

Kaspersky Security 10 для мобильных устройств

KASPERSKY[®] anti

Руководство по внедрению

Уважаемый пользователь!

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

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

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

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

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

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

Дата редакции документа: 22.01.2013

© ЗАО «Лаборатория Касперского», 2013

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

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ	5
В этом документе	5
Условные обозначения.....	7
ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ.....	8
Источники информации для самостоятельного поиска	8
Обсуждение программ «Лаборатории Касперского» на форуме	9
Обращение в Департамент продаж.....	9
Обращение в Отдел локализации и разработки технической документации	9
KASPERSKY SECURITY 10 ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ	10
Что нового	11
Комплект поставки.....	12
Полный дистрибутив Kaspersky Security 10	13
Дистрибутив плагина управления Kaspersky Security 10 для мобильных устройств.....	13
Дистрибутивы для самостоятельной установки	14
Аппаратные и программные требования	14
ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ ПРОГРАММЫ.....	15
Схемы развертывания программы для устройств под управлением Android	15
Схема развертывания через рассылку электронных сообщений	16
Схема развертывания через рассылку текстовых сообщений	17
Схема развертывания через рабочую станцию.....	18
Установка программы на устройство без участия администратора	18
Схема развертывания программы для устройств под управлением iOS.....	19
Схема развертывания программы для устройств под управлением BlackBerry, Symbian и Windows Mobile.....	20
ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ	21
Установка Сервера администрирования.....	22
Обновление компонента Сервер администрирования.....	22
Настройка параметров Сервера администрирования	23
Установка плагина управления Kaspersky Security для мобильных устройств.....	23
Развертывание Сервера мобильных устройств iOS MDM и подключение к нему устройств пользователей.....	24
Настройка рассылки электронных сообщений	24
Настройка способов доставки текстовых сообщений	25
Создание группы	26
Создание правила автоматического переноса устройств в группу администрирования.....	27
Создание групповой политики для Kaspersky Security 10 для мобильных устройств.....	28
ОБНОВЛЕНИЕ ПРЕДЫДУЩЕЙ ВЕРСИИ ПРОГРАММЫ.....	32
УСТАНОВКА НА УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ ANDROID.....	33
Установка программы через рассылку электронных сообщений.....	33
Создание инсталляционного пакета	33
Настройка параметров инсталляционного пакета	35
Создание автономного пакета установки	35
Рассылка электронных сообщений пользователям.....	36
Установка программы на мобильном устройстве после получения сообщения по электронной почте ..	37

Установка программы через рассылку текстовых сообщений	37
Создание инсталляционного пакета	37
Настройка параметров инсталляционного пакета	39
Создание автономного пакета установки	39
Рассылка текстовых сообщений пользователям	40
Установка программы на мобильном устройстве после получения текстового сообщения	40
Установка программы через рабочую станцию	41
Создание инсталляционного пакета	41
Настройка параметров инсталляционного пакета	43
Создание задачи удаленной установки	43
Доставка дистрибутива программы на мобильное устройство через рабочую станцию	45
Установка программы на мобильном устройстве через рабочую станцию	45
Установка программы без участия администратора	46
УСТАНОВКА НА УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ IOS	47
Настройка интерфейса Kaspersky Security Center для управления мобильными устройствами	47
Создание и рассылка iOS MDM-профиля	47
Установка программы на мобильное устройство iOS	48
УСТАНОВКА ЧЕРЕЗ РАБОЧИЕ СТАНЦИИ НА УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ BLACKBERRY, SYMBIAN И WINDOWS MOBILE	49
ПОДГОТОВКА ПРОГРАММЫ К РАБОТЕ НА УСТРОЙСТВЕ	50
АКТИВАЦИЯ ПРОГРАММЫ	51
УДАЛЕНИЕ ПРОГРАММЫ	52
Удаление программы с устройства под управлением Android	52
Разрешение пользователям удалять программу	52
Удаление программы с устройства без участия пользователя	53
Удаление программы с устройства под управлением BlackBerry, Symbian и Windows Mobile	54
Удаление программы с устройства под управлением iOS	55
ОБМЕН ИНФОРМАЦИЕЙ С KASPERSKY SECURITY NETWORK	56
ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ	57
Способы получения технической поддержки	57
Техническая поддержка по телефону	57
Получение технической поддержки через Kaspersky CompanyAccount	57
Электронный запрос в Службу технической поддержки	59
Электронный запрос в Антивирусную лабораторию	59
Электронный запрос на подпись APN-сертификата	59
ГЛОССАРИЙ	60
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»	62
ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ	63
УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ	63
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ	64

ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой *Руководство по внедрению Kaspersky Security 10 для мобильных устройств*.

Руководство адресовано техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Security 10 для мобильных устройств (далее Kaspersky Security), поддержка организаций, использующих программу.

Руководство предназначено для следующих целей:

- Дать общее описание принципов работы Kaspersky Security 10, системных требований, типичных сценариев развертывания, особенностей интеграции с другими приложениями.
- Помочь спланировать развертывание Kaspersky Security 10 для мобильных устройств в сети предприятия.
- Описать подготовку к установке Kaspersky Security 10 для мобильных устройств, установку и активацию программы.
- Дать рекомендации по поддержке и администрированию Kaspersky Security 10 для мобильных устройств после установки.
- Рассказать о дополнительных источниках информации о программе и способах получения технической поддержки.

В ЭТОМ РАЗДЕЛЕ

В этом документе.....	5
Условные обозначения	7

В ЭТОМ ДОКУМЕНТЕ

Этот документ содержит следующие разделы.

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 10 для мобильных устройств (см. стр. [10](#))

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security 10 для мобильных устройств.

Типичные схемы развертывания программы (см. стр. [15](#))

В этом разделе описаны типичные схемы развертывания Kaspersky Security 10 для мобильных устройств.

Подготовка к установке программы (см. стр. [21](#))

В этом разделе описана процедура настройки управления мобильными устройствами через Kaspersky Security Center для развертывания программы Kaspersky Security.

Обновление предыдущей версии программы (см. стр. [32](#))

В этом разделе представлена информация об обновлении предыдущей версии Kaspersky Security 10 для мобильных устройств.

Установка на устройства под управлением Android (см. стр. [33](#))

В этом разделе описаны варианты установки Kaspersky Security 10 для мобильных устройств на устройства под управлением операционной системы Android™.

Установка на устройства под управлением iOS (см. стр. [47](#))

В этом разделе описана процедура установки Kaspersky Security 10 для мобильных устройств на устройства под управлением операционной системы iOS.

Установка через рабочие станции на устройства под управлением BlackBerry, Symbian и Windows Mobile (см. стр. [49](#))

В этом разделе описана процедура установки Kaspersky Security 10 для мобильных устройств на устройства под управлением операционных систем BlackBerry®, Symbian и Windows® Mobile.

Подготовка программы к работе на устройстве (см. стр. [50](#))

В этом разделе представлена информация о первоначальной настройке параметров подключения к Серверу администрирования на устройствах пользователей.

Активация программы (см. стр. [51](#))

В этом разделе представлена информация об активации программы.

Удаление программы (см. стр. [52](#))

В этом разделе представлена информация об удалении программы Kaspersky Security 10 для мобильных устройств с устройств пользователей.

Обмен информацией с Kaspersky Security Network (см. стр. [56](#))

В этом разделе представлена информация о взаимодействии программы Kaspersky Security с облачным сервисом Kaspersky Security Network.

Обращение в Службу технической поддержки (см. стр. [57](#))

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

Глоссарий

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

ЗАО «Лаборатория Касперского»

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

Информация о стороннем коде

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

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 <i>Базы устарели</i> .	Курсивом выделены следующие смысловые элементы текста: <ul style="list-style-type: none"> 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 <code>help</code> Появится следующее сообщение: Укажите дату в формате ДД:ММ:ГГ.	Специальным стилем выделены следующие типы текста: <ul style="list-style-type: none"> 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.....	8
Обсуждение программ «Лаборатории Касперского» на форуме.....	9
Обращение в Департамент продаж.....	9
Обращение в Отдел локализации и разработки технической документации.....	9

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. [57](#)).

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/targeted_security) 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/ks10mob>) 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, 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.

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 ДЕПАРТАМЕНТ ПРОДАЖ

Если у вас возникли вопросы по выбору, приобретению или продлению срока использования программы, вы можете связаться с нашими специалистами из Департамента продаж одним из следующих способов:

- Позвонив по телефонам нашего центрального офиса в Москве (<http://www.kaspersky.ru/contacts>).
- Отправив письмо с вопросом по электронному адресу sales@kaspersky.com.

Обслуживание осуществляется на русском и английском языках.

ОБРАЩЕНИЕ В ОТДЕЛ ЛОКАЛИЗАЦИИ И РАЗРАБОТКИ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

Для обращения в Группу разработки документации требуется отправить письмо по адресу docfeedback@kaspersky.com. В качестве темы письма нужно указать «Kaspersky Help Feedback: Kaspersky Security 10 для мобильных устройств».

KASPERSKY SECURITY 10 ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Kaspersky Security 10 для мобильных устройств обеспечивает защиту мобильных устройств, работающих под управлением операционных систем Android, iOS, BlackBerry, Microsoft® Windows Mobile и Symbian, от вирусов и других программ, представляющих угрозу, нежелательных вызовов и SMS, а также веб-угроз. Программа позволяет контролировать сетевую активность пользователя, а также защищать конфиденциальную информацию от несанкционированного доступа. Для защиты от каждого вида угроз предназначены разные компоненты. Это дает возможность гибко настраивать параметры программы в зависимости от нужд конкретного пользователя. Доступность компонентов зависит от операционной системы мобильного устройства.

Kaspersky Security 10 для мобильных устройств поддерживает работу с системой удаленного администрирования Kaspersky Security Center. С помощью этой системы администратор сети организации может дистанционно:

- устанавливать программу на мобильные устройства;
- настраивать параметры работы программы как для группы устройств, так и индивидуально для каждого отдельного устройства;
- формировать отчеты о работе компонентов программы, установленной на мобильных устройствах;
- удалять программу с Android-устройств.

В Kaspersky Security 10 для мобильных устройств включены следующие компоненты защиты:

- **Антивирус.** Позволяет обнаруживать и устранять угрозы на мобильном устройстве, используя антивирусные базы программы и дополнительно облачный сервис Kaspersky Security Network. В состав Антивируса входят следующие компоненты: защита, проверка и обновление.
- **Защита** позволяет обнаруживать угрозы в открытых файлах, а также проверять новые программы и предотвращать заражение устройства в режиме реального времени.
- **Проверка** запускается по требованию для всей файловой системы, оперативной памяти или папки. Полная проверка позволяет проверить на наличие вредоносных объектов всю файловую систему устройства, а проверка папки — конкретную папку. Полная проверка и проверка папки обнаруживают угрозы в файлах, которые установлены и не открыты, а также угрозы в файлах, которые открыты в данный момент. Проверка памяти позволяет обнаружить угрозы только в тех файлах, которые открыты в данный момент.
- **Обновление** позволяет загружать новые антивирусные базы программы.
- **Личные контакты.** Позволяет скрывать конфиденциальную информацию пользователя в то время, когда его устройство используют другие лица. Компонент скрывает или отображает всю информацию, связанную с указанными номерами абонентов, например, данные в списке контактов, а также историю разговоров и SMS-переписку с этими контактами. Компонент позволяет также скрывать доставку входящих вызовов и SMS с указанных номеров абонентов.
- **Анти-Вор.** Защищает информацию на устройстве от несанкционированного доступа в случае потери или кражи устройства. Компонент предоставляет возможность с помощью SMS-команды или при помощи Kaspersky Security Center заблокировать устройство, найти его, или удалить с него данные.
- **Фильтр вызовов и SMS.** Компонент позволяет блокировать нежелательные сообщения и вызовы в зависимости от выбранного режима. Фильтрация сообщений и вызовов осуществляется с помощью списков разрешенных и запрещенных контактов. В зависимости от настроек компонент блокирует или доставляет вызовы и SMS от запрещенных и разрешенных контактов. Дополнительно к выбранному режиму компонент позволяет включить разрешение входящих событий со всех номеров из записной книги устройства (Контактов) или блокирование входящих событий с номеров, содержащих буквы.

- **Веб-Фильтр.** Позволяет блокировать вредоносные веб-сайты, цель которых — распространить вредоносный код, а также поддельные (фишинговые) веб-сайты, цель которых — украсть конфиденциальные данные пользователя, такие как пароли от онлайн-банков, онлайн-аукционов или систем оплаты, и получить доступ к его финансовым счетам. Компонент проверяет веб-сайты до открытия, используя облачный сервис Kaspersky Security Network. По результатам проверки Веб-Фильтр загружает веб-сайт, который признан надежным, и блокирует веб-сайт, который признан вредоносным. Компонент также поддерживает фильтрацию веб-сайтов по категориям, определенным в Kaspersky Security Network, что позволяет администратору ограничить доступ, например, к веб-страницам в категории «Азартные игры» или «Социальные сети».
- **Сетевой экран.** Контролирует сетевые подключения на мобильном устройстве. Компонент позволяет задать соединения, которые будут разрешены или заблокированы.
- **Контроль программ.** Позволяет через Kaspersky Security Center настроить параметры запуска программ на мобильном устройстве пользователя. Администратор имеет возможность указать программы, обязательные к установке на устройстве пользователя, а также создать списки разрешенных и запрещенных для запуска программ. Компонент блокирует попытки запуска запрещенных программ, информация о таких попытках доступна в отчетах Kaspersky Security Center. Компонент также поддерживает создание и использование контейнера — специальной оболочки для мобильных программ, позволяющей контролировать действия содержащейся в контейнере программы, тем самым защищая корпоративные данные на устройстве. Программы в контейнере можно использовать как разрешенные или обязательные к установке программы.
- **Управление устройством.** Позволяет настроить обязательное использование пароля для разблокировки мобильного устройства, а также минимальную длину этого пароля. Кроме того, позволяет запретить использование на устройстве Wi-Fi сетей, камеры или Bluetooth.
- **Шифрование.** Защищает информацию от просмотра посторонними лицами при несанкционированном доступе к устройству. После перехода устройства в режим энергосбережения компонент шифрует выбранные несистемные папки, сохраненные в памяти устройства или на карте памяти. Данные в зашифрованных папках доступны только после ввода секретного кода.

