Kaspersky Security Center 10

Начало работы

ВЕРСИЯ ПРОГРАММЫ: 10 MAINTENANCE RELEASE 1

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 06.09.2013

http://www.kaspersky.ru
http://support.kaspersky.ru

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

В этом документе описаны действия, с помощью которых вы можете быстро начать работу с программой Kaspersky Security Center 10 (далее также – Kaspersky Security Center) и развернуть в сети систему защиты, построенную на основе программ «Лаборатории Касперского».

Документ адресован администраторам компьютерных сетей организаций, а также организациям, предоставляющим SaaS-услуги (далее – сервис-провайдерам).

Здесь подробно описан простой сценарий установки Kaspersky Security Center, когда система защиты разворачивается без использования иерархии Серверов администрирования в сети одной организации на нескольких компьютерах с установленной операционной системой Microsoft® Windows®.

В случаях, когда шаги настройки работы программы для сервис-провайдера отличаются от шагов настройки работы программы для администратора сети организации, действия сервис-провайдера описаны отдельно.

В документе описана также процедура перехода с версии 9.0 на версию 10.

Подробная информация о программе Kaspersky Security Center содержится в *Руководстве по внедрению* и *Руководстве администратора Kaspersky Security Center*.

В ЭТОМ РАЗДЕЛЕ

В ЭТОМ ДОКУМЕНТЕ

Документ *Начало работы Kaspersky Security Center* содержит введение, разделы с описанием типичных задач, которые выполняет Kaspersky Security Center, и заключение.

Источники информации о программе (см. стр. 8)

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

Kaspersky Security Center (см. стр. 10)

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security Center.

Лицензирование программы (см. стр. 11)

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, способах активации программы, а также о продлении срока действия лицензии.

Интерфейс программы (см. стр. 17)

В этом разделе описаны основные параметры интерфейса Kaspersky Security Center.

Условные обозначения

Текст документа сопровождается смысловыми элементами, на которые мы рекомендуем вам обращать особое внимание, – предупреждениями, советами, примерами.

Для выделения смысловых элементов используются условные обозначения. Условные обозначения и примеры их использования приведены в таблице ниже.

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. В предупреждениях содержится информация о возможных нежелательных действиях, которые могут привести к потере информации, сбоям в работе оборудования или операционной системы.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания могут содержать полезные советы, рекомендации, особые значения параметров или важные частные случаи в работе программы.
Пример: ...	Примеры приведены в блоках на желтом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие смысловые элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши нужно 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 пользователю.
<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 и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

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

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска

Вы можете использовать следующие источники для самостоятельного поиска информации о программе:

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

Если вы не нашли решения возникшей проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Техническая поддержка по телефону» на стр. 39).

Для использования источников информации на веб-сайте «Лаборатории Касперского» необходимо подключение к интернету.

Страница на веб-сайте «Лаборатории Касперского»

Веб-сайт «Лаборатории Касперского» содержит отдельную страницу для каждой программы.

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

Страница http://www.kaspersky.ru содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница на веб-сайте Службы технической поддержки (База знаний)

База знаний – раздел веб-сайта Службы технической поддержки, содержащий рекомендации по работе с программами «Лаборатории Касперского». База знаний состоит из справочных статей, сгруппированных по темам.

На странице программы в Базе знаний (http://support.kaspersky.ru/ksc10) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

Электронная справка

В состав электронной справки программы входят файлы справки.

Контекстная справка содержит сведения о каждом окне программы: перечень и описание параметров и ссылки на задачи, в которых эти параметры используются.

Полная справка содержит информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя.

Документация

В комплект поставки программы включены документы, с помощью которых вы можете установить и активировать программу на компьютерах корпоративной сети и настроить параметры ее работы, а также получить сведения об основных приемах работы с программой.

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.

Обращение в Отдел локализации и разработки технической документации

Если у вас возникли вопросы, связанные с документацией к программе, вы можете обратиться к специалистам Группы разработки документации. Например, вы можете присылать нашим специалистам отзывы о документации.

KASPERSKY SECURITY CENTER

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security Center.

Программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ «Лаборатории Касперского».

Программа Kaspersky Security Center адресована администраторам компьютерных сетей организаций и сотрудникам, отвечающим за защиту компьютеров в организациях.

SPE-версия программы адресована организациям, предоставляющим SaaS-услуги (далее – *сервис-провайдерам*).

При помощи Kaspersky Security Center вы можете:

- Формировать иерархию Серверов администрирования для управления сетью собственной организации, а также сетями удаленных офисов или организаций-клиентов.

  Под *организациями-клиентами* здесь подразумеваются организации, антивирусную защиту которых обеспечивает сервис-провайдер.

- Формировать иерархию групп администрирования для управления набором клиентских компьютеров как единым целым.

- Управлять системой антивирусной безопасности, построенной на основе программ «Лаборатории Касперского».

- Централизованно создавать образы операционных систем и разворачивать их на клиентских компьютерах по сети, а также выполнять удаленную установку программ «Лаборатории Касперского» и других производителей программного обеспечения.

- Удаленно управлять программами «Лаборатории Касперского» и других производителей, установленными на клиентских устройствах: устанавливать обновления, искать и закрывать уязвимости.

- Централизованно распространять ключи программ «Лаборатории Касперского» на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

- Получать статистику и отчеты о работе программ и устройств.

- Получать уведомления о критических событиях в работе программ «Лаборатории Касперского».

- Контролировать доступ устройств в сеть организации с помощью правил ограничения доступа и «белого» списка устройств. Для управления доступом устройств в сеть организации используются NAC-агенты.

- Управлять мобильными устройствами, поддерживающими протоколы Exchange ActiveSync® или iOS Mobile Device Management (iOS MDM).

- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных носителях, и доступом пользователей к зашифрованным данным.

- Проводить инвентаризацию оборудования, подключенного к сети организации.

- Централизованно работать с файлами, помещенными антивирусными программами на карантин или в резервное хранилище, а также с файлами, обработка которых антивирусными программами отложена.

ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, способах активации программы, а также о продлении срока действия лицензии.

В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении

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

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

Считается, что вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при установке программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы или не использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения. С лицензией связан уникальный код активации вашего экземпляра Kaspersky Security Center.

Лицензия включает в себя право на получение следующих видов услуг:

- Использование программы на одном или нескольких устройствах.

  Количество устройств, на которых вы можете использовать программу, определяется условиями Лицензионного соглашения.

- Обращение в Службу технической поддержки «Лаборатории Касперского».

- Получение прочих услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами в течение срока действия лицензии.

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

Предусмотрены следующие типы лицензий:

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

  Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security Center продолжает работу в режиме ограниченной функциональности.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы. Предусмотрено несколько вариантов лицензирования Kaspersky Security Center.

  По истечении срока действия коммерческой лицензии программа продолжает работу в режиме ограниченной функциональности (см. раздел «Об ограничениях базовой функциональности» на стр. 14). Для продолжения использования Kaspersky Security Center в режиме полной функциональности требуется продлить срок действия коммерческой лицензии.

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

ВАРИАНТЫ ЛИЦЕНЗИРОВАНИЯ KASPERSKY SECURITY CENTER

В Kaspersky Security Center лицензия может распространяться на разные группы функциональности.

Базовая функциональность Консоли администрирования

Доступны следующие функции:

- создание виртуальных Серверов администрирования для управления сетью удаленных офисов или организаций-клиентов;
- формирование иерархии групп администрирования для управления набором устройств как единым целым;
- контроль состояния антивирусной безопасности организации;
- удаленная установка программ;
- просмотр списка образов операционных систем, доступных для удаленной установки;
- централизованная настройка параметров программ, установленных на клиентских компьютерах;
- просмотр и изменение существующих групп лицензионных программ;
- получение статистики и отчетов о работе программ, а также уведомлений о критических событиях;
- управление процессом шифрования и защиты данных;
- просмотр и редактирование вручную списка оборудования, обнаруженного в результате опроса сети;
- централизованная работа с файлами, помещенными на карантин или в резервное хранилище, а также с файлами, обработка которых отложена.

Программа Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе продуктов «Лаборатории Касперского», предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта «Лаборатории Касперского» (http://www.kaspersky.ru).

Единицей управления для базовой функциональности является виртуальный Сервер администрирования, доступно создание до 10 виртуальных Серверов администрирования.

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования (см. раздел «Об ограничениях базовой функциональности» на стр. 14).

