KASPERSKY lab

ПАКЕТ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД ЛЁГКИЙ АГЕНТ

Краткое руководство по установке

www.kaspersky.ru

СОДЕРЖАНИЕ

О РУКОВОДСТВЕ

Данный документ представляет собой краткое описание и руководство по установке пакета программного обеспечения Kaspersky Security для виртуальных сред Лёгкий агент.

Целью данного руководства является предоставление доступного и краткого источника информации по указанной теме.

Доступность означает, что информация изложена таким образом, чтобы понимание написанного, требовало только минимальных знаний концепций и технологий, используемых в связи с работой Лёгкого агента.

Краткость означает предоставление только наиболее важной (либо достаточной) для понимания информации.

Однако, доступная и краткая форма предполагает невозможность предоставления исчерпывающей информации. Исчерпывающая информация по затронутым здесь вопросам содержится в следующих документах:
- Руководство администратора Kaspersky Security для виртуальных сред 3.0 Лёгкий агент (далее также Руководство администратора)
- Руководство администратора Kaspersky Security Center

Руководство адресовано широкому кругу специалистов, заинтересованных в получении информации по указанной теме. Вместе с тем, для полного понимания содержания документа, требуется обладать следующими знаниями:
- Общая компьютерная грамотность
- Минимальное знакомство с технологиями:
  - Гипервизоры / Виртуальные машины
  - Службы Active Directory

Используемые условные обозначения:

Элементы интерфейса продуктов, с которыми необходимо взаимодействовать, выполняя описанные действия.

Ссылка.

Обратите внимание.

КОМПОНЕНТЫ ПРОДУКТА И ИХ ВЗАИМОДЕЙСТВИЕ

Программная архитектура комплексного решения защиты Kaspersky Security для виртуальных сред Лёгкий агент разработана с учетом специфики работы виртуальных сред, и нацелена на обеспечение комплексной защиты виртуальных машин, с учетом необходимости экономичного и эффективного расходования ресурсов гипервизора.

Поддерживается работа со следующими семействами гипервизоров:
- Microsoft Windows Server (Hyper-V)
- VMware ESXi
- Citrix XenServer
- Kernel-based Virtual Machine (KVM)

Поддерживается работа как с автономными гипервизорами, так и с гипервизорами, объединёнными в кластер.

Полный список всех версий поддерживаемых гипервизоров смотрите в Руководстве администратора.

Все действия, связанные с установкой и управлением работой Kaspersky Security для виртуальных сред Лёгкий агент осуществляются с помощью консоли Kaspersky Security Center с установленными компонентами управления Kaspersky Security для виртуальных сред Лёгкий агент.

Kaspersky Security Center (далее также KSC) – это единая консоль (сервер администрирования) для управления решениями «Лаборатории Касперского» для защиты рабочих мест и управления всеми защитными продуктами.

Основными компонентами Kaspersky Security для виртуальных сред Лёгкий агент являются:
- **Лёгкий агент**

  Во избежание путаницы следует отметить, что один из основных компонентов, именуется так же, как и сам пакет программного обеспечения – **Лёгкий агент**. В данном руководстве под термином Лёгкий агент понимается компонент устанавливаемый на виртуальные машины. В тех случаях, когда речь идет о пакете в целом, используется его полное наименование – K**aspersky Security для виртуальных сред Лёгкий агент**.

- **Сервер защиты (SVM)**

  Сервер защиты входит в состав Виртуальной машины защиты (англ. Secure Virtual Machine, далее также SVM), работающей под управлением ОС GNU/Linux. Для работы с продуктом, значения терминов Сервер защиты и SVM можно считать полностью идентичными. В данном руководстве в основном используется термин SVM.

- **Сервер интеграции**

  Сервер интеграции поставляется в составе инсталляционного пакета компонентов управления Kaspersky Security для виртуальных сред Лёгкий агент.

Экземпляр Лёгкого агента должен быть установлен на каждой виртуальной машине, которую необходимо защитить.

В данном руководстве виртуальные машины с установленным компонентом Лёгкий агент, также могут именоваться, как **защищаемые виртуальные машины**.

Полный список поддерживаемых гостевых операционных систем и требования к виртуальной аппаратной платформе защищаемых виртуальных машин смотрите в Руководстве администратора.

Лёгкий агент так же может быть установлен на мастер-образы (шаблоны) виртуальных машин, используемые поддерживаемыми VDI решениями.

Полный список поддерживаемых VDI решений и подробное описание способов работы с ними смотрите в Руководстве администратора.

Каждый Лёгкий агент должен быть постоянно подключен к SVM.

SVM разворачивается на гипервизоре средствами Мастера установки SVM, входящего в состав компонентов управления Kaspersky Security для виртуальных сред Лёгкий агент, устанавливыемых на машине KSC.

Наиболее предпочтительным способом предоставления Лёгким агентам информации о доступных SVM является использование Сервера интеграции, устанавливаемого в составе компонентов управления Kaspersky Security для виртуальных сред Лёгкий агент на машину KSC. Этот компонент собирает данные о текущем состоянии подключенных SVM и передает эти данные подключенным Лёгким агентам.

Независимо от выбранного способа предоставления информации о SVM, каждый Лёгкий агент автоматически подключаются к оптимальной из доступных для него SVM. Предпочтение отдается наименее загруженным SVM, имеющим активную лицензию, и находящейся на том же гипервизоре, что и защищаемая виртуальная машина.

Подробное описание алгоритма выбора оптимальной виртуальной машины защиты смотрите в Руководстве администратора.

Процедура настройки способов предоставления информации о SVM описана в разделе Способы предоставления Лёгким агентам информации о доступных SVM данного руководства.

Следует отметить, что Лёгкий агент может устанавливать соединение SVM, независимо от того находится ли он на том же гипервизоре, что и защищаемая виртуальная машина, или на другом гипервизоре, доступном по сети. Однако, с целью улучшения производительности, рекомендуется разворачивать SVM на том же гипервизоре, где расположены защищаемые с её помощью виртуальные машины. При использовании системных ресурсов, выделенных по умолчанию, SVM может взаимодействовать с 50-70 Лёгкими агентами, установленными на защищаемых виртуальных машинах со средней офисной активностью пользователей.