В ЭТОМ РАЗДЕЛЕ

Что нового.....	11
Комплект поставки.....	12
Аппаратные и программные требования.....	14

Что нового

Отличия Kaspersky Security 10 для мобильных устройств от предыдущей версии программы состоят в следующем:

- Добавлена схема развертывания программы на Android-устройствах через Kaspersky Security Center с помощью рассылки текстовых сообщений на телефонные номера пользователей или сообщений корпоративной электронной почты на корпоративные почтовые адреса пользователей.
- Добавлена поддержка устройств с операционной системой Android версии 4.0 и выше.
- Добавлена поддержка устройств с операционной системой iOS. На этих устройствах Kaspersky Security 10 выполняет блокирование веб-сайтов заданных категорий и обнаруживает взлом системы (jailbreak).
- Добавлена дистанционная установка программы на iOS-устройства и ее дальнейшее администрирование при помощи Kaspersky Security Center.
- Добавлена возможность блокирования веб-ресурсов на основе категорий, заданных в облачном сервисе Kaspersky Security Network, что позволяет ограничить доступ к веб-ресурсам, квалифицированным как вредоносные или фишинговые, а также к веб-ресурсам из категорий, выбранных в качестве нежелательных.

- Добавлена поддержка создания и использования контейнеров – мобильных программ в специальной оболочке, позволяющей контролировать действия содержащейся в контейнере программы, тем самым защищая корпоративные данные на устройстве. Программы в контейнере можно использовать как разрешенные или обязательные к установке программы.
- Добавлена эвристическая проверка при функционировании защиты.
- Добавлено обнаружение доступа к устройству с правами администратора (root-доступа) для Android-устройств и jailbreak для iOS-устройств, а также выбор действий в случае их обнаружения.
- Для Android-устройств добавлены следующие возможности:
 - возможность через Kaspersky Security Center указывать программы, разрешенные или запрещенные к запуску на устройстве, а также задать программы, обязательные к установке на устройстве пользователя.
 - проверка новых программ сразу после установки при помощи облачного сервиса Kaspersky Security Network.
 - обнаружение рекламных программ и программ, которые могут быть использованы злоумышленниками для нанесения вреда устройству или корпоративным данным пользователя.
 - активация программы Kaspersky Security 10 как Администратора устройства. Это предоставляет расширенные возможности для защиты Android-устройств.
 - удаление программы с устройства из ее параметров на устройстве или дистанционно через Kaspersky Security Center.
- Расширена функциональность компонента Анти-Вор: теперь можно дистанционно запустить функции Анти-Вора и удалить все данные с устройства при помощи команды, отправленной из Kaspersky Security Center.
- Улучшена функциональность компонента Фильтр вызовов и SMS: для списков разрешенных и запрещенных контактов добавлена возможность импорта из журнала вызовов и списка SMS-сообщений.
- Расширен список событий, которые фиксируются в отчеты о работе программы.

КОМПЛЕКТ ПОСТАВКИ

В состав дистрибутива программы Kaspersky Security 10 для мобильных устройств входит следующее:

- `sc_package` — набор установочных файлов (см. раздел «Полный дистрибутив Kaspersky Security 10» на стр. [13](#)) для четырех поддерживаемых программой Kaspersky Security 10 операционных систем.
- `ak_plugin` — плагин управления программой (см. раздел «Дистрибутив плагина управления Kaspersky Security 10 для мобильных устройств» на стр. [13](#)) Kaspersky Security 10 с помощью Kaspersky Security Center.
- `standalone` — установочные файлы программы (см. раздел «Дистрибутивы для самостоятельной установки» на стр. [14](#)) для всех поддерживаемых операционных систем; могут использоваться для установки программы без участия администратора.

В ЭТОМ РАЗДЕЛЕ

Полный дистрибутив Kaspersky Security 10.....	13
Дистрибутив плагина управления Kaspersky Security 10 для мобильных устройств.....	13
Дистрибутивы для самостоятельной установки	14

Полный дистрибутив KASPERSKY SECURITY 10

В состав дистрибутива программы входит самораспаковывающийся архив `sc_package`, который содержит файлы, необходимые для установки программы на мобильных платформах Android, BlackBerry, Symbian и Windows Mobile:

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` — набор файлов, необходимый для установки программы на устройства с операционной системой Android;
- `endpoint_8_0_0_37_ru.cab` — установочный файл программы для операционной системы Microsoft Windows Mobile;
- `endpoint8_mobile_8_1_44_ru.sisx` — установочный файл программы для операционной системы Symbian;
- `endpoint8_Mobile_8_1_29_ru.zip` — установочный файл программы для операционной системы BlackBerry;
- `installer.ini` — конфигурационный файл с параметрами подключения к Серверу администрирования;
- `KSM_10_1_75_ru.apk` — установочный файл программы для операционной системы Android;
- `kmlisten.exe` — утилита доставки инсталляционного пакета на мобильное устройство через рабочую станцию;
- `kmlisten.ini` — конфигурационный файл с настройками для утилиты доставки инсталляционного пакета;
- `kmlisten.kpd` — файл с описанием программы.
- комплект документации:
 - Руководство по внедрению Kaspersky Security 10 для мобильных устройств;
 - контекстная справка плагина управления Kaspersky Security 10 для мобильных устройств;
 - контекстная справка программы для операционной системы Android;
 - контекстная справка программы для операционной системы iOS;
 - контекстная справка программы для операционной системы BlackBerry;
 - контекстная справка программы для операционной системы Symbian;
 - контекстная справка программы для операционной системы Windows Mobile.

Дистрибутив плагина управления KASPERSKY SECURITY 10 для мобильных устройств

В состав дистрибутива программы входит самораспаковывающийся архив `ak_plugin`, который содержит исполняемый файл `klcfginst.exe` — установочный файл плагина управления программой Kaspersky Security 10 для мобильных устройств с помощью системы удаленного администрирования Kaspersky Security Center.

ДИСТРИБУТИВЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ УСТАНОВКИ

В состав дистрибутива программы входит папка `standalone`, которая содержит установочные файлы для всех поддерживаемых операционных систем:

- `KSM_10_1_75_ru.apk` — установочный файл программы Kaspersky Security 10 для операционной системы Android;
- `KSM_10_1_32_unsigned.app.zip` — установочный файл программы Kaspersky Security 10 для операционной системы iOS;
- `endpoint_8_0_0_37_ru.cab` — установочный файл программы для операционной системы Microsoft Windows Mobile;
- `endpoint8_mobile_8_1_44_ru.sisx` — установочный файл программы для операционной системы Symbian;
- `endpoint8_Mobile_8_1_29_ru.zip` — установочный файл программы для операционной системы BlackBerry;
- Комплект документации:
 - Руководство по внедрению Kaspersky Security 10 для мобильных устройств;
 - контекстная справка плагина управления Kaspersky Security 10 для мобильных устройств;
 - контекстная справка программы для операционной системы Android;
 - контекстная справка программы для операционной системы Microsoft Windows Mobile;
 - контекстная справка программы для операционной системы Symbian OS;
 - контекстная справка программы для операционной системы BlackBerry.

АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ

Для работы программы Kaspersky Security 10 для мобильных устройств на мобильных устройствах пользователей устройства должны удовлетворять следующим программным требованиям:

- Android 2.2, 2.3, 3.0, 3.1, 3.2, 4.0, 4.1.
- Apple iOS 4.0, 4.1, 4.2, 4.3, 5.0, 5.1, 6.0.
- BlackBerry 4.5, 4.6, 4.7, 5.0, 6.0, 7.0, 7.1.
- Symbian OS 9.1, 9.2, 9.3, 9.4 Series 60® UI.
- Symbian^3, Symbian Anna, Symbian Belle (только для мобильных устройств Nokia®).
- Windows Mobile 5.0, 6.0, 6.1, 6.5.

Для развертывания Kaspersky Security 10 для мобильных устройств в сети система удаленного администрирования должна удовлетворять следующим программным требованиям:

- Kaspersky Security Center 10.0.

ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ ПРОГРАММЫ

В этом разделе описаны типичные схемы развертывания Kaspersky Security 10 для мобильных устройств.

Схемы развертывания Kaspersky Security зависят от того, какая операционная система установлена на мобильных устройствах пользователей.

В ЭТОМ РАЗДЕЛЕ

Схемы развертывания программы для устройств под управлением Android[15](#)

Схема развертывания программы для устройств под управлением iOS[19](#)

Схема развертывания программы для устройств под управлением BlackBerry, Symbian и Windows Mobile[20](#)

СХЕМЫ РАЗВЕРТЫВАНИЯ ПРОГРАММЫ ДЛЯ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ ANDROID

Установка программы на устройства под управлением операционной системы Android может быть выполнена следующими способами:

- Через рассылку пользователям электронных сообщений со ссылкой на дистрибутив программы (см. раздел «Схема развертывания через рассылку электронных сообщений» на стр. [16](#)).
- Через рассылку пользователям текстовых сообщений (SMS) со ссылкой на дистрибутив программы (см. раздел «Схема развертывания через рассылку текстовых сообщений» на стр. [17](#)).
- Через рабочие станции, к которым пользователи подключают мобильные устройства (см. раздел «Схема развертывания через рабочую станцию» на стр. [18](#)).

Перед установкой программы вам требуется включить мобильные устройства пользователей в состав управляемых компьютеров и создать групповую политику, чтобы передать на мобильные устройства данные о лицензии и параметры работы программы. После этого вы готовите дистрибутив программы для установки на мобильные устройства пользователей. Копирование дистрибутива на мобильные устройства и установку программы на мобильных устройствах пользователи выполняют самостоятельно.

Пользователи могут также установить дистрибутив Kaspersky Security на свое мобильное устройство без участия администратора (см. раздел «Установка программы на устройство без участия администратора» на стр. [18](#)), как стандартное Android-приложение.

В ЭТОМ РАЗДЕЛЕ

Схема развертывания через рассылку электронных сообщений[16](#)

Схема развертывания через рассылку текстовых сообщений[17](#)

Схема развертывания через рабочую станцию[18](#)

Установка программы на устройство без участия администратора[18](#)

СХЕМА РАЗВЕРТЫВАНИЯ ЧЕРЕЗ РАССЫЛКУ ЭЛЕКТРОННЫХ СООБЩЕНИЙ

Схема развертывания программы через рассылку по электронной почте позволяет доставить пользователям специально подготовленный дистрибутив программы, содержащий настройки подключения к Серверу администрирования, так что пользователям не потребуется указывать их вручную. Такой дистрибутив называется автономный пакет установки.

Схема состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Security Center. На этом этапе обеспечивается возможность подключения мобильных устройств к Серверу администрирования (см. раздел «Подготовка к установке программы» на стр. [21](#)).
2. Установка плагина управления Kaspersky Security 10 для мобильных устройств.
3. Создание групп для мобильных устройств в составе управляемых компьютеров в системе Kaspersky Security Center.

В эти группы вручную или на основании правил автоматического переноса будут помещаться устройства с установленной программой Kaspersky Security 10 для мобильных устройств.

4. Создание групповой политики для управления параметрами Kaspersky Security 10 для мобильных устройств.
5. Создание правила автоматического перемещения мобильных устройств в группу.
6. Проверка учетных записей пользователей на наличие адреса электронной почты.
7. Создание инсталляционного пакета для Kaspersky Security 10 для мобильных устройств.
8. Настройка параметров инсталляционного пакета для Kaspersky Security 10 для мобильных устройств.
9. Создание автономного пакета установки для Kaspersky Security 10 для мобильных устройств.

На этом этапе автономный пакет содержит настройки подключения к Серверу администрирования и доступен в папке общего доступа и на веб-сервере Kaspersky Security Center. При формировании рассылки вы можете выбрать любой из ресурсов и указать ссылку на нужный, либо включить автономный пакет установки в состав письма как вложенный файл.

10. Формирование и отправка письма со ссылкой на автономный пакет пользователям мобильных устройств.

Ссылка может быть отправлена в виде текста или в виде QR-кода для считывания непосредственно на мобильном устройстве.

11. Скачивание автономного пакета установки на мобильное устройство. На этом этапе пользователь загружает на устройство заранее настроенный дистрибутив программы, приложенный к письму или размещенный на доступном ресурсе.
12. Установка программы на мобильном устройстве.
13. Активация программы (см. стр. [51](#)) на мобильных устройствах пользователей.

Вышеописанная схема развертывания программы на устройства под управлением Android подходит только для установки Kaspersky Security 10 для мобильных устройств. Плагин управления Kaspersky Security 10 для Kaspersky Security Center поддерживает также управление устройствами с установленной предыдущей версией программы. Для использования полной функциональности программы специалисты «Лаборатории Касперского» рекомендуют обновить предыдущую версию (см. раздел «Обновление предыдущей версии программы» на стр. [32](#)).

СХЕМА РАЗВЕРТЫВАНИЯ ЧЕРЕЗ РАССЫЛКУ ТЕКСТОВЫХ СООБЩЕНИЙ

Схема развертывания программы через рассылку с помощью текстовых сообщений позволяет доставить пользователям специально подготовленный дистрибутив программы, содержащий настройки подключения к Серверу администрирования, так что пользователям не потребуется указывать их вручную. Такой дистрибутив называется автономный пакет установки.

