KASPERSKY lab

Kaspersky Security для виртуальных сред 4.0 Легкий агент

Руководство по внедрению

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.

Дата редакции документа: 20.01.2017

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

Содержание

Об эт ом руководстве

Руководство по внедрению Kaspersky Security для виртуальных сред 4.0 Легкий агент (далее также «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.

Вы можете применять информацию в этом руководстве для выполнения следующих задач:

- планирование установки программы (учитывая принципы работы программы, системные требования, типовые схемы развертывания, особенности совместимости с другими программами);
- подготовка к установке, установка и активация Kaspersky Security;
- настройка программы после установки;
- обновление и удаление программы.

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. 13)

Этот раздел содержит описание источников информации о программе.

Kaspersky Security для виртуальных сред 4.0 Легкий агент (см. стр. 16)

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

Аппаратные и программные требования (см. стр. 23)

Этот раздел содержит информацию об аппаратных и программных требованиях к программе Kaspersky Security.

Архитектура программы (см. стр. 28)

Этот раздел содержит описание компонентов Kaspersky Security и их взаимодействия.

Подготовка к установке программы (см. стр. 39)

Этот раздел содержит информацию о подготовительных действиях перед установкой программы Kaspersky Security.

Установка программы (см. стр. 57)

Этот раздел содержит пошаговые инструкции по установке программы и описание изменений в Kaspersky Security Center после установки программы.

Активация программы (см. стр. 112)

В этом разделе описана процедура активации программы.

Обновление антивирусных баз (см. стр. 126)

В этом разделе описана процедура обновления антивирусных баз программы.

Запуск и остановка программы (см. стр. 131)

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

Состояние защиты виртуальной машины (см. стр. 133)

Этот раздел содержит информацию об оценке состояния защиты виртуальной машины.

Обновление предыдущей версии программы (см. стр. 134)

Этот раздел содержит информацию об обновлении предыдущей версии программы.

Изменение конфигурации SVM (см. стр. 142)

Этот раздел содержит информацию о том, как изменить конфигурацию SVM (виртуальная машина защиты) с установленным компонентом Сервер защиты.

Просмотр и изменение параметров Сервера интеграции (см. стр. 157)

Этот раздел содержит информацию о том, как посмотреть и изменить параметры Сервера интеграции.

Удаление программы (см. стр. 162)

Этот раздел содержит информацию о том, как удалить программу Kaspersky Security из виртуальной инфраструктуры.

Обращение в Службу технической поддержки (см. стр. 172)

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

Приложение. Описание журнала работы мастера (см. стр. 175)

Этот раздел содержит сведения о том, какая информация записывается в журнал работы мастера во время развертывания SVM и во время изменения конфигурации SVM.

Глоссарий (см. стр. 178)

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

АО «Лаборатория Касперского» (см. стр. 183)

Этот раздел содержит информацию об АО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 185)

Этот раздел содержит информацию о стороннем коде.

Уведомления о товарных знаках (см. стр. 186)

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: …	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.

Пример текста	Описание условного обозначения
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.
<Имя пользователя>	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. 172).

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

Страница Kaspersky Security на веб-сайте «Лаборатории Касперского»

На странице Kaspersky Security (http://www.kaspersky.ru/business-security/virtualization-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 программы 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.

Чтобы поддерживать программу Kaspersky Security в актуальном состоянии, требуется *обновление* баз программы, используемых для обнаружения угроз.

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 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;

- через командную строку для Легкого агента для Linux;

- 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 (см. раздел «Файлы, необходимые для установки программы» на стр. 43), 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 программы 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. 36).

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;
- через командную строку для Легкого агента для Linux;
- 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 программы 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 (см. раздел «Установка Агента администрирования

Kaspersky Security Center на виртуальные машины» на стр. 77). 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 (см. раздел «Установка плагинов управления Kaspersky Security и Сервера интеграции» на стр. 59).

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. 33).

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.

- 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.

- Осуществляет работу с ключами и контроль лицензионных ограничений.

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 (см. раздел «Установка компонента Сервер защиты» на стр. 66). 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. 34). Легкий агент выбирает оптимальную для подключения SVM в соответствии с алгоритмом выбора SVM (см. раздел «Об алгоритме выбора SVM» на стр. 35).

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. 36). 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. 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 или в локальном интерфейсе.

Способ, который используют Легкие агенты для Linux для обнаружения SVM, вы можете выбрать в политике для Легкого агента для Linux.

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. 35).

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.

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 (см. раздел «Установка плагинов управления Kaspersky Security и Сервера интеграции» на стр. 59).

2. Настроить параметры подключения SVM к Серверу интеграции. Настройка параметров подключения выполняется при создании политики для Сервера защиты 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 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.

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 (см. раздел «Просмотр и изменение параметров Сервера интеграции» на стр. 157).

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 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.
- *Задачи* реализуют такие функции программы, как добавление ключа, проверку виртуальных машин, обновление баз и модулей программы.

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.

Информацию о настройке политик и задач для Kaspersky Security см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

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

Подготовка к установке программы

Этот раздел содержит информацию о подготовительных действиях перед установкой программы Kaspersky Security.

В этом разделе

Подготовительные действия

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

Общие действия

- Проверить состав компонентов Kaspersky Security Center (см. раздел «Требования к составу компонентов Kaspersky Security Center» на стр. 47), а также соответствие компонентов Kaspersky Security Center и компонентов виртуальной инфраструктуры аппаратным и программным требованиям к программе Kaspersky Security (см. раздел «Аппаратные и программные требования» на стр. 23).
- Убедиться в том, что на виртуальных машинах, которые вы планируете защищать с помощью Kaspersky Security, не установлено антивирусное программное обеспечение.
- Загрузить файлы, необходимые для установки программы, с веб-сайта «ЛабораторииКасперского» (см. раздел «Файлы, необходимые для установки программы» на стр. 43).

- Убедиться в том, что образ SVM не поврежден. Подробнее о способах проверки образа SVM см. на странице программы в Базе знаний (http://support.kaspersky.ru/ksv4). Вы также можете выполнить проверку целостности образа SVM в ходе развертывания SVM. Проверка выполняется на шаге выбора образа SVM в мастере установки (см. раздел «Шаг 3. Выбор образа SVM» на стр. 71). Если файл образа поврежден или версия образа не поддерживается, мастер отобразит сообщение об ошибке.

- Убедиться в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика между виртуальными машинами, разрешено прохождение сетевого трафика через порты, используемые при установке и работе программы (см. раздел «Настройка портов, используемых программой» на стр. 48).

- Если в сети используется динамическая IP-адресация, обеспечить возможность маршрутизации сетевого трафика от SVM до компьютера, на котором установлен Сервер администрирования Kaspersky Security Center.

- Если вы хотите, чтобы виртуальные машины с установленными компонентами Kaspersky Security автоматически перемещались в группы администрирования после установки программы, требуется создать группы администрирования в Консоли управления Kaspersky Security Center и настроить правила автоматического перемещения виртуальных машин в группы администрирования (см. раздел «Настройка правил перемещения виртуальных машин в группы администрирования» на стр. 54).

Гипервизор Microsoft Windows Server (Hyper-V)

Если в виртуальной инфраструктуре установлен гипервизор Microsoft Windows Server (Hyper-V), перед началом установки компонентов Kaspersky Security вам нужно также выполнить следующие действия:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлен пакет служб интеграции (Integration Services).

- Убедиться в том, что на гипервизоре включен общий сетевой ресурс ADMIN$. На гипервизорах Microsoft Windows Server 2012 R2 Hyper-V для включения общего сетевого ресурса ADMIN$ требуется предварительно установить роль файлового сервера (File Server) с помощью мастера настройки сервера.

- Убедиться в том, что на диске, на котором находится общий сетевой ресурс ADMIN$, достаточно места для размещения образа SVM. В ходе установки компонента Сервер защиты образ SVM копируется на общий сетевой ресурс ADMIN$, затем оттуда переносится в папку, указанную в мастере установки.

- Убедиться в том, что на гипервизорах, не входящих в домен Active Directory, установлено программное обеспечение удаленного управления Windows Remote Management (WinRM) версии 3.0. Windows Remote Management (WinRM) версии 3.0 входит в состав установочного пакета Windows Management Framework 3.0, доступного для загрузки с сайта Microsoft: http://www.microsoft.com/en-us/download/details.aspx?id=34595.

- Если вы хотите использовать доменную учетную запись для подключения SVM к гипервизору, требуется убедиться, что выполняются следующие условия:

  - SVM имеет возможность определять адрес гипервизора с помощью службы доменных имен (DNS) того домена, в котором находится гипервизор, на котором разворачивается SVM.

  - DNS-сервер имеет прямую и обратную записи для SVM.

  - Зоны, содержащие записи о SVM и гипервизоре, на котором развернута SVM, интегрированы с Active Directory.

  - Компьютер, с которого запускается мастер установки компонента Сервер защиты, имеет возможность разрешать имена гипервизоров, на которых разворачивается SVM.

- Если вы хотите, чтобы имя пользователя и пароль учетной записи для подключения к гипервизору, указываемые во время развертывания SVM, передавались в зашифрованном виде, вы можете настроить защищенное соединение с использованием SSL-сертификата между гипервизором, на котором будет развернута SVM, и компьютером, где установлена Консоль администрирования Kaspersky Security Center.

Гипервизор VMware ESXi

Если в виртуальной инфраструктуре установлен гипервизор Vmware ESXi, перед началом установки компонентов Kaspersky Security вам нужно также выполнить следующие действия:

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

Гипервизор Citrix XenServer

Если в виртуальной инфраструктуре установлен гипервизор Citrix XenServer, перед началом установки компонентов Kaspersky Security вам нужно также выполнить следующие действия:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлена программа XenTools.
- Если вы используете схему лицензирования по количеству ядер в физических процессорах на гипервизорах, требуется убедиться, что на гипервизоре в конфигурационном файле /etc/ssh/sshd_config присутствует директива Ciphers с перечислением следующих шифров и хеш-функций, поддерживаемых со стороны SVM:
  - aes256-cbc;
  - aes256-ecb;
  - aes256-cfb;
  - aes256-ofb;
  - aes256-ctr

Файлы, необходимые для установки программы

Перед установкой программы вам требуется загрузить с веб-сайта «Лаборатории Касперского» файлы, необходимые для установки компонентов программы Kaspersky Security.

Плагины управления Kaspersky Security и Сервер интеграции

Для установки плагинов управления Kaspersky Security, Сервера интеграции и Консоли управления Сервера интеграции вам требуется загрузить с веб-сайта «Лаборатории Касперского» файл SecurityCenterComponents_4.0.X.X_setup.exe, где 4.0.X.X – номер версии программы.

Файл необходимо разместить на компьютере, где установлен Kaspersky Security Center.

Сервер защиты

Для развертывания SVM вам требуется загрузить с веб-сайта «Лаборатории Касперского» архив, содержащий образ SVM и конфигурационный файл в формате XML (файл описания образа).

В комплект поставки Kaspersky Security входят следующие архивы для установки Сервера защиты на гипервизоры разных типов:

- SVM.image_Hyper-V_4.0.X.X.vhdx.zip, где 4.0.X.X – номер версии программы. Этот архив используется для установки Сервера защиты на гипервизор Microsoft Windows Server (Hyper-V), содержит образ SVM в формате VHDX и конфигурационный файл SVM.image_manifest_4.0.X.X.xml, где 4.0.X.X – номер версии программы.
- SVM.image_XenServer_4.0.X.X.xva.zip, где 4.0.X.X – номер версии программы. Этот архив используется для установки Сервера защиты на гипервизор Citrix XenServer, содержит образ SVM в формате XVA и конфигурационный файл SVM.image_manifest_4.0.X.X.xml.

- SVM.image_VMware_4.0.X.X.ova, где 4.0.X.X – номер версии программы. Этот архив используется для установки Сервера защиты на гипервизор VMware ESXi, содержит образ SVM в формате OVA и конфигурационный файл SVM.image_manifest_4.0.X.X.xml.

- SVM.image_KVM_4.0.X.X.raw.gz, где 4.0.X.X – номер версии программы. Этот архив используется для установки Сервера защиты на гипервизор KVM, содержит образ SVM в формате RAW и конфигурационный файл SVM.image_manifest_4.0.X.X.xml.

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

Легкий агент для Windows

Для установки компонента Легкий агент для Windows вам требуется загрузить с веб-сайта «Лаборатории Касперского» архив Agent_4.0.X.X_sfx_<идентификатор языка>.exe, где 4.0.X.X – номер версии программы; <идентификатор языка> – идентификатор языка Легкого агента для Windows: ru, en, fr, de и другие.

Вы можете использовать файл Agent_4.0.X.X_sfx_<идентификатор языка>.exe в качестве дистрибутива программы для создания установочного пакета Легкого агента для Windows в Kaspersky Security Center (см. раздел «Создание установочного пакета Легкого агента для Windows» на стр. 82).

Если вы хотите создать установочный пакет для установки Легкого агента для Windows на виртуальные машины, на которых используется технология Citrix Provisioning Services, или если вы хотите установить Легкий агент для Windows с помощью мастера установки, вам нужно предварительно распаковать архив Agent_4.0.X.X_sfx_<идентификатор языка>.exe.

Архив Agent_4.0.X.X_sfx_<идентификатор языка>.exe содержит следующие файлы:

- incompatible.txt – файл содержит список программ, несовместимых с программой Kaspersky Security, используется при установке Легкого агента для Windows;

- Ksvla.kud – файл описания программы, используется для создания установочного пакета Легкого агента для Windows в Kaspersky Security Center;

- Ksvla_x64.msi – файл используется для установки Легкого агента для Windows на 64-разрядную операционную систему;
- Ksvla_x86.msi – файл используется для установки Легкого агента для Windows на 32-разрядную операционную систему;
- license.txt – файл содержит текст Лицензионного соглашения, в котором указано, на каких условиях вы можете пользоваться программой;
- setup.exe – файл используется для установки Легкого агента для Windows с помощью мастера установки.

Легкий агент для Linux

Для установки компонента Легкий агент для Linux вам требуется загрузить с веб-сайта «Лаборатории Касперского» следующие файлы:

- пакет для установки Легкого агента для Linux (в зависимости от операционной системы виртуальной машины и менеджера пакетов, используемого в операционной системе):
  - lightagent_4.0.X-X_amd64.deb – для 64-разрядной операционной системы;
  - lightagent_4.0.X-X_i386.deb – для 32-разрядной операционной системы;
  - lightagent-4.0.X-X.x86_64.rpm – для 64-разрядной операционной системы;
  - lightagent-4.0.X-X.i686.rpm – для 32-разрядной операционной системы;
- архив для установки Легкого агента для Linux через Kaspersky Security Center (в зависимости от менеджера пакетов, используемого в операционной системе виртуальной машины):
  - lightagent-4.0.X-X_deb-<идентификатор языка>.tar.gz – для установки из пакета формата DEB;
  - lightagent-4.0.X-X_rpm-<идентификатор языка>.tar.gz – для установки из пакета формата RPM;

где:

- 4.0.X-X – номер версии программы;
- <идентификатор языка> – двухбуквенный идентификатор языка: ru, en, fr, de и другие.

Архивы для установки Легкого агента для Linux через Kaspersky Security Center lightagent-4.0.X-X_deb-<идентификатор языка>.tar.gz и lightagent-4.0.X-X_rpm-<идентификатор языка>.tar.gz содержат следующие файлы, необходимые для установки Легкого агента через Kaspersky Security Center (см. раздел «Установка Легкого агента для Linux через Kaspersky Security Center» на стр. 104):

- akinstall.sh – файл используется для установки Легкого агента для Linux через Kaspersky Security Center;
- license.txt – файл содержит текст Лицензионного соглашения, в котором указано, на каких условиях вы можете пользоваться программой;
- lightagent.ini – конфигурационный файл первоначальной настройки, используется для установки Легкого агента для Linux из командной строки;
- lightagent.kud – файл описания программы, используется для создания установочного пакета Легкого агента для Linux в Kaspersky Security Center.

Агент администрирования Kaspersky Security Center

Если вы хотите управлять работой компонента Легкий агент для Linux с помощью Kaspersky Security Center, на той виртуальной машине, на которой будет установлен Легкий агент для Linux, нужно установить Агент администрирования Kaspersky Security Center версии 10.1.1-X, где 10.1.1-X – номер версии.

Для установки компонента Агент администрирования версии 10.1.1-X вам требуется загрузить с веб-сайта «Лаборатории Касперского» один из следующих пакетов (в зависимости от менеджера пакетов, используемого в операционной системе виртуальной машины):

- klnagent-10.1.1-X.i386.rpm;
- klnagent_10.1.1-X_i386.deb.

На виртуальной машине с компонентом Легкий агент для Windows вы можете использовать Агент администрирования, который входит в комплект поставки программы Kaspersky Security Center 10 Service Pack 2 или Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

Требования к составу компонентов Kaspersky Security Center

Для установки и функционирования программы Kaspersky Security требуются следующие компоненты Kaspersky Security Center:

- Сервер администрирования.

  На Сервере администрирования должны быть настроены следующие службы:

  - Служба Activation Proxy – используется при активации программы Kaspersky Security. Настройка службы Activation Proxy осуществляется в свойствах Сервера администрирования Kaspersky Security Center. Если служба Activation Proxy отключена, активация программы с помощью кода активации невозможна.

  - Служба KSN Proxy – обеспечивает обмен данными между программой Kaspersky Security и Kaspersky Security Network. Настройка службы KSN Proxy выполняется в свойствах Сервера администрирования Kaspersky Security Center. Если служба KSN Proxy отключена, обмен данными между Kaspersky Security и Kaspersky Security Network не производится.

    Подробнее о службах Activation Proxy и KSN Proxy см. в документации Kaspersky Security Center.