В случае необходимости защиты большого количества виртуальных машины или в случае защиты высоконагруженных виртуальных машин, для SVM следует выделить соответствующее количество дополнительных ресурсов, или дополнительно развернуть необходимое количество SVM. Ограничений на количество одновременно работающих SVM внутри одного и того же гипервизора нет.

Описание виртуальной аппаратной платформы, предоставляемой SVM по умолчанию, а также формулы для расчета необходимых ресурсов смотрите в Руководстве администратора.

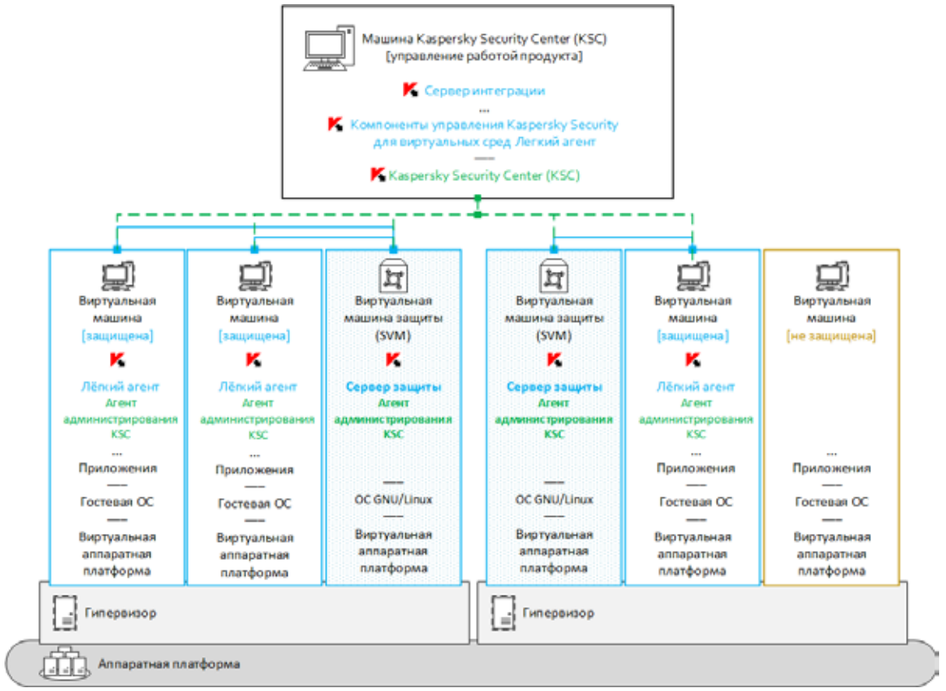
Все основные параметры совместной работы – в том числе правила, по которым SVM будут предоставлять доступ Лёгким агентам, и правила, по которым Лёгкие агенты будут осуществлять обнаружение доступных им SVM – определяются совместно групповыми политиками SVM и Лёгких агентов, создаваемыми в консоли KSC.

Лёгкие агенты и SVM взаимодействуют с KSC (в том числе, получают параметры политик и задач) по средствам Агента администрирования KSC.

Процедура Создания и распространения групповых политик описана в разделе Групповые политики данного руководства.

Часть работы по защите виртуальной машины Лёгкий агент осуществляет самостоятельно, однако файлы защищаемой виртуальной машины, проверка которых требует большого количества ресурсов передаются на SVM. SVM, проверяет полученные файлы и выдает вердикт. Обновления антивирусных баз и компонентов, Лёгкие агенты также получают от SVM, к которому они подключены. Такая распределенная архитектура отвечает требованию экономичного и эффективного использования ресурсов гипервизора. Перенося большую часть нагрузки на SVM, Kaspersky Security для виртуальных сред Лёгкий агент значительно снижает нагрузку на каждую отдельную защищаемую виртуальную машину, что в конечном итоге положительно сказывается на её быстродействии, без ущерба целям безопасности.

Полный список всех функций Лёгкого агента и SVM, а также подробное описание их взаимодействия смотрите в Руководстве администратора.



Общая схема работы Kaspersky Security для виртуальных сред Лёгкий агент

ОБЩИЙ ПОРЯДОК УСТАНОВКИ ПРОДУКТА

Для целей данного руководства далее приведен обобщенный пример установки, содержащий описание только ключевых этапов процесса, не зависящих от деталей конкретного окружения (тип гипервизора, гостевые ОС, сетевая архитектура и т.д.).

Основные действия по развертыванию Kaspersky Security для виртуальных сред Лёгкий агент в виртуальную среду выполняются в следующем порядке:
- установить компоненты управления на машину KSC;
- развернуть SVM на гипервизоре;
- активировать продукт добавив лицензионный ключ в хранилище KSC и распространив его на SVM;
- установить Лёгкие агенты на защищаемые виртуальные машины. Для этого необходимо выполнить следующие действия:
  - установить Агенты администрирования KSC на защищаемые виртуальные машины;
  - создать инсталляционный пакет для удаленной установки Лёгких агентов средствами консоли KSC;
  - используя созданный пакет, установить Лёгкие агент на защищаемые виртуальные машины.
- настроить работу продукта создав и применив групповые политики для Лёгких агентов и Серверов защиты (SVM);
- создать задачи обновления баз и модулей продукта, и настроить расписание её выполнения.

УСТАНОВКА КОМПОНЕНТОВ УПРАВЛЕНИЯ НА МАШИНУ KASPERSKY SECURITY CENTER

Для целей данного руководства предполагается, что машина с установленным KSC уже подготовлена.

Подробное описание функциональности и способов установки данного ПО смотрите в руководстве администратора KSC.

Компоненты управления Kaspersky Security для виртуальных сред Лёгкий агент (в том числе: Сервер интеграции, плагины управления Лёгкими агентами и Серверами защиты) поставляются в составе общего инсталляционного пакета. Установку необходимо произвести с помощью мастера установки, запущенного под учетной записью, обладающей правами администратора на машине KSC.

Если машина KSC, на которой производится установка, входит в состав домена Active Directory, то в момент установки, права на управление Сервером интеграции получат учетные записи из групп локальных и доменных администраторов, а также члены группы KLAdmins.

Если машина KSC, на которой производится установка, не входит в состав домена Active Directory, то мастер установки компонентов управления предложит создать пароль учетной записи администратора Сервера интеграции.