Рассылка текстовых сообщений (SMS) со ссылкой на автономный пакет установки возможна только на устройства с GSM-модулем.

Схема состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Security Center. На этом этапе обеспечивается возможность подключения мобильных устройств к Серверу администрирования (см. раздел «Подготовка к установке программы» на стр. [21](#)).
2. Установка плагина управления Kaspersky Security 10 для мобильных устройств.
3. Создание групп для мобильных устройств в составе управляемых компьютеров в системе Kaspersky Security Center.

В эти группы вручную или основании правил автоматического переноса будут помещаться устройства с установленной программой Kaspersky Security 10 для мобильных устройств.

4. Создание групповой политики для управления параметрами Kaspersky Security 10 для мобильных устройств.
5. Создание правила автоматического перемещения мобильных устройств в группу.
6. Настройка способа доставки текстовых сообщений (SMS) пользователям.
7. Проверка учетных записей пользователей на наличие телефонных номеров.
8. Создание инсталляционного пакета для Kaspersky Security 10 для мобильных устройств.
9. Настройка параметров инсталляционного пакета для Kaspersky Security 10 для мобильных устройств.
10. Создание автономного пакета установки для Kaspersky Security 10 для мобильных устройств.

На данном этапе автономный пакет содержит настройки подключения к Серверу администрирования и доступен в папке общего доступа и на веб-сервере Kaspersky Security Center. При формировании рассылки вам необходимо выбрать путь на веб-сервер Kaspersky Security Center.

11. Формирование и отправка текстового сообщения со ссылкой на автономный пакет установки пользователям мобильных устройств.
12. Загрузка автономного пакета установки на мобильное устройство. На этом этапе пользователь загружает на устройство подготовленный дистрибутив программы с веб-сервера Kaspersky Security Center.
13. Установка программы на мобильном устройстве.
14. Активация программы (см. стр. [51](#)) на мобильных устройствах пользователей.

Вышеописанная схема развертывания программы на устройства под управлением Android подходит только для установки Kaspersky Security 10 для мобильных устройств. Плагин управления Kaspersky Security 10 для Kaspersky Security Center поддерживает также управление устройствами с установленной предыдущей версией программы. Для использования полной функциональности программы специалисты «Лаборатории Касперского» рекомендуют обновить предыдущую версию (см. раздел «Обновление предыдущей версии программы» на стр. [32](#)).

СХЕМА РАЗВЕРТЫВАНИЯ ЧЕРЕЗ РАБОЧУЮ СТАНЦИЮ

Развертывание программы через рабочую станцию используется в том случае, когда пользователи подключают мобильные устройства к рабочим компьютерам.

Развертывание через рабочую станцию состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Security Center. На этом этапе обеспечивается возможность подключения мобильных устройств к Серверу администрирования (см. раздел «Подготовка к установке программы» на стр. [21](#)).

2. Установка плагина управления Kaspersky Security 10 для мобильных устройств.

3. Создание групп для мобильных устройств в составе управляемых компьютеров в системе Kaspersky Security Center.

В эти группы вручную или в основании правил автоматического переноса будут помещаться устройства с установленной программой Kaspersky Security 10 для мобильных устройств.

4. Создание правила автоматического перемещения мобильных устройств в группу.
5. Создание групповой политики для управления параметрами Kaspersky Security 10 для мобильных устройств.
6. Создание инсталляционного пакета для задачи удаленной установки Kaspersky Security 10 для мобильных устройств.
7. Настройка параметров инсталляционного пакета для задачи удаленной установки Kaspersky Security 10 для мобильных устройств.
8. Создание задачи удаленной установки, с помощью которой на рабочие станции пользователей доставляется дистрибутив программы Kaspersky Security 10 для мобильных устройств и устанавливается утилита доставки дистрибутива на мобильные устройства.
9. Загрузка дистрибутива программы на мобильное устройство. На этом этапе пользователь при помощи утилиты kmlisten.exe копирует дистрибутив программы на мобильное устройство.
10. Установка программы на мобильном устройстве. На этом этапе пользователь выполняет установку программы на мобильном устройстве.
11. Активация программы (см. стр. [51](#)) на мобильном устройстве пользователя.

УСТАНОВКА ПРОГРАММЫ НА УСТРОЙСТВО БЕЗ УЧАСТИЯ АДМИНИСТРАТОРА

Непосредственная загрузка установочного файла на устройство используется в случаях, когда пользователям удобно самостоятельно установить программу, например, скачав установочный файл на Google Play.

В этом случае вы не готовите дистрибутив программы, и пользователь самостоятельно указывает параметры подключения к Серверу администрирования (см. раздел «Подготовка программы к работе на устройстве» на стр. [50](#)) при первом запуске программы.

Схема развертывания состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Security Center. На этом этапе обеспечивается возможность подключения мобильных устройств к Серверу администрирования (см. раздел «Подготовка к установке программы» на стр. [21](#)).
2. Установка плагина управления Kaspersky Security 10 для мобильных устройств.

3. Создание групп для размещения мобильных устройств, на которые будет доставляться дистрибутив программы Kaspersky Security 10 для мобильных устройств.
4. Создание правила автоматического перемещения мобильных устройств в группу.
5. Создание политики для управления параметрами Kaspersky Security 10 для мобильных устройств.
6. Установка программы на мобильном устройстве. На этом этапе пользователь выполняет установку программы на мобильном устройстве.
7. Первоначальная настройка программы. На этом этапе пользователь указывает настройки подключения мобильного устройства к Серверу администрирования (см. раздел «Подготовка программы к работе на устройстве» на стр. [50](#)).
8. Активация программы (см. стр. [51](#)) на мобильном устройстве.

СХЕМА РАЗВЕРТЫВАНИЯ ПРОГРАММЫ ДЛЯ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ iOS

Для доставки программы Kaspersky Security на устройства используются средства iOS MDM. С помощью политик, применяемых к группам управляемых устройств, осуществляется централизованное управление параметрами программы. Более подробную информацию см. в *Руководстве администратора Kaspersky Security Center*.

Развертывание программы на мобильные устройства под управлением операционной системы iOS осуществляется через iOS MDM сервер и состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Security Center. На этом этапе обеспечивается возможность подключения мобильных устройств к Серверу администрирования.
2. Развертывание Сервера мобильных устройств iOS MDM и подключение к нему устройств пользователей. На этом этапе обеспечивается возможность подключения мобильных устройств под управлением iOS к Серверу администрирования. Более подробную информацию см. в *Руководстве по внедрению Kaspersky Security Center*.
3. Установка плагина управления Kaspersky Security 10 для мобильных устройств.
4. Создание групп для централизованного управления параметрами программы, установленной на мобильных устройствах пользователей.
5. Создание правила автоматического перемещения обнаруженных при синхронизации мобильных устройств в группу.
6. Создание политики для управления параметрами Kaspersky Security 10 для мобильных устройств.
7. Проверка учетных записей пользователей на наличие адреса электронной почты или номера телефона для отправки текстового сообщения.
8. Создание iOS MDM-профиля для возможности управления устройством с помощью Kaspersky Security Center и доставка профиля на устройства пользователей (см. раздел «Создание и рассылка iOS MDM-профиля» на стр. [47](#)).
9. Установка iOS MDM-профиля на устройства пользователей (см. раздел «Создание и рассылка iOS MDM-профиля» на стр. [47](#)).
10. Установка программы (см. раздел «Установка программы на мобильное устройство iOS» на стр. [48](#)) на мобильные устройства пользователей. На этом этапе пользователь выполняет установку программы на мобильном устройстве.

11. Первоначальная настройка программы (см. раздел «Подготовка программы к работе на устройстве» на стр. [50](#)) на устройствах пользователей. На этом этапе пользователь указывает настройки подключения к Серверу администрирования.
12. Активация программы (см. стр. [51](#)) на мобильных устройствах пользователей.

СХЕМА РАЗВЕРТЫВАНИЯ ПРОГРАММЫ ДЛЯ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ BLACKBERRY, SYMBIAN И WINDOWS MOBILE

Комплект поставки Kaspersky Security 10 для мобильных устройств (см. раздел «Комплект поставки» на стр. [12](#)) содержит дистрибутивы программы для различных операционных систем. Для платформ BlackBerry, Symbian и Windows Mobile в него входят дистрибутивы Kaspersky Endpoint Security 8.0 for Smartphone.

Плагин управления Kaspersky Security 10 для мобильных устройств, который устанавливается в системе удаленного администрирования Kaspersky Security Center, поддерживает управление устройствами с программой Kaspersky Endpoint Security 8.0 for Smartphone.

Схема развертывания программы для устройств под управлением операционных систем BlackBerry, Symbian и Windows Mobile состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Security Center. На этом этапе обеспечивается возможность подключения мобильных устройств к Серверу администрирования (см. раздел «Подготовка к установке программы» на стр. [21](#)).
2. Установка плагина управления Kaspersky Security 10 для мобильных устройств.
3. Создание групп для мобильных устройств в составе управляемых компьютеров в системе Kaspersky Security Center.

В эти группы вручную или в основании правил автоматического переноса будут помещаться устройства с установленной программой Kaspersky Security 10 для мобильных устройств.
4. Создание правила автоматического перемещения мобильных устройств в группу.
5. Создание политики для управления параметрами Kaspersky Security 10 для мобильных устройств.
6. Создание инсталляционного пакета для задачи удаленной установки Kaspersky Security 10 для мобильных устройств.
7. Настройка параметров инсталляционного пакета для задачи удаленной установки Kaspersky Security 10 для мобильных устройств.
8. Создание задачи удаленной установки, с помощью которой на рабочие станции пользователей доставляется дистрибутив программы Kaspersky Endpoint Security 8.0 for Smartphone и устанавливается утилита доставки дистрибутива на мобильные устройства.
9. Доставка дистрибутива программы на мобильное устройство. На этом этапе пользователь при помощи утилиты kmlisten.exe копирует дистрибутив программы на мобильное устройство.
10. Установка программы на мобильном устройстве. На этом этапе пользователь выполняет установку программы на мобильном устройстве.
11. Активация программы (см. стр. [51](#)) на мобильных устройствах пользователей.

ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ

Перед тем как приступить к развертыванию программы Kaspersky Security, вам необходимо настроить управление мобильными устройствами через Kaspersky Security Center. Для этого следует выполнить следующие действия:

1. Установить или убедиться, что в сети организации установлены компоненты Kaspersky Security Center: Сервер администрирования и Консоль управления (см. *Руководство по развертыванию Kaspersky Security Center*).
2. Убедиться, что установленные компоненты соответствуют программным требованиям (см. раздел «Аппаратные и программные требования» на стр. [14](#)) для установки программы Kaspersky Security 10 для мобильных устройств.

При установке Сервера администрирования (см. раздел «Установка Сервера администрирования» на стр. [22](#)) должен быть установлен компонент Поддержка мобильных устройств, обеспечивающий управление защитой мобильных устройств через Kaspersky Security Center. Если этот компонент не был установлен или версия Сервера администрирования не соответствует требованиям для установки Kaspersky Security 10 для мобильных устройств, то администратору следует удалить старую версию компонента и установить ту версию, которая указана в программных требованиях, предварительно выполнив резервное копирование данных Сервера администрирования.

3. Настроить поддержку мобильных устройств в параметрах Сервера администрирования (см. раздел «Настройка параметров Сервера администрирования» на стр. [23](#)).
4. Установить на рабочем месте администратора плагин управления (см. раздел «Установка плагина управления Kaspersky Security для мобильных устройств» на стр. [23](#)) программой Kaspersky Security 10 для мобильных устройств.
5. Если это необходимо, развернуть Сервер мобильных устройств iOS MDM (см. раздел «Развертывание Сервера мобильных устройств iOS MDM и подключение к нему устройств пользователей» на стр. [24](#)).
6. Создать отдельную группу администрирования (см. раздел «Создание группы» на стр. [26](#)) для мобильных устройств.
7. Настроить параметры автоматического переноса (см. раздел «Создание правила автоматического переноса устройств в группу администрирования» на стр. [27](#)) всех устройств, на которые будет установлена программа, в эту группу.
8. Создать групповую политику (см. раздел «Создание групповой политики для Kaspersky Security 10 для мобильных устройств» на стр. [28](#)) для Kaspersky Security, которая будет применяться ко всем мобильным устройствам, помещенным в соответствующую группу администрирования.
9. Если это необходимо, настроить параметры рассылки электронных сообщений (см. раздел «Настройка рассылки электронных сообщений» на стр. [24](#)) пользователям (см. *Руководство администратора Kaspersky Security Center*).
10. Если это необходимо, настроить параметры рассылки текстовых сообщений (см. раздел «Настройка способов доставки текстовых сообщений» на стр. [25](#)) пользователям (см. *Руководство администратора Kaspersky Security Center*).

В ЭТОМ РАЗДЕЛЕ

Установка Сервера администрирования	22
Обновление компонента Сервер администрирования	22
Настройка параметров Сервера администрирования	23
Установка плагина управления Kaspersky Security для мобильных устройств	23
Развертывание Сервера мобильных устройств iOS MDM и подключение к нему устройств пользователей	24
Настройка рассылки электронных сообщений	24
Настройка способов доставки текстовых сообщений	25
Создание группы	26
Создание правила автоматического переноса устройств в группу администрирования	27
Создание групповой политики для Kaspersky Security 10 для мобильных устройств	28

УСТАНОВКА СЕРВЕРА АДМИНИСТРИРОВАНИЯ

Установка Сервера администрирования описана в *Руководстве по развертыванию Kaspersky Security Center*. Для обеспечения управления защитой мобильных устройств через Kaspersky Security Center на шаге **Выбор компонентов** необходимо установить флажок **Поддержка мобильных устройств**.