- Консоль администрирования. Консоль администрирования требуется установить на рабочем месте администратора.

- Агент администрирования. Агент администрирования осуществляет взаимодействие между Сервером администрирования и виртуальными машинами с установленной программой Kaspersky Security.

  Агент администрирования требуется установить на все виртуальные машины, которые вы хотите защищать (см. раздел «Установка Агента администрирования Kaspersky Security Center на виртуальные машины» на стр. 77).

  > 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.

На виртуальную машину, где будет установлен Легкий агент для Windows, вы можете установить Агент администрирования, который входит в комплект поставки программы Kaspersky Security Center 10 Service Pack 2 или Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

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

Настройка портов, используемых программой

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

Таблица 2. Порты, используемые программой

Порт и протокол	Направление	Назначение и описание
80 TCP 443 TCP	От мастера развертывания и изменения конфигурации в Kaspersky Security Center к серверу VMware vCenter.	Для развертывания SVM на гипервизоре Vmware ESXi с помощью сервера VMware vCenter.
135 TCP / UDP 445 TCP / UDP	От мастера развертывания и изменения конфигурации в Kaspersky Security Center к гипервизору Microsoft Windows Server (Hyper-V).	Для развертывания SVM на гипервизоре Microsoft Windows Server (Hyper-V).
80 TCP 443 TCP	От мастера развертывания и изменения конфигурации в Kaspersky Security Center к гипервизору Citrix XenServer.	Для развертывания SVM на гипервизоре Citrix XenServer.

Порт и протокол	Направление	Назначение и описание
22 TCP	От мастера развертывания и изменения конфигурации в Kaspersky Security Center к гипервизору KVM.	Для развертывания SVM на гипервизоре KVM.
22 TCP	От мастера развертывания и изменения конфигурации в Kaspersky Security Center к SVM.	Для изменения конфигурации SVM.
80 TCP 443 TCP	От SVM к серверу VMware vCenter.	Для взаимодействия SVM с гипервизором VMware ESXi с помощью сервера VMware vCenter.
135 TCP / UDP 445 TCP / UDP 5985 TCP 5986 TCP	От SVM к гипервизору Microsoft Windows Server (Hyper-V).	Для взаимодействия SVM с гипервизором Microsoft Windows Server (Hyper-V).
22 TCP 80 TCP 443 TCP	От SVM к гипервизору Citrix XenServer.	Для взаимодействия SVM с гипервизором Citrix XenServer.
22 TCP	От SVM к гипервизору KVM.	Для взаимодействия SVM с гипервизором KVM.
9876 UDP	От Легкого агента к группе Multicast.	Для получения Легким агентом информации обо всех доступных для подключения SVM на всех гипервизорах виртуальной инфраструктуры с помощью многоадресной рассылки (Multicast).

Порт и протокол	Направление	Назначение и описание
9876 UDP	От SVM к группе Multicast или к Легкому агенту.	Для передачи информации Легким агентам о доступных SVM с помощью многоадресной рассылки (Multicast) или с использованием списка адресов SVM.
7271 TCP	От SVM к Серверу интеграции.	Для взаимодействия SVM и Сервера интеграции.
7271 TCP	От Легкого агента к Серверу интеграции.	Для взаимодействия Легкого агента и Сервера интеграции.
8000 UDP	От Легкого агента к SVM.	Для получения Легким агентом информации о состоянии SVM.
11111 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение сведений о лицензии) от Легкого агента на SVM.
9876 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента на SVM.
80 TCP	От Легкого агента к SVM.	Для обновления баз и модулей программы на Легком агенте.
15000 UDP	От Kaspersky Security Center к SVM.	Для управления программой через Kaspersky Security Center на SVM.
15000 UDP	От Kaspersky Security Center к Легким агентам.	Для управления программой через Kaspersky Security Center на Легких агентах.

Порт и протокол	Направление	Назначение и описание
13000 TCP	От SVM к Kaspersky Security Center.	Для управления программой через Kaspersky Security Center на SVM.
14000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления программой через Kaspersky Security Center на Легких агентах.

Если Легкий агент, установленный на защищенной виртуальной машине, получает информацию о SVM с помощью многоадресной рассылки (Multicast) (см. раздел «О подключении Легкого агента к SVM» на стр. 33), то для подключения Легкого агента к Серверу защиты, установленному на SVM, требуется обеспечить маршрутизацию пакетов по протоколу IGMP версии 3 для группы 239.255.76.65:9876.

После установки Легкий агент выполняет настройку межсетевого экрана Microsoft Windows, чтобы разрешить входящий и исходящий трафик для процесса avp.exe. Если для межсетевого экрана Microsoft Windows используется доменная политика, требуется настроить правила для входящих и исходящих подключений для процесса avp.exe в доменной политике. Если используется другой межсетевой экран, требуется настроить правило для подключений для процесса avp.exe для этого межсетевого экрана.

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

Учетные записи для установки и работы программы

Для установки плагинов управления Kaspersky Security и Сервера интеграции требуется учетная запись, которая входит в группу локальных администраторов на компьютере, где выполняется установка (см. раздел «Установка плагинов управления Kaspersky Security и Сервера интеграции» на стр. 59).

Если компьютер, где установлена Консоль администрирования Kaspersky Security Center, входит в домен Microsoft Windows, для запуска Консоли управления Сервера интеграции требуется доменная учетная запись, которая входит в группу KLAdmins, или учетная запись, которая входит в группу локальных администраторов.

Гипервизор VMware ESXi

Для развертывания и работы SVM на гипервизоре VMware ESXi требуются следующие учетные записи:

- Для развертывания и изменения конфигурации SVM требуется учетная запись администратора со следующими правами:
  - Datastore.Allocate space
  - Datastore.Low level file operations
  - Datastore.Remove file
  - Global.Cancel task
  - Global.Licenses
  - Host.Config.Virtual machine autostart configuration
  - Host.Inventory.Modify cluster
  - Network.Assign network
  - Tasks.Create task
  - vApp.Import

- Virtual machine.Configuration.Add new disk
- Virtual machine.Configuration.Add or remove device
- Virtual machine.Interaction.Power Off
- Virtual machine.Interaction.Power On
- Virtual machine.Inventory.Create new
- Virtual machine.Inventory.Remove
- Virtual machine.Provisioning.Customize

- Для работы SVM требуется учетная запись, которой назначена предустановленная системная роль ReadOnly.

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

О создании учетной записи в инфраструктуре VMware см. в документации VMware.

Гипервизор Microsoft Windows Server (Hyper-V)

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

- root\cimv2;
- root\virtualization;
- root\virtualization\v2 (для версий серверных операционных систем Microsoft Windows, начиная с версии Windows Server 2012 R2).

Гипервизор Citrix XenServer

Для развертывания и работы SVM на гипервизоре Citrix XenServer требуется учетная запись с правами Pool Administrator.

Гипервизор KVM

Для развертывания и работы SVM на гипервизоре KVM требуется учетная запись администратора со следующими правами:

- на создание удаленной интерактивной сессии с гипервизором через SSH посредством ввода пароля для аутентификации;
- на выполнение команд с помощью утилиты virsh (утилита для командной строки Linux, предназначенная для управления виртуальными машинами и гипервизорами KVM);
- на изменение содержимого директории пула хранилища образов виртуальных машин (точное расположение определяется сервисом libvirtd);
- на изменение содержимого папки с временными файлами (/tmp);
- на монтирование образов виртуальных машин внутри папки /mnt. Если такой папки нет, нужны права для создания этой папки в корневой директории.

Для работы SVM требуется учетная запись на гипервизоре KVM со следующими правами:

- на создание удаленной интерактивной сессии с гипервизором через SSH посредством ввода пароля для аутентификации;
- на выполнение команд, предназначенных для получения информации о виртуальной инфраструктуре, с помощью утилиты virsh (read-only команды);
- на изменение содержимого папки с временными файлами (/tmp).

О создании учетной записи см. в документации KVM.

Настройка правил перемещения виртуальных машин в группы администрирования

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

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

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

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

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

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

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

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

   Подробнее о настройке правил перемещения виртуальных машин в группы см. в документации Kaspersky Security Center.
6. Нажмите на кнопку **ОК**, чтобы закрыть окно **Новое правило**.

   Новое правило отобразится в списке правил раздела **Перемещение компьютеров**.
7. Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства:Нераспределенные устройства**.

При создании правил перемещения виртуальных машин в группы администрирования вы можете использовать теги (см. раздел «Изменения в Kaspersky Security Center после установки программы» на стр. 110). SVM и защищенные виртуальные машины

с установленным Агентом администрирования Kaspersky Security Center автоматически передают информацию о тегах в Kaspersky Security Center.

Установка программы

Этот раздел содержит следующую информацию:

- описание порядка установки компонентов программы;
- инструкции по установке компонентов программы;
- описание изменений в Kaspersky Security Center после установки программы.

В этом разделе

Порядок установки программы

Установка программы Kaspersky Security для виртуальных сред 4.0 Легкий агент в виртуальной инфраструктуре состоит из следующих этапов:

1. Установка плагинов управления Kaspersky Security, Сервера интеграции и Консоли управления Сервера интеграции (см. раздел «Установка плагинов управления Kaspersky Security и Сервера интеграции» на стр. 59).
    - Для управления программой при помощи Kaspersky Security Center используются следующие плагины управления:
        - Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows;

- Kaspersky Security для виртуальных сред 4.0 Легкий агент для Linux;
- Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты.

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

- Сервер интеграции должен быть установлен на том компьютере, где установлен Сервер администрирования Kaspersky Security Center.
- Консоль управления Сервера интеграции должна быть установлена на компьютере, где установлена Консоль администрирования Kaspersky Security Center.

2. Установка компонента Сервер защиты Kaspersky Security (см. раздел «Установка компонента Сервер защиты» на стр. 66). Установка компонента Сервер защиты выполняется путем развертывания SVM на гипервизорах.

   После установки компонента Сервер защиты нужно выполнить следующие действия:

   - Активировать программу (см. раздел «Об активации программы» на стр. 112).
   - Обновить антивирусные базы программы (см. раздел «Обновление антивирусных баз» на стр. 126).

3. Установка компонента Агент администрирования Kaspersky Security Center. Если вы хотите управлять работой компонента Легкий агент через Kaspersky Security Center, требуется установить Агент администрирования на виртуальные машины и шаблоны виртуальных машин (см. раздел «Установка Агента администрирования Kaspersky Security Center на виртуальные машины» на стр. 77).

4. Установка на виртуальные машины компонента Легкий агент для Windows (см. раздел «Установка компонента Легкий агент для Windows» на стр. 79) и / или Легкий агент для Linux (см. раздел «Установка компонента Легкий агент для Linux» на стр. 103).

Установка плагинов управления Kaspersky Security и Сервера интеграции

Вы можете установить плагины управления Kaspersky Security, Сервер интеграции и Консоль управления Сервера интеграции одним из следующих способов:

- в интерактивном режиме с помощью мастера (см. раздел «Установка с помощью мастера» на стр. 61);
- в тихом режиме из командной строки (см. раздел «Установка из командной строки» на стр. 64).

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

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

- если на компьютере установлена только Консоль администрирования Kaspersky Security Center, устанавливаются плагины управления Kaspersky Security и Консоль управления Сервера интеграции;
- если на компьютере установлены Сервер администрирования Kaspersky Security Center и Консоль администрирования Kaspersky Security Center, устанавливаются плагины управления Kaspersky Security, Сервер интеграции и Консоль управления Сервера интеграции.

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

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

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

Если ранее в вашей виртуальной инфраструктуре был установлен Сервер интеграции и при его удалении вы сохранили данные, используемые в работе Сервера интеграции (см. раздел «Удаление плагинов управления Kaspersky Security и Сервера интеграции» на стр. 170), эти данные используются автоматически при повторной установке Сервера интеграции.

После установки плагины управления Kaspersky Security отображаются в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center (см. раздел «Просмотр списка установленных плагинов управления Kaspersky Security» на стр. 65).

В этом разделе

Установка с помощью мастера

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

1. На компьютере, где установлены Консоль администрирования и Сервер администрирования, запустите файл SecurityCenterComponents_4.0.X.X_setup.exe, где 4.0.X.X – номер версии программы. Этот файл входит в комплект поставки (см. раздел «Файлы, необходимые для установки программы» на стр. 43).

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

   Запустится мастер установки.

2. Следуйте указаниям мастера.

В этом разделе

Шаг 1. Выбор языка локализации

В этом окне используется язык локализации операционной системы, установленной на компьютере, где запущен мастер.

На этом шаге выберите язык локализации мастера и компонентов Kaspersky Security.

Перейдите к следующему шагу мастера.

Шаг 2. Просмотр Лицензионного соглашения

На этом шаге ознакомьтесь с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочтите Лицензионное соглашение и, если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**.

Перейдите к следующему шагу мастера.

Шаг 3. Создание пароля учетной записи администратора Сервера интеграции

Этот шаг отображается, если на компьютере, на котором запущен мастер, установлен Сервер администрирования Kaspersky Security Center и компьютер не входит в домен Microsoft Windows.

Для управления Сервером интеграции будет использоваться учетная запись администратора Сервера интеграции *admin*. Имя учетной записи недоступно для изменения.

Создайте пароль учетной записи администратора Сервера интеграции. Для этого введите пароль в полях **Пароль** и **Подтверждение пароля**.

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

Перейдите к следующему шагу мастера.

Шаг 4. Ввод или изменение пароля учетной записи svm

Этот шаг отображается, если на компьютере, на котором запущен мастер, обнаружен установленный Сервер интеграции, который использовался для работы программы Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Защита без агента.

В целях безопасности требуется указать пароль учетной записи svm, который использовался для подключения SVM к Серверу интеграции.

В полях **Пароль** и **Подтверждение пароля** введите пароль учетной записи svm, заданный ранее, или введите новый пароль учетной записи svm.

Перейдите к следующему шагу мастера.

Шаг 5. Ввод номера порта для подключения к Серверу интеграции

Этот шаг отображается, если на компьютере, на котором запущен мастер, установлен Сервер администрирования Kaspersky Security Center и порт, используемый по умолчанию для подключения к Серверу интеграции, занят. По умолчанию для подключения к Серверу интеграции используется порт 7271.

Укажите номер порта для подключения к Серверу интеграции в поле **Порт**.

Перейдите к следующему шагу мастера.

Шаг 6. Запуск установки и обновления компонентов

На этом шаге отображается информация о действиях, которые выполнит мастер над плагинами управления, Сервером интеграции и Консолью управления Сервера интеграции.

Мастер выполнит обновление компонентов Kaspersky Security, если на компьютере обнаружены компоненты предыдущих версий.

Нажмите на кнопку **Далее**, чтобы начать выполнение перечисленных действий.

Шаг 7. Установка и обновление компонентов

На этом шаге мастер выполняет установку и / или обновление компонентов. Дождитесь завершения работы мастера. Если в ходе работы мастера возникает ошибка, мастер выполняет откат внесенных изменений.

Шаг 8. Завершение работы мастера

На этом шаге отображается информация о результатах работы мастера.

Информация о работе мастера записывается в журналы работы мастера. Журналы работы мастера представляют собой файлы в формате TXT и сохраняются на том компьютере, где был запущен мастер, в папке %temp%. Если работа мастера завершилась с ошибкой, вы можете использовать эти журналы при обращении в Службу технической поддержки.

Чтобы закрыть окно мастера, нажмите на кнопку **Завершить**.

Установка из командной строки

► *Чтобы установить плагины управления Kaspersky Security и компоненты Сервера интеграции из командной строки,*

в командной строке введите одну из следующих команд:

- если компьютер, на котором выполняется установка, входит в домен Microsoft Windows:

  `SecurityCenterComponents_4.0.X.X_setup.exe -q --lang=<идентификатор языка> --accept-eula=<yes>`

- если компьютер, на котором выполняется установка, не входит в домен Microsoft Windows:

  `SecurityCenterComponents_4.0.X.X_setup.exe -q --lang=<идентификатор языка> --accept-eula=<yes> --viisPass=<пароль>`

где:

- `4.0.X.X` – номер версии программы.
- `<идентификатор языка>` – двухбуквенный идентификатор языка компонентов.
- `<пароль>` – пароль для учетной записи администратора Сервера интеграции. Учетная запись администратора Сервера интеграции admin используется

для управления Сервером интеграции, если компьютер, на котором установлен Сервер интеграции, не входит в домен Microsoft Windows.

- `accept-eula=<yes>` означает, что вы принимаете условия Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки программы (см. раздел «Комплект поставки» на стр. 22). Согласие с условиями Лицензионного соглашения является необходимым условием для установки плагинов управления Kaspersky Security и компонентов Сервера интеграции.

  Вы можете ознакомиться с текстом Лицензионного соглашения перед установкой программы. Для этого в командной строке введите следующую команду:

  `SecurityCenterComponents_4.0.X.X_setup.exe lang=<идентификатор языка> --show-eula`

  Текст Лицензионного соглашения выводится в файл license_<идентификатор языка>.txt в папке tmp.

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

Установка плагинов управления Kaspersky Security и компонентов Сервера интеграции занимает некоторое время. Информацию о результате установки вы можете посмотреть в файле:

%temp%\Kaspersky_Security_for_Virtualization_4.0_Light_Agent_Silent_Mode_Result_{0}.log,

где {0} – время завершения установки, указанное в формате dd_MM_yyyy_HH_mm_ss.

Просмотр списка установленных плагинов управления Kaspersky Security

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

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Сервер администрирования** и выполните одно из следующих действий:

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

- Откройте окно свойств Сервера администрирования по ссылке **Свойства сервера администрирования**. Ссылка находится в рабочей области в блоке **Сервер администрирования**.

Откроется окно **Свойства: Сервер администрирования**.