В момент первого, после установки компонентов управления, запуска консоли KSC, вам будет предложено создать групповую задачу загрузки обновлений антивирусных баз и модулей на SVM, и групповую задачу поиска вирусов для Лёгких агентов.

Процедура создания задачи загрузки обновлений антивирусных баз и компонентов на SVM описана в одноименном разделе данного руководства.

РАЗВЕРТЫВАНИЕ ВИРТУАЛЬНОЙ МАШИНЫ ЗАЩИТЫ (SVM)

Перед началом развертывания SVM убедитесь, что выполнены следующие условия:
- Вы имеете учетную запись на машине KSC, обладающую необходимыми правами доступа.
- Оборудование или программное обеспечение, используемое для контроля трафика (брандмауэр/межсетевой экран/файервол) не блокируют соединения, используемые для работы продукта.

Полный список соединений приведен в разделе Используемые порты данного руководства.

- Машина KSC имеет доступ к локальной сети, используемой для работы виртуальной инфраструктуры.
- Вы имеете учетную запись на гипервизоре с правами доступа необходимыми для установки SVM.

Полный список прав, которые необходимо предоставить для установки SVM учетным записям каждого из поддерживаемых типов гипервизора смотрите в Руководстве администратора.

- Файлы образа SVM и файл описания образов SVM доступны на машине KSC.

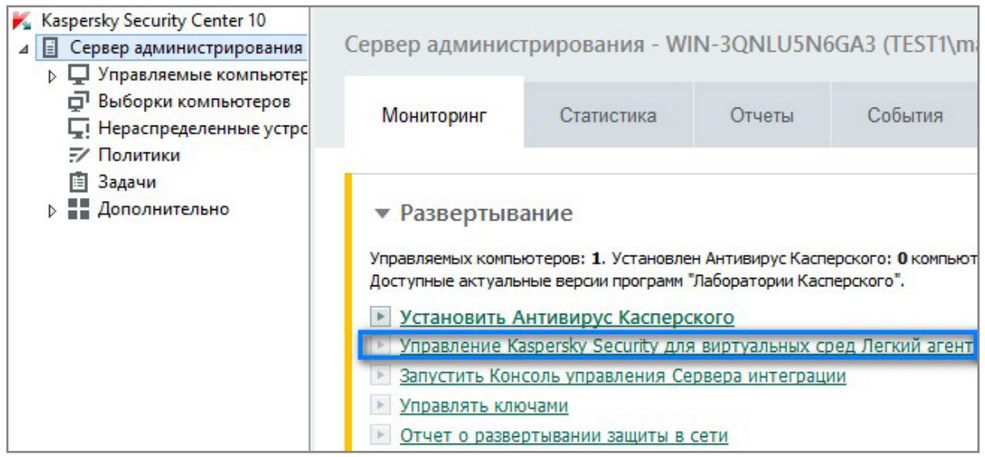
Для каждого поддерживаемого типа гипервизора поставляется соответствующий образ SVM. Файл описания образа SVM поставляется вместе с файлами образов SVM, и во время установки должен находиться в той же папке, что и сами образы. Имя этого файла имеет следующий формат: **SVM.image_manifest_*.xml**

Образы SVM для Microsoft Windows Server (Hyper-V) и Citrix XenServer поставляются в архивах. Перед началом установки их необходимо разархивировать.

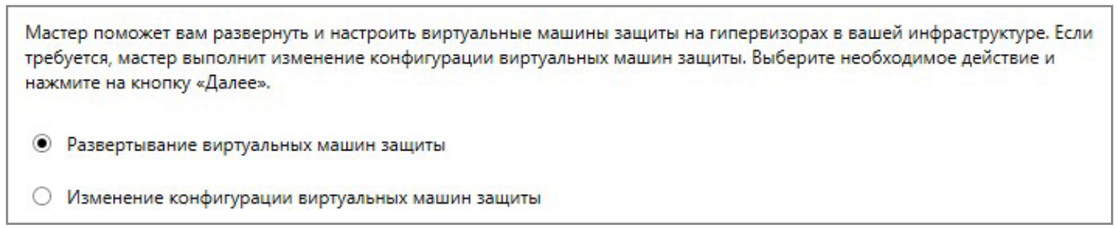
- В том случае, если вы собираетесь использовать статический IP-адрес для настройки сети на SVM, запросите соответствующие параметры у администратора сети.

Развертывание и конфигурирование SVM на гипервизоре производится с помощью Мастера установки SVM (далее также Мастер), входящего в состав плагина управления Серверами защиты.

Для запуска Мастера перейдите на узел **Сервер администрирования** и кликните по элементу **Управление Kaspersky Security для виртуальных сред Лёгкий агент**.



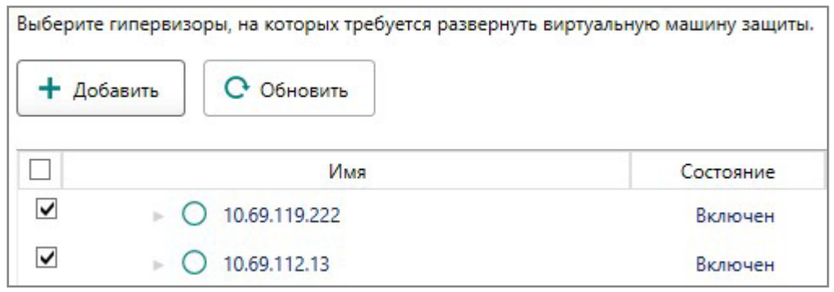
После запуска Мастера выберите опцию **Развертывание виртуальных машин защиты**.



На шаге Выбор гипервизоров необходимо установить соединение мастера с гипервизором (или несколькими гипервизорами). Для этого кликните кнопку **Добавить**, в открывшемся диалоге выберите тип используемого гипервизора, укажите его адрес (IP-адрес или FQDN), а также логин и пароль учетной записи гипервизора, от имени которой будет производиться установка SVM.

Для подключения к гипервизорам VMware ESXi необходимо использовать адрес управляющего ими сервера VMware vCenter Server.

После подключения к гипервизорам отметьте те из них, где будут развернуты SVM.