При установке компонента Поддержка мобильных устройств создается *сертификат Сервера администрирования для мобильных устройств*. Он используется для аутентификации мобильных устройств при обмене данными с Сервером администрирования. Обмен информацией производится с использованием SSL-протокола (Secure Socket Layer). Без сертификата для мобильных устройств на Сервере администрирования установить соединение между Сервером администрирования и мобильными устройствами невозможно.

Сертификат для мобильных устройств хранится в папке установки программы Kaspersky Security Center во вложенной папке Cert. При первой синхронизации мобильного устройства с Сервером администрирования копия сертификата доставляется на устройство и сохраняется на нем локально.

ОБНОВЛЕНИЕ КОМПОНЕНТА СЕРВЕР АДМИНИСТРИРОВАНИЯ

Если при установке Сервера администрирования не был установлен флажок **Поддержка мобильных устройств** или установлена устаревшая версия Kaspersky Security Center, в которой не поддерживается работа с Kaspersky Security 10 для мобильных устройств, то следует обновить установленную версию компонента Сервер администрирования.

➡ Чтобы обновить установленную версию компонента Сервер администрирования, выполните следующие действия:

1. Выполните резервное копирование данных Сервера администрирования (см. *Руководство администратора Kaspersky Security Center*).
2. Установите версию Сервера администрирования, которая указана в программных требованиях для установки программы Kaspersky Security 10 для мобильных устройств (см. раздел «Аппаратные и программные требования» на стр. [14](#)).

3. На шаге **Выбор компонентов** установите флажок **Поддержка мобильных устройств**.

Без поддержки мобильных устройств в Сервере администрирования вы не сможете управлять защитой мобильных устройств с помощью Kaspersky Security Center.

4. Восстановите данные Сервера администрирования из резервной копии (см. *Руководство администратора Kaspersky Security Center*).

НАСТРОЙКА ПАРАМЕТРОВ СЕРВЕРА АДМИНИСТРИРОВАНИЯ

Для обеспечения синхронизации мобильных устройств с Сервером администрирования перед установкой Kaspersky Security 10 для мобильных устройств следует настроить в свойствах Сервера администрирования параметры подключения мобильных устройств.

- Чтобы настроить в свойствах Сервера администрирования параметры подключения мобильных устройств, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому будут подключены мобильные устройства.
2. Откройте контекстное меню и выберите пункт **Свойства**.

Откроется окно свойств Сервера администрирования.
3. Откройте раздел **Параметры**.
4. Установите флажок **Открывать порт для мобильных устройств** в блоке **Параметры подключения к Серверу администрирования**.
5. В поле **Порт для мобильных устройств** укажите порт, по которому Сервер администрирования будет ожидать подключение мобильных устройств.

По умолчанию используется порт 13292. Если флажок не установлен или порт указан неверно, устройства не смогут подключиться к серверу и передать или получить информацию.

УСТАНОВКА ПЛАГИНА УПРАВЛЕНИЯ KASPERSKY SECURITY ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Для получения доступа к интерфейсу управления программой при помощи Kaspersky Security Center на рабочее место администратора требуется установить плагин управления программой Kaspersky Security 10 для мобильных устройств.

- Чтобы установить плагин управления программой Kaspersky Security 10 для мобильных устройств, скопируйте из дистрибутива программы установочный файл плагина `klcfinst.exe` и запустите его на рабочем месте администратора.

Установка сопровождается мастером и не требует настройки параметров.

Убедиться, что плагин для программы Kaspersky Security 10 для мобильных устройств установлен, вы можете, просмотрев список установленных плагинов управления программами в разделе **Дополнительно** в окне свойств Сервера администрирования. Подробнее см. в *Руководстве администратора Kaspersky Security Center*.

РАЗВЕРТЫВАНИЕ СЕРВЕРА МОБИЛЬНЫХ УСТРОЙСТВ iOS MDM И ПОДКЛЮЧЕНИЕ К НЕМУ УСТРОЙСТВ ПОЛЬЗОВАТЕЛЕЙ

Для установки Kaspersky Security на мобильные устройства пользователей под управлением iOS требуется, чтобы в составе Kaspersky Security Center был развернут Сервер мобильных устройств iOS MDM и мобильные устройства пользователей были к нему подключены. Сервер администрирования осуществляет управление мобильными устройствами iOS при помощи Сервера мобильных устройств iOS MDM. Мобильные iOS-устройства, находящиеся под управлением Сервера администрирования, называются *мобильными устройствами iOS MDM*.

➡ Чтобы подключить мобильные устройства iOS MDM, выполните следующие действия:

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

На данный момент поддерживается только локальная установка, удаленная установка не поддерживается.

2. Получите сертификат Apple Push Notification Service (см. раздел «Электронный запрос на подпись APN-сертификата» на стр. 59) (APN-сертификат), используя сервис Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Более подробную информацию по получению APN-сертификатов см. *Руководство администратора Kaspersky Security Center*.

3. Установите на Сервере администрирования APN-сертификат.

Без APN-сертификата невозможно сформировать корректный MDM профиль, так как для его создания необходимы данные из APN-сертификата. Только после установки APN-сертификата вы сможете быть уверены в своевременной доставке команд на устройства.

4. Отправьте пользователю мобильного устройства iOS ссылку для скачивания iOS MDM-профиля.

Пользователь устанавливает iOS MDM-профиль на мобильное устройство iOS.

Мобильное устройство подключается к Серверу мобильных устройств iOS MDM по доступному интернет-каналу. Подключенные мобильные устройства iOS MDM отображаются в папке **Мобильные устройства iOS MDM**, вложенной в папку **Мобильные устройства**.

НАСТРОЙКА РАССЫЛКИ ЭЛЕКТРОННЫХ СООБЩЕНИЙ

Если вы планируете использовать рассылку сообщений корпоративной электронной почты во время развертывания программы, а именно:

- использовать схему развертывания с помощью рассылки электронных сообщений (см. раздел «Схема развертывания через рассылку электронных сообщений» на стр. 16) для мобильных устройств под управлением Android;
- отправлять iOS MDM профиль (см. раздел «Создание и рассылка iOS MDM-профиля» на стр. 47) пользователям на адреса корпоративной электронной почты в процессе подключения их устройств к Серверу администрирования (см. раздел «Схема развертывания программы для устройств под управлением iOS» на стр. 19);

то вам нужно убедиться, что параметры почтовой рассылки Сервера администрирования указаны правильно.

➡ Чтобы настроить отправку уведомлений по электронной почте, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому вы планируете подключить мобильные устройства.
2. 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**.
3. В разделе **Уведомление** выберите **Электронная почта** в качестве типа уведомления.
4. В поле **SMTP-сервер** укажите адрес почтового сервера.
В качестве адреса можно использовать IP-адрес или имя компьютера в сети Windows (NetBIOS-имя).
5. В поле **Порт SMTP-сервера** укажите номер коммуникационного порта SMTP-сервера.
По умолчанию указан порт 25.
6. Нажмите **Применить**, чтобы изменения вступили в силу.

НАСТРОЙКА СПОСОБОВ ДОСТАВКИ ТЕКСТОВЫХ СООБЩЕНИЙ

Если вы планируете использовать рассылку текстовых сообщений на телефонные номера пользователей во время развертывания программы, а именно:

- использовать схему развертывания с помощью рассылки текстовых сообщений (см. раздел «Схема развертывания через рассылку электронных сообщений» на стр. [16](#)) для мобильных устройств под управлением Android;
- отправлять iOS MDM-профиль (см. раздел «Создание и рассылка iOS MDM-профиля» на стр. [47](#)) пользователям с помощью SMS на корпоративные телефонные номера в процессе подключения их устройств к Серверу администрирования (см. раздел «Схема развертывания программы для устройств под управлением iOS» на стр. [19](#));

то вам нужно убедиться, что параметры рассылки текстовых сообщений Сервера администрирования указаны правильно.

Существует два способа массовой рассылки текстовых сообщений пользователям с помощью Kaspersky Security Center:

- Через почтовый шлюз — для этого в настройках Kaspersky Security Center указываются SMTP-сервер и порт.
Подробные сведения об использовании методов Kaspersky Security Center для рассылки уведомлений пользователям см. в *Руководстве администратора Kaspersky Security Center*.
- Через выбранное мобильное устройство под управлением Android, выступающее в роли отправителя SMS-сообщений с уведомлениями о событиях в работе Kaspersky Security Center.

Чтобы назначить мобильное устройство отправителем всех текстовых сообщений от имени Kaspersky Security Center, необходимо установить на него специальную утилиту Kaspersky SMS Broadcasting. Утилита Kaspersky SMS Broadcasting устанавливается на мобильное устройство как стандартное Android-приложение. После установки утилита Kaspersky SMS Broadcasting запрашивает адрес и порт Сервера администрирования Kaspersky Security Center и после синхронизации устройство появляется разделе **Отправители SMS** окна свойств папки **Отчеты и уведомления** в качестве возможного устройства-отправителя в списке возможных устройств-отправителей. Рекомендуется использовать мобильное устройство с Kaspersky SMS Broadcasting в качестве отправителя SMS, например, если вы хотите получать отчеты о доставке текстовых сообщений.

➤ Чтобы настроить способ рассылки текстовых сообщений, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. 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**.
3. В разделе **Уведомления** выберите в качестве типа уведомления **SMS**.
4. Укажите предпочитаемый метод рассылки текстовых сообщений:
 - выберите **Отправлять SMS через почтовый шлюз** и укажите его параметры, если вы хотите рассылать сообщения через SMS-центр;
 - выберите **Отправлять SMS с помощью утилиты Kaspersky SMS Broadcasting** и выберите мобильное устройство-отправитель в разделе **Отправители SMS**, если вы хотите рассылать текстовые сообщения пользователям с мобильного устройства, на котором установлена утилита Kaspersky SMS Broadcasting.

Подробные сведения об использовании методов Kaspersky Security Center для рассылки уведомлений пользователям см. в *Руководстве администратора Kaspersky Security Center*.

СОЗДАНИЕ ГРУППЫ

Централизованная настройка параметров программы Kaspersky Security, установленной на мобильных устройствах пользователей, выполняется через применение к этим устройствам групповых политик.

Для того чтобы применять политику к группе устройств, перед установкой Kaspersky Security на устройства пользователей рекомендуется создать для этих устройств отдельную группу в папке **Управляемые компьютеры**.

После этого нужно настроить автоматическое перемещение в эту группу устройств, на которые (см. раздел «Создание правила автоматического переноса устройств в группу администрирования» на стр. 27) вы хотите установить Kaspersky Security. Затем необходимо задать общие для всех устройств параметры с помощью групповой политики (см. раздел «Создание групповой политики для Kaspersky Security 10 для мобильных устройств» на стр. 28).

➤ Чтобы создать группу, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли откройте папку **Управляемые компьютеры**.
3. Если вы хотите создать подгруппу существующей группы, в папке **Управляемые компьютеры** выберите вложенную папку, в которой вы хотите создать подгруппу.
4. Запустите процесс создания группы 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**.
5. 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.

Если для установки Kaspersky Security вы используете установку программы на мобильные устройства через рабочие станции, то вы можете дополнительно создать на Сервере администрирования группу для рабочих станций, к которым пользователи подключают мобильные устройства. Затем для этой группы необходимо создать групповую задачу для удаленной установки программы Kaspersky Security. Таким образом вы сможете установить программу сразу через все рабочие станции, входящие в состав группы.

Подробные сведения о работе с группами администрирования см. в *Руководстве администратора Kaspersky Security Center*.

СОЗДАНИЕ ПРАВИЛА АВТОМАТИЧЕСКОГО ПЕРЕНОСА УСТРОЙСТВ В ГРУППУ АДМИНИСТРИРОВАНИЯ

Централизованное управление параметрами программы Kaspersky Security, установленной на мобильных устройствах пользователей, возможно только когда эти устройства находятся в созданной заранее группе администрирования (см. раздел «Создание группы» на стр. [26](#)) узла **Управляемые компьютеры**, для которой определена групповая политика (см. раздел «Создание групповой политики для Kaspersky Security 10 для мобильных устройств» на стр. [28](#)).

Если правило автоматического перемещения обнаруживаемых в сети мобильных устройств не задано, то при первой синхронизации устройства с Сервером администрирования оно автоматически попадает во вложенную папку **KSM10** папки **Домены**, содержащейся в папке **Нераспределенные компьютеры**. Групповая политика (см. раздел «Создание групповой политики для Kaspersky Security 10 для мобильных устройств» на стр. [28](#)) к этому устройству не применяется.

Администратор может настроить автоматический перенос мобильных устройств из папки **Нераспределенные компьютеры** в заданную группу папки **Управляемые компьютеры**.

➡ Чтобы создать правило автоматического перемещения мобильных устройств в группу, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли откройте папку **Нераспределенные компьютеры**.
3. Откройте окно свойств папки **Нераспределенные компьютеры** одним из следующих способов:
 - с помощью пункта контекстного меню **Свойства** этой папки.
 - по ссылке **Настроить правила перемещения компьютеров в группы администрирования** в рабочей области папки.

В результате откроется окно **Свойства: Нераспределенные компьютеры**.

4. В разделе **Перемещение компьютеров** нажмите на кнопку **Добавить**, чтобы запустить процесс создания правила автоматического перемещения устройств в группу администрирования.

Откроется окно **Новое правило**.