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

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

   - **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows**;
   - **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Linux**;
   - **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты**.

Установка компонента Сервер защиты

Компонент Сервер защиты поставляется в виде образа SVM. Установка Сервера защиты Kaspersky Security выполняется посредством развертывания SVM на гипервизоре.

SVM требуется развернуть на тех гипервизорах в виртуальной инфраструктуре, виртуальные машины которых вы хотите защищать с помощью программы Kaspersky Security. На одном гипервизоре может быть развернуто несколько SVM.

Во время установки компонента Сервер защиты вы можете указать несколько гипервизоров, на которых будут развернуты SVM.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите Сервер администрирования.
3. По ссылке **Управление Kaspersky Security для виртуальных сред 4.0 Легкий агент** запустите мастер. Ссылка находится в рабочей области в блоке **Развертывание**.
4. Следуйте указаниям мастера.

Во время установки мастер сохраняет в журнал работы мастера информацию, указанную вами на каждом шаге мастера (см. раздел «Приложение. Описание журнала работы мастера» на стр. 175).

Журнал работы мастера сохраняется на том компьютере, где был запущен мастер, в файле %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\4.0.0.0\KasperskyDeploymentWizard.log.

> Информация в файле перезаписывается при каждом запуске мастера. Чтобы использовать информацию журнала работы мастера в дальнейшем, нужно сохранить файл в место постоянного хранения.

Вы можете использовать журнал работы мастера при обращении в Службу технической поддержки, в случае если развертывание SVM завершилось с ошибкой.

В этом разделе

Шаг 1. Выбор действия

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

Перейдите к следующему шагу мастера.

Шаг 2. Выбор гипервизоров для развертывания SVM

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

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

Если для управления виртуальной инфраструктурой вы используете Microsoft System Center Virtual Machine Manager (далее «Microsoft SCVMM»), вы можете указать параметры подключения к Microsoft SCVMM, чтобы добавить в список все гипервизоры, которые находятся под его управлением.

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

1. Нажмите на кнопку **Добавить**.

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

2. Укажите следующие параметры подключения к гипервизорам или к серверу управления виртуальной инфраструктурой, под управлением которого работают гипервизоры:

   - **Тип**.

     Раскрывающийся список для выбора типа гипервизора или сервера управления виртуальной инфраструктурой.

   - **Адреса**.

     Адреса гипервизоров, на которых вы хотите развернуть SVM, или адрес сервера управления виртуальной инфраструктурой, под управлением которого работают гипервизоры.

Вы можете указать в качества адреса гипервизора или сервера управления виртуальной инфраструктурой его IP-адрес в формате IPv4 или полное доменное имя (FQDN). Вы можете указать IP-адреса или полные доменные имена гипервизоров через точку с запятой или с новой строки.

Количество правильно распознанных адресов отображается под списком адресов.

- **Имя пользователя**.

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

- **Пароль**.

  Пароль учетной записи, которая используется для подключения мастера к серверу управления виртуальной инфраструктурой или к гипервизору.

3. Нажмите на кнопку **Подключиться**.

   Окно **Параметры подключения к виртуальной инфраструктуре** закроется, выбранные гипервизоры добавятся в список гипервизоров. Если подключение к гипервизору или серверу управления виртуальной инфраструктурой не удалось установить, информация об ошибках подключения отображается в таблице.

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

- **Имя**.

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

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

к значку отображается описание ограничения или ошибки подключения.

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

- удалить из списка выбранный гипервизор или все гипервизоры под управлением выбранного сервера управления виртуальной инфраструктурой;
- открыть окно **Параметры подключения к виртуальной инфраструктуре** для изменения параметров учетной записи, под которой выполняется подключение к выбранному гипервизору или серверу управления виртуальной инфраструктурой.

- **Состояние**.

  Состояние гипервизора или SVM.

  Для гипервизора указывается одно из следующих значений: *Включен*, *Выключен*, *Режим самообслуживания*. Если не удалось установить подключение к гипервизору, в графе отображается *Соединение не установлено*. Для SVM указывается одно из следующих значений: *Запущена*, *Остановлена*.

- **Защита**.

  Номер версии образа SVM.

Чтобы обновить список гипервизоров в таблице, нажмите на кнопку **Обновить** над списком.

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

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

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

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

Перейдите к следующему шагу мастера.

Шаг 3. Выбор образа SVM

На этом шаге укажите файл образа SVM для развертывания на гипервизоре. Файл образа SVM и конфигурационный файл в формате XML должны быть размещены в одной папке. Если вы устанавливаете Сервер защиты на гипервизоры разных типов, в одной папке должны быть размещены файлы образов SVM для каждого типа гипервизоров и конфигурационный файл в формате XML (см. раздел «Файлы, необходимые для установки программы» на стр. 43).

Чтобы указать образ SVM, нажмите на кнопку **Обзор** и в открывшемся окне выберите конфигурационный файл в формате XML.

В нижней части окна отобразится следующая информация:

- **Название программы**.

  Название программы, которая установлена на SVM.

- **Версия SVM**.

  Номер версии образа SVM.

- **Производитель**.

  Производитель программы, которая установлена на SVM.

- **Издатель**.

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

- **Описание**.

  Краткое описание образа SVM.

- **Размер виртуального диска**.

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

- Сведения о результатах проверки файла образа SVM для каждого типа гипервизоров. Рекомендуется выполнить проверку целостности файла образа SVM по ссылке **Проверить**. Если файл образа изменен или поврежден в процессе его передачи

от издателя к конечному пользователю или формат образа не поддерживается, мастер отобразит сообщение об ошибке. В этом случае повторно загрузите архив с файлами, необходимыми для развертывания SVM, с веб-сайта «Лаборатории Касперского».

Если проверка файла образа не выполнялась, в строке отображается **Проверка не проводилась**.

Перейдите к следующему шагу мастера.

Шаг 4. Ввод параметров SVM

На этом шаге укажите следующие параметры SVM для каждого из гипервизоров:

- **Имя SVM**.

  Полное доменное имя (FQDN) SVM.

- **Хранилище**.

  Хранилище данных гипервизора для образа SVM.

- **Имя сети**.

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

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

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

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

- **Идентификатор VLAN**.

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

Если виртуальная локальная сеть не используется, в графе отображается *N/A*.

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

Если вы хотите, чтобы мастер использовал динамическое выделение места на диске для развертывания SVM на гипервизорах VMware, установите флажок **Использовать динамическое выделение места в хранилище гипервизора VMware ESXi**. В хранилище данных гипервизора для SVM резервируется минимально необходимый объем. При необходимости этот объем увеличивается. Если флажок снят, динамическое выделение места на диске не используется. В хранилище данных гипервизора для SVM сразу резервируется требуемый объем.

Перейдите к следующему шагу мастера.

Шаг 5. Настройка сетевых параметров SVM

На этом шаге настройте сетевые параметры SVM. Для этого выполните одно из следующих действий:

- Если вы хотите использовать для всех SVM сетевые параметры, полученные по протоколу DHCP, выберите вариант **Динамическая IP-адресация (DHCP)**. Если вы хотите указать IP-адрес DNS-сервера и альтернативного DNS-сервера для каждой SVM, снимите флажок **Использовать список DNS-серверов, полученных по DHCP** и укажите IP-адреса DNS-серверов в графах таблицы **DNS-сервер** и **Альтернативный DNS-сервер**. По умолчанию используются IP-адреса DNS-серверов, полученные по протоколу DHCP.

  Если на предыдущем шаге вы указали несколько виртуальных сетей для SVM, по умолчанию сетевые параметры для SVM будут получены от сервера DHCP по первой виртуальной сети из списка указанных сетей.

- Если вы хотите назначить сетевые параметры SVM вручную, выберите вариант **Статическая IP-адресация** и укажите следующие сетевые параметры для каждой SVM:

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

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

Перейдите к следующему шагу мастера.

Шаг 6. Ввод параметров подключения к Kaspersky Security Center

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

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

- **Адрес**.

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

- **Порт**.

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

- **SSL-порт**.

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

Перейдите к следующему шагу мастера.

Шаг 7. Создание пароля конфигурирования и пароля учетной записи root

На этом шаге создайте пароль конфигурирования и пароль учетной записи root на SVM. Пароль конфигурирования требуется для изменения конфигурации SVM. Учетная запись root используется для настройки SVM.

> Рекомендуется использовать в паролях символы латинского алфавита и цифры.

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

Перейдите к следующему шагу мастера.

Шаг 8. Запуск развертывания SVM

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

Чтобы запустить развертывание SVM, перейдите к следующему шагу мастера.

Шаг 9. Развертывание SVM

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

Информация о процессе и результате развертывания каждой SVM отображается в окне мастера.

После завершения развертывания SVM автоматически включается.

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

Перейдите к следующему шагу мастера.

Шаг 10. Завершение развертывания SVM

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

Мастер отображает ссылки, по которым вы можете открыть журнал работы мастера и краткий отчет.

Краткий отчет содержит информацию о результатах выполнения этапов развертывания каждой SVM. Краткий отчет сохраняется во временном файле. Чтобы использовать информацию отчета в дальнейшем, нужно сохранить файл в место постоянного хранения.

Журнал работы мастера содержит информацию, указанную вами на каждом шаге мастера. Если развертывание SVM завершилось с ошибкой, вы можете использовать журнал работы мастера при обращении в Службу технической поддержки.

Журнал работы мастера сохраняется на том компьютере, на котором был запущен мастер, в файле %LocalAppData%\Kaspersky_Lab\SvmDeploymentWizard.log и не содержит информации об учетных записях.

Завершите работу мастера.

После завершения работы мастера в виртуальной инфраструктуре рекомендуется выполнить действия, завершающие установку компонента Сервер защиты (см. раздел «Завершение установки компонента Сервер защиты» на стр. 77).

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

Завершение установки компонента Сервер защиты

После установки Сервера защиты рекомендуется выполнить следующие действия:

- Проверить системную дату на SVM средствами используемого гипервизора. Несоответствие системной даты на Сервере администрирования и системной даты на SVM может привести к ошибке соединения SVM с Kaspersky Security Center и неверной работе программы.

- Указать учетную запись, которую SVM использует для подключения к гипервизору или серверу управления виртуальной инфраструктурой. Для этого требуется изменить конфигурацию SVM (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Рекомендуется использовать учетную запись, которая создана для работы программы (см. раздел «Учетные записи для установки и работы программы» на стр. 52). По умолчанию для подключения SVM к гипервизору или серверу управления виртуальной инфраструктурой используется учетная запись, которую вы указали на втором шаге процедуры развертывания SVM.

После развертывания SVM на гипервизоре вы можете изменить выделенные под SVM ресурсы гипервизора, например, в соответствии с рекомендациями специалистов «Лаборатории Касперского» (см. раздел «Аппаратные и программные требования» на стр. 23). Производительность SVM вы можете регулировать с помощью выделенных для нее ресурсов.

Установка Агента администрирования Kaspersky Security Center на виртуальные машины

Если вы хотите управлять работой компонента Легкий агент с помощью Kaspersky Security Center, перед началом установки компонента Легкий агент вам требуется установить на виртуальных машинах и шаблонах виртуальных машин компонент Агент администрирования Kaspersky Security Center. Агент администрирования обеспечивает взаимодействие между Сервером администрирования Kaspersky Security Center и защищенными виртуальными машинами. Если Агент администрирования не установлен

на защищенной виртуальной машине, управление работой Легкого агента на этой виртуальной машине осуществляется только через локальный интерфейс (в случае Легкого агента для Windows) или через командную строку (в случае Легкого агента для Linux).

Вы можете установить Агент администрирования одним из следующих способов:

- На виртуальные машины с операционной системой Windows:
  - Локально на каждой виртуальной машине с помощью мастера установки. Этот способ рекомендуется для установки Агента администрирования на шаблоны виртуальных машин.
  - Удаленно через Kaspersky Security Center с помощью мастера развертывания защиты или задачи удаленной установки программы. Установочный пакет для удаленной установки Агента администрирования формируется автоматически при установке программы Kaspersky Security Center и располагается в папке **Инсталляционные пакеты**.

    В свойствах установочного пакета Агента администрирования в разделе **Дополнительно** рекомендуется установить флажок **Оптимизировать параметры для VDI (Virtual Desktop Infrastructure)**. Подробнее об удаленной установке программ через Kaspersky Security Center см. в документации Kaspersky Security Center.
- На виртуальные машины с операционной системой Linux – средствами операционной системы Linux.

  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. Пакеты, необходимые для установки Агента администрирования версии 10.1.1-X, входят в комплект поставки программы Kaspersky Security для виртуальных сред 4.0 Легкий агент (см. раздел «Файлы, необходимые для установки программы» на стр. 43).

► *Чтобы установить Агент администрирования локально на виртуальной машине или шаблоне виртуальных машин с операционной системой Windows, выполните следующие действия:*

1. Запустите на виртуальной машине исполняемый файл setup.exe. Файл setup.exe входит в комплект поставки программы Kaspersky Security Center и находится в папке Packages\NetAgent.

Запустится мастер установки.

2. Следуйте указаниям мастера установки.

3. Если вы устанавливаете Агент администрирования на виртуальную машину, в ходе установки на шаге «Дополнительные параметры» установите флажок **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**. Если флажок установлен, отключена инвентаризация программ и оборудования и проверка исполняемых файлов на наличие уязвимостей при запуске мастера.

   Если вы устанавливаете Агент администрирования на шаблон виртуальных машин, в ходе установки на шаге «Дополнительные параметры» установите следующие флажки:

   - **Включить динамический режим для VDI**. Если флажок установлен, после выключения виртуальной машины эта виртуальная машина не отображается в Консоли администрирования Kaspersky Security Center.

   - **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**. Если флажок установлен, отключена инвентаризация программ и оборудования и проверка исполняемых файлов на наличие уязвимостей при запуске мастера.

Подробнее об установке компонента Агент администрирования Kaspersky Security Center см. в документации Kaspersky Security Center.

Установка компонента Легкий агент для Windows

Компонент Легкий агент для Windows может быть установлен на виртуальную машину несколькими способами:

- Локально с помощью мастера установки (см. раздел «Установка Легкого агента для Windows с помощью мастера установки» на стр. 85).

Этот способ рекомендуется для установки компонента Легкий агент для Windows на шаблоны виртуальных машин (см. раздел «Установка Легкого агента для Windows на шаблон виртуальных машин» на стр. 98).

- Из командной строки (см. раздел «Установка Легкого агента для Windows из командной строки» на стр. 93).
- Удаленно с рабочего места администратора с помощью программы Kaspersky Security Center (см. раздел «Установка Легкого агента для Windows через Kaspersky Security Center» на стр. 81).
- Удаленно с рабочего места администратора через редактор управления групповыми политиками службы каталогов (Active Directory Group Policies) (см. раздел «Установка Легкого агента для Windows через редактор управления групповыми политиками службы каталогов» на стр. 96).

Вы можете установить Легкий агент для Windows на виртуальные машины в составе инфраструктуры, в которой используются следующие решения для виртуализации:

- Citrix XenDesktop (см. раздел «Совместимость с технологией Citrix Personal vDisk» на стр. 100);
- Citrix Provisioning Services (см. раздел «Совместимость с технологией Citrix Provisioning Services» на стр. 100).

Перед началом установки компонента Легкий агент для Windows (в том числе и удаленной) рекомендуется закрыть все программы, работающие в операционной системе виртуальной машины.

В этом разделе

Установка Легкого агента для Windows через Kaspersky Security Center

Вы можете установить Легкий агент для Windows удаленно с рабочего места администратора с помощью программы Kaspersky Security Center. Для установки используется установочный пакет, который содержит набор параметров, необходимых для установки программы (см. раздел «Создание установочного пакета Легкого агента для Windows» на стр. 82). Установка выполняется с помощью мастера развертывания защиты или с помощью задачи удаленной установки программы.

Подробнее об удаленной установке программ через Kaspersky Security Center см. в документации Kaspersky Security Center.

В этом разделе

Создание установочного пакета Легкого агента для Windows

Установочный пакет требуется для удаленной установки компонента Легкий агент для Windows через Kaspersky Security Center.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли в папке **Дополнительно / Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Нажмите на кнопку **Создать инсталляционный пакет**, чтобы запустить мастер создания инсталляционного пакета.
4. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы «Лаборатории Касперского».**
5. В открывшемся окне мастера введите имя нового установочного пакета и перейдите к следующему шагу мастера.
6. В окне мастера **Выбор дистрибутива программы для установки** выберите дистрибутив программы Kaspersky Security. Для этого выполните следующие действия:

   a. Нажмите на кнопку **Выбрать** и укажите путь к дистрибутиву в стандартном окне Windows **Открыть**. В качестве дистрибутива программы вы можете выбрать один из следующих файлов из комплекта поставки Kaspersky Security:

      - Самораспаковывающийся архив Agent_4.0.X.X_sfx_<идентификатор языка>.exe, где 4.0.X.X – номер версии программы; <идентификатор языка> – двухбуквенный идентификатор языка Легкого агента для Windows: ru, en, fr, de и другие.
      - Файл Ksvla.kud, который содержится в самораспаковывающемся архиве Agent_4.0.X.X_sfx_<идентификатор языка>.exe. Если вы хотите использовать файл Ksvla.kud, вам требуется предварительно распаковать архив.

      Если вы хотите создать установочный пакет для установки Легкого агента для Windows на виртуальные машины, на которых используется технология Citrix Provisioning Services, вам нужно использовать файл Ksvla.kud. Предварительно

требуется внести следующее изменение в файл Ksvla.kud: в секции `[Setup]` добавить параметр `/pINSTALLONPVS=1` в конце строки `Params=/s /pAKINSTALL=1 /pEULA=1`.

b. Нажмите на кнопку **Открыть**.