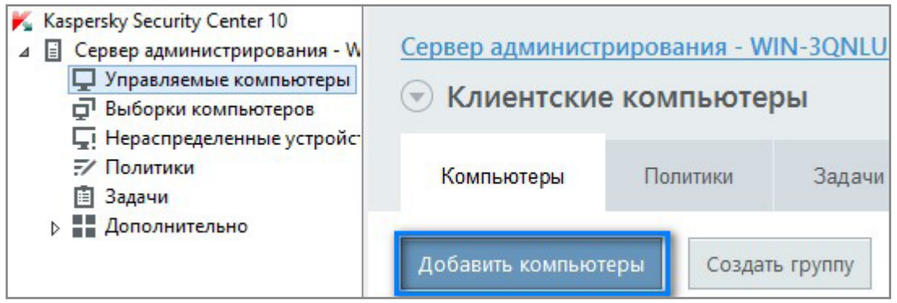
Мастер позволяет одновременно разворачивать несколько SVM на разных гипервизорах, независимо от их типа.

На шаге Выбор образа виртуальной машины защиты укажите путь к файлу описания образа SVM.

На шаге Параметры учетных записей на виртуальной машине защиты задайте пароли, которые могут быть использованы в дальнейшем для изменения конфигурации SVM с помощью Мастера, или настройки SVM через соединение по SSH с использованием учетной записи root ОС GNU/Linux.

Подробное описание остальных Мастера шагов смотрите в Руководстве администратора.

После завершения работы Мастера, развернутую SVM необходимо добавить в группу компьютеров, управляемых KSC. Для этого перейдите на вкладку **Компьютеры** узла **Управляемые компьютеры**, кликните по кнопке **Добавить компьютеры** и следуйте указаниям Мастера добавления клиентских компьютеров.



Для удобства работы с управляемыми компьютерами, в консоли KSC предусмотрена возможность создания отдельных групп внутри узла Управляемые компьютеры. Например, можно создать отдельные группы для защищаемых виртуальных машин и для SVM. Подробное описание данной функциональности смотрите в Руководстве администратора KSC.

Взаимодействие SVM и KSC обеспечивается средствами Агента администрирования KSC включенного в состав образа SVM.

На этом процесс развертывания SVM завершен.

Практически все параметры, задаваемые в момент развертывания SVM, можно впоследствии изменить воспользовавшись функцией **Изменение конфигурации виртуальных машин защиты** Мастера установки SVM. Подробности описание данной функциональности смотрите в Руководстве администратора.

УСТАНОВКА ЛЁГКОГО АГЕНТА. ДОСТУПНЫЕ СПОСОБЫ УСТАНОВКИ И ПРИМЕР УДАЛЕННОЙ УСТАНОВКИ СРЕДСТВАМИ KASPERSKY SECURITY CENTER

Инсталляционный пакет Лёгкого агента поставляется в самораспаковывающемся архиве. Перед началом установки его необходимо разархивировать.

Установка Лёгкого агента на виртуальные машины может быть выполнена несколькими способами:
- локально в интерактивном режиме с помощью мастера установки;
- в тихом режиме из командной строки;
- удаленно средствами KSC;
- удаленно через редактор управления групповыми политиками службы каталогов (Active Directory Group Policies).

Для целей данного руководства далее будет описан только способ установки Лёгкого агента удаленно средствами KSC.

Подробное описание остальных способов установки Лёгкого агента смотрите в Руководстве администратора.

Установка агента администрирования kaspersky security center. Добавление виртуальных машин в группу компьютеров, управляемых kaspersky security center

Виртуальные машины, на которых планируется удаленная установка Лёгких агентов, должны быть добавлены в группу компьютеров, управляемых KSC.

Взаимодействие виртуальных машин и KSC обеспечивается средствами Агента администрирования KSC. Агента администрирования поставляется в составе пакета KSC.

В отличии от SVM, образы которой поставляются с заранее интегрированным Агентом администрирования KSC, на других виртуальных машинах его необходимо установить самостоятельно.

Установить Агент администрирования KSC можно одним из следующих способов:

- удаленно средствами KSC, используя инсталляционный пакет для удаленной установки Агента администрирования, формируемого автоматически при установке KSC;

  Инсталляционный пакет для удаленной установки Агента администрирования средствами KSC располагается в узле Инсталляционные пакеты консоли KSC.

  Рекомендуется использовать данный способ в случае необходимости управления Лёгкими агентами, работающими на постоянных виртуальных машинах (не VDI).

- локально в интерактивном режиме с помощью мастера установки;

  Инсталляционный пакет (дистрибутив) Агента администрирования KSC располагается по такому пути: **%programfiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Share\Packages\NetAgent_xx.x.xxx**

  Рекомендуется использовать данный способ в случае необходимости управления Лёгкими агентами, работающими на виртуальных машинах, созданных из мастер-образов (шаблонов) поддерживаемых VDI решений. В этом случае Агент администрирования KSC (как и Лёгкий агент) должен быть установлен, средствами локального инсталляционного пакета, с использованием опции **Включить динамический режим для VDI** задаваемой на шаге Дополнительные параметры.

  Если в вашей VDI используются постоянные виртуальные машины опцию **Включить динамический режим для VDI** рекомендуется не использовать.

  Также, в случае локальной установки Агента администрирования KSC на шаге Сервер администрирования укажите адрес (IP-адрес или FQDN) машины KSC, и на шаге Дополнительные параметры установите флажок **Оптимизировать для виртуальной инфраструктуры настройки Агента администрирования KSC**...

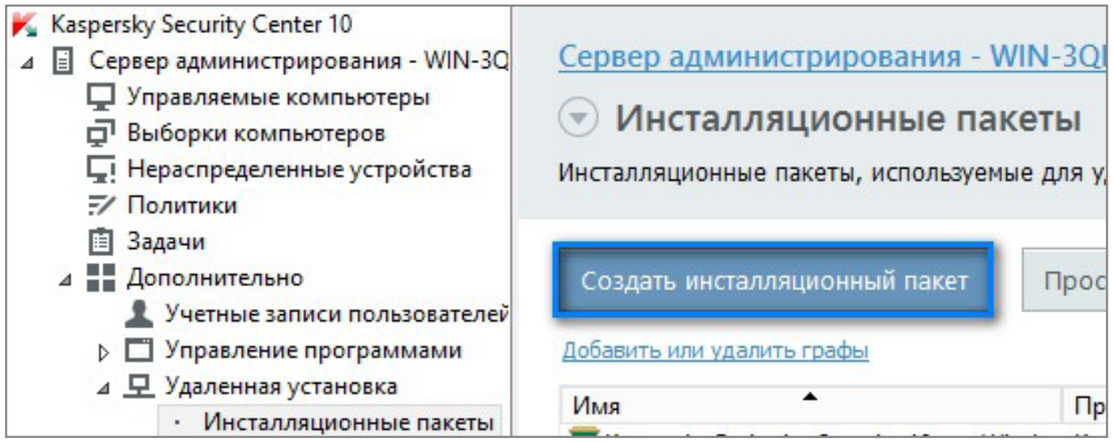
Подробное описание функциональности и способов установки Агента администрирования KSC смотрите в руководстве администратора KSC.