5. В разделе **Общие** выполните следующие действия:
 - Введите имя правила.
 - Укажите группу, в которую должны помещаться мобильные устройства, на которые будет установлена программа Kaspersky Security. Для этого нажмите на кнопку **Выбрать** справа от поля **Группа, в которую следует перемещать компьютеры** и в открывшемся окне выберите группу.
 - В блоке **Выполнение правила** выберите вариант **Выполняется один раз для каждого компьютера**.

- Установите флажок **Перемещать только компьютеры, не размещенные в группах администрирования** для того, чтобы в результате применения правила уже распределенные в другие группы администрирования мобильные устройства не перемещались в выбранную группу.
 - Установите флажок **Включить правило**, чтобы правило применялось для только что обнаруженных устройств.
6. В разделе **Программы** выберите один или несколько типов операционной системы устройств, которые будут перемещаться в указанную группу: Android, BlackBerry, iOS, Symbian или Windows Mobile.
 7. Нажмите на кнопку **ОК**.



Правило создано, включено и отображается в списке правил перемещения устройств (см. раздел **Перемещение компьютеров** в окне свойств папки **Нераспределенные компьютеры**).

В результате выполнения правила программа переносит все соответствующие заданным условиям устройства из папки **Нераспределенные компьютеры** в указанную вами группу. Мобильные устройства, ранее распределенные в папку **Нераспределенные компьютеры**, также могут быть перемещены в нужную группу узла **Управляемые компьютеры** вручную. Подробные сведения об управлении группами администрирования и работе с нераспределенными устройствами см. в *Руководстве администратора Kaspersky Security Center*.

СОЗДАНИЕ ГРУППОВОЙ ПОЛИТИКИ ДЛЯ KASPERSKY SECURITY 10 ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

В этом разделе описано создание политики для устройств, использующих Kaspersky Security 10 для мобильных устройств.

Все параметры работы Kaspersky Security на устройствах, включая данные для активации программы, расписание обновления баз программы, расписание проверки устройства, настройки фильтрации, определяются через применяемую к группе политику или через локальные параметры программы на устройстве. При помощи политик могут быть централизованно установлены одинаковые значения параметров работы программы для всех мобильных устройств, входящих в состав группы администрирования. Подробно о политиках и группах см. в *Руководстве администратора для Kaspersky Security Center*.

Атрибут «замок»  определяет запрет на изменение параметров в локальных параметрах программы через Консоль администрирования и через интерфейс программы на мобильном устройстве. Если атрибут «замок» имеет вид , параметры доступны для изменения в локальных параметрах программы.

Информация о параметрах программы, заданных в политиках, сохраняется на Сервере администрирования и распространяется на мобильные устройства в ходе синхронизации. В параметры, заданные политикой, пользователь вносит изменения на мобильном устройстве, если это разрешено политикой. После удаления политики или прекращения ее действия программа продолжает работу с параметрами, заданными в политике. В дальнейшем эти параметры пользователь может изменить вручную.

Политики, сформированные для устройств в группе администрирования, отображаются в рабочей области группы на закладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус. В одной группе для программы Kaspersky Security 10 для мобильных устройств, так же как и для других программ, можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

При создании политики вы можете настроить минимальный набор параметров, без которых программа не будет работать. Остальные значения параметров устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке программы. Вы можете изменять политику после ее создания.

➡ **Чтобы создать политику для программы Kaspersky Security 10 для мобильных устройств, выполните следующие действия:**

1. В дереве консоли выберите группу администрирования, для которой нужно создать политику.
2. В рабочей области группы выберите закладку **Политики** и запустите мастер создания политики по ссылке **Создать политику**.

В результате запускается мастер создания политики. Следуйте его указаниям.

Задайте значения параметров на следующих шагах:

- На шаге **Выбор программы для создания групповой политики** выберите Kaspersky Security 10 для мобильных устройств в качестве программы, для которой создается политика.

Если программа Kaspersky Security 10 для мобильных устройств отсутствует в списке, это значит, что не установлен плагин управления этой программой.

- На шаге **Проверка устройства** укажите следующие параметры проверки по требованию, применимые на устройствах под управлением операционных систем Android, Symbian и Windows Mobile:
 - включите / отключите проверку только исполняемых файлов следующих форматов: EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF;
 - включите / отключите проверку файлов в архивах;
 - включите / отключите автоматическое лечение обнаруженных вредоносных объектов;
 - сформируйте расписание, согласно которому программа будет запускать полную проверку файловой системы устройства.
- На шаге **Защита** задайте параметры защиты, применимые на устройствах под управлением операционных систем Android, Symbian и Windows Mobile:
 - включите / отключите защиту:
 - для устройств под управлением Windows Mobile и Symbian: автоматическую проверку всех запускаемых программ, а также файлов, которые пользователь открывает и сохраняет на устройстве;
 - для устройств под управлением Android: автоматическую проверку новых программ сразу после их установки.
 - включите / отключите расширенный режим защиты — проверку программ сразу после их установки, а также всех файлов при любом действии пользователя с ними (только для Android-устройств);
 - включите / отключите дополнительную проверку новых программ до их первого запуска на устройстве при помощи облачного сервиса Kaspersky Security Network (только для Android-устройств);
 - включите / отключите обнаружение рекламных программ и легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя (только для Android-устройств);
 - включите / отключите проверку только исполняемых файлов следующих форматов: EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF;
 - выберите действие, выполняемое при обнаружении вредоносного объекта, если лечение невозможно.
- На шаге **Обновление** задайте следующие параметры для обновления баз программы, применимые для устройств под управлением операционных систем Android, Symbian и Windows Mobile:
 - укажите, будет ли выполняться обновление по расписанию, если устройство находится в зоне роуминга;
 - выберите сервер, с которого программа будет загружать обновления на мобильные устройства пользователей;
 - сформируйте расписание, согласно которому будут загружаться обновления.

- На шаге **Анти-Вор** укажите параметры защиты информации на мобильном устройстве при его потере или краже, применимые для устройств под управлением операционных систем Android, BlackBerry, Symbian и Windows Mobile:
 - **Включить Удаление данных** — включите / отключите возможность дистанционно удалить с устройства персональные и корпоративные данные пользователя или все данные. Данные удаляются по команде администратора без возможности восстановления.
 - **Включить Блокирование** — включите / отключите возможность дистанционно заблокировать мобильное устройство пользователя по команде администратора.
 - **Включить SIM-контроль** — включите / отключите возможность дистанционно заблокировать мобильное устройство в случае смены SIM-карты или при включении без нее по команде администратора.
 - **Включить GPS-поиск** — включите / отключите возможность дистанционно определить географические координаты устройства, а также получить их в SMS-сообщении или в сообщении на указанный адрес электронной почты по команде администратора.
- На шаге **Сеть** определите параметры синхронизации мобильных устройств с Сервером администрирования и параметры фильтрации входящих и исходящих соединений.
 - укажите периодичность синхронизации — частоту подключения мобильных устройств к Серверу администрирования по HTTP-протоколу;
 - разрешите / запретите автоматическую синхронизацию, если устройство находится в зоне роуминга (недоступно для Android-устройств);

Для устройств под управлением Windows Mobile и Symbian:

- выберите режим работы Сетевого экрана, в соответствии с которым программа разрешает или запрещает входящие и исходящие соединения, и укажите, нужно ли уведомлять пользователя о блокировке соединения.

Для устройств под управлением Android и iOS:

- включите / отключите Веб-Фильтр — блокирование доступа пользователя к веб-сайтам нежелательных категорий, и выберите эти категории.

- На шаге **Контроль программ** для устройств под управлением Android укажите настройки запуска программ, установленных на устройстве, и сформируйте список разрешенных, запрещенных и обязательных программ:
 - установите режим ограничения запуска программ на устройстве пользователя: выберите **Запрещенные программы**, чтобы пользователи могли запускать все программы, кроме программ, указанных в списке программ как **Запрещенные**, или выберите **Разрешенные программы**, чтобы пользователи могли запускать только программы, указанные в списке программ как **Разрешенные**.
 - включите / отключите формирование отчета о запуске запрещенных программ на мобильном устройстве пользователя.
 - сформируйте список, содержащий программы, запрещенные и разрешенные для запуска на мобильном устройстве, а также обязательные программы (то есть программы, рекомендованные пользователю для самостоятельной установки на мобильном устройстве). Для этого укажите заранее созданные пакеты мобильных приложений (в том числе и контейнеры), хранящиеся на Веб-сервере Kaspersky Security Center, либо путь к файлам с расширением apk на другом HTTP-сервере.
 - выберите действие, которое будет совершаться программой, если обнаружит, что к системе устройства пользователя получен доступ с правами администратора.
 - включите / отключите формирование отчета об установленных программах на мобильном устройстве пользователя.

- На шаге **Управление устройством** укажите настройки и ограничения, применимые только для устройств под управлением Android:
 - включите / отключите требование использовать пароль и установите его минимальную длину;
 - запретите / разрешите использование на устройстве Wi-Fi, камеры и Bluetooth;
 - настройте параметры почтового клиента TouchDown для доступа пользователей к корпоративной почте со своих устройств.
- На шаге **Дополнительные параметры** определите параметры компонентов Шифрование и Фильтр вызовов и SMS, а также настройки удаления программы.

Для устройств под управлением Android, BlackBerry, Symbian и Windows Mobile:

- включите / отключите использование компонента Фильтр вызовов и SMS, предотвращающего прием нежелательных вызовов и текстовых сообщений на основе сформированного пользователем списка запрещенных и разрешенных контактов.

Для устройств под управлением Symbian и Windows Mobile:

- включите / отключите для пользователей возможность самостоятельно использовать и настраивать компонент Личные контакты, скрывающий конфиденциальные данные для выбранных контактов.
- укажите, через какой промежуток времени после перехода устройства в режим энергосбережения включается запрет доступа к зашифрованным папкам. Чтобы восстановить доступ, пользователю необходим секретный код программы, указанный при ее первом запуске.
- сформируйте списки папок для шифрования.

Для устройств под управлением Android:

- разрешите / запретите пользователям самостоятельно удалять программу Kaspersky Security 10 для мобильных устройств со своих устройств;
- установите флажок около **Удалить с устройства Kaspersky Security 10 для мобильных устройств**, чтобы удалить программу без участия пользователей со всех устройств из группы, к которой применяется создаваемая политика.
- На шаге **Лицензирование** укажите параметры активации программы (см. стр. 51) на устройствах пользователей. Вы можете выбрать ключ из списка ключей, размещенных в хранилище Kaspersky Security Center. С помощью этого ключа информация о лицензии на программу будет передана на устройства пользователей.

Для активации программы на мобильных устройствах необходимо, чтобы в политике был установлен запрет на изменение параметров, относящихся к активации.

- На заключительном шаге выберите статус **Активная политика**, если хотите, чтобы именно эта политика применялась для группы.

Статус политики можно изменить позднее в ее свойствах.

ОБНОВЛЕНИЕ ПРЕДЫДУЩЕЙ ВЕРСИИ ПРОГРАММЫ

При обновлении предыдущей версии программы необходимо учитывать, что Kaspersky Security поставляется совместно с плагином управления программой Kaspersky Security через Kaspersky Security Center.

Перед установкой плагина управления Kaspersky Security 10 необходимо удалить предыдущую версию плагина. При этом сохраняются уже существующие группы администрирования в папке **Управляемые компьютеры**, созданные для централизованного управления параметрами Kaspersky Security, и правила автоматического перемещения устройств из папки **Нераспределенные компьютеры** в эти группы. Групповые политики, созданные для предыдущей версии программы, тоже сохраняются. Новые параметры политик, реализующие новую функциональность Kaspersky Security 10, появятся в существовавших политиках и будут иметь значения по умолчанию.

Вы можете установить Kaspersky Security 10 на мобильное устройство с установленной программой Kaspersky Endpoint Security 8 for Smartphone. При первом запуске программы Kaspersky Security 10 на мобильном устройстве пользователю будет предложено удалить предыдущую версию. Рекомендуется удалять предыдущую версию программы.

Обратите внимание, что для платформ BlackBerry, Symbian и Windows Mobile дистрибутив программы Kaspersky Security 10 содержит файлы предыдущей версии программы; новая функциональность для этих платформ не поддерживается.

УСТАНОВКА НА УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ ANDROID

В этом разделе описаны варианты установки Kaspersky Security 10 для мобильных устройств на устройства под управлением операционной системы Android.

В ЭТОМ РАЗДЕЛЕ

Установка программы через рассылку электронных сообщений	33
Установка программы через рассылку текстовых сообщений	37
Установка программы через рабочую станцию	41
Установка программы без участия администратора	46

УСТАНОВКА ПРОГРАММЫ ЧЕРЕЗ РАССЫЛКУ ЭЛЕКТРОННЫХ СООБЩЕНИЙ

Для установки Kaspersky Security через рассылку сообщений по электронной почте необходимо создать инсталляционный пакет для этой программы и настроить в нем параметры подключения к Серверу администрирования. Затем на основе инсталляционного пакета вам требуется сформировать автономный пакет установки и распространить его среди пользователей мобильных устройств посредством рассылки электронных писем, содержащих либо сам пакет, либо ссылку на веб-сервер Kaspersky Security Center, папку общего доступа администратора или другой ресурс, куда вы хотите выложить автономный пакет установки программы.

Пользователь самостоятельно загружает дистрибутив программы на мобильное устройство. По окончании загрузки на устройстве запускается мастер установки программы. Следуя указаниям мастера, пользователь выполняет установку Kaspersky Security 10 для мобильных устройств на своем устройстве.