В окне мастера **Выбор дистрибутива программы для установки** отобразится название программы.

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

Перейдите к следующему шагу мастера.

7. В окне мастера **Лицензионное соглашение** ознакомьтесь с условиями Лицензионного соглашения, которое заключается между вами и «Лабораторией Касперского». Для продолжения создания установочного пакета требуется принять условия Лицензионного соглашения. Установите флажок **Принимаю условия Лицензионного соглашения** и перейдите к следующему шагу мастера.

8. Мастер загружает файлы, необходимые для установки программы, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.

9. В окне мастера **Параметры удаленной установки программы** укажите следующие параметры установки Легкого агента для Windows:

   - Выберите тип установки:

     - **Установка компонентов защиты**. Выберите этот вариант, если вы хотите установить на виртуальную машину компоненты защиты Легкого агента для Windows с параметрами, рекомендуемыми специалистами «Лаборатории Касперского».

     - **Установка компонентов защиты и контроля**. Выберите этот вариант, если вы хотите установить на виртуальную машину компоненты защиты и компоненты

контроля Легкого агента для Windows с параметрами, рекомендуемыми специалистами «Лаборатории Касперского».

- При необходимости укажите путь к папке установки.
- Если вы хотите перенести ранее сохраненные параметры Легкого агента в установочный пакет, нажмите на кнопку **Обзор** и в открывшемся окне **Выбор конфигурационного файла** выберите файл с расширением cfg.

Перейдите к следующему шагу мастера.

10. В открывшемся окне мастер создает установочный пакет и выводит сообщение об окончании процедуры. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Созданный установочный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно / Удаленная установка** во вложенной папке **Инсталляционные пакеты**. Вы можете использовать один и тот же установочный пакет многократно.

После создания установочного пакета вы можете изменить параметры установки Легкого агента для Windows или выполнить более детальную настройку параметров установки (например, определить состав устанавливаемых компонентов Легкого агента) (см. раздел «Настройка параметров установочного пакета Легкого агента для Windows» на стр. 84).

Настройка параметров установочного пакета Легкого агента для Windows

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли в папке **Дополнительно / Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В списке установочных пакетов выберите установочный пакет Легкого агента и откройте окно **Свойства: <имя установочного пакета>** одним из следующих способов:
   - двойным щелчком мыши;

- по правой клавише мыши вызовите контекстное меню и выберите пункт **Свойства**;
- по ссылке **Открыть окно свойств инсталляционного пакета**, расположенной справа от списка задач в блоке с параметрами установочного пакета.

4. В разделе **Параметры** вы можете изменить параметры установки Легкого агента для Windows, настроенные при создании установочного пакета, а также указать компоненты Легкого агента, которые должны быть установлены на защищенной виртуальной машине:

   - Если флажок рядом с названием компонента установлен, Kaspersky Security установит компонент на виртуальной машине. Если компонент уже установлен, то ничего не изменится.
   - Если флажок рядом с названием компонента не установлен, Kaspersky Security удалит компонент. Если компонент не был установлен, то ничего не изменится.

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

5. Нажмите на кнопку **ОК** в окне **Свойства: <имя установочного пакета>**.

Установка Легкого агента для Windows с помощью мастера установки

Перед началом установки компонента Легкий агент для Windows рекомендуется закрыть все программы, работающие в операционной системе виртуальной машины.

► *Чтобы установить компонент Легкий агент для Windows с помощью мастера установки, выполните следующие действия:*

1. Запустите самораспаковывающийся архив Agent_4.0.X.X_sfx_ru.exe, где 4.0.X.X – номер сборки программы. Этот файл входит в комплект поставки (см. раздел «Файлы, необходимые для установки программы» на стр. 43).

   Запустится мастер распаковки, следуйте его указаниям.

2. В операционной системе виртуальной машины, которую вы хотите защищать, запустите файл setup.exe.

   Запустится мастер установки Легкого агента для Windows.

3. Следуйте указаниям мастера установки Легкого агента для Windows.

Перед установкой Легкого агента для Windows на виртуальную машину, которую вы хотите защищать, мастер установки проверяет выполнение следующих условий:

- Соответствие операционной системы виртуальной машины программным требованиям Kaspersky Security (см. раздел «Аппаратные и программные требования» на стр. 23).

  Если условие не выполнено, на экран выводится уведомление об этом.

- Отсутствие на виртуальной машине несовместимого программного обеспечения. Мастер установки выполняет поиск установленных на виртуальной машине программ, одновременная работа которых с Легким агентом может привести к конфликтам. Если такие программы найдены, мастер установки отображает их список и запрос на подтверждение удаления. После подтверждения мастер установки пытается удалить программы автоматически. Если при удалении программ требуется перезагрузка, мастер установки перезагружает виртуальную машину. Вы можете ознакомиться со списком несовместимого программного обеспечения в файле incompatible.txt, который входит в комплект поставки Kaspersky Security.

  Если на виртуальной машине обнаружены программы, которые мастер установки не может удалить автоматически, вам предлагается удалить их вручную.

Во время установки выполняется проверка виртуальной машины на наличие активного заражения. В случае обнаружения угрозы и невозможности ее лечения установка завершается с ошибкой. Для нейтрализации угрозы рекомендуется использовать утилиты KVRT и Rescue Disc. Описание утилит см. в Базе знаний (http://support.kaspersky.ru/11102).

В этом разделе

Шаг 1. Стартовое окно мастера установки

Если условия для установки компонента Легкий агент для Windows соответствуют предъявляемым требованиям, открывается стартовое окно мастера установки. Стартовое окно мастера установки содержит информацию о начале установки Легкого агента для Windows на виртуальную машину, которую вы хотите защищать.

Перейдите к следующему шагу мастера установки.

Шаг 2. Просмотр Лицензионного соглашения

На этом шаге ознакомьтесь с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочтите Лицензионное соглашение и, если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**.

Перейдите к следующему шагу мастера.

Шаг 3. Выбор типа установки

На этом шаге выберите тип установки компонента Легкий агент.

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.

Если вы устанавливаете Легкий агент на виртуальную машину с гостевой настольной операционной системой Microsoft Windows, для выбора доступны следующие параметры:

- **Установка компонентов защиты**. Выберите этот вариант, если вы хотите установить на виртуальную машину компоненты защиты Легкого агента с параметрами, рекомендуемыми специалистами «Лаборатории Касперского».

- **Установка компонентов защиты и контроля**. Выберите этот вариант, если вы хотите установить на виртуальную машину компоненты защиты и компоненты контроля Легкого агента с параметрами, рекомендуемыми специалистами «Лаборатории Касперского».

- **Выборочная установка**. Установите этот флажок, если вы хотите выбрать папку, в которую будет установлена программа (см. раздел «Шаг 5. Выбор папки для установки» на стр. 90), и компоненты Легкого агента для установки (см. раздел «Шаг 4. Выбор компонентов Легкого агента для установки» на стр. 89).

Если вы устанавливаете Легкий агент на виртуальную машину с гостевой серверной операционной системой Microsoft Windows, для выбора доступны следующие варианты:

- **Полная установка**. Выберите этот вариант, если вы хотите установить на виртуальную машину компоненты защиты Легкого агента с параметрами, рекомендуемыми специалистами «Лаборатории Касперского».

- **Выборочная установка**. Выберите этот вариант, если вы хотите выбрать папку, в которую будет установлена программа (см. раздел «Шаг 5. Выбор папки для установки» на стр. 90), и компоненты защиты Легкого агента для установки (см. раздел «Шаг 4. Выбор компонентов Легкого агента для установки» на стр. 89).

Перейдите к следующему шагу мастера установки.

Шаг 4. Выбор компонентов Легкого агента для установки

Этот шаг выполняется, если вы установили флажок **Выборочная установка** или выбрали вариант **Выборочная установка** на шаге «Выбор типа установки» (см. раздел «Шаг 3. Выбор типа установки» на стр. 88).

На этом шаге вы можете выбрать компоненты Легкого агента, которые вы хотите установить.

Если вы устанавливаете Легкий агент на виртуальную машину с настольной операционной системой Microsoft Windows, по умолчанию для установки выбраны следующие компоненты:

- все компоненты защиты, если вы выбрали тип установки «Установка компонентов защиты»;
- все компоненты защиты и все компоненты контроля, если вы выбрали тип установки «Установка компонентов защиты и контроля».

Если вы устанавливаете Легкий агент на виртуальную машину с серверной операционной системой Microsoft Windows, по умолчанию для установки выбраны все компоненты защиты. Компоненты контроля не устанавливаются на виртуальную машину с серверной операционной системой Microsoft Windows.

Чтобы выбрать компонент Легкого агента для последующей установки, откройте контекстное меню по левой клавише мыши на значке рядом с названием компонента и выберите пункт **Компонент будет установлен на локальный жесткий диск**. Информацию о том, какие задачи выполняет выбранный компонент и сколько места на жестком диске требуется для установки компонента, вы можете посмотреть в нижней части окна мастера установки.

Чтобы узнать подробную информацию о свободном дисковом пространстве на виртуальной машине, которую вы хотите защищать, нажмите на кнопку **Диск**. Информация отображается в открывшемся окне **Доступное дисковое пространство**.

Чтобы отказаться от установки компонента Легкого агента, откройте контекстное меню по левой клавише мыши на значке рядом с названием компонента и выберите пункт **Компонент будет недоступен**.

Чтобы вернуться к списку устанавливаемых по умолчанию компонентов Легкого агента, нажмите на кнопку **Сброс**.

Перейдите к следующему шагу мастера установки.

Шаг 5. Выбор папки для установки

> Этот шаг выполняется, если вы установили флажок **Выборочная установка** или выбрали вариант **Выборочная установка** на шаге «Выбор типа установки» (см. раздел «Шаг 3. Выбор типа установки» на стр. 88).

На этом шаге укажите путь к папке, в которую будет установлен Легкий агент для Windows. Для этого нажмите на кнопку **Обзор** и выберите папку для установки в открывшемся окне **Изменение текущей папки для установки программы**.

Чтобы просмотреть информацию о свободном дисковом пространстве виртуальной машины, которую вы хотите защищать, нажмите на кнопку **Диск**. Информация отображается в открывшемся окне **Доступное дисковое пространство**.

Перейдите к следующему шагу мастера установки.

Шаг 6. Настройка доверенной зоны

На этом шаге вы можете сформировать доверенную зону для компонента Легкий агент для Windows.

Доверенная зона – это сформированный администратором системы список файлов, папок, объектов и программ, которые Kaspersky Security не контролирует в процессе работы.

Список окна **Исключения** содержит названия компаний-производителей программ или названия 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 Provisioning Services**, **Citrix Profile Manager**, **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 установки.

Шаг 7. Запуск установки

Поскольку в операционной системе виртуальной машины, которую вы хотите защищать, могут присутствовать вредоносные программы, способные помешать установке компонента Легкий агент, установку рекомендуется защищать.

По умолчанию защита установки включена.

Выключать защиту установки рекомендуется в том случае, когда невозможно выполнить установку Легкого агента для Windows. Например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop. Причиной этому может быть включенная защита установки Легкого агента для Windows. В этом случае прервите установку и запустите мастер установки повторно. На этом шаге снимите флажок **Защитить процесс установки**.

Если вы устанавливаете Легкий агент для Windows на виртуальную машину, на которой используется технология Citrix Provisioning Services, установите флажок **Обеспечить совместимость с Citrix Provisioning Services**.

Если вы устанавливаете Легкий агент для Windows на шаблон временных виртуальных машин, установите флажок **Установка на шаблон для временных пулов VDI** (см. раздел «Установка Легкого агента для Windows на шаблон виртуальных машин» на стр. 98). Обновления, требующие перезагрузки защищенной виртуальной машины, не будут устанавливаться на виртуальных машинах, созданных из этого шаблона. При получении обновлений, требующих перезагрузки защищенной виртуальной машины, Легкий агент будет отправлять в Kaspersky Security Center сообщение о необходимости обновления баз и модулей программы на шаблоне защищенных виртуальных машин.

> Об установке Легкого агента для Windows на шаблоны виртуальных машин см. также в Базе знаний (http://support.kaspersky.ru/13108).

Флажок **Добавить путь к файлу avp.com в системную переменную %PATH%** включает или выключает функцию, которая добавляет в системную переменную %PATH% путь к файлу avp.com. Если флажок установлен, то для запуска Легкого агента для Windows или любых задач Легкого агента из командной строки не требуется вводить путь к исполняемому файлу. Достаточно ввести название исполняемого файла и команду для запуска соответствующей задачи.

Чтобы запустить установку Легкого агента для Windows, нажмите на кнопку **Установить**.

Во время установки Легкого агента для Windows на виртуальную машину возможен разрыв текущих сетевых соединений. Большинство разорванных соединений восстанавливается через некоторое время.

Шаг 8. Установка компонента Легкий агент для Windows

На этом шаге выполняется установка компонента Легкий агент для Windows. Установка занимает некоторое время, дождитесь ее завершения.

Шаг 9. Завершение установки

На этом шаге завершите работу мастера.

Компонент Легкий агент для Windows запускается автоматически на виртуальной машине после установки.

Легкий агент для Windows подключается к SVM. Сервер защиты передает Легкому агенту сведения о лицензии.

Легкий агент для Windows проверяет наличие пакета обновлений в папке на той SVM, к которой он подключен. При наличии пакета обновлений Легкий агент для Windows устанавливает на защищенной виртуальной машине обновления баз и модулей программы, необходимые для своей работы.

Установка Легкого агента для Windows из командной строки

Установку Легкого агента из командной строки требуется выполнять с правами администратора.

► *Чтобы установить Легкий агент для Windows из командной строки в интерактивном режиме,*

введите в командной строке одну из следующих команд:

- `setup.exe`
- `msiexec /i <название установочного пакета в формате MSI>`.

Запустится мастер установки программы. Следуйте его указаниям.

Файл setup.exe и установочный пакет в формате MSI входят в комплект поставки программы Kaspersky Security (см. раздел «Файлы, необходимые для установки программы» на стр. 43).

► *Чтобы установить Легкий агент для Windows из командной строки в тихом режиме (без запуска мастера установки),*

введите в командной строке одну из следующих команд:

- `setup.exe /s /pEULA=1 /pALLOWREBOOT=1|0`
- `msiexec /i <название установочного пакета в формате MSI> EULA=1 ALLOWREBOOT=1|0 /qn`,

где:

- `EULA=1` означает, что вы принимаете условия Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки программы (см. раздел «Комплект поставки» на стр. 22). Согласие с условиями Лицензионного соглашения является необходимым условием для установки программы.
- `ALLOWREBOOT=1|0` означает согласие или запрет на автоматическую перезагрузку виртуальной машины, если она потребуется после установки. Параметр необязательный. Если в команде не указано значение параметра `ALLOWREBOOT`, по умолчанию считается, что вы запрещаете перезагрузку виртуальной машины после установки программы. Автоматическая перезагрузка виртуальной машины может быть выполнена только в режиме тихой установки (с ключом `/qn`).

  Перезагрузка виртуальной машины может потребоваться, если во время установки Легкого агента для Windows обнаружено и удалено стороннее антивирусное программное обеспечение.

► *Чтобы установить Легкий агент на виртуальную машину, на которой используется технология Citrix Provisioning Services,*

введите в командной строке одну из следующих команд:

- `setup.exe /pINSTALLONPVS=1`
- `msiexec /i <название установочного пакета в формате MSI> INSTALLONPVS=1`.

► *Чтобы установить Легкий агент Легкий агент на шаблон временных виртуальных машин,*

укажите в команде параметр `USEPVMDETECTION=1`, например: `setup.exe /pUSEPVMDETECTION=1`.

► *Чтобы установить Легкий агент с паролем на действия с программой,*

введите в командной строке одну из следующих команд:

- `setup.exe /pKLLOGIN=<имя пользователя> /pKLPASSWD=***** /pKLPASSWDAREA=<область действия пароля>`
- `msiexec /i <название установочного пакета в формате MSI> KLLOGIN=<имя пользователя> KLPASSWD=***** KLPASSWDAREA=<область действия пароля>`.

Вместо `<область действия пароля>` вы можете указать один или несколько следующих значений параметра KLPASSWDAREA через ";":

- `SET`. Установка пароля на изменение параметров программы.
- `EXIT`. Установка пароля на завершение работы программы.
- `DISPROTECT`. Установка пароля на выключение компонентов защиты и остановку задач проверки.
- `DISPOLICY`. Установка пароля на выключение политики Kaspersky Security Center.
- `UNINST`. Установка пароля на удаление программы с виртуальной машины.
- `DISCTRL`. Установка пароля на выключение компонентов контроля (Контроль запуска программ, Контроль активности программ, Контроль устройств, Веб-Контроль).

Во время установки программы из командной строки вы можете использовать следующие файлы:

- Файл setup.ini. Файл содержит общие параметры установки программы и используется при установке компонента Легкий агент через командную строку или редактор

управления групповыми политиками службы каталогов (см. раздел «Установка Легкого агента для Windows через редактор управления групповыми политиками службы каталогов» на стр. 96). Файл setup.ini создается вручную. Описание параметров файла setup.ini см. на странице программы в Базе знаний (http://support.kaspersky.ru/13176).

- Конфигурационный файл install.cfg. Файл содержит параметры компонента Легкий агент и используется для импорта параметров Легкого агента при установке Легкого агента и при создании политики для Легкого агента, а также для переноса настроенных параметров программы на другую защищенную виртуальную машину. Конфигурационный файл создается в локальном интерфейсе Легкого агента (см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

Файлы setup.ini и install.cfg должны быть расположены в одной папке с установочным пакетом Kaspersky Security для виртуальных сред 4.0 Легкий агент.