Функциональность Kaspersky Security Center, Service Provider Edition (далее – SPE)

Функциональность SPE-версии программы дублирует базовую функциональность Консоли администрирования, но допускается создание более 10 виртуальных Серверов администрирования.

SPE-версия программы поставляется на особых условиях партнерам «Лаборатории Касперского». Более подробную информацию о программе партнерства вы можете найти на веб-сайте «Лаборатории Касперского», на странице http://www.kaspersky.ru/partners.

Функциональность Системное администрирование

Доступны следующие функции:

- удаленная установка операционных систем;
- удаленная установка обновлений программного обеспечения, поиск и закрытие уязвимостей;
- управление доступом устройств в сеть организации (NAC);
- инвентаризация оборудования;
- управление группами лицензионных программ;
- удаленное подключение к клиентским компьютерам.

Единицей управления для функциональности Системного администрирования является клиентский компьютер в группе «Управляемые компьютеры».

Функциональность Управление мобильными устройствами

Функциональность Управления мобильными устройствами предназначена для управления мобильными устройствами Exchange ActiveSync и iOS MDM.

Для мобильных устройств Exchange ActiveSync доступны следующие функции:

- создание и редактирование профилей управления мобильными устройствами, назначение профилей почтовым ящикам пользователей;
- настройка параметров работы мобильного устройства (синхронизация почты, использование приложений, пароль пользователя, шифрование данных, подключение съемных носителей);
- установка сертификатов на мобильные устройства.

Для мобильных устройств iOS MDM доступны следующие функции:

- создание и редактирование конфигурационных профилей, установка конфигурационных профилей на мобильные устройства;
- установка приложений на мобильное устройство через App Store или с помощью манифест-файлов (.plist);
- возможность блокировать мобильное устройство, сбрасывать пароль мобильного устройства и удалять все данные с мобильного устройства.

Также в рамках функциональности Управление мобильными устройствами доступно выполнение команд, предусмотренных соответствующими протоколами.

Единицей управления функциональности Управления мобильными устройствами является мобильное устройство. Мобильное устройство считается управляемым, как только оно подключается к Серверу мобильных устройств.

ОБ ОГРАНИЧЕНИЯХ БАЗОВОЙ ФУНКЦИОНАЛЬНОСТИ

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования. Далее приведено описание ограничений, которые накладываются на работу программы в этом режиме.

Управление мобильными устройствами

Невозможно создать новый профиль и назначить его мобильному устройству (iOS MDM) или почтовому ящику (Exchange ActiveSync). Изменение существующих профилей и их назначение почтовым ящикам доступно всегда.

Управление программами

Невозможно запустить задачи установки и удаления обновлений. Все задачи, запущенные до истечения срока действия лицензии, выполняются до конца, но последние обновления не устанавливаются. Например, если до истечения срока действия лицензии была запущена задача установки критических обновлений, то будут установлены только критические обновления, найденные до истечения срока действия лицензии.

Запуск и редактирование задач синхронизации, поиска уязвимостей и обновления базы уязвимостей доступны всегда. Ограничения также не накладываются на просмотр, поиск и сортировку записей в списке уязвимостей и обновлений.

Удаленная установка операционных систем и программ

Невозможно запустить задачи снятия и установки образа операционной системы. Задачи, запущенные до истечения срока действия лицензии, выполняются до конца.

Управление доступом в сеть

NAC-агент и NAC переводятся в режим «Выключен» без возможности включения.

Инвентаризация оборудования

Недоступен сбор информации о новых устройствах с помощью NAC и Сервера мобильных устройств. При этом информация о компьютерах и подключаемых устройствах обновляется.

Не работают оповещения об изменении конфигурации устройств.

Список оборудования доступен для просмотра и редактирования вручную.

Управление группами лицензионных программ

Невозможно добавить новый ключ.

Не рассылаются оповещения о том, что превышены ограничения на использование ключей.

Удаленное подключение к клиентским компьютерам

Удаленное подключение к клиентским компьютерам недоступно.

Антивирусная безопасность

Антивирус использует базы, установленные до истечения срока действия лицензии.

О коде активации

Код активации – это код, который вы получаете, приобретая коммерческую лицензию на использование Kaspersky Security Center. Код активации представляет собой уникальную последовательность из двадцати латинских букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

Для активации программы при помощи кода активации необходимо подключение к серверам активации «Лаборатории Касперского» через интернет. Если подключение к серверам активации и доступ в интернет отсутствуют, активация программы выполняется с помощью файла ключа (см. раздел «О файле ключа» на стр. 15).

Отсчет срока действия лицензии начинается с даты активации программы. Если вы приобрели лицензию, допускающую использование Kaspersky Security Center на нескольких устройствах, то отсчет срока действия лицензии начинается с даты первого применения кода активации.

Если код активации был утерян или случайно удален после активации программы, для его восстановления обратитесь в Службу технической поддержки «Лаборатории Касперского».

О файле ключа

Файл ключа – это файл вида xxxxxxx.key.

Файл ключа используется для активации программы. Файл ключа содержит всю необходимую для активации информацию.Для активации программы с помощью файла ключа не требуется подключение к серверам активации и доступ в интернет.

Для получения файла ключа или его восстановления после случайного удаления, вы можете отправить запрос в Службу технической поддержки (см. раздел «Обращение в Службу технической поддержки» на стр. 39).

Файл ключа содержит следующую информацию:

- Ключ – уникальная буквенно-цифровая последовательность. Ключ может использоваться, например, для получения технической поддержки «Лаборатории Касперского».
- Ограничения на использование программы. В файле ключа Kaspersky Security Center может содержаться до трех ограничений: количество виртуальных Серверов администрирования, количество управляемых компьютеров и количество управляемых мобильных устройств. Тип ограничения определяется действующей лицензией (см. раздел «Варианты лицензирования Kaspersky Security Center» на стр. 12).
- Дата создания файла ключа – дата создания файла ключа на сервере активации.
- Срок действия лицензии – срок использования программы, предусмотренный в Лицензионном соглашении и отсчитываемый с даты первой активации программы с помощью этого файла ключа (например, один год).

  Срок действия лицензии истекает не позднее, чем срок годности файла ключа, с помощью которого по этой лицензии была активирована программа.

- Срок годности файла ключа – установленный срок с даты создания файла ключа. Активировать программу с помощью данного файла ключа можно только до истечения этого срока.

  Срок годности файла ключа автоматически считается истекшим с момента истечения срока действия лицензии на использование программы, активированной с помощью этого файла ключа.

О ПРЕДОСТАВЛЕНИИ ДАННЫХ

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме информацию о контрольных суммах обрабатываемых файлов (MD5), информацию для определения репутации URL, а также статистические данные для защиты от спама. Также вы соглашаетесь на сбор и передачу с клиентских компьютеров, находящихся под управлением Kaspersky Security Center, информации от установленных программных средств и кодов возврата, получаемых после установки этих программных средств. Переданная с клиентских компьютеров информация будет использована для устранения проблем в программном обеспечении или для изменения его функциональности.

Вся полученная информация не содержит персональных данных и иной конфиденциальной информации. Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями. Вы можете получить более подробную информацию о предоставлении данных на веб-сайте http://support.kaspersky.ru и в Положении о Kaspersky Security Network, поставляемом с программой.

ИНТЕРФЕЙС ПРОГРАММЫ

В этом разделе описаны основные параметры интерфейса Kaspersky Security Center.

Просмотр, создание, изменение и настройка групп администрирования, централизованное управление работой установленных на клиентских устройствах программ «Лаборатории Касперского» осуществляется с рабочего места администратора. Интерфейс управления обеспечивает компонент Консоль администрирования. Он представляет собой специализированную автономную оснастку, интегрированную в Microsoft Management Console (MMC), поэтому интерфейс Kaspersky Security Center является стандартным для MMC. Подробнее см. *Руководство администратора Kaspersky Security Center*.

Главное окно программы (см. рис. ниже) содержит меню, панель инструментов, панель обзора и рабочую область.

Меню обеспечивает управление окнами и предоставляет доступ к справочной системе. Пункт меню **Действие** дублирует команды контекстного меню для текущего объекта дерева консоли.

Панель обзора отображает пространство имен **Kaspersky Security Center** в виде дерева консоли.

Набор кнопок в панели инструментов обеспечивает прямой доступ к некоторым пунктам меню. Набор кнопок в панели инструментов изменяется в зависимости от текущего узла или папки дерева консоли.

Вид рабочей области главного окна зависит от того, к какому узлу (папке) дерева консоли она относится и какие функции выполняет.