После завершения установки виртуальные машины с установленными Агентами администрирования KSC следует добавить в группу компьютеров, управляемых KSC.

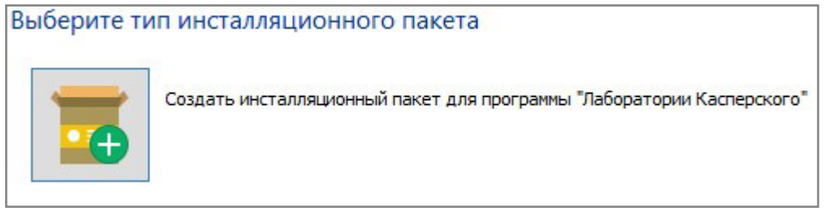
Как и в случае с SVM, для этого перейдите вкладку Компьютеры, узла **Управляемые компьютеры** или узла вложенной группы, в которую вы хотите добавить виртуальные машины, кликните по кнопке **Добавить компьютеры** и следуйте указаниям Мастера добавления клиентских компьютеров.

Создание инсталляционного пакета для удаленной установки

Для удаленной установки средствами KSC необходимо создать инсталляционный пакет Лёгкого агента. Для этого перейдите на узел **Инсталляционные пакеты**, и кликните кнопку **Создать инсталляционный пакет**.



В открывшемся Мастере создания инсталляционного пакета выберите опцию **Создать инсталляционный пакет для программы «Лаборатории Касперского»**.



На шаге Выбор дистрибутива программы для установки укажите путь к файлу **Ksvla3.kud** входящему в состав инсталляционного пакета Лёгкого агента. Остальные файлы, входящие в инсталляционный пакет Лёгкого агента должны находиться в той же папке.

По умолчанию в мастере создания инсталляционного пакета установлен флажок Скопировать обновления из хранилища в инсталляционный пакет. Это значит, что KSC включит в инсталляционный пакет все обновления антивирусных баз и модулей Лёгкого агента, загруженные в хранилище KSC к моменту создания пакета.

Подробное описание остальных шагов мастера смотрите в Руководстве администратора.

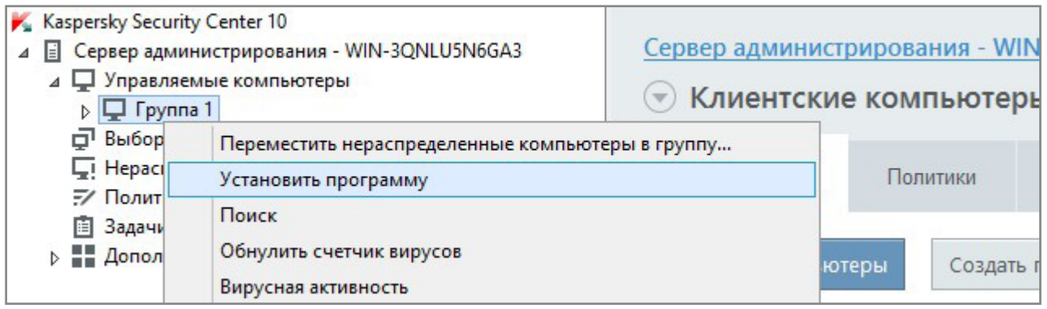
После завершения работы мастера будет создан инсталляционный пакет Лёгкого агента, который средствами KSC может быть установлен на удаленных виртуальных машинах.

Удаленная установка лёгкого агента средствами kaspersky security center

После того как виртуальные машины, которые необходимо защитить, добавлены в группу компьютеров, управляемых KSC и создан инсталляционный пакет для удаленной установки Лёгкого агента, можно приступать непосредственно к установке.

Для этого необходимо с помощью Мастера развертывания защиты создать и запустить задачу удаленной установки программы.

Для запуска Мастера развертывания защиты кликните правой кнопкой по выбранной управляемой виртуальной машине (или группе управляемых виртуальных машин) и выберите опцию **Установить программу**.



Если выбрана группа управляемых виртуальных машин, будет создана групповая задача развертывания Лёгкого агента, в результате работы которой, на каждую виртуальную машину входящую в выбранную группу и работающую под управлением одной из поддерживаемых ОС будет установлен Лёгкий агент.

На шаге Выбор инсталляционного пакета выберите созданный ранее инсталляционный пакет Лёгкого агента.

Подробное описание остальных шагов мастера смотрите в Руководстве администратора.

После завершения работы мастера будет создана задача, в результате выполнения которой Лёгкий агент будет установлен на выбранную виртуальную машину или группу виртуальных машин.

ЛИЦЕНЗИРОВАНИЕ И АКТИВАЦИЯ

Подробно о лицензировании программы смотрите в Руководстве администратора.

Для целей данного руководства далее будет описана процедура активации Kaspersky Security для виртуальных сред Лёгкий агент.

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

Для активации программы необходимо использовать Ключ, предоставляемый вместе с Лицензионным сертификатом (документом, содержащим информацию о приобретённой лицензии).

Ключ – это уникальная буквенно-цифровая последовательность. Ключ обеспечивает использование программы в соответствии с условиями, указанными в Лицензионном сертификате (типом лицензии, сроком действия лицензии, лицензионным ограничением).