В ЭТОМ РАЗДЕЛЕ

Создание инсталляционного пакета	33
Настройка параметров инсталляционного пакета	35
Создание автономного пакета установки	35
Рассылка электронных сообщений пользователям	36
Установка программы на мобильном устройстве после получения сообщения по электронной почте	37

СОЗДАНИЕ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Инсталляционный пакет Kaspersky Security 10 для мобильных устройств представляет собой самораспаковывающийся архив `ak_package.exe`, в состав которого входят файлы, необходимые для установки программы на мобильных устройствах:

- `endpoint_8_0_0_37_ru.cab` – установочный файл программы для операционной системы Windows Mobile;
- `endpoint8_mobile_8_1_44_ru.sisx` – установочный файл программы для операционной системы Symbian;

- endpoint8_Mobile_8_1_29_ru.zip – установочный файл программы для операционной системы BlackBerry;
- KSM_10_1_75_ru.apk – установочный файл программы для операционной системы Android;
- installer.ini – конфигурационный файл с параметрами подключения к Серверу администрирования;
- kmlisten.ini – конфигурационный файл с параметрами для утилиты доставки инсталляционного пакета;
- kmlisten.kpd – файл с описанием программы;
- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe – набор файлов, необходимый для установки программы на устройства с операционной системой Android;
- kmlisten.exe – утилита доставки дистрибутива программы на мобильное устройство через рабочую станцию.

➡ Чтобы создать инсталляционный пакет для установки Kaspersky Security 10 для мобильных устройств, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Запустите процесс создания инсталляционного пакета одним из следующих способов:
 - в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать** → **Инсталляционный пакет**;
 - в контекстном меню списка инсталляционных пакетов выберите пункт **Создать** → **Инсталляционный пакет**;
 - по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

В результате запускается мастер создания инсталляционного пакета. Следуйте его указаниям.

Обратите внимание на настройку параметров на следующих шагах:

- В окне мастера **Выберите тип инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы «Лаборатории Касперского»**.
- В окне мастера **Выбор дистрибутива программы для установки** при помощи кнопки **Выбрать** откройте папку, куда вы поместили дистрибутив программы и выберите самораспаковывающийся архив ak_package.exe. Если архив был распакован ранее, то вы можете выбрать входящий в состав архива файл с описанием программы kmlisten.kpd. В результате в поле ввода отобразится имя программы и номер версии.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

Прежде чем использовать созданный инсталляционный пакет для установки программы, необходимо настроить параметры инсталляционного пакета (см. раздел «Настройка параметров инсталляционного пакета» на стр. [35](#)).

НАСТРОЙКА ПАРАМЕТРОВ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Настройка инсталляционного пакета для программы Kaspersky Security 10 для мобильных устройств необходима для того, чтобы мобильное устройство использовало правильные параметры подключения к Серверу администрирования.

➡ Чтобы настроить параметры инсталляционного пакета, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому вы хотите подключить мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В контекстном меню инсталляционного пакета для программы Kaspersky Security выберите пункт **Свойства**.
4. На закладке **Параметры** укажите параметры подключения мобильных устройств к Серверу администрирования и имя группы, в которую будут автоматически добавлены мобильные устройства после первой синхронизации с Сервером администрирования. Для этого выполните следующие действия:

- В блоке **Подключение к Серверу администрирования** в поле **Адрес сервера** укажите имя Сервера администрирования для подключения мобильных устройств в том формате, в каком он был указан при установке компонента **Поддержка мобильных устройств** во время развертывания Сервера администрирования.

То есть, в зависимости от формата имени Сервера администрирования для компонента **Поддержка мобильных устройств**, укажите DNS-имя или IP-адрес Сервера администрирования. В поле **Номер SSL-порта** укажите номер порта, открытый на Сервере администрирования для подключения мобильных устройств. По умолчанию используется порт 13292.

- В блоке **Размещение компьютеров по группам** в поле **Имя группы** введите имя группы, в которую будут добавлены мобильные устройства после первой синхронизации с Сервером администрирования (по умолчанию KSM10).

Указанная группа будет создана автоматически в папке **Нераспределенные компьютеры**.

- В блоке **Действия при установке** установите флажок **Запрашивать адрес электронной почты**, чтобы при первом запуске программа запрашивала у пользователя его адрес корпоративной электронной почты.

Адрес электронной почты пользователя используется для формирования имени мобильных устройств при добавлении их в группу администрирования. Имя мобильного устройства под управлением Android формируется по шаблону <адрес электронной почты пользователя (модель мобильного устройства – device ID)>.

5. Чтобы применить указанные параметры, нажмите на кнопку **Применить**.

СОЗДАНИЕ АВТОНОМНОГО ПАКЕТА УСТАНОВКИ

➡ Чтобы создать автономный пакет установки, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Выберите инсталляционный пакет для программы Kaspersky Security 10 для мобильных устройств.

4. Запустите процесс создания автономного пакета одним из следующих способов:

- в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать автономный пакет**;
- в контекстном меню списка инсталляционных пакетов выберите пункт **Создать автономный пакет**;
- по ссылке **Создать автономный пакет установки** в блоке управления списком инсталляционных пакетов.

В результате запустится мастер создания автономного пакета установки. Следуйте его указаниям.

Обратите внимание, что при создании автономного пакета не нужно указывать, что создается пакет для установки Агента администрирования.

После завершения работы мастера, если на последнем этапе был установлен флажок **Открыть список автономных пакетов**, откроется окно, содержащее список всех имеющихся автономных пакетов. При выборе пакета программа отображает расположение файла пакета на веб-сервере Kaspersky Security Center (поле **URL**) и в заданной папке общего доступа администратора (поле **Путь**).

На данном этапе установочный файл программы Kaspersky Security 10 для мобильных устройств готов к распространению среди пользователей. При рассылке по электронной почте вы можете указать в качестве ресурса для скачивания пользователями установочного файла программы как адрес, содержащийся в поле **URL** (адрес автономного пакета на веб-сервере Kaspersky Security Center), так и адрес, указанный как **Путь** (сетевой путь к папке общего доступа).

Рекомендуется скопировать адрес подготовленного автономного пакета в буфер обмена, чтобы затем добавить ссылку для загрузки нужного установочного файла в электронное сообщение для пользователей.

РАССЫЛКА ЭЛЕКТРОННЫХ СООБЩЕНИЙ ПОЛЬЗОВАТЕЛЯМ

➡ Чтобы разослать пользователям электронное письмо со ссылкой на автономный пакет установки программы Kaspersky Security 10 для мобильных устройств, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли выберите папку **Учетные записи пользователей**.
3. Выберите одного или нескольких пользователей.
4. В контекстном меню выберите пункт **Отправить сообщение по эл. почте**.

Откроется окно создания электронного сообщения.

5. Укажите следующие параметры:

- Заполните тему сообщения.
- Введите текст сообщения, указав ссылку на расположение автономного пакета установки на веб-сервере Kaspersky Security Center или путь к нему в вашей папке общего доступа.
- Установите флажки **Использовать основной почтовый адрес** и **Использовать дополнительный почтовый адрес**, если требуется использовать соответственно основной и дополнительный почтовый адрес пользователей.
- Если требуется создавать QR-коды для ссылок, установите флажок **Создавать для URL в тексте графические QR-коды и отправлять их в почтовом сообщении**.

6. Нажмите **ОК**, чтобы начать процесс рассылки.

УСТАНОВКА ПРОГРАММЫ НА МОБИЛЬНОМ УСТРОЙСТВЕ ПОСЛЕ ПОЛУЧЕНИЯ СООБЩЕНИЯ ПО ЭЛЕКТРОННОЙ ПОЧТЕ

После получения от администратора письма с ссылкой на автономный пакет пользователь загружает дистрибутив на свое устройство одним из доступных ему способов. Автономный пакет содержит установочный файл для операционной системы Android с заранее определенными настройками подключения к Серверу администрирования.

После завершения загрузки пользователь открывает на устройстве установочный файл, в результате автоматически запускается мастер установки программы. Пользователь следует указаниям мастера установки на устройстве.

Если при создании инсталляционного пакета были указаны все параметры подключения устройства к Серверу администрирования, то первоначальная настройка программы (см. раздел «Подготовка программы к работе на устройстве» на стр. 50) пользователем не потребуется.

По умолчанию операционная система Android не разрешает установку программ не из Google Play. Если установка программы не происходит, пользователю следует разрешить установку приложений из внешних источников в настройках своего Android-устройства.

УСТАНОВКА ПРОГРАММЫ ЧЕРЕЗ РАССЫЛКУ ТЕКСТОВЫХ СООБЩЕНИЙ

Для установки Kaspersky Security через рассылку текстовых сообщений (SMS) необходимо создать инсталляционный пакет для этой программы и настроить в нем параметры подключения к Серверу администрирования. Затем на основе инсталляционного пакета требуется сформировать автономный пакет установки и распространить его среди пользователей мобильных устройств посредством рассылки текстовых сообщений, содержащих ссылку на веб-сервер Kaspersky Security Center или другой ресурс, куда вы хотите выложить автономный пакет установки программы.

Пользователь самостоятельно загружает дистрибутив программы на мобильное устройство из указанного в рассылке сетевого ресурса. По окончании загрузки на устройстве запускается мастер установки программы. Следуя указаниям мастера, пользователь выполняет установку Kaspersky Security 10 для мобильных устройств на своем устройстве.

В ЭТОМ РАЗДЕЛЕ

Создание инсталляционного пакета	37
Настройка параметров инсталляционного пакета	39
Создание автономного пакета установки	39
Рассылка текстовых сообщений пользователям	40
Установка программы на мобильном устройстве после получения текстового сообщения	40

СОЗДАНИЕ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Инсталляционный пакет Kaspersky Security 10 для мобильных устройств представляет собой самораспаковывающийся архив `ak_package.exe`, в состав которого входят файлы, необходимые для установки программы на мобильных устройствах:

- `endpoint_8_0_0_37_ru.cab` – установочный файл программы для операционной системы Windows Mobile;
- `endpoint8_mobile_8_1_44_ru.sisx` – установочный файл программы для операционной системы Symbian;

- endpoint8_Mobile_8_1_29_ru.zip – установочный файл программы для операционной системы BlackBerry;
- ksm_10_1_75_ru.apk – установочный файл программы для операционной системы Android;
- installer.ini – конфигурационный файл с параметрами подключения к Серверу администрирования;
- kmlisten.ini – конфигурационный файл с параметрами для утилиты доставки инсталляционного пакета;
- kmlisten.kpd – файл с описанием программы;
- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe – набор файлов, необходимый для установки программы на устройства с операционной системой Android;
- kmlisten.exe – утилита доставки дистрибутива программы на мобильное устройство через рабочую станцию.

➡ Чтобы создать инсталляционный пакет для установки Kaspersky Security 10 для мобильных устройств, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Запустите процесс создания инсталляционного пакета одним из следующих способов:
 - в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать** → **Инсталляционный пакет**;
 - в контекстном меню списка инсталляционных пакетов выберите пункт **Создать** → **Инсталляционный пакет**;
 - по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

В результате запускается мастер создания инсталляционного пакета. Следуйте его указаниям.

Обратите внимание на настройку параметров на следующих шагах:

- В окне мастера **Выберите тип инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы «Лаборатории Касперского»**.
- В окне мастера **Выбор дистрибутива программы для установки** при помощи кнопки **Выбрать** откройте папку, куда вы поместили дистрибутив программы и выберите самораспаковывающийся архив ak_package.exe. Если архив был распакован ранее, то вы можете выбрать входящий в состав архива файл с описанием программы kmlisten.kpd. В результате в поле ввода отобразится имя программы и номер версии.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

Прежде чем использовать созданный инсталляционный пакет для установки программы, необходимо настроить параметры инсталляционного пакета (см. раздел «Настройка параметров инсталляционного пакета» на стр. [39](#)).

НАСТРОЙКА ПАРАМЕТРОВ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Настройка инсталляционного пакета для программы Kaspersky Security 10 для мобильных устройств необходима для того, чтобы мобильное устройство использовало правильные параметры подключения к Серверу администрирования.

➤ Чтобы настроить параметры инсталляционного пакета, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому вы хотите подключить мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В контекстном меню инсталляционного пакета для программы Kaspersky Security выберите пункт **Свойства**.
4. На закладке **Параметры** укажите параметры подключения мобильных устройств к Серверу администрирования и имя группы, в которую будут автоматически добавлены мобильные устройства после первой синхронизации с Сервером администрирования. Для этого выполните следующие действия:

- В блоке **Подключение к Серверу администрирования** в поле **Адрес сервера** укажите имя Сервера администрирования для подключения мобильных устройств в том формате, в каком он был указан при установке компонента **Поддержка мобильных устройств** во время развертывания Сервера администрирования.

То есть, в зависимости от формата имени Сервера администрирования для компонента **Поддержка мобильных устройств**, укажите DNS-имя или IP-адрес Сервера администрирования. В поле **Номер SSL-порта** укажите номер порта, открытый на Сервере администрирования для подключения мобильных устройств. По умолчанию используется порт 13292.

- В блоке **Размещение компьютеров по группам** в поле **Имя группы** введите имя группы, в которую будут добавлены мобильные устройства после первой синхронизации с Сервером администрирования (по умолчанию KSM10).

Указанная группа будет создана автоматически в папке **Нераспределенные компьютеры**.

- В блоке **Действия при установке** установите флажок **Запрашивать адрес электронной почты**, чтобы при первом запуске программа запрашивала у пользователя его адрес корпоративной электронной почты.

Адрес электронной почты пользователя используется для формирования имени мобильных устройств при добавлении их в группу администрирования. Имя мобильного устройства под управлением Android формируется по шаблону <адрес электронной почты пользователя (модель мобильного устройства – device ID)>.