Рисунок 1. Главное окно программы Kaspersky Security Center

ЗАПУСК ПРОГРАММЫ

В этом разделе описан запуск программы Kaspersky Security Center.

Kaspersky Security Center запускается автоматически при запуске Сервера администрирования.

- *Чтобы запустить Консоль администрирования программы,*

  выберите пункт **Kaspersky Security Center** в программной группе **Kaspersky Security Center** стандартного меню **Пуск** → **Программы**.

Программная группа **Kaspersky Security Center** создается на рабочих местах администраторов при установке компонента Консоль администрирования.

РАЗВЕРТЫВАНИЕ СИСТЕМЫ ЗАЩИТЫ

В этом разделе описаны два возможных сценария развертывания системы защиты сети организации:

- развертывание системы защиты внутри организации;
- развертывание системы защиты сети организации-клиента (при работе с SPE-версией программы).

Если вам требуется развернуть систему защиты внутри организации, которая включает в себя удаленные офисы, не входящие в сеть организации, вы можете воспользоваться сценарием развертывания антивирусной защиты для сервис-провайдеров.

Подробно действия, входящие в перечисленные сценарии развертывания защиты, описаны в разделе «Решение типовых задач» (см. стр. 21).

В ЭТОМ РАЗДЕЛЕ

РАЗВЕРТЫВАНИЕ АНТИВИРУСНОЙ ЗАЩИТЫ ВНУТРИ ОРГАНИЗАЦИИ

Чтобы развернуть в сети организации систему защиты, выполните следующие действия:

1. Установите и настройте Сервер администрирования и Консоль администрирования (см. раздел «Установка компонентов программы Kaspersky Security Center» на стр. 22).
2. Создайте группы администрирования и добавьте в них клиентские компьютеры (см. раздел «Создание групп администрирования» на стр. 22).
3. Удаленно установите на выбранные клиентские компьютеры Агент администрирования и необходимые программы «Лаборатории Касперского» (см. раздел «Удаленная установка программы» на стр. 28).
4. Если требуется, выполните обновление баз программ «Лаборатории Касперского» на клиентских компьютерах (подробнее см. *Руководство администратора Kaspersky Security Center*).
5. Если требуется, выполните дополнительную настройку установленных программ с помощью политик (см. раздел «Настройка политики для программы» на стр. 32) и локальных параметров программ (см. раздел «Просмотр и изменение локальных параметров программы» на стр. 32).
6. Настройте параметры уведомлений администратора о событиях на клиентских устройствах (см. раздел «Настройка параметров уведомлений» на стр. 32).
7. Проверьте работу уведомлений о событиях в работе системы защиты (см. раздел «Проверка полученных обновлений» на стр. 30).
8. Просмотрите отчеты (см. раздел «Создание и просмотр отчета» на стр. 33) и настройте автоматическую рассылку нужных отчетов по электронной почте (см. раздел «Создание задачи рассылки отчета» на стр. 34).
9. Настройте автоматическую установку программ на новые компьютеры в сети (см. раздел «Настройка автоматической установки программ» на стр. 29).

В результате этих действий в компьютерной сети организации будет развернута система защиты.

РАЗВЕРТЫВАНИЕ СИСТЕМЫ ЗАЩИТЫ СЕТИ ОРГАНИЗАЦИИ-КЛИЕНТА

Чтобы развернуть в сети организации-клиента систему антивирусной защиты, выполните следующие действия:

1. Установите Сервер администрирования и Консоль администрирования на рабочее место администратора (см. раздел «Установка компонентов программы Kaspersky Security Center» на стр. 22).

2. Установите Kaspersky Security Center Web-Console на рабочее место администратора (см. раздел «Установка Kaspersky Security Center Web-Console» на стр. 24).

3. Настройте Сервер администрирования для работы с Kaspersky Security Center Web-Console (подробнее см. *Руководство по внедрению Kaspersky Security Center*).

4. Создайте и настройте виртуальный Сервер администрирования, под управлением которого находится сеть организации-клиента (см. раздел «Создание виртуального Сервера администрирования» на стр. 24).

5. Назначьте и настройте агент обновлений в сети организации-клиента (см. раздел «Назначение агента обновлений. Настройка параметров агента обновлений» на стр. 24).

6. Настройте параметры инсталляционного пакета Агента администрирования, который вы будете использовать для установки Агента администрирования на компьютеры организации-клиента (см. раздел «Настройка инсталляционного пакета Агента администрирования» на стр. 26).

7. Удаленно установите на выбранные клиентские компьютеры Агент администрирования и необходимые программы «Лаборатории Касперского» (см. раздел «Удаленная установка программы» на стр. 28).

8. Если требуется, выполните дополнительную настройку установленных программ с помощью политик (см. раздел «Настройка политики для программы» на стр. 32) и локальных параметров программ (см. раздел «Просмотр и изменение локальных параметров программы» на стр. 32).

После выполнения этих действий в компьютерной сети организации-клиента будет развернута система защиты.

РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

В разделе описаны основные операции, которые вы можете выполнять с помощью Kaspersky Security Center.

В ЭТОМ РАЗДЕЛЕ

УСТАНОВКА КОМПОНЕНТОВ ПРОГРАММЫ KASPERSKY SECURITY CENTER

Чтобы установить Сервер администрирования и Консоль администрирования, выполните следующие действия:

1. Выберите компьютер, на котором будут установлены Сервер и Консоль администрирования. Рекомендуется устанавливать эти компоненты на компьютер, входящий в домен.

   Сервер и Консоль администрирования Kaspersky Security Center 10 могут быть установлены на том же самом компьютере, на котором работают Сервер и Консоль администрирования версии 9.0.

   Рекомендуется производить установку, обладая правами администратора домена. Это позволит автоматически создать группы пользователей **KLAdmins** и **KLOperators** и предоставить необходимые права учетной записи, под которой будет работать Сервер администрирования.

2. Запустите исполняемый файл setup.exe и следуйте указаниям мастера установки.

3. Выберите стандартный тип установки. Большинство параметров в этом случае задается автоматически.

   Выборочный тип установки подробно описывается в *Руководстве по внедрению Kaspersky Security Center*.

   После этого на компьютер будут установлены необходимые для работы программы, если они не были установлены ранее:

   - Microsoft Windows Installer версии 3.1;
   - Microsoft Data Access Components (MDAC) версии 2.8;
   - Microsoft .NET Framework 2.0;
   - Microsoft SQL Server® 2008 R2 Express Edition.

   Установленные программы не требуют обслуживания или администрирования.

На следующем этапе работы мастера начнется копирование файлов установки, и будет создана база данных, в которой Сервер администрирования централизованно хранит информацию об антивирусной защите сети.

По завершении работы мастера установки можно сразу запустить Консоль администрирования и выполнить первоначальную настройку параметров программы с помощью мастера первоначальной настройки.

СОЗДАНИЕ ГРУПП АДМИНИСТРИРОВАНИЯ

Иерархия групп администрирования формируется в главном окне программы Kaspersky Security Center в папке **Управляемые компьютеры**. Группы администрирования отображаются в виде папок в дереве консоли (см. рис. ниже).

Сразу после установки Kaspersky Security Center группа **Управляемые компьютеры** содержит только пустую папку **Серверы администрирования**.

Наличие или отсутствие папки **Серверы администрирования** в дереве консоли определяется параметрами пользовательского интерфейса. Для включения отображения этой папки нужно перейти в меню **Вид** → **Настройка интерфейса** и в открывшемся окне **Настройка интерфейса** установить флажок **Отображать подчиненные Серверы администрирования**.

При создании иерархии групп администрирования в состав папки **Управляемые компьютеры** можно включать клиентские компьютеры и виртуальные машины и добавлять вложенные группы. В папку **Серверы администрирования** можно добавлять подчиненные Серверы администрирования.

Каждая созданная группа, как и группа **Управляемые компьютеры**, сначала содержит только пустую папку **Серверы администрирования** для работы с подчиненными Серверами администрирования этой группы. Информация о политиках, задачах этой группы, а также о входящих в ее состав устройствах отображается на соответствующих закладках в рабочей области этой группы.