Для Kaspersky Security для виртуальных сред Лёгкий агент используются ключи следующих типов:

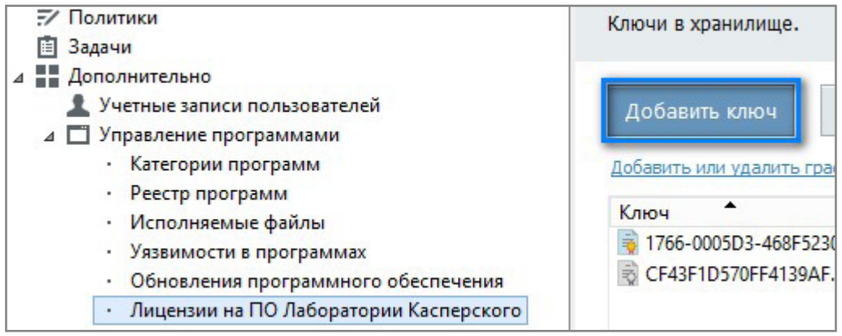
- Серверный ключ – ключ, предназначенный для использования программы для защиты виртуальных машин с серверной операционной системой
- Настольный ключ – ключ, предназначенный для использования программы для защиты виртуальных машин с настольной операционной системой
- Ключ с ограничением по ядрам – ключ,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

Допускается совместное использование Серверного ключа и Настольного ключа на одной и той же SVM. Подробно о смешенном применении ключей смотрите в Руководстве администратора.

Ключ может быть предоставлен либо в качестве файла ключа, либо в качестве кода активации.

Активация Лёгкого агента производится средствами KSC.

Сперва следует добавить ключ в хранилище ключей KSC. Для это перейдите на узел **Лицензии на ПО Лаборатории Касперского** и кликните кнопку **Добавить ключ**.



В открывшемся Мастере добавления ключа, выберите подходящий вам способ активации – с помощью кода активации, либо с помощью файла ключа – и следуйте указаниям мастера.

После завершения работы мастера ключ добавляется в хранилище ключей KSC, и теперь его необходимо распространить на SVM.

Для этого находясь в том же узле Лицензии на ПО Лаборатории Касперского, кликните кнопку **Распространить ключ на управляемые компьютеры**. В открывшемся Мастере создания задачи активации программы выберите программу **Kaspersky Security для виртуальных сред Лёгкий агент – Сервер защит**ы.

На шаге Добавление ключа выберите ключ, добавленный в хранилище ключей KSC.

На следующем шаге выберите опцию **Выбрать компьютеры, обнаруженные в сети Сервером администрирования** и на шаге **Выбор клиентских компьютеров** отметьте SVM, добавленную в группу управляемых компьютеров.

Подробное описание остальных шагов мастера смотрите в Руководстве администратора.

После завершения работы мастера будет создана задача, выполнение которой распространит ключ на выбранную SVM.

Каждый Лёгкий агент активируется автоматически используя ключ активации, распространенный на SVM, к которому он в данный момент подключен.

Если на SVM ключ отсутствует, или не соответствует типу защищаемой виртуальной машины, а также в случае, если достигнуто лицензионное ограничение, Лёгкий агент не будет активирован.

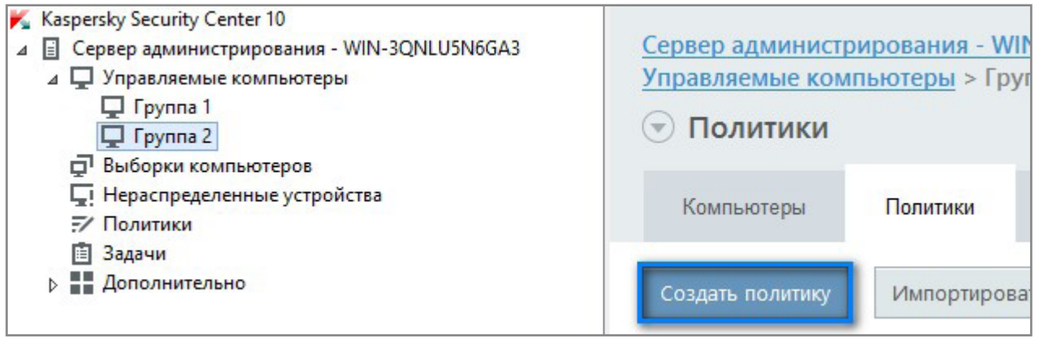
Не активированный Лёгкий агент функционирует в режиме ограниченной функциональности:
- работают только компоненты Лёгкого агента Файловый Антивирус и Сетевой экран;
- выполняются только задачи полной проверки, выборочной проверки и проверки важных областей;
- обновление антивирусных баз и модулей программы, необходимых для работы Лёгкого агента, выполняется только один раз.

УПРАВЛЕНИЕ РАБОТОЙ

Настраивать и управлять работой Kaspersky Security для виртуальных сред Лёгкий агент следует путем создания, редактирования и применения групповых политик, а также путем создания и выполнения групповых и индивидуальных задач.

ГРУППОВЫЕ ПОЛИТИКИ

Для создания групповой политики выберите необходимую группу управляемых компьютеров, перейдите на вкладку **Политики** и кликните кнопку **Создать политику**.



В открывшемся Мастере создания политики, на шаге Выбор программы для создания групповой политики выберите компонент, для которого будет создана политика:
- **Kaspersky Security для виртуальных сред Лёгкий агент** – для создания политики Лёгких агентов
- **Kaspersky Security для виртуальных сред Лёгкий агент - Сервер защиты** – для создания политики Сервера защиты

Подробное описание остальных шагов мастера смотрите в Руководстве администратора.

После завершения работы мастера в выбранной группе управляемых компьютеров будет создана политика, параметры которой будут применены ко всем машинам соответствующего типа (Лёгким агентам или Серверам защиты (SVM)) входящим в данную группу.

Следует отметить, что, хотя ограничения на создание однотипных политик нет, в одной группе управляемых компьютеров одновременно может быть активна только одна политика из относящихся к одному и тому же типу.

Подробно о работе с групповыми политиками, а также о работе с групповыми и индивидуальными задачами смотрите в Руководстве администратора.