5. Чтобы применить указанные параметры, нажмите на кнопку **Применить**.

СОЗДАНИЕ АВТОНОМНОГО ПАКЕТА УСТАНОВКИ

➤ Чтобы создать автономный пакет установки, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Выберите инсталляционный пакет для программы Kaspersky Security 10 для мобильных устройств.

4. Запустите процесс создания автономного пакета одним из следующих способов:

- в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать автономный пакет**;
- в контекстном меню списка инсталляционных пакетов выберите пункт **Создать автономный пакет**;
- по ссылке **Создать автономный пакет установки** в блоке управления списком инсталляционных пакетов.

В результате запустится мастер создания автономного пакета установки. Следуйте его указаниям.

Обратите внимание, что при создании автономного пакета не нужно указывать, что создается пакет для установки Агента администрирования.

После завершения работы мастера, если на последнем этапе был установлен флажок **Открыть список автономных пакетов**, откроется окно, содержащее список всех имеющихся автономных пакетов. При выборе пакета программа отображает расположение файла пакета на веб-сервере Kaspersky Security Center (поле **URL**) и в заданной папке общего доступа администратора (поле **Путь**).

На данном этапе установочный файл программы <PRODUCT_NAME> готов к распространению среди пользователей. При рассылке текстовых сообщений (SMS) пользователям вам следует указывать ссылку для скачивания, содержащуюся в поле **URL** (адрес автономного пакета на веб-сервере Kaspersky Security Center).

Рекомендуется скопировать адрес подготовленного автономного пакета в буфер обмена, чтобы затем добавить ссылку для загрузки нужного установочного файла в текстовое сообщение (SMS) для пользователей.

РАССЫЛКА ТЕКСТОВЫХ СООБЩЕНИЙ ПОЛЬЗОВАТЕЛЯМ

➡ Чтобы разослать пользователям текстовое сообщение со ссылкой на автономный пакет установки программы Kaspersky Security, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли выберите папку **Учетные записи пользователей**.
3. Выберите одного или несколько пользователей.
4. В контекстном меню выберите пункт **Отправить SMS-сообщение**.

Откроется окно создания SMS.

5. Выберите тип телефонного номера пользователя, на который необходимо отправить сообщение, установив один или несколько флажков около **Использовать мобильный номер**, **Использовать дополнительный телефонный номер** или **Использовать основной телефонный номер**.
6. Введите текст сообщения, указав ссылку на автономный пакет установки, размещенный на веб-сервере. Сообщение с таким текстом получат выбранные пользователи.
7. Нажмите **ОК**, чтобы начать процесс рассылки.

УСТАНОВКА ПРОГРАММЫ НА МОБИЛЬНОМ УСТРОЙСТВЕ ПОСЛЕ ПОЛУЧЕНИЯ ТЕКСТОВОГО СООБЩЕНИЯ

После получения от администратора текстового сообщения с ссылкой на автономный пакет пользователь загружает дистрибутив на свое устройство одним из доступных ему способов. Автономный пакет содержит установочный файл для операционной системы Android с заранее определенными настройками подключения к Серверу администрирования.

После завершения загрузки пользователь открывает на устройстве установочный файл, в результате автоматически запускается мастер установки программы. Пользователь следует указаниям мастера установки на устройстве.

Если при создании инсталляционного пакета были указаны все параметры подключения устройства к Серверу администрирования, то первоначальная настройка программы (см. раздел «Подготовка программы к работе на устройстве» на стр. 50) пользователем не требуется.

По умолчанию операционная система Android не разрешает установку программ не из Google Play. Если установка программы не происходит, пользователю следует разрешить установку приложений из внешних источников в настройках своего Android-устройства.

УСТАНОВКА ПРОГРАММЫ ЧЕРЕЗ РАБОЧУЮ СТАНЦИЮ

Для установки Kaspersky Security через рабочую станцию следует сформировать инсталляционный пакет и настроить его параметры, затем создать и запустить задачу удаленной установки для тех рабочих станций, к которым подключаются мобильные устройства пользователей. Для создания задачи администратор может воспользоваться любым из предусмотренных в Kaspersky Security Center способов:

- создать групповую задачу удаленной установки, если рабочие станции входят в состав группы;
- создать задачу для набора компьютеров, если рабочие станции входят в состав разных групп или находятся в группе **Нераспределенные компьютеры**;
- воспользоваться мастером удаленной установки.

В результате выполнения задачи удаленной установки на рабочие станции пользователей доставляется инсталляционный пакет с дистрибутивом программы Kaspersky Security 10 для мобильных устройств, а также устанавливается и автоматически запускается утилита доставки дистрибутива программы на мобильные устройства `kmlisten.exe`. Утилита отслеживает подключение мобильных устройств к компьютеру. Как только пользователь подключает к рабочей станции устройство, удовлетворяющее системным требованиям для установки Kaspersky Security 10 для мобильных устройств, утилита выводит на экран сообщение с предложением установить программу на подключенное мобильное устройство. В случае если пользователь соглашается с установкой, утилита загружает дистрибутив программы на мобильное устройство. По окончании загрузки на устройстве запускается мастер установки программы. Следуя указаниям мастера, пользователь самостоятельно выполняет установку Kaspersky Security 10 для мобильных устройств на своем устройстве.

В ЭТОМ РАЗДЕЛЕ

Создание инсталляционного пакета	41
Настройка параметров инсталляционного пакета	43
Создание задачи удаленной установки	43
Доставка дистрибутива программы на мобильное устройство через рабочую станцию	45
Установка программы на мобильном устройстве через рабочую станцию	45

СОЗДАНИЕ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Инсталляционный пакет Kaspersky Security 10 для мобильных устройств представляет собой самораспаковывающийся архив `ak_package.exe`, в состав которого входят файлы, необходимые для установки программы на мобильных устройствах:

- `endpoint_8_0_0_37_ru.cab` – установочный файл программы для операционной системы Windows Mobile;
- `endpoint8_mobile_8_1_44_ru.sisx` – установочный файл программы для операционной системы Symbian;

- endpoint8_Mobile_8_1_29_ru.zip – установочный файл программы для операционной системы BlackBerry;
- ksm_10_1_75_ru.apk – установочный файл программы для операционной системы Android;
- installer.ini – конфигурационный файл с параметрами подключения к Серверу администрирования;
- kmlisten.ini – конфигурационный файл с параметрами для утилиты доставки инсталляционного пакета;
- kmlisten.kpd – файл с описанием программы;
- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe – набор файлов, необходимый для установки программы на устройства с операционной системой Android;
- kmlisten.exe – утилита доставки дистрибутива программы на мобильное устройство через рабочую станцию.

➡ Чтобы создать инсталляционный пакет для установки Kaspersky Security 10 для мобильных устройств, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Запустите процесс создания инсталляционного пакета одним из следующих способов:
 - в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать** → **Инсталляционный пакет**;
 - в контекстном меню списка инсталляционных пакетов выберите пункт **Создать** → **Инсталляционный пакет**;
 - по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

В результате запускается мастер создания инсталляционного пакета. Следуйте его указаниям.

Обратите внимание на настройку параметров на следующих шагах:

- В окне мастера **Выберите тип инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы «Лаборатории Касперского»**.
- В окне мастера **Выбор дистрибутива программы для установки** при помощи кнопки **Выбрать** откройте папку, куда вы поместили дистрибутив программы и выберите самораспаковывающийся архив ak_package.exe. Если архив был распакован ранее, то вы можете выбрать входящий в состав архива файл с описанием программы kmlisten.kpd. В результате в поле ввода отобразится имя программы и номер версии.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

Прежде чем использовать созданный инсталляционный пакет для установки программы, необходимо настроить параметры инсталляционного пакета (см. раздел «Настройка параметров инсталляционного пакета» на стр. [43](#)).

НАСТРОЙКА ПАРАМЕТРОВ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Настройка инсталляционного пакета для программы Kaspersky Security 10 для мобильных устройств необходима для того, чтобы мобильное устройство использовало правильные параметры подключения к Серверу администрирования.

➡ Чтобы настроить параметры инсталляционного пакета, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому вы хотите подключить мобильные устройства.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В контекстном меню инсталляционного пакета для программы Kaspersky Security выберите пункт **Свойства**.
4. На закладке **Параметры** укажите параметры подключения мобильных устройств к Серверу администрирования и имя группы, в которую будут автоматически добавлены мобильные устройства после первой синхронизации с Сервером администрирования. Для этого выполните следующие действия:

- В блоке **Подключение к Серверу администрирования** в поле **Адрес сервера** укажите имя Сервера администрирования для подключения мобильных устройств в том формате, в каком он был указан при установке компонента **Поддержка мобильных устройств** во время развертывания Сервера администрирования.

То есть, в зависимости от формата имени Сервера администрирования для компонента **Поддержка мобильных устройств**, укажите DNS-имя или IP-адрес Сервера администрирования. В поле **Номер SSL-порта** укажите номер порта, открытый на Сервере администрирования для подключения мобильных устройств. По умолчанию используется порт 13292.

- В блоке **Размещение компьютеров по группам** в поле **Имя группы** введите имя группы, в которую будут добавлены мобильные устройства после первой синхронизации с Сервером администрирования (по умолчанию KSM10).

Указанная группа будет создана автоматически в папке **Нераспределенные компьютеры**.

- В блоке **Действия при установке** установите флажок **Запрашивать адрес электронной почты**, чтобы при первом запуске программа запрашивала у пользователя его адрес корпоративной электронной почты.

Адрес электронной почты пользователя используется для формирования имени мобильных устройств при добавлении их в группу администрирования. Имя мобильного устройства под управлением Android формируется по шаблону <адрес электронной почты пользователя (модель мобильного устройства – device ID)>.

5. Чтобы применить указанные параметры, нажмите на кнопку **Применить**.

СОЗДАНИЕ ЗАДАЧИ УДАЛЕННОЙ УСТАНОВКИ

Для удаленной установки программного обеспечения с помощью Kaspersky Security Center следует создать задачу удаленной установки. Сформированная задача удаленной установки будет запускаться на выполнение в соответствии со своим расписанием.

Подробные сведения об удаленной установке программ см. в *Руководстве по внедрению Kaspersky Security Center*.

Задача удаленной установки Kaspersky Security для выбранной группы администрирования может быть создана несколькими способами:

- с помощью *мастера создания задачи удаленной установки*
- на выбранные клиентские компьютеры, к которым будут подключаться мобильные устройства;
- на компьютеры из группы администрирования, к которым будут подключаться мобильные устройства.
- с помощью *мастера удаленной установки*.

В зависимости от того, какой способ установки был выбран, последовательность шагов мастера и настраиваемые параметры могут отличаться. Обратите внимание на настройку параметров на следующих шагах:

- Выбор типа задачи. На этом шаге укажите, что задача удаленной установки создается для программы Kaspersky Security Center, тип задачи – **Удаленная установка программы**.
- Выбор инсталляционного пакета. На этом шаге выберите уже сформированный инсталляционный пакет, который содержит дистрибутив программы Kaspersky Security 10 для мобильных устройств, а также все настройки для подключения мобильных устройств с установленной программой к Серверу администрирования. Вы также можете создать инсталляционный пакет непосредственно на этом шаге, однако он не будет содержать настроек подключения и пользователям придется вручную производить первоначальную настройку программы. В случае создания инсталляционного пакета следует указать самораспаковывающийся архив `sc_package.exe`. Если архив был распакован ранее, то вы можете указать входящий в состав архива файл с описанием программы `kmlisten.kpd`.
- Выбор метода установки. Удаленная установка программ на рабочие станции в Kaspersky Security Center осуществляется одним из двух методов: методом форсированной установки или методом установки с помощью сценария входа. Метод форсированной установки позволяет провести удаленную установку программного обеспечения на конкретные рабочие станции. Метод установки с помощью сценария входа позволяет закрепить запуск задачи удаленной установки за конкретной учетной записью пользователя (нескольких пользователей).

Для мастера удаленной установки и мастера создания групповой задачи этот шаг отсутствует, поскольку в этом случае выполняется установка на конкретные рабочие станции и используется метод форсированной установки. Для установки программы Kaspersky Security 10 для мобильных устройств с помощью задачи для набора компьютеров администратор может воспользоваться любым методом.

Подробнее о методах удаленной установки программ см. в *Руководстве администратора Kaspersky Security Center*.

- Выбор компьютеров для установки. На этом шаге вам будет предложено сформировать список рабочих станций, через которые программа будет устанавливаться на мобильные устройства. Вы можете выбрать один из следующих вариантов:
 - **Установить на группу управляемых компьютеров.** Используйте этот вариант, если на этапе подготовки к установке программы вы создали группу администрирования в папке **Управляемые компьютеры** и переместили в нее все компьютеры, к которым подключаются мобильные устройства.
 - **Выбрать компьютеры для установки.** Выберите этот вариант, если группа не создавалась. На следующем шаге мастер предложит вам сформировать список компьютеров для установки программы.
- Выбор способа загрузки инсталляционного пакета. На этом шаге вам будет предложено настроить параметры доставки инсталляционного пакета на рабочие станции. Доставка инсталляционного пакета на рабочие станции может быть выполнена двумя способами:
 - **С помощью Агента администрирования.** Выберите этот способ, если на рабочих станциях, через которые устанавливается Kaspersky Security 10 для мобильных устройств, Агент администрирования установлен и подключен к текущему Серверу администрирования.

Если Агент администрирования не установлен, но вы планируете его установить, вы можете воспользоваться совместной установкой, предлагаемой на следующем шаге мастера.

