперского». Источником обновлений для Kaspersky Security является хранилище Сервера администрирования Kaspersky Security Center.

К

Ключ

Уникальная буквенно-цифровая последовательность. Ключ обеспечивает использование программы в соответствии с условиями Лицензионного соглашения (типом лицензии, сроком действия лицензии, лицензионными ограничениями). Вы можете использовать программу только при наличии в ней ключа.

Ключ с ограничением по ядрам

Ключ программы для защиты виртуальных машин независимо от установленной на них операционной системы. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин на гипервизорах, в которых используется определенное количество ядер физических процессоров.

Код активации

Код, который предоставляет вам «Лаборатория Касперского» при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky Security. Этот код требуется для активации программы.

Код активации представляет собой последовательность из двадцати латинских букв и цифр в формате XXXXX-XXXXX-XXXXX-XXXXX.

Л

Лицензионное соглашение

Юридическое соглашение между вами и АО «Лаборатория Касперского», в котором указано, на каких условиях вы можете использовать программу.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации «Лаборатория Касперского». Документ содержит информацию о предоставляемой лицензии.

Лицензия

Ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Н

Настольный ключ

Ключ программы для защиты виртуальных машин с настольной операционной системой.

О

Объекты автозапуска

Набор программ, необходимых для запуска и работы установленных на вашей виртуальной машине операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать такие объекты, что может привести, например, к блокированию запуска операционной системы.

Р

Резервное хранилище

Специализированное хранилище для резервных копий тех файлов, которые были удалены или изменены в процессе лечения.

С

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах «Лаборатории Касперского» и управления ими.

Серверный ключ

Ключ программы для защиты виртуальных машин с серверной операционной системой.

Сигнатурный анализ

Технология обнаружения угроз, которая использует базы программы «Лаборатории Касперского», содержащие описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов «Лаборатории Касперского» этот метод анализа всегда включен.

Ф

Файл ключа

Файл вида xxxxxxxx.key, который предоставляет вам «Лаборатория Касперского» при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky Security. Файл ключа требуется для активации программы.

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Э

Эвристический анализ

Технология обнаружения угроз, информация о которых еще не занесена в базы программы «Лаборатории Касперского». Позволяет находить файлы, которые могут содержать вредоносную программу, не указанную в базах, или новую модификацию известного вируса.

АО «Лаборатория Касперского»

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

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

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с 34 офисами в 31 стране мира. В компании работает более 3000 квалифицированных специалистов.

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

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

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

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

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

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

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

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

CentOS – товарный знак компании Red Hat, Inc.

Citrix, Citrix Provisioning Services, XenApp, XenDesktop, XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

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

Microsoft, Active Directory, Hyper-V, Windows, Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

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

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

VMware, VMware ESXi, VMware Horizon, VMware vCenter, VMware vSphere, PowerCLI – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Предметный указатель

K

S

А

Б

З

К

Л

О

П

С

Ф