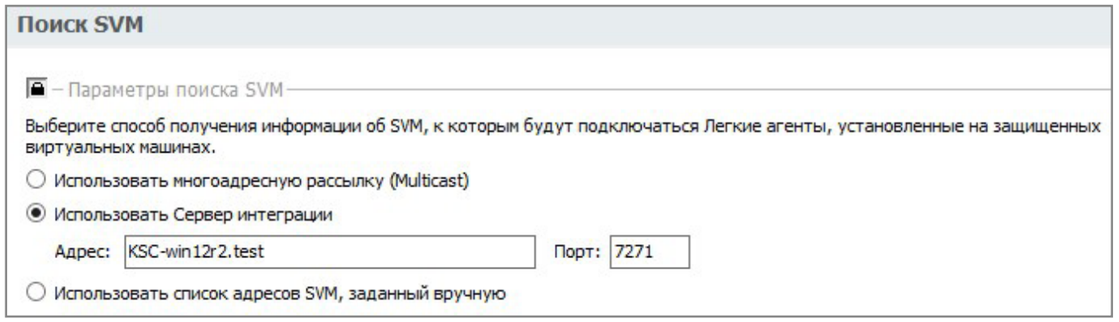
СПОСОБЫ ПРЕДОСТАВЛЕНИЯ ЛЁГКИМ АГЕНТАМ ИНФОРМАЦИИ О ДОСТУПНЫХ SVM

Предоставление Лёгкими агентами информации о доступных SVM задается групповыми политиками и может осуществляться одним из следующих способов:

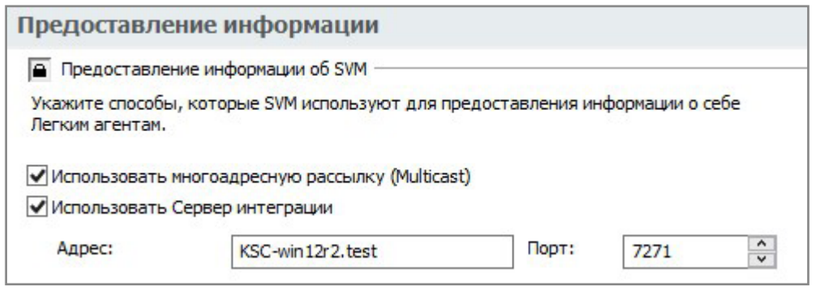
- **Многоадресная рассылка (Multicast).** Используя многоадресную рассылку (Multicast) SVM передают информацию о себе всем работающим в этом же режиме Лёгким агентам. Данный способ используется по умолчанию
- **Сервер интеграции.** SVM передают информацию о себе на Сервер интеграции. Легкие агенты получают эту информацию от Сервера интеграции. Рекомендуется использовать данный способ как наиболее гибкий и отказоустойчивый.
- **Список адресов SVM.** Лёгкому агенту предоставляется список SVM сформированный вручную.

Подробное описание способов предоставления Лёгким агентам информации о доступных SVM смотрите в Руководстве администратора.

Для того чтобы настроить работу по одному из предложенных способов, необходимо соответствующим образом задать параметры **Поиска SVM** в политике Лёгких агентов



и параметры **Предоставления информации** в политике SVM.



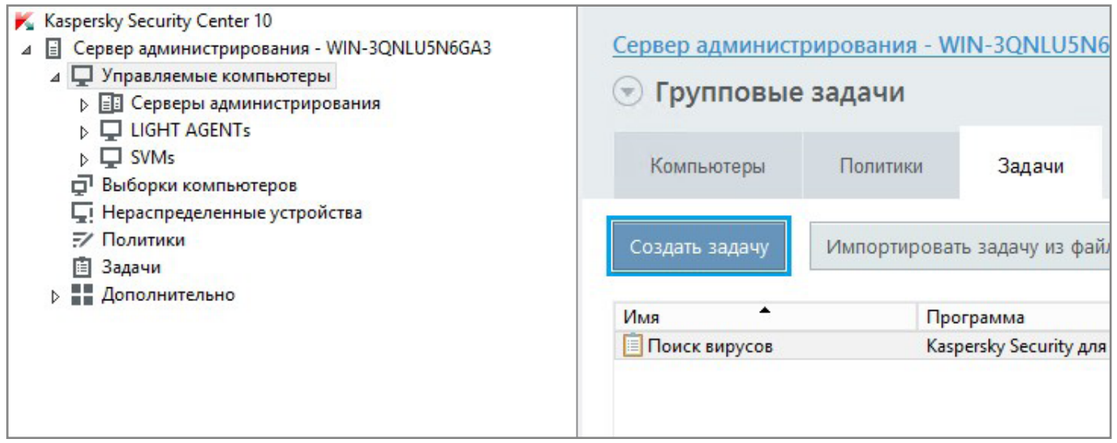
В один и тот же момент времени Лёгкие агенты могут работать только с одним из доступных способов получения информации об SVM. SVM, однако, может одновременно предоставлять сервис Лёгким агентам работающим с любым из описанных способов.

ЗАДАЧА ЗАГРУЗКИ ОБНОВЛЕНИЙ АНТИВИРУСНЫХ БАЗ И МОДУЛЕЙ НА SVM

Обеспечение доставки обновлений является важнейшим условием эффективной работы продукта.

Как было отмечено выше, в момент первого, после установки компонентов управления, запуска консоли KSC, автоматически инициируется процедура создания задачи загрузки обновлений антивирусных баз и модулей на SVM. Если задача ещё не была создана, следует самостоятельно инициировать ее создание.

Для этого, перейдите на вкладку **Задачи** узла **Управляемые компьютеры**, кликните кнопку **Создать задачу**.



В открывшемся Мастере создания задачи выберите задачу **Обновление баз** для продукта **Kaspersky Security для виртуальных сред Лёгкий агент – Сервер защиты** и следуйте указаниям мастера.

Для обеспечения своевременной доставки обновлений на шаге Настройка расписания запуска задачи рекомендуется использовать опцию Запуск по расписанию: При загрузке обновлений в хранилище.

Следует отметить, что данная задача должна быть создана в той же группе управляемых компьютеров где расположены (или будут расположены) развернутые SVM. Если машины SVM находятся в различных группах, то задача обновления баз должна присутствовать в каждой из этих групп.

Следует отметить, что по умолчанию вложенные группы наследуют задачи из родительских групп. Таким образом, если создать задачу непосредственно в узле Управляемые компьютеры, то она будет унаследована всеми вложенными группами.

ИСПОЛЬЗУЕМЫЕ ПОРТЫ

Для установки и работы Kaspersky Security для виртуальных сред Лёгкий агент в настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика необходимо разрешить следующие соединения.