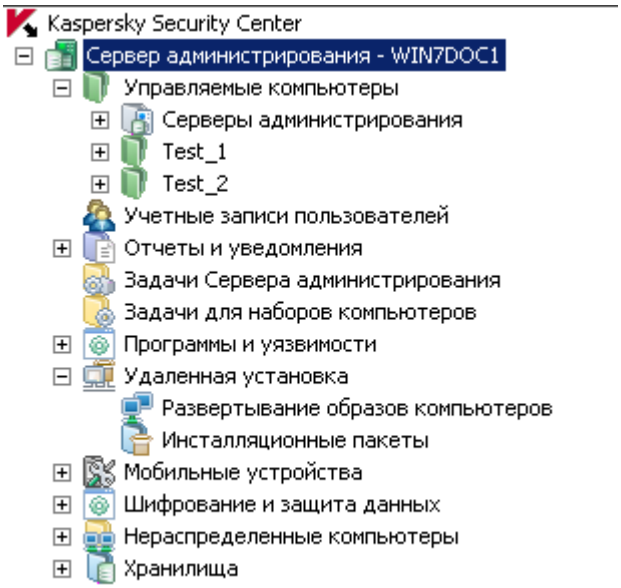

Рисунок 2. Просмотр иерархии групп администрирования

Чтобы создать группу администрирования, выполните следующие действия:

1. В дереве консоли откройте папку **Управляемые компьютеры**.
2. Если вы хотите создать подгруппу существующей группы администрирования, в папке **Управляемые компьютеры** выберите вложенную папку, соответствующую группе, в состав которой должна входить новая группа администрирования.

   Если вы создаете новую группу администрирования верхнего уровня иерархии, этот шаг можно пропустить.
3. Запустите процесс создания группы администрирования одним из следующих способов:
   - с помощью команды контекстного меню **Создать** → **Группу**;
   - по ссылке **Создать подгруппу**, расположенной в рабочей области главного окна программы на закладке **Группы**.
4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем.

УСТАНОВКА KASPERSKY SECURITY CENTER WEB-CONSOLE

- *Чтобы установить Kaspersky Security Center Web-Console на рабочее место администратора,*

  запустите файл setup.exe, входящий в состав дистрибутива программы Kaspersky Security Center Web-Console.

В результате запустится мастер установки Kaspersky Security Center Web-Console, который предложит вам провести настройку параметров установки. Следуйте его указаниям.

СОЗДАНИЕ ВИРТУАЛЬНОГО СЕРВЕРА АДМИНИСТРИРОВАНИЯ

- *Чтобы добавить виртуальный Сервер администрирования в состав выбранной группы администрирования, выполните следующие действия:*

  1. В дереве консоли в папке группы администрирования выберите узел **Серверы администрирования**.
  2. Запустите процесс создания виртуального Сервера администрирования одним из следующих способов:
     - в контекстном меню узла **Серверы администрирования** выберите пункт **Создать** → **Виртуальный Сервер администрирования**.
     - по ссылке **Добавить виртуальный Сервер администрирования** в рабочей области.

  В результате запустится мастер создания виртуального Сервера администрирования. Следуйте его указаниям.

НАЗНАЧЕНИЕ АГЕНТА ОБНОВЛЕНИЙ. НАСТРОЙКА ПАРАМЕТРОВ АГЕНТА ОБНОВЛЕНИЙ

- *Чтобы назначить компьютер агентом обновлений организации-клиента, выполните следующие действия:*

  1. Создайте автономный пакет установки Агента администрирования. Выполните следующие действия:
     a. В дереве консоли выберите виртуальный Сервер администрирования, под управлением которого находится сеть организации-клиента.
     b. В папке **Удаленная установка** виртуального Сервера администрирования выберите вложенную папку **Инсталляционные пакеты**.
     c. В рабочей области папки выберите или создайте инсталляционный пакет Агента администрирования.
     d. Откройте окно свойств инсталляционного пакета Агента администрирования.
     e. В разделе **Подключение** в строке **Адрес сервера** проверьте адрес виртуального Сервера администрирования. Адрес должен быть указан в следующем формате: `<Адрес главного Сервера администрирования>/<Имя виртуального Сервера администрирования>`.

f. Запустите процесс создания автономного пакета установки для этого инсталляционного пакета одним из следующих способов:

- в контекстном меню инсталляционного пакета выберите пункт **Создать автономный пакет установки**;
- по ссылке **Создать автономный пакет установки** в блоке работы с выбранным инсталляционным пакетом.

g. Откройте список созданных автономных пакетов установки инсталляционного пакета Агента администрирования одним из следующих способов:

- в завершающем окне мастера создания автономного пакета установите флажок **Открыть список автономных пакетов**;
- в контекстном меню инсталляционного пакета выберите пункт **Показать список автономных пакетов**.

h. В открывшемся списке автономных пакетов выберите созданный автономный пакет и укажите способ доставки автономного пакета администратору организации-клиента.

2. Обратитесь к администратору организации-клиента для локальной установки Агента администрирования на клиентский компьютер, выбранный агентом обновлений.

После установки Агента администрирования на клиентский компьютер, выбранный агентом обновлений, этот компьютер отображается в папке **Управляемые компьютеры** виртуального Сервера администрирования.

Kaspersky Security Center автоматически назначает этот компьютер агентом обновлений и настраивает его в качестве шлюза соединений при первом соединении с Сервером администрирования.

Если вам требуется назначить компьютер агентом обновлений вручную, выполните следующие действия:

a. Откройте окно свойств папки **Управляемые компьютеры** виртуального Сервера администрирования.

b. В разделе **Агенты обновлений** выберите клиентский компьютер, который будет выполнять роль агента обновлений, нажав на кнопку **Добавить**.

c. Откройте окно свойств агента обновлений и выполните следующие действия:

- Настройте параметры опроса сети агентом обновлений в разделе **Опрос сети**.
- Выберите раздел **Дополнительно** и установите флажок **Шлюз соединений** для использования агента обновлений в качестве шлюза соединений в сети организации-клиента.

В результате выбранный клиентский компьютер становится агентом обновлений организации-клиента и используется в этой организации в качестве шлюза соединений с виртуальным Сервером администрирования.

Вы можете назначить компьютер агентом обновлений вручную только в том случае, если автоматическое назначение отключено (раздел **Параметры** окна свойств виртуального Сервера администрирования).

НАСТРОЙКА ИНСТАЛЛЯЦИОННОГО ПАКЕТА АГЕНТА АДМИНИСТРИРОВАНИЯ

Перед установкой Агента администрирования на компьютеры организации-клиента требуется настроить параметры инсталляционного пакета Агента администрирования, который будет использоваться для удаленной установки.

Чтобы настроить инсталляционный пакет Агента администрирования для установки на компьютеры организации-клиента, выполните следующие действия:

1. В дереве консоли выберите виртуальный Сервер администрирования, под управлением которого находится сеть организации-клиента.

2. В папке **Удаленная установка** виртуального Сервера администрирования выберите вложенную папку **Инсталляционные пакеты**.

3. В рабочей области выберите или создайте инсталляционный пакет Агента администрирования, который будет использоваться для установки Агента администрирования на компьютеры организации-клиента.

4. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета Агента администрирования.

5. В окне свойств настройте следующие параметры инсталляционного пакета:

   - В разделе **Подключение** в строке **Адрес сервера** укажите тот же адрес виртуального Сервера администрирования, что и при локальной установке Агента администрирования на агент обновлений (см. раздел «Назначение агента обновлений. Настройка параметров агента обновлений» на стр. 24).

   - В разделе **Дополнительно** установите флажок **Подключаться к Серверу администрирования через шлюз соединений**. В строке **Адрес шлюза соединений** укажите адрес агента обновлений. В качестве адреса компьютера можно использовать IP-адрес или имя компьютера в сети Windows.

6. Нажмите на кнопку **ОК**.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Kaspersky Security Center позволяет управлять мобильными устройствами, поддерживающими протоколы Exchange ActiveSync и iOS Mobile Device Management (iOS MDM).

Сбор информации о мобильных устройствах и хранение их профилей выполняют Серверы мобильных устройств. *Сервер мобильных устройств* – это компонент Kaspersky Security Center, который предоставляет администратору доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования.

Существуют два вида Серверов мобильных устройств:

- Сервер мобильных устройств Exchange ActiveSync. Устанавливается на клиентский компьютер, на котором установлен сервер Microsoft Exchange, и позволяет получать данные с сервера Microsoft Exchange и передавать их на Сервер администрирования. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими протокол Exchange ActiveSync.

- Сервер мобильных устройств iOS MDM. Устанавливается на клиентский компьютер и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

Для мобильных устройств Exchange ActiveSync доступны следующие функции:

- создание и редактирование профилей управления мобильными устройствами, назначение профилей почтовым ящикам пользователей;
- настройка параметров работы мобильного устройства (синхронизация почты, использование приложений, пароль пользователя, шифрование данных, подключение съемных носителей);
- установка сертификатов на мобильные устройства.