Установка Легкого агента для Windows через редактор управления групповыми политиками службы каталогов

С помощью редактора управления групповыми политиками службы каталогов (Active Directory Group Policies) вы можете устанавливать компонент Легкий агент для Windows на виртуальные машины, связанные с выбранным объектом групповой политики, без использования Kaspersky Security Center.

Подробную информацию о работе с редактором управления групповыми политиками службы каталогов см. в *Справочной системе к Microsoft Windows*.

Перед началом установки компонента Легкий агент для Windows рекомендуется закрыть все программы, работающие в операционной системе виртуальной машины.

► *Чтобы установить Легкий агент для Windows через редактор управления групповыми политиками службы каталогов, выполните следующие действия:*

1. Создайте сетевую папку общего доступа на том компьютере, на котором установлен контроллер домена.

2. Поместите в сетевую папку общего доступа следующие файлы:

   - установочный пакет Kaspersky Security в формате MSI;
   - файл setup.ini с указанным значением параметра `Eula`, равным 1.

   Описание параметров файла setup.ini см. на странице программы в Базе знаний (http://support.kaspersky.ru/13176).

3. Откройте окно Microsoft Windows **Управление групповыми политиками**.

4. В дереве окна **Управление групповыми политиками** выберите объект групповой политики (Group Policy Object), с которым связаны виртуальные машины, предназначенные для установки Легкого агента для Windows.

5. По правой клавише мыши вызовите контекстное меню объекта групповой политики и выберите пункт **Изменить**.

   Откроется редактор управления групповыми политиками службы каталогов.

6. Создайте новый установочный пакет редактора управления групповыми политиками. Для этого выполните следующие действия:

   a. В дереве консоли выберите **Объект групповой политики \ Конфигурация компьютера \ Политики \ Конфигурация программ \ Установка программного обеспечения**.

   b. По правой клавише мыши откройте контекстное меню узла **Установка программного обеспечения**.

   c. В контекстном меню выберите пункт **Создать** → **Пакет**.

      Откроется стандартное окно Microsoft Windows **Открыть**.

   d. В стандартном окне Microsoft Windows **Открыть** укажите путь к установочному пакету Kaspersky Security в формате MSI.

Откроется окно **Развертывание программы**.

e. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный**.

f. Нажмите на кнопку **ОК**.

Групповая политика будет применена на каждой виртуальной машине, связанной с объектом групповой политики, при следующем запуске виртуальных машин. В результате компонент Легкий агент для Windows будет установлен на все виртуальные машины, связанные с выбранным объектом групповой политики.

Установка Легкого агента для Windows на шаблон виртуальных машин

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

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

2. Установите компонент Легкий агент для Windows на шаблон виртуальных машин. Установка выполняется в интерактивном режиме с помощью мастера установки (см. раздел «Установка Легкого агента для Windows с помощью мастера установки» на стр. 85).

3. На шаге 7 мастера (см. раздел «Шаг 7. Запуск установки» на стр. 92) установите флажок **Установка на шаблон для временных пулов VDI**, если из шаблона будет создана инфраструктура VDI одного из следующих типов:

   - каталог Citrix XenDesktop random;
   - каталог Citrix XenDesktop static с использованием Citrix Personal vDisk;
   - каталог Citrix XenDesktop static без сохранения изменений пользователя;
   - automated-пул VMware Horizon View типа linked clone.

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

сообщение о необходимости обновления баз и модулей программы на шаблоне защищенных виртуальных машин.

Не рекомендуется устанавливать флажок **Установка на шаблон для временных пулов VDI**, если из шаблона будет создана инфраструктура VDI одного из следующих типов:

- каталог Citrix XenDesktop static dedicated с использованием локальных дисков;
- automated-пул VMware Horizon View типа full clone.

4. Настройте подключение Легкого агента к SVM в локальном интерфейсе Легкого агента для Windows (подробнее см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*). После подключения к SVM Сервер защиты передает Легкому агенту сведения о лицензии. Вам требуется дождаться получения Легким агентом сведений о лицензии.
5. Легкий агент проверяет наличие пакета обновлений в папке на той SVM, к которой он подключен. При наличии пакета обновлений Легкий агент для Windows устанавливает на защищенной виртуальной машине обновления баз и модулей программы, необходимые для своей работы.

   Вы можете дождаться получения Легким агентом обновления баз и модулей программы или запустить задачу обновление вручную в локальном интерфейсе Легкого агента для Windows, а затем выполнить проверку шаблона виртуальных машин на наличие вредоносных программ (подробнее см. в *Руководстве пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows*).

   Рекомендуется перезагрузить шаблон виртуальных машин для оптимизации процесса загрузки операционной системы.
6. Создайте заново виртуальные машины из обновленного шаблона. См. подробнее в документации к виртуальной инфраструктуре.

Об установке Легкого агента на шаблоны виртуальных машин см. также в Базе знаний (http://support.kaspersky.ru/13108).

Совместимость с технологией Citrix Provisioning Services

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

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

Чтобы обеспечить совместимость программы с технологией Citrix Provisioning Services, требуется установить Легкий агент одним из следующих способов:

- С помощью мастера установки. На шаге 7 мастера установить флажок **Обеспечить совместимость с Citrix Provisioning Services**.
- Из командной строки с параметром INSTALLONPVS=1 (см. раздел «Установка Легкого агента для Windows из командной строки» на стр. 93).
- Удаленно через Kaspersky Security Center. При создании установочного пакета используйте файл Ksvla.kud (см. раздел «Создание установочного пакета Легкого агента для Windows» на стр. 82).

В локальном интерфейсе Легкого агента вы можете посмотреть информацию о совместимости с технологией Citrix Provisioning Services. Сведения о том, включена ли поддержка Citrix Provisioning Services, отображаются в окне **Поддержка**, которое открывается из главного окна программы.

Совместимость с технологией Citrix Personal vDisk

Вы можете установить Легкий агент на виртуальную машину, на которой используется технология Citrix Personal vDisk, одним из способов, предусмотренных для установки Легкого агента.

Программное обеспечение Citrix Personal vDisk должно быть установлено на виртуальной машине до установки компонента Легкий агент.

Чтобы обеспечить совместимость с технологией Citrix Personal vDisk, в ходе установки программа автоматически добавляет в файл custom_files_rules.txt следующую секцию:

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
[Rule-End]
```

Изменение состава установленных компонентов Легкого агента для Windows

После установки Легкого агента для Windows на виртуальной машине вы можете изменить состав установленных компонентов Легкого агента одним из следующих способов:

- С помощью групповой задачи изменения состава компонентов программы. Задача создается в Kaspersky Security Center. В процессе выполнения задачи программа Kaspersky Security устанавливает или удаляет компоненты Легкого агента для Windows на защищенных виртуальных машинах в соответствии с настроенным списком компонентов.
- Путем повторной удаленной установки Легкого агента для Windows через Kaspersky Security Center с использованием установочного пакета, в котором изменен список компонентов Легкого агента для Windows (см. раздел «Настройка параметров установочного пакета Легкого агента для Windows» на стр. 84).

► *Чтобы изменить состав установленных компонентов Легкого агента для Windows с помощью групповой задачи изменения состава компонентов 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, если вы хотите создать задачу для всех защищенных 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 защищенных 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 **Изменение состава компонентов программы** и перейдите к следующему шагу мастера.

5. Выберите тип установки Легкого агента и перейдите к следующему шагу мастера.

6. Если вы создаете задачу для одной или нескольких виртуальных машин, укажите способ выбора виртуальных машин. В зависимости от указанного вами способа выбора виртуальных машин в открывшемся окне выполните одно из следующих действий:

   - В списке обнаруженных виртуальных машин укажите виртуальные машины, на которых вы хотите изменить состав установленных компонентов Легкого агента. Для этого установите флажок в списке слева от названия виртуальной машины.

   - Нажмите на кнопку **Добавить** или **Добавить IP-интервал** и задайте адреса виртуальных машин вручную.

   - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов виртуальных машин.

   - Нажмите на кнопку **Выбрать** и в открывшемся окне укажите название выборки, содержащей виртуальные машины, на которых вы хотите изменить состав установленных компонентов Легкого агента.

   Перейдите к следующему шагу мастера создания задачи.

7. Настройте режим запуска задачи и перейдите к следующему шагу мастера.

8. Укажите имя создаваемой задачи и перейдите к следующему шагу мастера.

9. Завершите работу мастера создания задачи. Созданная задача отображается в списке задач для выбранной группы администрирования на закладке **Задачи** или в папке **Задачи**.

10. Выберите созданную задачу в списке задач и откройте окно **Свойства: <имя задачи>** двойным щелчком мыши или с помощью пункта **Свойства** контекстного меню.

11. В разделе **Параметры** укажите, какие компоненты Легкого агента должны быть установлены на защищенной виртуальной машине:

    - Если флажок рядом с названием компонента установлен, Kaspersky Security установит компонент на виртуальной машине. Если компонент уже установлен, то ничего не изменится.

    - Если флажок рядом с названием компонента не установлен, Kaspersky Security удалит компонент. Если компонент не был установлен, то ничего не изменится.

12. Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства: <имя задачи>**.

13. Запустите задачу изменения состава компонентов или дождитесь ее запуска по расписанию.

Установка компонента Легкий агент для Linux

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

- Из командной строки (см. раздел «Установка Легкого агента для Linux из командной строки» на стр. 107).

- Удаленно с рабочего места администратора с помощью программы Kaspersky Security Center (см. раздел «Установка Легкого агента для Linux через Kaspersky Security Center» на стр. 104).

Перед установкой Легкого агента для Linux требуется установить Агент администрирования Kaspersky Security Center (см. раздел «Установка Агента администрирования Kaspersky Security Center на виртуальные машины» на стр. 77).

В этом разделе

Установка Легкого агента для Linux через Kaspersky Security Center

Вы можете установить Легкий агент для Linux удаленно с рабочего места администратора с помощью программы Kaspersky Security Center. Установка выполняется с помощью мастера развертывания защиты или с помощью задачи удаленной установки программы. Для установки используется установочный пакет, который содержит набор параметров, необходимых для установки программы (см. раздел «Создание установочного пакета Легкого агента для Linux» на стр. 106).

Перед созданием установочного пакета требуется выполнить подготовку дистрибутива Легкого агента для Linux (см. раздел «Подготовка дистрибутива Легкого агента для Linux» на стр. 105).

Возможность установки Агента администрирования на виртуальную машину с операционной системой Linux через Kaspersky Security Center не поддерживается. Поэтому при установке Легкого агента для Linux с помощью задачи удаленной установки программы в окне **Дополнительно** не устанавливайте флажок **Установить Агент администрирования совместно с данной программой**.

Подробнее об удаленной установке программ через Kaspersky Security Center см. в документации Kaspersky Security Center.

В этом разделе

Подготовка дистрибутива Легкого агента для Linux

► *Чтобы подготовить дистрибутив Легкого агента для Linux для создания установочного пакета, выполните следующие действия:*

1. В папку, доступную для Сервера администрирования Kaspersky Security Center, распакуйте один из следующих архивов (в зависимости от менеджера пакетов, используемого в операционной системе виртуальной машины):

   - lightagent-4.0.X-X_rpm-<идентификатор языка>.tar.gz (для установки из пакета в формате RPM);
   - lightagent-4.0.X-X_deb-<идентификатор языка>.tar.gz (для установки из пакета в формате DEB);

   где:

   - 4.0.X-X – номер версии программы;
   - <идентификатор языка> – двухбуквенный идентификатор языка: ru, en, fr, de и другие.

2. Скопируйте в ту же папку один из следующих пакетов (в зависимости от операционной системы виртуальной машины и менеджера пакетов, используемого в ней):

   - lightagent-4.0.X-X.i686.rpm (для 32-разрядной операционной системы);
   - lightagent-4.0.X-X.x86_64.rpm (для 64-разрядной операционной системы);
   - lightagent_4.0.X-X_i386.deb (для 32-разрядной операционной системы);
   - lightagent_4.0.X-X_amd64.deb (для 64-разрядной операционной системы);

   где 4.0.X-X – номер версии программы.

Создание установочного пакета Легкого агента для Linux

Установочный пакет требуется для удаленной установки компонента Легкий агент для Linux через Kaspersky Security Center.

Перед созданием установочного пакета требуется выполнить подготовку дистрибутива Легкого агента для Linux (см. раздел «Подготовка дистрибутива Легкого агента для Linux» на стр. 105).

► *Чтобы создать установочный пакет Легкого агента для Linux, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли в папке **Дополнительно / Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Нажмите на кнопку **Создать инсталляционный пакет**, чтобы запустить мастер создания инсталляционного пакета.
4. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы «Лаборатории Касперского».**
5. В открывшемся окне мастера введите имя нового установочного пакета и перейдите к следующему шагу мастера.
6. В окне мастера **Выбор дистрибутива программы для установки** выберите дистрибутив Kaspersky Security. Для этого нажмите на кнопку **Выбрать** и в открывшемся стандартном окне Windows **Открыть** укажите путь к файлу lightagent.kud.

   В окне мастера **Выбор дистрибутива программы для установки** отобразится название программы.

   Перейдите к следующему шагу мастера.
7. В окне мастера **Лицензионное соглашение** ознакомьтесь с условиями Лицензионного соглашения, которое заключается между вами и «Лабораторией Касперского». Для продолжения создания установочного пакета требуется принять условия

Лицензионного соглашения. Установите флажок **Принимаю условия Лицензионного соглашения** и перейдите к следующему шагу мастера.

8. Мастер загружает файлы, необходимые для установки программы, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.

9. Завершите работу мастера.

Созданный установочный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно / Удаленная установка** во вложенной папке **Инсталляционные пакеты**. Вы можете использовать один и тот же установочный пакет многократно.

Установка Легкого агента для Linux из командной строки

Компонент Легкий агент для Linux распространяется в пакетах форматов DEB и RPM.

► *Чтобы установить Легкий агент для Linux из командной строки, выполните одну из следующих команд (в зависимости от операционной системы виртуальной машины и менеджера пакетов, используемого в операционной системе):*

- `# rpm -i lightagent-4.0.X-X.i686.rpm` – для установки из пакета формата RPM на 32-разрядную операционную систему;
- `# rpm -i lightagent-4.0.X-X.x86_64.rpm` – для установки из пакета формата RPM на 64-разрядную операционную систему;
- `# dpkg -i lightagent_4.0.X-X_i386.deb` – для установки из пакета формата DEB на 32-разрядную операционную систему;
- `# dpkg -i lightagent_4.0.X-X_amd64.deb` – для установки из пакета формата DEB на 64-разрядную операционную систему;

где `4.0.X-X` – номер версии программы.

После запуска команды установка выполняется автоматически.

После завершения установки Легкого агента для Linux требуется выполнить его первоначальную настройку одним из следующих способов:

- в интерактивном режиме (см. раздел «Первоначальная настройка Легкого агента для Linux в интерактивном режиме» на стр. 108);
- в тихом режиме (см. раздел «Первоначальная настройка Легкого агента для Linux в тихом режиме» на стр. 109).

Если вы не выполните первоначальную настройку Легкого агента для Linux, антивирусная защита виртуальной машины не будет работать.

Первоначальная настройка Легкого агента для Linux в интерактивном режиме

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

1. Выполните следующую команду:

   ```
   /opt/kaspersky/lightagent/bin/lightagent-setup.pl
   ```

   Запустится скрипт первоначальной настройки программы.

2. Ознакомьтесь с текстом Лицензионного соглашения, которое заключается между вами и «Лабораторией Касперского». Для этого нажмите на клавишу **ENTER**. Для завершения просмотра используйте клавишу **Q**. После выхода из режима просмотра введите yes (или y), если вы согласны с условиями Лицензионного соглашения.

   Для продолжения первоначальной настройки Легкого агента для Linux требуется принять условия Лицензионного соглашения.

3. Укажите идентификатор языка событий Легкого агента для Linux, отправляемых в Kaspersky Security Center: ru, en, fr, de или другой.

   По умолчанию скрипт первоначальной настройки программы предлагает использовать идентификатор языка en. Нажмите на клавишу **ENTER**, чтобы подтвердить

использование английского языка для событий или укажите другой идентификатор языка.

4. Подтвердите путь к исходным кодам ядра операционной системы или укажите другой путь к исходным кодам ядра.

   Если скрипт первоначальной настройки программы обнаруживает исходные коды ядра операционной системы в папке по умолчанию, на экране отображается найденный путь. Чтобы подтвердить путь к исходным кодам ядра операционной системы, нажмите на клавишу **ENTER**.

   Скрипт первоначальной настройки программы запускает компиляцию модуля ядра операционной системы Linux на виртуальной машине. Компилируется модуль, необходимый для работы задачи постоянной защиты.

   Если компиляция модуля ядра не производилась, задача постоянной защиты не обрабатывает операции над объектами файловой системы защищенной виртуальной машины.

5. Выполняется настройка Легкого агента для Linux. Если во время настройки возникают ошибки, информация о них отображается на экране.

Первоначальная настройка Легкого агента для Linux в тихом режиме

► *Чтобы запустить первоначальную настройку Легкого агента для Linux в тихом режиме,*

выполните следующую команду:

```
/opt/kaspersky/lightagent/bin/lightagent-setup.pl \
--auto-install=<путь к конфигурационному файлу>
```

где:

<путь к конфигурационному файлу> – полный путь к конфигурационному файлу первоначальной настройки lightagent.ini (см. раздел «Файлы, необходимые для установки программы» на стр. 43). Программа будет использовать параметры, указанные в этом файле, при выполнении первоначальной настройки Легкого агента для Linux.

Конфигурационный файл первоначальной настройки содержит следующие параметры:

- EULA_AGREED – согласие с условиями Лицензионного соглашения. Значение по умолчанию: yes. Обязательный параметр
- CONNECTOR_LOCALE – идентификатор языка Легкого агента для Linux. Значение по умолчанию: en.
- DEFAULT_KERNEL_SOURCES – использовать путь к исходным кодам ядра операционной системы, обнаруженным программой в папке по умолчанию. Значение по умолчанию: yes.

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

Изменения в Kaspersky Security Center после установки программы

После установки Kaspersky Security в виртуальной инфраструктуре SVM и защищенные виртуальные машины с установленным Агентом администрирования передают информацию о себе в Kaspersky Security Center. По умолчанию Kaspersky Security Center добавляет виртуальные машины с установленной программой Kaspersky Security в папку **Нераспределенные устройства**.

В Консоли администрирования Kaspersky Securit Center SVM отображается под именем, которое вы указали во время развертывания этой SVM. Имя защищенной виртуальной машины совпадает с сетевым именем виртуальной машины (hostname). Если на Сервере администрирования Kaspersky Security Center уже зарегистрирована виртуальная машина с таким именем, то к имени новой виртуальной машины добавляется окончание с порядковым номером, например: <Имя>~1, <Имя>~2.

Вы можете вручную переместить виртуальные машины в группу администрирования **Управляемые компьютеры** или вложенные группы администрирования (подробнее о перемещении виртуальных машин в группы администрирования см. в документации Kaspersky Security Center).

Если перед установкой программы вы настроили правила перемещения виртуальных машин в группы администрирования (см. раздел «Настройка правил перемещения виртуальных машин в группы администрирования» на стр. 54), Kaspersky Security Center перемещает виртуальные машины с установленной программой Kaspersky Security в указанные группы администрирования в соответствии с настроенными правилами перемещения виртуальных машин.

После развертывания на гипервизоре SVM передает в Kaspersky Security Center следующие теги:

- %HvName%=<имя гипервизора> – имя гипервизора, на котором работает SVM.
- %HvType%=<тип гипервизора> – тип гипервизора.

Защищенная виртуальная машина с установленным Агентом администрирования Kaspersky Security Center после подключения к SVM, работающей на том же гипервизоре, передает в Kaspersky Security Center следующие теги:

- %HvName%=<имя гипервизора> – имя гипервизора, на котором работает защищенная виртуальная машина.
- %HvType%=<тип гипервизора> – тип гипервизора.
- %VmType%=<Persistent / Nonpersistent> – признак определяет, является ли виртуальная машина временной виртуальной машиной.

Вы можете использовать указанные теги при создании правил перемещения SVM и защищенных виртуальных машин в группы администрирования.

Активация программы

Этот раздел содержит информацию об активации программы.

В этом разделе

Об активации программы

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

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 ключей Kaspersky Security Center одним из следующих способов:

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

Вы можете добавить ключ в хранилище ключей Kaspersky Security Center во время создания задачи активации программы или предварительно (см. раздел «Процедура активации программы» на стр. 116).

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.

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

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 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 (см. раздел «Удаление компонента Сервер защиты» на стр. 163).

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. 118).

   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. 117) или во время создания задачи активации программы.

2. Запустите задачу активации программы.

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 выберите файл с расширением key в открывшемся окне.
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. 118).

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 в папке **Управляемые компьютеры** выберите папку с названием этой группы администрирования. В рабочей области выберите закладку **Задачи** и 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 и нажмите на кнопку **Создать задачу**.
  - В дереве консоли в папке **Дополнительно** / **Управление программами** выберите вложенную папку **Лицензии на ПО Лаборатории Касперского** и 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 из хранилища 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. 117), нажмите на кнопку **Добавить**. Откроется окно **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. 117).

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 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, 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.

Запуск задачи активации программы

► *Чтобы запустить задачу 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 запустить задачу активации программы. В рабочей области выберите закладку **Задачи**.
   - Выберите папку **Задачи** дерева консоли.
3. В списке задач выберите задачу активации программы, которую вы хотите запустить.
4. 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.

Обновление антивирусных баз

Этот раздел содержит информацию о том, как обновить антивирусные базы программы.

В этом разделе

Об обновлении антивирусных баз

После установки или обновления Kaspersky Security необходимо выполнить обновление антивирусных баз программы.

Для обновления требуется действующая лицензия на использование программы.

Источником обновлений для программы Kaspersky Security является хранилище Сервера администрирования Kaspersky Security Center.

Обновление антивирусных баз выполняется следующим образом:

1. Компонент Сервер защиты загружает пакет обновлений из хранилища Сервера администрирования в папку на SVM.

   Загрузка пакета обновлений выполняется с помощью *задачи обновления* на Сервере защиты. Задача запускается из Kaspersky Security Center и выполняется на SVM. Чтобы успешно загрузить пакет обновлений из хранилища Сервера администрирования, SVM должна иметь доступ к Серверу администрирования Kaspersky Security Center.

2. Обновления баз устанавливаются из папки на SVM:

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

   - Компонент Легкий агент проверяет наличие пакета обновлений в папке на той SVM, к которой он подключен. При наличии пакета обновлений Легкий агент устанавливает на защищенной виртуальной машине обновления баз, необходимых для работы Легкого агента. Обновление баз выполняется с помощью *задачи обновления* на Легком агенте. Запуск задачи обновления на Легком агенте выполняется по расписанию. По умолчанию задан автоматический режим запуска задачи. Задача запускается каждые два часа.

Подробную информацию об обновлении баз и модулей программы см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

► *Чтобы обновить антивирусные базы на SVM, 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. Запустите вручную задачу загрузки обновлений в хранилище или дождитесь запуска задачи по расписанию. Убедитесь в том, что задача загрузки обновлений в хранилище выполнена успешно (см. подробнее в документации Kaspersky Security Center).

3. Создайте задачу обновления на Сервере защиты (см. раздел «Создание задачи обновления на Сервере защиты» на стр. 128).

4. Дождитесь запуска по расписанию задачи обновления или запустите задачу вручную (см. раздел «Запуск и остановка задачи обновления на Сервере защиты» на стр. 129).

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. 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 вручную запустить или остановить задачу.

Запуск и остановка задачи обновления на Сервере защиты

Вне зависимости от выбранного режима запуска задачи обновления на Сервере защиты вы можете запускать и останавливать задачу в любой момент.

► *Чтобы запустить или остановить 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 запустить или остановить задачу обновления, созданную для всех SVM. В рабочей области выберите закладку **Задачи**.

- Выберите в папке **Управляемые компьютеры** дерева консоли папку с названием группы администрирования, для SVM которой вы хотите запустить или остановить задачу обновления. В рабочей области выберите закладку **Задачи**.

- Выберите папку **Задачи** дерева консоли, если вы хотите запустить или остановить задачу обновления, созданную для одной или нескольких SVM.

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.

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. 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. 112).

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 (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.

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.

Обновление предыдущей версии программы

Этот раздел содержит информацию об обновлении предыдущей версии программы.

В этом разделе

Порядок обновления предыдущей версии программы

Вы можете обновить до Kaspersky Security для виртуальных сред 4.0 Легкий агент следующие версии программы:

- Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент;
- Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2.

Обновление программы состоит из следующих этапов:

1. Обновление Kaspersky Security Center 10 до версии Kaspersky Security Center 10 Service Pack 2 или Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 (подробнее см. в документации Kaspersky Security Center).
2. Обновление плагинов управления Kaspersky Security, Сервера интеграции и Консоли управления Сервера интеграции (см. раздел «Об обновлении плагинов управления Kaspersky Security и Сервера интеграции» на стр. 136).

3. Обновление компонента Сервер защиты. Обновление выполняется путем развертывания SVM с новой версией компонента Сервер защиты на гипервизорах. Развертывание выполняется с помощью мастера установки (см. раздел «Установка компонента Сервер защиты» на стр. 66).

   SVM с предыдущей версией компонента Сервер защиты продолжают работать на гипервизорах. Они обеспечивают защиту виртуальных машин с версией программы Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2 во время обновления программы. Вы можете удалить SVM с предыдущей версией компонента Сервер защиты после обновления компонента Легкий агент на всех защищенных виртуальных машинах (см. п. 5).

   После развертывания SVM с новой версией компонента Сервер защиты требуется выполнить следующие действия:

   - Активировать программу на SVM с новой версией компонента Сервер защиты (см. раздел «Об активации программы» на стр. 112).
   - Обновить антивирусные базы программы на SVM с новой версией компонента Сервер защиты (см. раздел «Обновление антивирусных баз» на стр. 126).

   > Если вы используете схему лицензирования по количеству ядер, используемых в физических процессорах на гипервизорах, после активации программы на SVM с новой версией компонента Сервер защиты Kaspersky Security может отправлять в Kaspersky Security Center событие о превышении лицензионного ограничения. Вы можете игнорировать это событие.

4. Обновление компонента Легкий агент на защищенных виртуальных машинах (см. раздел «Об обновлении компонента Легкий агент для Windows» на стр. 141).

5. Удаление SVM с предыдущей версией компонента Сервер защиты. После обновления компонента Легкий агент на всех защищенных виртуальных машинах вам требуется удалить на гипервизорах SVM с предыдущей версией компонента Сервер защиты. Удаление SVM выполняется через консоль управления виртуальной инфраструктурой (см. подробнее в документации к используемым гипервизорам).

Удаленные SVM продолжают отображаться в Консоли администрирования Kaspersky Security Center. По истечении срока, установленного в параметрах Kaspersky Security Center (подробнее см. в документации Kaspersky Security Center), SVM автоматически удаляются из Консоли администрирования.

Вы можете вручную удалить SVM с предыдущей версией компонента Сервер защиты из Консоли администрирования Kaspersky Security Center сразу после завершения процедуры обновления.

Об обновлении плагинов управления Kaspersky Security и Сервера интеграции

Обновление программы версии Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент

Если на компьютере установлены компоненты управления Kaspersky Security версии Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент (плагины управления Kaspersky Security, Сервер интеграции, Консоль управления Сервера интеграции), вам нужно обновить их. Обновление выполняется путем установки новой версии плагинов управления Kaspersky Security, Сервера интеграции и Консоли управления Сервера интеграции (см. раздел «Установка плагинов управления Kaspersky Security и Сервера интеграции» на стр. 59).

Удалять плагины управления версии Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент не требуется.

Обновленные плагины позволяют управлять версией программы Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, установленной на SVM и защищенных виртуальных машинах. Политики и задачи, настроенные с помощью плагинов управления версии Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, конвертируются автоматически в политики и задачи Kaspersky Security для виртуальных сред 4.0 Легкий агент после первого открытия и сохранения параметров в политике и задаче. При этом параметры, отсутствующие в политиках и задачах версии Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, принимают значения по умолчанию.

Если Консоль администрирования Kaspersky Security Center установлена на нескольких компьютерах, требуется обновить плагины управления Kaspersky Security на всех компьютерах. Параметры программы в плагинах управления Kaspersky Security разных версий различаются. Поэтому использование плагинов управления разных версий может привести к рассинхронизации между настроенными и используемыми параметрами программы.

Если после обновления плагинов управления Kaspersky Security в работе программы возникают ошибки, вы можете вернуться к использованию плагинов управления предыдущей версии. Для этого вам требуется удалить плагины управления Kaspersky Security новой версии (см. раздел «Удаление плагинов управления Kaspersky Security и Сервера интеграции» на стр. 170), затем установить плагины управления предыдущей версии.

Обновление программы версии Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2

Если на компьютере установлены плагины управления Kaspersky Security версии Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2, обновление плагинов управления Kaspersky Security и Сервера интеграции состоит из следующих этапов:

1. Установка новой версии плагинов управления Kaspersky Security, установка Сервера интеграции и Консоли управления Сервера интеграции (см. раздел «Установка плагинов управления Kaspersky Security и Сервера интеграции» на стр. 59).

   Плагины управления версии Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2 продолжают работать. С их помощью вы можете управлять версией программы Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2, установленной на SVM и защищенных виртуальных машинах.

2. Конвертирование политик и задач версии Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2. Мастер конвертации политик и задач Kaspersky Security Center позволяет создать новые политики и задачи, использующие параметры политик и задач предыдущей версии программы Kaspersky Security (см. раздел «Процедура конвертации политик и задач Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2» на стр. 138).

   Вы также можете создать новые политики на основе имеющихся с помощью мастера создания политики. Для этого на шаге «Выбор программы для создания групповой

политики» требуется установить флажок **Взять параметры из существующей политики предыдущей версии программы**. Подробнее о создании политик см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

3. Удаление плагинов управления Kaspersky Security версии Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2. Для удаления плагинов управления Kaspersky Security используйте стандартные средства удаления программ в операционной системе. В списке программ требуется выбрать для удаления программу Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2.

После завершения обновления программы вы можете удалить политики и задачи, созданные для программы версии Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2.

Процедура конвертации политик и задач Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2

► *Чтобы сконвертировать политики и задачи Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите Сервер администрирования.

3. По правой клавише мыши откройте контекстное меню и выберите пункт **Все задачи** → **Мастер конвертации политик и задач**.

   Запустится мастер конвертации политик и задач.

4. Следуйте указаниям мастера конвертации политик и задач.

В этом разделе

Шаг 1. Выбор программы, для которой нужно конвертировать политики и задачи

На этом шаге в списке **Название программы** выберите один из следующих вариантов:

- **Kaspersky Security для виртуальных сред 4.0 Легкий агент – Сервер защиты** – если вы хотите сконвертировать политики для Сервера защиты и задачи, которые выполняются на SVM.
- **Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows** – если вы хотите сконвертировать политики для Легкого агента и задачи, которые созданы в Kaspersky Security Center и выполняются на защищенных виртуальных машинах.

Перейдите к следующему шагу мастера конвертации политик и задач.

Шаг 2. Конвертация политик

На этом шаге выберите политики для конвертации. Чтобы выбрать политику, установите флажок слева от названия этой политики.

Перейдите к следующему шагу мастера конвертации политик и задач.

Если для конвертации вы выбрали политику для Сервера защиты, в которой включено использование служб Kaspersky Security Network, откроется окно **Kaspersky Security Network**. В этом окне вы можете ознакомиться 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 продолжить процедуру конвертации политик и задач, выполните одно из следующих действий:

- Нажмите на кнопку **Принять**, если вы хотите включить использование служб Kaspersky Security Network.
- Нажмите на кнопку **Отклонить**, если вы хотите выключить использование служб Kaspersky Security Network.

Шаг 3. Конвертация задач

На этом шаге выберите задачи для конвертации. Чтобы выбрать задачу, установите флажок слева от названия этой задачи.

Перейдите к следующему шагу мастера конвертации политик и задач.

Шаг 4. Завершение работы мастера конвертации политик и задач

На этом шаге завершите работу мастера конвертации политик и задач.

Сконвертированные политики отобразятся в списке политик на закладке **Политики** папки с названием группы администрирования. Сконвертированные политики получают следующее имя: «<имя исходной политики> (конвертированная)».

Сконвертированные задачи отобразятся в списке задач на закладке **Задачи** папки с названием группы администрирования или в папке **Задачи**. Сконвертированные задачи получают следующее имя: «<имя исходной задачи> (конвертированная)».

Сконвертированные политики и задачи используют параметры политик и задач предыдущей версии программы Kaspersky Security. Параметры, которые отсутствовали в политиках и задачах предыдущей версии программы, в сконвертированных политиках и задачах принимают значения по умолчанию.

Вы можете удалить исходные политики и задачи после завершения обновления программы (см. в документации Kaspersky Security Center).

Об обновлении компонента Легкий агент для Windows

Обновление компонента Легкий агент для Windows выполняется путем установки новой версии компонента Легкий агент для Windows на защищенных виртуальных машинах. Установка выполняется локально на виртуальной машине или удаленно через Kaspersky Security Center или редактор управления групповыми политиками службы каталогов.

Для обновленного Легкого агента для Windows используются задачи и параметры работы программы, настроенные для предыдущей версии Легкого агента для Windows.

При обновлении Легкого агента для Windows на защищенной виртуальной машине сохраняются резервные копии файлов, созданные при лечении или удалении файлов. Вы можете работать с файлами резервного хранилища через интерфейс программы.

После запуска на виртуальной машине обновленный Легкий агент подключается к SVM с новой версией компонента Сервер защиты.

Если после обновления Легкого агента для Windows в работе программы возникают ошибки, вы можете вернуться к использованию предыдущей версии компонента Легкий агент для Windows. Для этого вам требуется удалить новую версию компонента Легкий агент для Windows на виртуальной машине, затем установить предыдущую версию компонента Легкий агент для Windows.

Изменение конфигурации SVM

Вы можете изменить конфигурацию SVM:

- пароль конфигурирования и пароль учетной записи root;
- режим удаленного доступа для учетной записи root;
- сетевые параметры SVM;
- количество виртуальных сетей, которые SVM используют для связи с виртуальными машинами и Сервером администрирования Kaspersky Security Center;
- адреса гипервизоров, заданные на SVM;
- параметры подключения SVM к Серверу администрирования Kaspersky Security Center;
- имя и пароль учетной записи для подключения SVM к гипервизору или серверу управления виртуальной инфраструктурой.

► *Чтобы изменить конфигурацию SVM, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите Сервер администрирования.
3. По ссылке **Управление Kaspersky Security для виртуальных сред 4.0 Легкий агент** запустите мастер. Ссылка находится в рабочей области в блоке **Развертывание**.

   Вы можете изменить конфигурацию SVM с установленной версией программы Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2. Для этого по ссылке **Управление Kaspersky Security для виртуальных сред Легкий агент** запустите мастер. В этом случае параметры, отсутствующие в версии программы Kaspersky Security для виртуальных сред 3.0 Легкий агент Maintenance Release 2, не отображаются в мастере. Например, невозможно изменить количество виртуальных сетей, которые использует SVM, или изменить адрес гипервизора, заданный на SVM.

4. Следуйте указаниям мастера.

Во время изменения конфигурации SVM мастер сохраняет в журнал работы мастера информацию, указанную вами на каждом шаге мастера (см. раздел «Приложение. Описание журнала работы мастера» на стр. 175).

Вы можете использовать журнал работы мастера при обращении в Службу технической поддержки в случае, если изменение конфигурации SVM завершилось с ошибкой.

Журнал работы мастера сохраняется на компьютере, где был запущен мастер, в файле %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\4.0.0.0\KasperskyDeploymentWizard.log.

Информация в файле перезаписывается при каждом запуске мастера. Чтобы использовать информацию журнала работы мастера в дальнейшем, нужно сохранить файл в место постоянного хранения.

В этом разделе

Выбор действия

На этом шаге выберите вариант **Изменение конфигурации SVM**.

Перейдите к следующему шагу мастера.

Выбор SVM для изменения конфигурации

На этом шаге выберите SVM, конфигурацию которых вы хотите изменить.

В таблице отображается список гипервизоров и SVM, развернутых на гипервизорах. Вы можете добавить в список гипервизоры, на которых вы хотите изменить конфигурацию SVM.

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

1. Нажмите на кнопку **Добавить**.

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

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

   - **Тип**.

     Раскрывающийся список для выбора типа гипервизора или сервера управления виртуальной инфраструктурой.

   - **Адреса**.

Список адресов гипервизоров, на которых вы хотите изменить конфигурацию SVM, или адрес сервера управления виртуальной инфраструктурой, под управлением которого работают гипервизоры.

Вы можете указать в качестве адреса гипервизора или сервера управления виртуальной инфраструктурой его IP-адрес в формате IPv4 или полное доменное имя (FQDN). Вы можете указать IP-адреса или полные доменные имена через точку с запятой или с новой строки.

Количество правильно распознанных адресов отображается под списком адресов.

- **Имя пользователя**.

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

- **Пароль**.

  Пароль учетной записи, которая используется для подключения мастера к гипервизору или к серверу управления виртуальной инфраструктурой.

3. Нажмите на кнопку **Подключиться**.

   Окно **Параметры подключения к виртуальной инфраструктуре** закроется, выбранные гипервизоры добавятся в список гипервизоров. Если не удалось установить подключение к гипервизору или серверу управления виртуальной инфраструктурой, информация об ошибках подключения отображается в таблице.

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

- **Имя**.

  Имя гипервизора или имя SVM, развернутой на гипервизоре.

  Если имеются ограничения для изменения конфигурации SVM

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

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

- удалить из списка выбранный гипервизор или все гипервизоры под управлением выбранного сервера управления виртуальной инфраструктурой;
- открыть окно **Параметры подключения к виртуальной инфраструктуре** для изменения параметров учетной записи, под которой выполняется подключение к выбранному гипервизору или серверу управления виртуальной инфраструктурой.

- **Состояние**.

  Состояние гипервизора или SVM.

  Для гипервизора указывается одно из следующих значений: *Включен*, *Выключен*, *Режим самообслуживания*. Если не удалось установить подключение к гипервизору, в графе отображается *Соединение не установлено*. Для SVM указывается одно из следующих значений: *Запущена*, *Остановлена*.

- **Защита**.

  Номер версии образа SVM.

Чтобы обновить список гипервизоров в таблице, нажмите на кнопку **Обновить**, расположенную над списком.

► *Чтобы выбрать SVM для изменения конфигурации,*

установите в таблице флажки слева от названий SVM.

Вы можете выбирать только те SVM, для которых отсутствуют ограничения для изменения конфигурации.

Перейдите к следующему шагу мастера.

Ввод пароля конфигурирования

На этом шаге укажите пароль конфигурирования, который был создан при установке компонента Сервер защиты.

Перейдите к следующему шагу мастера.

Изменение адресов гипервизоров или серверов управления виртуальной инфраструктурой

На этом шаге вы можете изменить адреса гипервизоров или серверов управления виртуальной инфраструктурой, заданные на SVM.

Для этого установите флажок **Изменить адреса гипервизоров или серверов управления виртуальной инфраструктурой, заданные на SVM** и укажите в графе **Новый адрес** одно из следующих значений:

- для SVM на гипервизорах Microsoft Windows Server (Hyper-V), Citrix XenServer или KVM – новый IP-адрес в формате IPv4 или полное доменное имя (FQDN) каждого гипервизора, адрес которого требуется изменить;
- для SVM на гипервизорах Vmware ESXi – новый IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера Vmware vCenter, под управлением которого работают гипервизоры.

Перейдите к следующему шагу мастера.

Изменение списка виртуальных сетей для SVM

На этом шаге вы можете изменить количество виртуальных сетей, которые SVM должны использовать для связи с виртуальными машинами и Сервером администрирования Kaspersky Security Center. Для этого установите флажок **Изменить список виртуальных сетей**, затем для каждой SVM в графе **Имя сети** измените список используемых сетей.

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

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

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

Перейдите к следующему шагу мастера.

Изменение сетевых параметров SVM

На этом шаге вы можете изменить сетевые параметры SVM. Для этого установите флажок **Изменить сетевые параметры SVM**.

> Если вы изменили количество виртуальных сетей для одной или нескольких SVM, флажок **Изменить сетевые параметры SVM** не отображается. Вам требуется настроить сетевые параметры SVM, выбранных для изменения конфигурации.

► *Чтобы настроить сетевые параметры SVM, выполните одно из следующих действий:*

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

  Если вы хотите указать IP-адрес DNS-сервера и альтернативного DNS-сервера для каждой SVM, снимите флажок **Использовать список DNS-серверов, полученных по DHCP** и укажите IP-адреса DNS-серверов в таблице в графах **DNS-сервер** и **Альтернативный DNS-сервер**. По умолчанию используются IP-адреса DNS-серверов, полученные по протоколу DHCP.

Если SVM использует несколько виртуальных сетей, сетевые параметры будут получены от сервера DHCP по первой виртуальной сети из списка сетей, сформированного при развертывании SVM. Убедитесь, что мастер сможет подключиться к SVM с сетевыми параметрами первой виртуальной сети, полученными от сервера DHCP.

- Если вы хотите назначить сетевые параметры SVM вручную, выберите вариант **Статическая IP-адресация** и укажите следующие сетевые параметры для каждой SVM:
  - IP-адрес SVM (по умолчанию в графе указан текущий адрес SVM);
  - маска подсети;
  - шлюз;
  - DNS-сервер;
  - альтернативный DNS-сервер.

Перейдите к следующему шагу мастера.

Изменение параметров подключения к Kaspersky Security Center

На этом шаге вы можете изменить параметры подключения SVM к Серверу администрирования Kaspersky Security Center.

Для этого установите флажок **Изменить параметры подключения к Kaspersky Security Center** и укажите следующие параметры:

- **Адрес**.

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

- **Порт**.

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

- **SSL-порт**.

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

Перейдите к следующему шагу мастера.

Изменение пароля конфигурирования и параметров учетной записи root

На этом шаге вы можете изменить следующие параметры:

- Пароль конфигурирования – пароль, который используется для изменения конфигурации SVM. Для этого установите флажок **Изменить пароль конфигурирования** и укажите новый пароль конфигурирования в полях **Пароль** и **Подтверждение**.

- Пароль учетной записи root. Для этого установите флажок **Изменить пароль учетной записи root** и укажите новый пароль в полях **Пароль** и **Подтверждение**.

- Режим удаленного доступа к SVM для учетной записи root. Для этого установите флажок **Изменить режим удаленного доступа для учетной записи root**, затем выполните одно из следующих действий:

  - если вы хотите разрешить доступ для учетной записи root к SVM через SSH, установите флажок **Разрешить удаленный доступ для учетной записи root через SSH**;

  - вы хотите запретить для учетной записи root к SVM через SSH, снимите флажок **Разрешить удаленный доступ для учетной записи root через SSH**.

Перейдите к следующему шагу мастера.

Изменение параметров подключения к серверу VMware vCenter

Этот шаг отображается, если для изменения конфигурации выбраны SVM, развернутые на гипервизорах VMware ESXi.

На этом шаге вы можете изменить учетную запись, которую используют SVM для подключения к серверу VMware vCenter.

По умолчанию для подключения SVM к виртуальной инфраструктуре используется учетная запись, которую вы указали при установке компонента Сервер защиты (см. раздел «Шаг 2. Выбор гипервизоров для развертывания SVM» на стр. 68). В целях повышения безопасности рекомендуется использовать учетную запись, созданную для работы SVM. Требования к учетным записям см. в *Руководстве по внедрению Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

Если вы хотите изменить учетную запись, которую используют SVM для подключения к серверу VMware vCenter, установите флажок **Изменить учетную запись для подключения к серверу VMware vCenter** и введите параметры учетной записи в полях **Имя пользователя** и **Пароль**.

Указанная учетная запись будет использоваться в работе SVM для получения информации о виртуальной инфраструктуре.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к серверу VMware vCenter с именем и паролем указанной учетной записи. Если не удалось установить подключение, в окне отображается таблица с информацией об этом и описанием ошибки подключения. Проверьте параметры указанной учетной записи, при необходимости укажите другие имя и пароль учетной записи для подключения SVM к серверу VMware vCenter.

Изменение параметров подключения к гипервизорам Microsoft Windows Server (Hyper-V)

Этот шаг отображается, если для изменения конфигурации выбраны SVM, развернутые на гипервизорах Microsoft Windows Server (Hyper-V).

На этом шаге вы можете изменить учетную запись, которую SVM используют для подключения к гипервизорам Microsoft Windows Server (Hyper-V).

По умолчанию для подключения SVM к виртуальной инфраструктуре используется учетная запись, которую вы указали при установке компонента Сервер защиты (см. раздел «Шаг 2. Выбор гипервизоров для развертывания SVM» на стр. 68). В целях повышения безопасности рекомендуется использовать учетную запись, созданную для работы SVM. Требования к учетным записям см. в *Руководстве по внедрению Kaspersky Security для виртуальны сред 4.0 Легкий агент*.

Если вы хотите изменить учетную запись, которую SVM используют для подключения к гипервизорам Microsoft Windows Server (Hyper-V), установите флажок **Изменить учетную запись для подключения к гипервизорам Microsoft Windows Server (Hyper-V)** и введите параметры учетной записи в полях **Имя пользователя** и **Пароль**.

Указанная учетная запись будет использоваться в работе SVM для получения информации о виртуальной инфраструктуре.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к гипервизорам Microsoft Windows Server (Hyper-V), выбранным для изменения конфигурации SVM, с именем и паролем указанной учетной записи. Если не удалось установить подключение хотя бы к одному из гипервизоров, в окне отображается таблица с информацией об этом. В таблице для каждого гипервизора описана ошибка подключения. Проверьте параметры указанной учетной записи, при необходимости укажите другие имя и пароль учетной записи для подключения SVM к гипервизорам Microsoft Windows Server (Hyper-V).

Изменение параметров подключения к гипервизорам Citrix XenServer

Этот шаг отображается, если для изменения конфигурации выбраны SVM, развернутые на гипервизорах Citrix XenServer.

На этом шаге вы можете изменить учетную запись, которую SVM используют для подключения к гипервизорам Citrix XenServer.

По умолчанию для подключения SVM к виртуальной инфраструктуре используется учетная запись, которую вы указали при установке компонента Сервер защиты (см. раздел «Шаг 2. Выбор гипервизоров для развертывания SVM» на стр. 68). В целях повышения безопасности рекомендуется использовать учетную запись, созданную для работы SVM. Требования к учетным записям см. в *Руководстве по внедрению Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

Если вы хотите изменить учетную запись, которую SVM используют для подключения к гипервизорам Citrix XenServer, установите флажок **Изменить учетную запись для подключения к гипервизорам Citrix XenServer** и введите параметры учетной записи в полях **Имя пользователя** и **Пароль**.

Указанная учетная запись будет использоваться в работе SVM для получения информации о виртуальной инфраструктуре.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к гипервизорам Citrix XenServer, выбранным для изменения конфигурации SVM, с именем и паролем указанной учетной записи. Если не удалось установить подключение хотя бы к одному из гипервизоров, в окне отображается таблица с информацией об этом. В таблице для каждого гипервизора описана ошибка подключения. Проверьте параметры указанной учетной записи, при необходимости укажите другие имя и пароль учетной записи для подключения SVM к гипервизорам Citrix XenServer.

Изменение параметров подключения к гипервизорам KVM

Этот шаг отображается, если для изменения конфигурации выбраны SVM, развернутые на гипервизорах KVM.

На этом шаге вы можете изменить учетную запись, которую SVM используют для подключения к гипервизорам KVM.

По умолчанию для подключения SVM к виртуальной инфраструктуре используется учетная запись, которую вы указали при установке компонента Сервер защиты (см. раздел «Шаг 2. Выбор гипервизоров для развертывания SVM» на стр. 68). В целях повышения безопасности рекомендуется использовать учетную запись, созданную для работы SVM. Требования к учетным записям см. в *Руководстве по внедрению Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

Если вы хотите изменить учетную запись, которую SVM используют для подключения к гипервизорам KVM, установите флажок **Изменить учетную запись для подключения к гипервизорам KVM** и введите параметры учетной записи в полях **Имя пользователя** и **Пароль**.

Указанная учетная запись будет использоваться в работе SVM для получения информации о виртуальной инфраструктуре.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к гипервизорам KVM, выбранным для изменения конфигурации SVM, с именем и паролем указанной учетной записи. Если не удалось установить подключение хотя бы к одному из гипервизоров, в окне отображается таблица с информацией об этом. В таблице для каждого гипервизора описана ошибка подключения. Проверьте параметры указанной учетной записи, при необходимости укажите другие имя и пароль учетной записи для подключения SVM к гипервизорам KVM.

Запуск изменения конфигурации SVM

На этом шаге в окне мастера отображаются все ранее введенные параметры, необходимые для изменения конфигурации SVM.

Чтобы запустить изменение конфигурации SVM, перейдите к следующему шагу мастера.

Изменение конфигурации SVM

На этом шаге выполняется изменение конфигурации SVM.

Информация о процессе и результате изменения конфигурации каждой SVM отображается в окне мастера. Процесс занимает некоторое время. Дождитесь завершения процесса.

Перейдите к следующему шагу мастера.

Завершение изменения конфигурации SVM

На этом шаге отображается информация о результатах изменения конфигурации SVM.

Мастер отображает ссылки, по которым вы можете открыть краткий отчет и журнал работы мастера.

Краткий отчет содержит информацию о результатах выполнения этапов изменения конфигурации на всех SVM. Краткий отчет сохраняется во временном файле. Чтобы использовать информацию отчета в дальнейшем, нужно сохранить файл в место постоянного хранения.

Журнал работы мастера содержит информацию, указанную вами на каждом шаге мастера (см. раздел «Приложение. Описание журнала работы мастера» на стр. 175). Если во время изменения конфигурации SVM произошли ошибки, вы можете использовать журнал работы мастера при обращении в Службу технической поддержки.

Журнал работы мастера сохраняется на том компьютере, где был запущен мастер, в папке C:\Users\%user%\AppData\Local\KasperskyDeploymentWizard.log и не содержит информации об учетных записях.

Завершите работу мастера.

Просмотр и изменение параметров Сервера интеграции

В Консоли управления Сервера интеграции вы можете выполнить следующие действия:

- Посмотреть параметры Сервера интеграции и журнал работы Сервера интеграции.
- Изменить пароли учетных записей Сервера интеграции:
  - учетной записи администратора Сервера интеграции;
  - учетной записи для подключения SVM к Серверу интеграции;
  - учетной записи для подключения Легких агентов к Серверу интеграции.

> Имена учетных записей недоступны для изменения.

В этом разделе

Запуск Консоли управления Сервера интеграции

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

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

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите Сервер администрирования.

3. Запустите Консоль управления Сервера интеграции по ссылке **Запустить Консоль управления Сервера интеграции** в блоке **Развертывание**.

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

   - если компьютер, на котором установлена Консоль управления Сервера интеграции, не входит в домен Microsoft Windows;

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

   Укажите следующие параметры подключения:

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

   - Учетную запись для подключения к Серверу интеграции:

     - Если компьютер, где установлена Консоль управления Сервера интеграции, входит в домен и ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, вы можете использовать доменную учетную запись. Для этого установите флажок **Использовать доменную учетную запись**.

       Если вы хотите использовать учетную запись администратора Сервера интеграции, введите пароль администратора в поле **Пароль**.

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

Нажмите на кнопку **Подключить**.

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

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

Откроется Консоль управления Сервера интеграции.

Просмотр параметров Сервера интеграции

► *Чтобы посмотреть параметры Сервера интеграции, выполните следующие действия:*

1. Запустите Консоль управления Сервера интеграции (см. раздел «Запуск Консоли управления Сервера интеграции» на стр. 157).

   Откроется раздел **Параметры Сервера интеграции**.

   В разделе **Параметры Сервера интеграции** отображаются следующие параметры Сервера интеграции, к которому выполнено подключение:

   - версия Сервера интеграции;
   - имя учетной записи, под которой выполнено подключение к Серверу интеграции;

- тип аутентификации, который использовался при подключении к Серверу интеграции;
- IP-адрес в формате IPv4 или полное доменное имя (FQDN) и порт Сервера интеграции.

По ссылке **Посмотреть журнал работы** вы можете открыть журнал работы Сервера интеграции. Журнал работы открывается в текстовом редакторе Блокнот. О журналах Сервера интеграции см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

2. Чтобы закрыть Консоль управления, нажмите на кнопку **Закрыть**.

Изменение паролей учетных записей Сервера интеграции

► *Чтобы изменить параметры учетных записей Сервера интеграции, выполните следующие действия:*

1. Запустите Консоль управления Сервера интеграции (см. раздел «Запуск Консоли управления Сервера интеграции» на стр. 157).
2. В разделе **Учетные записи Сервера интеграции** выберите в таблице имя учетной записи, пароль которой вы хотите изменить.
3. По ссылке **Изменить пароль учетной записи** откройте окно **Пароль учетной записи** и введите новый пароль в полях **Пароль** и **Подтверждение пароля**.

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

4. Нажмите на кнопку **ОК** в окне **Пароль учетной записи**.
5. Нажмите на кнопку **Закрыть**, чтобы применить изменения и закрыть Консоль управления Сервера интеграции.

Если в политике для Сервера защиты настроено подключение SVM к Серверу интеграции и вы изменили пароль учетной записи для подключения SVM, вам требуется повторно настроить подключение SVM к Серверу интеграции в политике для Сервера защиты.

Если в политике для Легкого агента настроено подключение Легких агентов к Серверу интеграции и вы изменили пароль учетной записи для подключения Легких агентов, вам нужно повторно настроить подключение Легких агентов к Серверу интеграции в политике для Легкого агента для Windows и в политике для Легкого агента для Linux.

Новые параметры учетной записи для подключения к Серверу интеграции передаются в политику при сохранении параметров политики.

Удаление программы

Этот раздел содержит информацию о том, как удалить программу Kaspersky Security из виртуальной инфраструктуры.

В результате удаления программы Kaspersky Security виртуальные машины и данные пользователей окажутся незащищенными.

В этом разделе

Порядок удаления программы

Удаление программы Kaspersky Security из виртуальной инфраструктуры состоит из следующих этапов:

1. Удаление компонента Сервер защиты Kaspersky Security.

   Вы можете удалить Сервер защиты на всех или некоторых гипервизорах в виртуальной инфраструктуре (см. раздел «Удаление компонента Сервер защиты» на стр. 163).

2. Удаление компонента Легкий агент для Windows (см. раздел «Удаление компонента Легкий агент для Windows» на стр. 164) или Легкий агент для Linux (см. раздел «Удаление компонента Легкий агент для Linux» на стр. 168).

Вы можете удалить компонент Легкий агент на всех или некоторых виртуальных машинах.

3. Удаление компонента Легкий агент для Windows с шаблонов виртуальных машин (см. раздел «Удаление Легкого агента для Windows с шаблона виртуальных машин» на стр. 168).

4. Если на защищенных виртуальных машинах и шаблонах виртуальных машин был установлен Агент администрирования Kaspersky Security Center, требуется удалить компонент Агент администрирования с защищенных виртуальных машин и шаблонов виртуальных машин (см. раздел «Удаление Агента администрирования Kaspersky Security Center с виртуальных машин» на стр. 170).

5. Удаление плагинов управления Kaspersky Security, Сервера интеграции и Консоли управления Сервера интеграции (см. раздел «Удаление плагинов управления Kaspersky Security и Сервера интеграции» на стр. 170).

После удаления компонентов Сервер защиты и Легкий агент виртуальные машины, на которых были установлены эти компоненты, продолжают отображаться в Консоли администрирования Kaspersky Security Center. По истечении срока, заданного в параметрах Kaspersky Security Center (см. в документации Kaspersky Security Center), виртуальные машины автоматически удаляются из Консоли администрирования. Вы можете вручную удалить виртуальные машины из Консоли администрирования Kaspersky Security Center после завершения процедуры удаления программы.

Удаление компонента Сервер защиты

Для удаления компонента Сервер защиты требуется удалить SVM на гипервизорах.

Вы можете удалить SVM на всех или некоторых гипервизорах в виртуальной инфраструктуре. После удаления SVM на гипервизоре защищенные виртуальные машины, работающие на этом гипервизоре, подключаются к одной из SVM, работающих на другом гипервизоре (см. раздел «О подключении Легкого агента к SVM» на стр. 33).

Удаление SVM выполняется через консоль управления виртуальной инфраструктурой (см. подробнее в документации к используемым гипервизорам).

Удаление компонента Легкий агент для Windows

Вы можете удалить Легкий агент для Windows с виртуальной машины одним из следующих способов:

- локально в интерактивном режиме с помощью мастера установки (см. раздел «Удаление Легкого агента для Windows с помощью мастера установки» на стр. 165);
- из командной строки (см. раздел «Удаление Легкого агента для Windows из командной строки» на стр. 166);
- удаленно через Kaspersky Security Center (см. в документации Kaspersky Security Center);
- удаленно через редактор управления групповыми политиками службы каталогов (Active Directory Group Policies) (см. раздел «Удаление Легкого агента для Windows через редактор управления групповыми политиками службы каталогов» на стр. 167).

При удалении компонента Легкий агент для Windows с виртуальной машины удаляются все файлы, созданные во время работы программы.

В этом разделе

Удаление Легкого агента для Windows с помощью мастера установки

► *Чтобы удалить компонент Легкий агент для Windows с помощью мастера установки, выполните следующие действия:*

1. На виртуальной машине с установленным компонентом Легкий агент для Windows откройте список программ, используя стандартные средства удаления или изменения программ в операционной системе.
2. В списке программ выберите **Kaspersky Security для виртуальных сред 4.0 Легкий агент** и запустите мастер установки.
3. В окне мастера установки **Изменение, восстановление или удаление программы** нажмите на кнопку **Удаление**.
4. Следуйте указаниям мастера установки.

В этом разделе

Шаг 1. Подтверждение удаления компонента Легкий агент для Windows

Поскольку удаление компонента Легкий агент для Windows ставит под угрозу защиту виртуальной машины, требуется подтвердить ваше намерение удалить Легкий агент для Windows. Для подтверждения удаления нажмите на кнопку **Удалить**.

До завершения удаления компонента Легкий агент для Windows вы в любой момент можете отменить это действие, нажав на кнопку **Отмена**.

Шаг 2. Удаление компонента Легкий агент для Windows

На этом шаге мастер установки удаляет компонент Легкий агент для Windows с виртуальной машины. Дождитесь завершения удаления.

В процессе удаления может понадобиться перезагрузка операционной системы виртуальной машины. Если вы откажетесь от немедленной перезагрузки, завершение процедуры удаления будет отложено до того момента, когда операционная система будет перезагружена или виртуальная машина будет выключена и включена.

Удаление Легкого агента для Windows из командной строки

► *Чтобы удалить Легкий агент для Windows из командной строки в интерактивном режиме,*

введите в командной строке одну из следующих команд:

- `msiexec.exe /x {64D327ED-41E2-43CD-856A-612F5461BDBA}` или `setup.exe /x`, если на виртуальной машине установлена 32-разрядная операционная система.
- `msiexec.exe /x {A351D4C4-6E19-4B55-A150-FDED192DC463}` или `setup.exe /x`, если на виртуальной машине установлена 64-разрядная операционная система.

  Запустится мастер установки программы. Следуйте его указаниям.

► *Чтобы удалить Легкий агент для Windows из командной строки в тихом режиме (без запуска мастера установки программы),*

введите в командной строке одну из следующих команд:

- `msiexec.exe /x {64D327ED-41E2-43CD-856A-612F5461BDBA} /qn` или `setup.exe /s /x`, если на виртуальной машине установлена 32-разрядная операционная система.
- `msiexec.exe /x {A351D4C4-6E19-4B55-A150-FDED192DC463} /qn` или `setup.exe /s /x`, если на виртуальной машине установлена 64-разрядная операционная система.

Удаление Легкого агента для Windows через редактор управления групповыми политиками службы каталогов

С помощью редактора управления групповыми политиками службы каталогов (Active Directory Group Policies) вы можете удалять компонент Легкий агент для Windows с виртуальных машин, связанных с выбранным объектом групповой политики, без использования Kaspersky Security Center. Подробную информацию о работе с редактором управления групповыми политиками службы каталогов см. в *Справочной системе к Microsoft Windows*.

► *Чтобы удалить Легкий агент для Windows через редактор управления групповыми политиками службы каталогов, выполните следующие действия:*

1. Откройте окно Microsoft Windows **Управление групповыми политиками**.
2. В дереве окна **Управление групповыми политиками** выберите объект групповой политики (Group Policy Object), с которым связаны виртуальные машины, предназначенные для удаления Легкого агента для Windows.
3. По правой клавише мыши вызовите контекстное меню объекта групповой политики и выберите пункт **Изменить**.

   Откроется редактор управления групповыми политиками службы каталогов.
4. В дереве консоли выберите **Объект групповой политики \ Конфигурация компьютера \ Политики \ Конфигурация программ \ Установка программного обеспечения**.
5. В списке установочных пакетов выберите установочный пакет Kaspersky Security для виртуальных сред 4.0 Легкий агент.
6. По правой клавише мыши откройте контекстное меню установочного пакета и выберите пункт **Все задачи** → **Удалить**.

   Откроется окно **Удаление программ**.
7. В окне **Удаление программ** выберите параметр **Немедленное удаление этой программы с компьютеров всех пользователей**.

Групповая политика будет применена на каждой защищенной виртуальной машине, связанной с объектом групповой политики, при следующем запуске виртуальных машин.

В результате компонент Легкий агент для Windows будет удален на всех защищенных виртуальных машинах, связанных с выбранным объектом групповой политики.

После удаления может потребоваться перезагрузка виртуальных машин.

Удаление Легкого агента для Windows с шаблона виртуальных машин

► *Чтобы удалить компонент Легкий агент для Windows с шаблона виртуальных машин, выполните следующие действия:*

1. Включите на гипервизоре виртуальную машину, являющуюся шаблоном виртуальных машин.
2. Удалите компонент Легкий агент для Windows в интерактивном режиме с помощью мастера установки (см. раздел «Удаление Легкого агента для Windows с помощью мастера установки» на стр. 165).
3. Создайте заново виртуальные машины из обновленного шаблона. Подробнее см. в документации к виртуальной инфраструктуре.

Удаление компонента Легкий агент для Linux

Вы можете удалить Легкий агент для Linux с виртуальной машины одним из следующих способов:

- локально из командной строки;
- удаленно через Kaspersky Security Center (см. в документации Kaspersky Security Center).

► *Чтобы удалить Легкий агент для Linux из командной строки, выполните одну из следующих команд (в зависимости от менеджера пакетов, используемого в операционной системе):*

- `# rpm -e lightagent`, если Легкий агент был установлен из пакета формата RPM;
- `# dpkg -P lightagent`, если Легкий агент был установлен из пакета формата DEB.

Процедура удаления выполняется автоматически. Все задачи, которые выполнялись на виртуальной машине в момент удаления Легкого агента для Linux, будут остановлены.

При удалении Легкого агента для Linux программа предлагает запустить скрипт, который удаляет с защищенной виртуальной машины файлы, созданные во время работы программы в следующих папках:

- /etc/opt/kaspersky/lightagent/;
- /opt/kaspersky/lightagent/;
- /var/opt/kaspersky/lightagent/;
- /var/log/kaspersky/lightagent/.

► *Чтобы удалить файлы, созданные во время работы программы, с помощью скрипта, выполните следующие действия:*

1. Запустите скрипт, выполнив следующую команду:

   ```
   # /tmp/cleanup.pl
   ```

2. Подтвердите удаление файлов, введя `yes`. Если вы хотите отказаться от удаления файлов и остановить работу скрипта, введите `no`.

Вы также можете удалить файлы, созданные во время работы программы, вручную.

► *Чтобы вручную удалить файлы, созданные во время работы программы,* выполните следующую команду:

```
rm -rf <путь к папке>
```

После удаления Легкого агента для Linux рекомендуется выполнить перезагрузку виртуальной машины.

Удаление Агента администрирования Kaspersky Security Center с виртуальных машин

Вы можете удалить Агент администрирования Kaspersky Security Center с виртуальных машин и шаблонов виртуальных машин одним из следующих способов:

- С виртуальных машин с операционной системой Windows:
  - Локально в интерактивном режиме средствами операционной системы Windows. Этот способ рекомендуется для удаления Агента администрирования с шаблонов виртуальных машин.
  - Удаленно через Kaspersky Security Center с помощью задачи удаленной деинсталляции программы (см. в документации Kaspersky Security Center).
- С виртуальных машин с операционной системой Linux – средствами операционной системы Linux.

Удаление плагинов управления Kaspersky Security и Сервера интеграции

Вы можете удалить плагины управления Kaspersky Security, Сервер интеграции и Консоль управления Сервера интеграции одним из следующих способов:

- В интерактивном режиме с использованием стандартных средств удаления программ в операционной системе. В списке программ требуется выбрать для удаления **Kaspersky Security для виртуальных сред 4.0 Легкий агент – компоненты управления**. Удаление выполняется с помощью мастера.
- В тихом режиме из командной строки. В командной строке требуется ввести `SecurityCenterComponents_4.0.X.X_setup.exe -q -uninstall`, где `4.0.X.X` – номер версии программы.

При удалении Сервера интеграции с помощью мастера вы можете сохранить следующие данные, используемые в работе Сервера интеграции:

- SSL-сертификат, который используется для установки защищенного соединения с Сервером интеграции;
- параметры Сервера интеграции, в том числе пароли учетных записей Сервера интеграции;
- данные, сохраненные Сервером интеграции во время работы (см. раздел «О Сервере интеграции» на стр. 36);
- журналы Сервера интеграции.

Если вы хотите сохранить указанные данные, в окне запроса о сохранении данных нажмите на кнопку **Сохранить данные Сервера интеграции**. Сохраненные данные и параметры автоматически используются при повторной установке Сервера интеграции.

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. 13), 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).

Приложение. Описание журнала работы мастера

Во время развертывания SVM и во время изменения конфигурации SVM мастер сохраняет в журнал работы мастера всю информацию, указанную вами на каждом шаге мастера.

Во время развертывания SVM в журнале работы мастера сохраняется следующая информация:

- выбранное действие (развертывание SVM);
- тип гипервизора или сервера управления виртуальной инфраструктурой;
- адрес гипервизора или адрес сервера управления виртуальной инфраструктурой;
- версия гипервизора или версия сервера управления виртуальной инфраструктурой;
- имя гипервизора, версия установленной на гипервизоре операционной системы, количество виртуальных машин на гипервизоре;
- имя учетной записи, которая используется для подключения мастера установки к гипервизору или к серверу управления виртуальной инфраструктурой;
- имя учетной записи, которая используется для подключения SVM к гипервизору или к серверу управления виртуальной инфраструктурой;
- версия образа SVM;
- версии ранее развернутых SVM;
- статус издателя образа SVM;
- путь к файлу образа SVM и информация об образе SVM (производитель, описание, размер виртуального диска);
- статус проверки образа SVM;

- список всех гипервизоров Vmware ESXi под управлением одного сервера VMware vCenter, их состояние, статусы защиты и права учетной записи, которая используется для подключения к серверу Vmware vCenter (только при установке на гипервизор VMware ESXi);
- список и версии гипервизоров Vmware ESXi, выбранных для развертывания SVM (только при установке на гипервизор VMware ESXi);
- разрешено ли параллельное развертывание SVM на нескольких гипервизорах и количество параллельных сессий (только при установке на гипервизор VMware ESXi);
- параметры SVM на каждом из выбранных гипервизоров (имя, хранилище, имя сети);
- идентификатор VLAN (только при установке на гипервизор Microsoft Windows Server (Hyper-V));
- способ выделения места на диске (только при установке на гипервизор VMware ESXi);
- параметры подключения SVM к Серверу администрирования Kaspersky Security Center (IP-адрес, порт, SSL-порт);
- разрешен ли доступ для учетной записи root к SVM через SSH;
- тип аутентификации SVM на гипервизоре Microsoft Windows Server (Hyper-V): локальная, доменная;
- сетевые параметры SVM: IP-адрес, IP-адрес основного сетевого шлюза, IP-адреса основного и альтернативного DNS-серверов, маска подсети.

Во время изменения конфигурации SVM в журнале работы мастера сохраняется следующая информация:

- выбранное действие (изменение конфигурации SVM);
- IP-адреса или полные доменные имена гипервизоров, на которых выполняется изменение конфигурации SVM;
- IP-адреса или полные доменные имена SVM, на которых выполняется изменение конфигурации SVM;
- сведения о том, будут ли в результате изменения конфигурации изменены:

- параметры учетных записей для подключения к SVM (пароль конфигурирования, пароль учетной записи root, возможность подключения к SVM с использованием учетной записи root через SSH);
- адрес гипервизора или сервера управления виртуальной инфраструктурой, к которому подключается SVM;
- параметры учетной записи, которая используется для подключения SVM к гипервизору или к серверу управления виртуальной инфраструктурой;
- список виртуальных сетей, которые использует SVM;
- сетевые параметры SVM (IP-адрес, IP-адрес основного сетевого шлюза, IP-адреса основного и альтернативного DNS-серверов, маска подсети).

Журнал работы мастера сохраняется на том компьютере, где был запущен мастер, в файле %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\KasperskyDeploymentWizard.log и не содержит информации об учетных записях.

> Информация в файле перезаписывается при каждом запуске мастера. Чтобы использовать информацию журнала работы мастера в дальнейшем, нужно сохранить файл в место постоянного хранения.

Сведения, записанные в журнал работы мастера, не отправляются автоматически в «Лабораторию Касперского». Вы можете использовать журнал работы мастера при обращении в Службу технической поддержки в случае, если развертывание или изменение конфигурации SVM завершилось с ошибкой.

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» о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ «Лаборатории Касперского» на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

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.

Р

Резервная копия файла

Копия файла с виртуальной машины, которая создается при лечении или удалении этого файла. Резервные копии файлов хранятся в резервном хранилище в специальном формате и не представляют опасности.

Резервное хранилище

Специализированное хранилище для резервных копий тех файлов, которые были удалены или изменены в процессе лечения.

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.

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.

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 – 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

S

А

З

И

К

О

П

С

У