Source	Destination	Port	Protocol	Purpose
Light Agent	SVM	9876	TCP	To send file scanning requests from a Light Agent to the SVM.
Light Agent	SVM	1111	TCP	To transfer service requests (e.g., requests for license information) from a Light Agent to the SVM.
SVM	Light Agent	9876	UDP	To enable Light Agents to receive information abou all SVMs available on the network and their load levels.
Light Agent	SVM	8000	UDP	
SVM	KSC	7271	TCP	To provide interaction between an SVM and the Integration Server installed on the KSC machine.
Light Agent	KSC	7271	TCP	To provide interaction between Light Agents and the Integration Server installed on the KSC machine.
KSC Administration Agent	KSC	13000 14000	TCP	To manage Kaspersky Security for Virtualization Light Agent via the KSC machine.
SVM	KSC	13000 14000	TCP	
KSC	KSC Administration Agent	15000	TCP	
KSC	SVM	15000	TCP	
KSC	SVM	22	TCP	To enable the root account to access an SVM via SSH.
KSC	Microsoft Windows Server (Hyper-V)	135 445 1024 5000	TCP UDP	To deploy an SVM on a Microsoft Windows Server (Hyper-V) hypervisor.
SVM	Microsoft Windows Server (Hyper-V)	5985 5986	TCP Application level protocols HTTP and HTTPS are used.	To enable interaction between an SVM and the Microsoft Windows Server (Hyper-V) hypervisor.
KSC	Citrix XenServer	20 80 443	TCP Application level protocols HTTP and HTTPS (80, 443) are used.	To deploy an SVM on a Citrix XenServer hypervisor and to enable interaction between the SVM and the hypervisor.
SVM	Citrix XenServer			
KSC	VMware ESXi	80 443	TCP Application level protocols HTTP and HTTPS are used.	To deploy an SVM on a VMware ESXi hypervisor via a VMware vCenter server and to enable interaction between the SVM and the hypervisor.
SVM	VMware ESXi			
KSC	Kernel-based Virtual Machine (KVM)	22	TCP	To deploy an SVM on a Kernel-Based Virtual Machine (KVM) hypervisor and to enable interaction between the SVM and the KVM hypervisor.
SVM	Kernel-based Virtual Machine (KVM)			
Light Agent	SVM	445	TCP	To enable Light Agents to receive antivirus database and application module updates from the SVM.

Если Лёгкие агенты для взаимодействия с SVM используют многоадресную рассылку (Multicast), то необходимо 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 правило исключения для процесса avp.exe в доменной политике. Если используется другой межсетевой экран, требуется настроить правило исключения для процесса avp.exe для этого межсетевого экрана.

При установке Сервера интеграции в составе компонентов управления, мастер установки добавляет в межсетевой экран Microsoft Windows правила, разрешают входящий трафик на порты TCP:7271, TCP:7270.

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 виртуальная машина защиты и защищенные виртуальные машины. Поскольку трафик между виртуальной машиной защиты и защищенными виртуальными машинами не зашифрован и передается в открытом виде, в целях безопасности не рекомендуется использовать беспорядочный режим в сетевых сегментах с работающей виртуальной машиной защиты. Если такой режим необходим, например, для мониторинга трафика сторонними виртуальными машинами с целью выявления попыток несанкционированного доступа к сети и устранения сетевых неполадок, требуется настроить соответствующие ограничения, чтобы защитить трафик, пересылаемый между виртуальной машиной защиты и защищенными виртуальными машинами, от несанкционированного доступа.

КОНТРОЛЬНЫЙ СПИСОК ДЕЙСТВИЙ ПО УСТАНОВКЕ ПАКЕТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД ЛЁГКИЙ АГЕНТ

1. 1Подготовьте машину с установленным пакетом программного обеспечения KSC.
2. Установите компоненты управления Kaspersky Security для виртуальных сред Лёгкий агент на машину KSC.
3. Убедитесь, что гипервизор, на котором планируется развернуть Kaspersky Security для виртуальных сред Лёгкий агент доступен по сети для машины KSC.
4. Разместите файл образа SVM необходимого типа гипервизора и файл SVM.image_manifest_*.xml в одной папке, по пути доступному для учетной записи администратора KSC.
5. Подготовьте учетную запись гипервизора, обладающую правами необходимыми для установки SVM.
6. В консоли KSC запустите Мастер установки SVM и выберите опцию Развертывание виртуальной машины защиты.
7. Используя подготовленную учетную запись подключите Мастер установки SVM к гипервизару на котором планируется развернуть SVM.
8. Следуя подсказкам Мастера установки SVM укажите путь к файлу SVM.image_manifest_*.xml, и, задав необходимые параметры в остальных шагах мастера, запустите процесс развертывания SVM.
9. После завершения развертывания SVM, в консоли KSC добавьте новую SVM в группу управляемых компьютеров.
10. В консоли KSC добавьте лицензионный ключ Kaspersky Security для виртуальных сред Лёгкий агент в хранилище KSC.
11. Используя задачу Активация программы для продукта Kaspersky Security для виртуальных сред Лёгкий агент – Сервер защиты, распространите лицензионный ключ на развернутую SVM.
12. На виртуальных машинах, которые планируется защищать, установите Агента администрирования KSC.
13. В консоли KSC добавьте эти виртуальные машины в группу управляемых компьютеров.
14. Разместите все файлы инсталляционного пакета Лёгкого агента в одной папке, по пути доступному для учетной записи администратора KSC.
15. В консоли KSC, используя инсталляционный пакет Лёгкого агента, создайте инсталляционный пакет для удаленной установки.
16. С помощью Мастера развертывания защиты создайте и запустить задачу удаленной установки Лёгких агентов для подготовленной группы управляемых компьютеров.
17. Для настройки параметров работы Kaspersky Security для виртуальных сред Лёгкий агент, создайте и распространите групповые политики для компонентов Лёгкий агент и Сервер защиты (SVM).
18. Для обеспечения доставки обновлений баз и модулей на SVM и работающие с ними Лёгкие агенты, создайте задачу Обновление баз для продукта Kaspersky Security для виртуальных сред Лёгкий агент – Сервер защиты.

KASPERSKY lab

www.kaspersky.ru