Список функций, доступных для конкретного мобильного устройства, зависит от особенностей поддержки протокола Exchange ActiveSync на этом устройстве.

Для мобильных устройств iOS MDM доступны следующие функции:

- создание и редактирование конфигурационных профилей, установка конфигурационных профилей на мобильные устройства;
- установка приложений на мобильное устройство через App Store или с помощью манифест-файлов (.plist);
- возможность блокировать мобильное устройство, сбрасывать пароль мобильного устройства и удалять все данные с мобильного устройства.

Подробная информация об управлении мобильными устройствами приведена в *Руководстве администратора Kaspersky Security Center*.

Далее приведено краткое описание действий, которые необходимо выполнить для подключения к Серверу администрирования мобильных устройств, поддерживающих протоколы Exchange ActiveSync и iOS MDM.

Подключение мобильных устройств Exchange ActiveSync

Чтобы подключить мобильные устройства Exchange ActiveSync к Серверу администрирования, выполните следующие действия:

1. Установите Сервер мобильных устройств Exchange ActiveSync на клиентский компьютер с установленным сервером Microsoft Exchange.

   Рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync на сервер Microsoft Exchange с ролью Client Access Server (CAS). Если несколько серверов Microsoft Exchangec ролью Client Access Server объединены в массив (CAS Array), то рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync на каждый сервер Microsoft Exchange в массиве.

2. Создайте профили управления мобильными устройствами Exchange ActiveSync. Команды для работы с профилями управления мобильными устройствами доступны в разделе **Почтовые ящики** окна свойств Сервера мобильных устройств Exchange ActiveSync.

3. Назначьте профили управления мобильными устройствами Exchange ActiveSync почтовым ящикам пользователей.

Пользователь мобильного устройства подключает мобильное устройство к серверу Microsoft Exchange и получает уведомление о том, что его почтовый ящик находится под управлением профиля, который накладывает ограничения на подключаемое мобильное устройство. Подробнее о действиях пользователя мобильного устройства Exchange ActiveSync см. в *Руководстве по внедрению Kaspersky Endpoint Security 10 для мобильных устройств*.

Мобильное устройство пользователя, подключенное к серверу Microsoft Exchange, отображается в папке **Мобильные устройства Exchange ActiveSync**, вложенной в папку **Мобильные устройства** дерева консоли.

Подробнее подключение мобильных устройств Exchange ActiveSync к Серверу администрирования описано в *Руководстве по внедрению Kaspersky Security Center*.

Администратор может управлять мобильными устройствами Exchange ActiveSync, подключенными к Серверу администрирования. Информацию об управлении мобильными устройствами Exchange ActiveSync см. в *Руководстве администратора Kaspersky Security Center*.

Подключение мобильных устройств iOS MDM

- *Чтобы подключить мобильные устройства iOS MDM к Серверу администрирования, выполните следующие действия:*

1. Установите на выбранный клиентский компьютер Сервер мобильных устройств iOS MDM, который входит в состав инсталляционных пакетов Сервера администрирования по умолчанию.

2. Установите на Сервере администрирования сертификат Apple Push Notification Service (APNs-сертификат).

3. Отправьте пользователям мобильных устройств iOS ссылку для скачивания iOS MDM-профиля с помощью команды **Установить iOS MDM-профиль на мобильное устройство пользователя**. Команда доступна в папке **Учетные записи пользователей** дерева консоли.

   Пользователи мобильных устройств получают уведомление со ссылкой для скачивания iOS MDM-профиля с веб-портала Kaspersky Security Center. Пользователь самостоятельно переходит по полученной ссылке. После этого операционная система устройства спрашивает пользователя о его согласии на установку iOS MDM-профиля. Если пользователь соглашается, iOS MDM-профиль загружается на устройство.

После загрузки iOS MDM-профиля и синхронизации с Сервером администрирования мобильное устройство iOS MDM будет отображаться в папке **Мобильные устройства iOS MDM**, вложенной в папку **Мобильные устройства** дерева консоли.

Подробнее подключение мобильных устройств iOS MDM к Серверу администрирования описано в *Руководстве по внедрению Kaspersky Security Center*.

После подключения мобильного устройства iOS MDM к Серверу администрирования, можно установить на мобильное устройство iOS MDM конфигурационный профиль и provisioning-профиль. Подробно установка конфигурационного и provisioning-профиля описана в *Руководстве по внедрению Kaspersky Security Center.*

Администратор может управлять мобильными устройствами iOS MDM, подключенными к Серверу администрирования. Информацию об управлении мобильными устройствами iOS MDM см. в *Руководстве администратора Kaspersky Security Center*.

Удаленная установка программы

Некоторые программы «Лаборатории Касперского», управление которыми доступно через Kaspersky Security Center, могут быть установлены на клиентские устройства только локально (подробнее см. в Руководствах к программам «Лаборатории Касперского»).

- *Чтобы провести удаленную установку программы на клиентские компьютеры, выполните следующие действия:*

1. В дереве консоли перейдите в узел Сервера администрирования, под управлением которого находятся клиентские устройства.

2. В дереве консоли в папке **Удаленная установка** по ссылке **Запустить мастер удаленной установки** запустите мастер удаленной установки.

3. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет программы, которую вы хотите установить.

4. Следуйте указаниям мастера.

В результате работы мастера создается задача удаленной установки программы на клиентских устройствах. Мастер удаленной установки создает и запускает задачу удаленной установки выбранной программы. В зависимости от выбранного вами набора устройств или группы администрирования созданная задача размещается в папке **Задачи для наборов компьютеров** или в рабочей области выбранной группы администрирования, на закладке **Задачи**.

После завершения работы созданной задачи программа будет установлена на выбранные клиентские устройства.

Вы можете использовать указанный выше способ для установки антивирусной программы на клиентские устройства. Информацию об установке антивирусной программы на клиентские компьютеры группы администрирования вы можете посмотреть на закладке **Компьютеры** в рабочей области группы. Информацию об установке программы на набор клиентских компьютеров вы можете просмотреть в рабочей области папки **Нераспределенные компьютеры**. В списке компьютеров на закладке **Компьютеры** и в рабочей области папки **Нераспределенные компьютеры** в графе **Агент/Антивирус** отображается информация об установке на компьютеры Агента администрирования и антивирусной программы. Если в этой графе после обратной косой черты стоит знак плюс (+), антивирусная программа установлена успешно.

НАСТРОЙКА АВТОМАТИЧЕСКОЙ УСТАНОВКИ ПРОГРАММ

Чтобы настроить автоматическую установку программ на новые устройства в группе администрирования, выполните следующие действия:

1. Выберите в дереве консоли нужную вам группу администрирования.

2. Откройте окно свойств этой группы администрирования.

3. В разделе **Автоматическая установка** выберите инсталляционные пакеты, которые следует устанавливать на новые устройства, установив флажки рядом с названиями инсталляционных пакетов нужных программ. Нажмите на кнопку **ОК**.

В результате будут созданы групповые задачи, которые будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Если для автоматической установки указано несколько инсталляционных пакетов одной программы, задача установки будет создана только для последней версии программы.

СОЗДАНИЕ ЗАДАЧИ ЗАГРУЗКИ ОБНОВЛЕНИЙ В ХРАНИЛИЩЕ

Задача загрузки обновлений в хранилище Сервера администрирования создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище может быть создана в одном экземпляре. Поэтому вы можете создать задачу загрузки обновлений в хранилище только в случае, если она была удалена из списка задач Сервера администрирования.

Чтобы создать задачу загрузки обновлений в хранилище, выполните следующие действия:

1. В дереве консоли выберите папку **Задачи Сервера администрирования**.

2. Запустите процесс создания задачи одним из следующих способов:

   - В контекстном меню папки дерева консоли **Задачи Сервера администрирования** выберите пункт **Создать** → **Задачу**.

   - По ссылке **Создать задачу** в рабочей области.

В результате запускается мастер создания задачи. Следуйте его указаниям. В окне мастера **Тип задачи** выберите тип задачи **Загрузка обновлений в хранилище**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилище** появится в списке задач Сервера администрирования.

В результате выполнения задачи **Загрузка обновлений в хранилище** обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа.

Из папки общего доступа обновления распространяются на клиентские компьютеры и подчиненные Серверы администрирования.

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений «Лаборатории Касперского» – серверы «Лаборатории Касперского», на которых размещаются обновленные базы и программные модули.
- Главный Сервер администрирования.
- FTP- / HTTP-сервер или сетевая папка обновлений – FTP-, HTTP-сервер, локальная или сетевая папка, добавленная пользователем и содержащая актуальные обновления. При выборе локальной папки требуется указать папку на компьютере с установленным Сервером администрирования.

  Для обновления Сервера администрирования с FTP- / HTTP-сервера или из сетевой папки на эти ресурсы требуется скопировать правильную структуру папок с обновлениями, совпадающую со структурой, формируемой при использовании серверов обновлений «Лаборатории Касперского».

Выбор ресурса зависит от параметров задачи. По умолчанию обновление производится из интернета с серверов обновлений «Лаборатории Касперского».

ПРОВЕРКА ПОЛУЧЕННЫХ ОБНОВЛЕНИЙ

Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские компьютеры, выполните следующие действия:

1. В рабочей области папки **Задачи Сервера администрирования** дерева консоли выберите задачу **Загрузка обновлений в хранилище** в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
   - В контекстном меню задачи выберите пункт **Свойства**.
   - По ссылке **Изменить параметры задачи** в блоке работы с выбранной задачей.
3. В открывшемся окне свойств задачи в разделе **Проверка обновлений** установите флажок **Выполнять проверку обновлений перед распространением** и выберите задачу проверки обновлений одним из следующих способов:
   - Нажмите на кнопку **Выбрать**, чтобы выбрать уже сформированную задачу проверки обновлений.
   - Нажмите на кнопку **Создать**, чтобы создать задачу проверки обновлений.

     В результате запустится мастер создания задачи проверки обновлений. Следуйте его указаниям.

     В процессе создания задачи проверки обновлений необходимо выбрать группу администрирования, на компьютерах которой будет выполняться задача. Компьютеры, входящие в эту группу, называются *тестовыми компьютерами*.

     В качестве тестовых компьютеров рекомендуется использовать хорошо защищенные компьютеры с наиболее распространенной в сети организации программной конфигурацией. Это позволяет повысить качество проверки, снизить риск возникновения ложных срабатываний, а также вероятность обнаружения вирусов при проверке (при нахождении вирусов на тестовых компьютерах задача проверки обновлений считается завершившейся неудачно).
4. Закройте окно свойств задачи загрузки обновлений в хранилище, нажав на кнопку **ОК**.

В результате в рамках выполнения задачи загрузки обновлений в хранилище будет выполняться задача проверки полученных обновлений. Сервер администрирования будет копировать обновления с источника, сохранять их во временном хранилище и запускать задачу проверки обновлений. В случае успешного выполнения этой задачи обновления будут скопированы из временного хранилища в папку общего доступа Сервера администрирования (<Папка установки Kaspersky Security Center>\Share\Updates) и распространены на клиентские компьютеры, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи проверки обновлений размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится, и на Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции будут выполнены при следующем запуске задачи загрузки обновлений в хранилище, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых компьютеров выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты антивирусной программы;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования программы «Лаборатории Касперского».

Если ни одно из перечисленных условий ни на одном из тестовых компьютеров не выполняется, набор обновлений признается корректным и задача проверки обновлений считается успешно выполненной.

АВТОМАТИЧЕСКОЕ РАСПРОСТРАНЕНИЕ ОБНОВЛЕНИЙ НА КЛИЕНТСКИЕ КОМПЬЮТЕРЫ

Чтобы обновления выбранной вами программы автоматически распространялись на клиентские компьютеры сразу после загрузки обновлений в хранилище Сервера администрирования, выполните следующие действия:

1. Подключитесь к Серверу администрирования, под управлением которого находятся клиентские компьютеры.
2. Создайте задачу распространения обновлений этой программы для выбранных клиентских компьютеров одним из следующих способов:
   - Если требуется распространять обновления на клиентские компьютеры, входящие в выбранную группу администрирования, создайте задачу для выбранной группы.
   - Если требуется распространять обновления на клиентские компьютеры, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора компьютеров.

   В результате запустится мастер создания задачи. Следуйте его указаниям, выполнив следующие условия:

   a. В окне мастера **Тип задачи** в узле нужной вам программы выберите задачу распространения обновлений.

      Название задачи распространения обновлений, которое отображается в окне **Тип задачи**, зависит от программы, для которой создается задача. Подробнее о названиях задач обновления для выбранных программ «Лаборатории Касперского» см. в Руководствах к этим программам.

   b. В окне мастера **Расписание** в поле **Запуск по расписанию** выберите вариант запуска **При загрузке обновлений в хранилище**.

В результате созданная задача распространения обновлений будет запускаться для выбранных компьютеров каждый раз при загрузке обновлений в хранилище Сервера администрирования.

Если задача распространения обновлений нужной вам программы уже создана для выбранных компьютеров, для автоматического распространения обновлений на клиентские компьютеры в окне свойств задачи, в разделе **Расписание** нужно выбрать вариант запуска **При загрузке обновлений в хранилище** в поле **Запуск по расписанию**.

НАСТРОЙКА ПОЛИТИКИ ДЛЯ ПРОГРАММЫ

Чтобы настроить политику для программы, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для которой требуется настроить политику.
2. В рабочей области группы на закладке **Политики** выберите политику нужной вам программы.
3. Откройте окно свойств политики и выполните настройку параметров политики.

После сохранения внесенных изменений политика будет применена на компьютерах группы администрирования с измененными параметрами.

ПРОСМОТР И ИЗМЕНЕНИЕ ЛОКАЛЬНЫХ ПАРАМЕТРОВ ПРОГРАММЫ

Система администрирования Kaspersky Security Center позволяет удаленно управлять локальными параметрами программ на клиентских компьютерах через Консоль администрирования.

Локальные параметры программы – это параметры программы, индивидуальные для клиентского компьютера. С помощью Kaspersky Security Center вы можете устанавливать локальные параметры программ для клиентских компьютеров, входящих в группы администрирования.

Подробные описания параметров программ «Лаборатории Касперского» приводятся в Руководствах для этих программ.

Чтобы просмотреть или изменить локальные параметры программы, выполните следующие действия:

1. В рабочей области группы, в которую входит нужный вам клиентский компьютер, выберите закладку **Компьютеры**.
2. В окне свойств клиентского компьютера в разделе **Программы** выберите нужную вам программу.
3. Откройте окно свойств программы двойным щелчком мыши по названию программы или нажатием на кнопку **Свойства**.

В результате откроется окно локальных параметров выбранной программы, которые можно просмотреть и изменить.

Вы можете изменять значения тех параметров, изменение которых не запрещено групповой политикой (параметр не закрыт «замком» в политике).

НАСТРОЙКА ПАРАМЕТРОВ УВЕДОМЛЕНИЙ

Kaspersky Security Center предоставляет возможность настраивать параметры уведомления администратора о событиях на клиентских устройствах и выбирать способ уведомления:

- электронная почта;
- NET SEND (служба сообщений);
- SMS;
- исполняемый файл для запуска.

Уведомление средствами службы сообщений доступно только при работе под управлением операционных систем семейства Windows 5.X (Windows XP, Windows Server 2003).

Чтобы настроить параметры уведомлений о событиях на клиентских устройствах, выполните следующие действия:

1. В дереве консоли откройте окно свойств папки **Отчеты и уведомления** одним из следующих способов:

   - В контекстном меню папки дерева консоли **Отчеты и уведомления** выберите пункт **Свойства**.
   - В рабочей области папки **Отчеты и уведомления** на закладке **Уведомления** откройте окно по ссылке **Изменить параметры доставки уведомлений**.

2. В разделе **Уведомление** окна свойств папки **Отчеты и уведомления** настройте параметры уведомлений о событиях.

   В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Вы можете настроить параметры уведомления для события в окне свойств этого события. Быстрый доступ к параметрам событий осуществляется по ссылкам **Изменить параметры событий Kaspersky Endpoint Security** и **Изменить параметры событий Сервера администрирования**.

ПРОВЕРКА РАСПРОСТРАНЕНИЯ УВЕДОМЛЕНИЙ

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового «вируса» Eicar на клиентских компьютерах.

Чтобы проверить распространение уведомлений о событиях, выполните следующие действия:

1. Остановите задачу постоянной защиты файловой системы на клиентском компьютере и скопируйте тестовый «вирус» Eicar на клиентский компьютер. Снова включите задачу постоянной защиты файловой системы.

2. Запустите задачу проверки клиентских компьютеров для группы администрирования или набора компьютеров, в который входит клиентский компьютер с «вирусом» Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый «вирус» будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

   В папке дерева консоли **Отчеты и уведомления** во вложенной папке **События** в выборке **Последние события** отобразится запись об обнаружении «вируса».

Тестовый «вирус» Eicar НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может навредить вашему компьютеру. При этом большинство программ антивирусных компаний-производителей идентифицируют его как вирус. Загрузить тестовый «вирус» можно с официального веб-сайта организации EICAR.

СОЗДАНИЕ И ПРОСМОТР ОТЧЕТА

Чтобы сформировать и просмотреть отчет, выполните следующие действия:

1. В дереве консоли откройте папку **Отчеты и уведомления**, в которой представлен перечень шаблонов отчетов.

2. Выберите интересующий вас шаблон отчета в дереве консоли или в рабочей области на закладке **Отчеты**.

   В результате в рабочей области отображается отчет, сформированный по выбранному шаблону.

В отчете отображаются следующие данные:

- тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
- графическая диаграмма, отображающая наиболее характерные данные отчета;
- сводная таблица данных, отображающих вычисляемые показатели отчета;
- таблица детальных данных отчета.

СОХРАНЕНИЕ ОТЧЕТА

Чтобы сохранить сформированный отчет, выполните следующие действия:

1. В дереве консоли откройте папку **Отчеты и уведомления**, в которой представлен перечень шаблонов отчетов.
2. Выберите интересующий вас шаблон отчета в дереве консоли или в рабочей области на закладке **Отчеты**.
3. В контекстном меню выбранного шаблона отчета выберите пункт **Сохранить**.

В результате запустится мастер сохранения отчета. Следуйте его указаниям.

После завершения работы мастера откроется папка, в которую вы сохранили файл отчета.

СОЗДАНИЕ ЗАДАЧИ РАССЫЛКИ ОТЧЕТА

Рассылка отчетов в программе Kaspersky Security Center осуществляется с помощью задачи рассылки отчета. Отчеты можно рассылать по электронной почте или сохранять в выбранной папке, например, в папке общего доступа на Сервере администрирования или локальном компьютере.

Чтобы создать задачу рассылки одного отчета, выполните следующие действия:

1. В дереве консоли откройте папку **Отчеты и уведомления**, в которой представлен перечень шаблонов отчетов.
2. Выберите интересующий вас шаблон отчета в дереве консоли или в рабочей области на закладке **Отчеты**.
3. В контекстном меню шаблона отчета выберите пункт **Рассылка отчетов**.

В результате запускается мастер создания задачи рассылки выбранного отчета. Следуйте его указаниям.

Чтобы создать задачу рассылки нескольких отчетов, выполните следующие действия:

1. В дереве консоли выберите папку **Задачи Сервера администрирования**.
2. Запустите процесс создания задачи одним из следующих способов:
   - в контекстном меню папки дерева консоли **Задачи Сервера администрирования** выберите пункт **Создать** → **Задачу**.
   - по ссылке **Создать задачу** в рабочей области.

В результате запускается мастер создания задачи Сервера администрирования. Следуйте его указаниям. В окне мастера **Тип задачи** выберите тип задачи **Рассылка отчета**.

Созданная задача рассылки отчета отображается в папке дерева консоли **Задачи Сервера администрирования**.

Задача рассылки отчета создается автоматически в случае, если при установке Kaspersky Security Center были заданы параметры электронной почты.

ПРОСМОТР ОТЧЕТА О НАЙДЕННЫХ ВИРУСАХ

Чтобы просмотреть сводный отчет о найденных вирусах, выполните следующие действия:

1. В дереве консоли выберите папку **Отчеты и уведомления**.
2. В рабочей области папки на закладке **Статистика** выберите страницу **Антивирусная статистика**.

В информационных панелях этой страницы по умолчанию отображаются следующие данные, собранные за сутки:

- история вирусной активности;
- наиболее распространенные в сети вирусы;
- устройства, на которых обнаружено наибольшее количество вирусов;
- пользователи, на устройствах которых обнаружено наибольшее количество вирусов.

В папке дерева консоли **Отчеты и уведомления** вы также можете просмотреть подробный отчет о найденных в сети вирусах на закладке **Отчеты**. На этой закладке в блоке **Антивирусная статистика** вы можете перейти к подробным отчетам по следующим ссылкам:

- **Отчет о вирусах**.
- **Отчет о наиболее зараженных компьютерах**.
- **Отчет о пользователях зараженных компьютеров**.

В результате выбора нужного вам отчета в рабочей области отобразится подробная информация о найденных вирусах, собранная с момента установки Сервера администрирования.

Вы можете изменять параметры любого отчета: например, временной интервал, за который собирается отчет, или набор отображаемых в отчете полей (подробнее см. *Руководство администратора Kaspersky Security Center*).

ПРОСМОТР ИНФОРМАЦИИ О СОБЫТИЯХ

Чтобы просмотреть информацию о событиях в работе программ, выполните следующие действия:

1. В дереве консоли в папке **Отчеты и уведомления** выберите вложенную папку **События**.
2. Откройте выборку событий одним из следующих способов:
   - В дереве консоли раскройте папку **События** и выберите папку с нужной вам выборкой событий.
   - В рабочей области папки **События**, в блоке **Предопределенные выборки**, по ссылке, соответствующей названию нужной вам выборки событий.

   В результате в рабочей области будет представлен список событий выбранного типа, хранящихся на Сервере администрирования.

Вы можете сформировать собственную выборку событий (подробнее см. в *Руководстве администратора Kaspersky Security Center*).

ПРОСМОТР ТЕКУЩЕГО СОСТОЯНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Вы можете отслеживать состояние системы защиты клиентских компьютеров и устройств, находящихся под управлением Сервера администрирования **<Имя Сервера>** в рабочей области узла **<Имя Сервера>**. В блоках управления рабочей области отображается общая информация о состоянии следующих областей работы программы:

- развертывание защиты в сети (блок **Развертывание**);
- формирование структуры групп администрирования, содержащих управляемые компьютеры (блок **Управление компьютерами**);
- работа защиты на клиентских устройствах (блок **Защита компьютера и поиск вирусов**);
- обновление баз и модулей программ (блок **Обновление**);
- мониторинг и работа уведомлений (блок **Мониторинг**).

Вы можете оценить состояние системы защиты с помощью значков светофоров, расположенных в блоках управления. Если значок зеленого цвета, необходимые задачи в этой области выполнены. Если значок желтого или красного цвета, на эту область следует обратить внимание и при необходимости выполнить требуемые действия.

Помимо цветовой индикации в каждом блоке приводится краткое текстовое описание состояния системы защиты или возникшей проблемы, а также содержатся ссылки, с помощью которых вы можете перейти к выполнению основных задач блока.

Более подробную информацию о состоянии системы защиты можно просмотреть в папке **Отчеты и уведомления**.

СОЗДАНИЕ РЕЗЕРВНОЙ КОПИИ ДАННЫХ СЕРВЕРА АДМИНИСТРИРОВАНИЯ

Мастер первоначальной настройки Kaspersky Security Center формирует задачу создания резервной копии данных Сервера администрирования. По умолчанию резервная копия формируется ежедневно на компьютере с установленным Сервером администрирования в папке установки программы во вложенной папке Backup.

Чтобы вручную запустить формирование резервной копии данных Сервера администрирования, выполните следующие действия:

1. В дереве консоли выберите папку **Задачи Сервера администрирования**.
2. В рабочей области папки выберите задачу создания резервной копии данных Сервера администрирования (по умолчанию это задача **Резервное копирование данных Сервера администрирования**).
3. Запустите выбранную задачу.

Поскольку виртуальные Серверы администрирования используют базу данных главного Сервера администрирования, резервное копирование и восстановление данных виртуального Сервера осуществляется только в рамках резервного копирования и восстановления данных главного Сервера.

ПЕРЕХОД С KASPERSKY SECURITY CENTER 9.0 НА KASPERSKY SECURITY CENTER 10

В этом разделе описана процедура перехода с версии Kaspersky Security Center 9.0 на версию Kaspersky Security Center 10 и основные действия по первоначальной настройке работы программы в новой версии.

- *Чтобы перейти с версии Kaspersky Security Center9.0 на версию Kaspersky Security Center 10, выполните следующие действия:*

1. Для Kaspersky Security Center 9.0 создайте резервную копию данных Сервера администрирования при помощи утилиты *klbackup*. Эта утилита входит в состав дистрибутива программы и располагается в корне папки установки Kaspersky Security Center.

2. Установите Сервер администрирования и Консоль администрирования версии 10.

   Вы можете установить Сервер администрирования на компьютер, на котором установлена предыдущая версия Сервера администрирования. При обновлении до версии 10 данные и параметры предыдущей версии Сервера администрирования сохраняются.

   Если вы устанавливаете Сервер администрирования на другой компьютер, вы можете восстановить параметры предыдущей версии Сервера администрирования с помощью утилиты резервного копирования и восстановления данных (*klbackup*).

3. Выполните первоначальную настройку Сервера администрирования, если параметры не были перенесены с предыдущей версии Сервера администрирования.

4. Сформируйте структуру групп администрирования.

5. Выберите клиентские компьютеры, на которых нужно установить новую версию Агента администрирования и новые версии программ «Лаборатории Касперского».

6. Для выбранных компьютеров создайте задачу удаленной установки новой версии Агента администрирования и новых версий программ «Лаборатории Касперского». Для удаленной установки программ вы можете использовать инсталляционные пакеты, сформированные автоматически при установке Kaspersky Security Center 10.

7. Запустите созданную задачу.

   В результате на выбранные клиентские компьютеры будут установлены новые версии Агента администрирования и программ «Лаборатории Касперского».

8. Добавьте клиентские компьютеры, на которых проведена установка программ новых версий, в структуру групп администрирования.

В результате система защиты, построенная на программах более ранних версий, переходит под управление Kaspersky Security Center 10.

Вы можете конвертировать политики и задачи, созданные для более ранних версий программ «Лаборатории Касперского», в политики и задачи новой версии этих программ с помощью мастера конвертации политик и задач. Подробнее см. в *Руководстве администратора Kaspersky Security Center*.

ЗАКЛЮЧЕНИЕ

В этом разделе обобщена информация, представленная в документе.

В документе описан простой сценарий развертывания защиты в сети организации, а также действия, необходимые для быстрого развертывания защиты и начала работы с программой Kaspersky Security Center. Более полную информацию о возможностях Kaspersky Security Center и сценариях развертывания защиты см. в *Руководстве по внедрению Kaspersky Security Center* и в *Руководстве администратора Kaspersky Security Center*.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Этот раздел содержит информацию о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

В ЭТОМ РАЗДЕЛЕ

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации к программе или в одном из источников информации о программе (см. раздел «Источники информации о программе» на стр. 8), рекомендуем обратиться в Службу технической поддержки «Лаборатории Касперского». Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

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 по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос через систему Kaspersky CompanyAccount на веб-сайте Службы технической поддержки. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Техническая поддержка по телефону

Если возникла неотложная проблема, вы можете позвонить специалистам русскоязычной или международной технической поддержки http://support.kaspersky.ru/support/contacts.

Перед обращением в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами предоставления поддержки http://support.kaspersky.ru/support/rules. Это позволит нашим специалистам быстрее помочь вам.

Получение технической поддержки через Kaspersky CompanyAccount

Kaspersky CompanyAccount - это веб-сервис (https://companyaccount.kaspersky.com), предназначенный для отправки и отслеживания запросов в «Лабораторию Касперского».

Для доступа к Kaspersky CompanyAccount вам требуется зарегистрироваться на странице регистрации (https://support.kaspersky.com/companyaccount/registration) и получить логин и пароль. Для этого вам понадобится указать код активации или файл ключа (см. раздел «О файле ключа» на стр. 15).

В Kaspersky CompanyAccount вы можете выполнять следующие действия:

- отправлять запросы в Службу технической поддержки и Вирусную лабораторию;
- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших запросов в Службу технической поддержки;
- получать копию файла ключа в случае, если файл ключа был утерян или удален.

Электронный запрос в Службу технической поддержки

Вы можете отправить электронный запрос в Службу технической поддержки на русском, английском и других языках.

В полях формы электронного запроса вам нужно указать следующие сведения:

- тип запроса;
- название и номер версии программы;
- текст запроса.

Если требуется, вы также можете прикрепить к форме электронного запроса файлы.

Специалист Службы технической поддержки направляет ответ на ваш вопрос через систему Kaspersky CompanyAccount по адресу электронной почты, который вы указали при регистрации.

Электронный запрос в Вирусную лабораторию

Некоторые запросы требуется направлять не в Службу технической поддержки, а в Вирусную лабораторию.

Вы можете направлять запросы в Вирусную лабораторию в следующих случаях:

- если вы подозреваете, что файл или веб-ресурс содержит вирус, но Kaspersky Security Center не обнаруживает наличие угроз. Специалисты Вирусной лаборатории анализируют присылаемый файл или веб-адрес и при обнаружении неизвестного ранее вируса добавляют информацию о нем в базу данных, доступную при обновлении антивирусных программ «Лаборатории Касперского»;
- если Kaspersky Security Center определяет файл или веб-ресурс как содержащий вирус, но вы уверены, что файл или веб-ресурс не представляет угрозы.

Вы также можете направлять запросы в Вирусную лабораторию со страницы с формой запроса (http://support.kaspersky.ru/virlab/helpdesk.html), не регистрируясь в Kaspersky CompanyAccount. При этом вам не требуется указывать код активации программы. Приоритет заявок, созданных через форму запроса, ниже, чем у запросов, созданных через Kaspersky CompanyAccount.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» – известный в мире производитель систем защиты компьютеров от угроз: 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 для конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). По результатам исследования КОМКОН TGI-Russia 2009, «Лаборатория Касперского» – самый предпочитаемый производитель систем защиты для домашних пользователей в России.

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с центральным офисом в Москве и пятью региональными дивизионами, управляющими деятельностью компании в России, Западной и Восточной Европе, на Ближнем Востоке, в Африке, в Северной и Южной Америке, в Японии, Китае и других странах Азиатско-Тихоокеанского региона. В компании работает более 2000 квалифицированных специалистов.

Продукты. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает антивирусные приложения для настольных компьютеров и ноутбуков, для карманных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает программы и сервисы для защиты рабочих станций, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации 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 новых компьютерных угроз, создают средства их обнаружения и лечения и включают их в базы, используемые программами «Лаборатории Касперского». *Антивирусная база «Лаборатории Касперского» обновляется ежечасно*, *база Анти-Спама – каждые 5 минут*.

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 программ: среди них SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2010 году Антивирус Касперского получил несколько высших наград Advanced+ в тестах, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 300 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 200 тысяч.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Вирусная лаборатория:	newvirus@kaspersky.com (только для отправки возможно зараженных файлов в архивированном виде)
	http://support.kaspersky.ru/virlab/helpdesk.html
	(для запросов вирусным аналитикам)
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.

О ТЕХНОЛОГИИ NAC/ARP ENFORCEMENT

NAC/ARP Enforcement технология является правовой технологией для обеспечения и регулирования доступа к корпоративной сети путем соблюдения корпоративных политик безопасности для устройств.

Поведение и обязанности пользователя

Пользователь соглашается соблюдать применимые местные, государственные, национальные, международные и наднациональные законы и правила, а также спецификации, упомянутые в документации или соответствующих документах авторизованного поставщика, у которого пользователь приобрел программное обеспечение. Пользователь также соглашается:

- не использовать программное обеспечение для незаконных целей;
- не передавать или хранить данные, которые нарушают права интеллектуальной собственности или иные другие права третьих лиц, или являются незаконными, неразрешенными, клеветническими, оскорбительными, или нарушают конфиденциальность третьих лиц;
- не передавать или хранить данные, принадлежащие третьим лицам без заранее предусмотренного законом согласия владельца данных для передачи данных;
- не передавать данные, содержащие компьютерные вирусы или другие вредные компьютерные коды, файлы или программы;
- не проводить любые акты вмешательства или прерывания работы сервера или сетей, которые связаны с программным обеспечением;
- не пытаться получить несанкционированный доступ к компьютерным системам или сетям, которые связаны с программным обеспечением.

При использовании программного обеспечения пользователь ограничен конкретными правовыми рамками, действующими в стране, где программное обеспечение используется. Пожалуйста, обратите внимание, что использование этого программного обеспечения может повлиять на положения Закона о защите данных на уровне ЕС или на уровне государств — членов ЕС. Кроме того, при эксплуатации программного обеспечения, возможно, потребуется учесть положения коллективного трудового права.

ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА С ИСПОЛЬЗОВАНИЕМ KASPERSKY SECURITY NETWORK

«Лаборатория Касперского» предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков «Лаборатории Касперского» обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте «Лаборатории Касперского».

УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

ActiveSync, Microsoft, Windows, SQL Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Apple – зарегистрированный товарный знак Apple Inc.