- **Средствами Microsoft Windows из папки общего доступа.** Выберите этот способ, если Агент администрирования на рабочих станциях не установлен или подключен к другому Серверу администрирования. В этом случае передача необходимых для установки программы файлов осуществляется средствами Windows через папки общего доступа.
- Выбор дополнительного пакета для установки. На этом шаге вам будет предложено установить Агент администрирования на рабочие станции. Воспользуйтесь совместной установкой, если на предыдущем шаге был выбран способ загрузки инсталляционного пакета **С помощью Агента администрирования**, но Агент администрирования на рабочих станциях пока не установлен. В этом случае на рабочие станции сначала устанавливается Агент администрирования, после этого с помощью Агента администрирования доставляется инсталляционный пакет программы.

Совместная установка не требуется, если доставка дистрибутива на рабочие станции выполняется средствами Microsoft Windows или версия Агента администрирования, удовлетворяющая системным требованиям для установки Kaspersky Security 10 для мобильных устройств, уже установлена.

ДОСТАВКА ДИСТРИБУТИВА ПРОГРАММЫ НА МОБИЛЬНОЕ УСТРОЙСТВО ЧЕРЕЗ РАБОЧУЮ СТАНЦИЮ

Доставку дистрибутива программы Kaspersky Security на мобильное устройство выполняет утилита `kmlisten.exe`, установленная на рабочей станции в результате выполнения задачи удаленной установки. При подключении к компьютеру устройства, удовлетворяющего программным и аппаратным требованиям, утилита предложит пользователю установить Kaspersky Security 10 для мобильных устройств на подключенное мобильное устройство.

➡ Чтобы скопировать дистрибутив программы Kaspersky Security 10 для мобильных устройств с рабочей станции на мобильное устройство, пользователю необходимо выполнить следующие действия:

1. Подключить устройство к рабочей станции.

Если устройство удовлетворяет системным требованиям для установки программы, автоматически откроется окно утилиты `kmlisten.exe`.

2. В списке обнаруженных устройств выбрать одно или несколько устройств, на которые следует установить программу.
3. Нажать на кнопку **Установить**.

Утилита копирует дистрибутив программы на выбранные устройства и отобразит результаты работы. Установка Kaspersky Security автоматически запустится на мобильном устройстве после успешной загрузки дистрибутива.

Окно **KSM10** утилиты `kmlisten.exe` открывается и предлагает установить программу при каждом подключении мобильного устройства к компьютеру.

4. Если необходимо отключить отображение окна **KSM10** утилиты `kmlisten.exe`, которое предлагает установить программу, пользователю необходимо в этом окне установить флажок **Прекратить автоматический запуск программы для установки Kaspersky Security 10 для мобильных устройств**.

УСТАНОВКА ПРОГРАММЫ НА МОБИЛЬНОМ УСТРОЙСТВЕ ЧЕРЕЗ РАБОЧУЮ СТАНЦИЮ

После завершения загрузки инсталляционного пакета на мобильное устройство программа автоматически устанавливается на устройство без участия пользователя. Пользователь следует указаниям мастера установки на устройстве.

Если при создании инсталляционного пакета были указаны все параметры подключения устройства к Серверу администрирования, то первоначальная настройка программы (см. раздел «Подготовка программы к работе на устройстве» на стр. [50](#)) пользователем не потребуется.

По умолчанию операционная система Android не разрешает установку программ не из Google Play. Если установка программы не происходит, пользователю следует разрешить установку приложений из внешних источников в настройках своего Android-устройства.

УСТАНОВКА ПРОГРАММЫ БЕЗ УЧАСТИЯ АДМИНИСТРАТОРА

Непосредственная загрузка установочного файла на устройство используется в случаях, когда пользователям удобно самостоятельно установить программу, например, скачав установочный файл на Google Play.

В этом случае вы не готовите дистрибутив программы, и пользователь самостоятельно указывает параметры подключения к Серверу администрирования (см. раздел «Подготовка программы к работе на устройстве» на стр. [50](#)) при первом запуске программы.

По умолчанию операционная система Android не разрешает установку программ не из Google Play. Если установка программы не происходит, пользователю следует разрешить установку приложений из внешних источников в настройках своего Android-устройства.

УСТАНОВКА НА УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ IOS

В этом разделе описана процедура установки Kaspersky Security 10 для мобильных устройств на устройства под управлением операционной системы iOS.

В ЭТОМ РАЗДЕЛЕ

Настройка интерфейса Kaspersky Security Center для управления мобильными устройствами	47
Создание и рассылка iOS MDM-профиля.....	47
Установка программы на мобильное устройство iOS.....	48

НАСТРОЙКА ИНТЕРФЕЙСА KASPERSKY SECURITY CENTER ДЛЯ УПРАВЛЕНИЯ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

➤ Чтобы настроить интерфейс Kaspersky Security Center для управления мобильными устройствами, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В контекстном меню папки **Сервер администрирования** выберите пункт **Вид** → **Настройка интерфейса**.
3. В окне **Настройка интерфейса** установите флажок **Отображать управление мобильными устройствами**.
4. Нажмите на кнопку **ОК**.
5. Чтобы изменения вступили в силу, перезапустите Консоль администрирования.

СОЗДАНИЕ И РАССЫЛКА IOS MDM-ПРОФИЛЯ

iOS MDM-профиль позволяет рассылать конфигурационные профили iOS в фоновом режиме с помощью MDM-сервера, а также получать расширенную диагностическую информацию о мобильных устройствах. iOS MDM-профиль необходимо рассылать для того, чтобы Сервер администрирования мог обнаружить мобильные устройства под управлением iOS.

➤ Чтобы создать iOS MDM-профиль и отправить его на мобильное устройство, выполните следующие действия:

1. В дереве консоли выберите папку **Учетные записи пользователей**.
2. Выберите учетную запись пользователя, на мобильное устройство которого вы хотите установить iOS MDM-профиль.
3. В контекстном меню учетной записи пользователя мобильного устройства выберите пункт **Установить iOS MDM-профиль на мобильное устройство пользователя**.

Откроется окно **Установка iOS MDM-профиля**.

iOS MDM-профиль создается автоматически при его запросе через узел **Учетные записи пользователей**.

4. В окне **Установка iOS MDM-профиля** в поле **Список доступных Серверов мобильных устройств iOS MDM** выберите **Сервер мобильных устройств iOS MDM**, для которого необходимо создать iOS MDM-профиль.
5. В окне **Установка iOS MDM-профиля** укажите способ отправки пользователю уведомления об установке iOS MDM-профиля на мобильное устройство:
 - **С помощью SMS.** Установите флажок, чтобы отправить пользователю текстовое сообщение со ссылкой на скачивание MDM-профиля. В поле **Текст SMS** введите сообщение для пользователя или используйте сообщение по умолчанию. В раскрывающемся списке рядом с полем ввода **Текст SMS** выберите пункт **Одноразовый пароль** и укажите пароль пользователя.

Рассылка iOS MDM-профиля с помощью SMS возможна только на устройства с GSM-модулем.

- **По электронной почте.** Установите флажок, чтобы отправить пользователю по электронной почте уведомление, содержащее ссылку на загрузку MDM-профиля и созданный специально для этого сообщения QR-код. В поле **Тема** укажите тему сообщения. В поле **Текст уведомления** введите сообщение для пользователя. В раскрывающемся списке рядом с полем **Текст уведомления** выберите вариант **Одноразовый пароль** и задайте пароль пользователя.
6. Нажмите на кнопку **ОК**.

Пользователь мобильного устройства получает уведомление со ссылкой для скачивания iOS MDM-профиля с веб-портала. Пользователь самостоятельно переходит по полученной ссылке или QR-коду, тем самым загружая iOS MDM-профиль на свое устройство iOS.

После загрузки iOS MDM-профиля и синхронизации с Сервером администрирования устройство под управление iOS будет отображаться в папке **Мобильные устройства** во вложенной папке **Мобильные устройства iOS MDM**.

УСТАНОВКА ПРОГРАММЫ НА МОБИЛЬНОЕ УСТРОЙСТВО iOS

➡ Чтобы установить программу на мобильное устройство iOS, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. Откройте вложенную папку **Мобильные устройства iOS MDM** в папке **Мобильные устройства**.
3. Выберите одно или несколько устройств из списка.
4. Запустите процесс установки программы на устройство одним из следующих способов:
 - В контекстном меню выберите пункт **Установить приложение на устройство** и выберите из списка Kaspersky Security.
 - По ссылке **Установить приложение на устройство** в блоке выбранных устройств.

Пользователь должен подтвердить на устройстве команду установки программы.

Как только мобильное устройство пользователя синхронизируется с Сервером администрирования, пользователь получает запрос на установку программы. После получения согласия на установку на мобильное устройство программа автоматически загружается и устанавливается на устройство без участия пользователя. На устройстве появляется иконка приложения, в которой отображается прогресс скачивания приложения. Далее пользователь должен произвести первоначальную настройку программы (см. раздел «Подготовка программы к работе на устройстве» на стр. 50) на устройстве. Для этого пользователь указывает настройки подключения к Серверу администрирования, полученные от администратора по электронной почте и адрес своей электронной почты.

УСТАНОВКА ЧЕРЕЗ РАБОЧИЕ СТАНЦИИ НА УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ BLACKBERRY, SYMBIAN И WINDOWS MOBILE

Комплект поставки Kaspersky Security 10 для мобильных устройств (см. раздел «Комплект поставки» на стр. [12](#)) содержит дистрибутивы программы для различных операционных систем. Для платформ BlackBerry, Symbian и Windows Mobile в него входят дистрибутивы Kaspersky Endpoint Security 8.0 for Smartphone.

Плагин управления Kaspersky Security 10 для Kaspersky Security Center поддерживает управление устройствами с программой Kaspersky Endpoint Security 8.0 for Smartphone.

Установка программы на устройства под управлением операционных систем BlackBerry, Symbian и Windows Mobile происходит аналогично установке программы на устройства с Android через рабочие станции пользователей.

ПОДГОТОВКА ПРОГРАММЫ К РАБОТЕ НА УСТРОЙСТВЕ

Первоначальная настройка параметров подключения к Серверу администрирования не требуется в следующих случаях:

- на мобильное устройство под управлением операционной системы Android загружен автономный пакет или заранее настроенный установочный файл (например, при использовании схем развертывания с помощью рассылки текстовых или электронных сообщений).
- программа установлена на мобильное устройство после подключения к рабочей станции (при использовании схемы развертывания через рабочие станции для операционных систем Android, BlackBerry, Symbian, Windows Mobile).

В остальных случаях пользователю требуется один раз на устройстве указать параметры подключения к Серверу администрирования:

- **Адрес сервера**

Если в свойствах Сервера администрирования указан IP-адрес, то и пользователю нужно ввести этот IP-адрес. Если в свойствах Сервера администрирования указано DNS-имя, то пользователю нужно ввести это имя.

- **Номер SSL-порта**

Пользователю требуется указать номер порта, открытого на Сервере администрирования для подключения мобильных устройств. По умолчанию используется порт 13292. Номер порта указан в свойствах Сервера администрирования в разделе **Параметры**.

АКТИВАЦИЯ ПРОГРАММЫ

В Kaspersky Security Center лицензия может распространяться на различные группы функциональности. Для полноценного функционирования плагина управления Kaspersky Security 10 и самой программы Kaspersky Security на мобильных устройствах необходимо, чтобы приобретенная организацией лицензия на Kaspersky Security Center распространялась на функциональность Управление мобильными устройствами. Функциональность Управление мобильными устройствами предназначена для подключения мобильных устройств и управления ими средствами Exchange ActiveSync и iOS MDM, а также управления мобильными устройствами, на которых установлена программа Kaspersky Security 10.

Подробные сведения о лицензировании Kaspersky Security Center и вариантах лицензирования см. в разделе Лицензирование в *Руководстве администратора Kaspersky Security Center*.

Особенность активации программы Kaspersky Security 10 для мобильных устройств состоит в том, что информация о лицензии передается на мобильное устройство вместе с политикой (см. раздел «Создание групповой политики для Kaspersky Security 10 для мобильных устройств» на стр. [28](#)) при синхронизации устройства с Сервером администрирования. После установки программы устройство автоматически выходит на связь с Сервером администрирования каждые три часа. После применения политики устройство синхронизируется с Сервером администрирования с периодичностью, которая была указана в параметрах сети при создании политики. По умолчанию установлена периодичность синхронизации каждые 6 часов.

Для того чтобы выполнить активацию программы на мобильном устройстве, вам требуется создать политику для группы (см. раздел «Создание групповой политики для Kaspersky Security 10 для мобильных устройств» на стр. [28](#)), в которую входит устройство, и указать для этой политики ключ из хранилища Сервера администрирования, добавленный с помощью кода активации или файла ключа. Когда мобильное устройство в очередной раз установит соединение с Сервером администрирования, информация о лицензии будет загружена на устройство вместе с политикой. Таким образом, программа Kaspersky Security 10, установленная на устройстве, будет активирована.

Если активация программы не произошла в течение трех дней с момента установки Kaspersky Security 10 на мобильное устройство, то программа автоматически переключается в режим работы с ограниченной функциональностью. В этом режиме работы большинство компонентов отключены. При переходе в режим работы с ограниченной функциональностью программа прекращает выполнять автоматическую синхронизацию с Сервером администрирования. Поэтому, если по каким-то причинам активация программы не произошла в течение трех дней с момента установки, пользователь должен вручную выполнить синхронизацию с Сервером администрирования.

УДАЛЕНИЕ ПРОГРАММЫ

В этом разделе представлена информация об удалении программы Kaspersky Security 10 для мобильных устройств с устройств пользователей.

Способ удаления Kaspersky Security зависит от того, под управлением какой операционной системы работают мобильные устройства.

В ЭТОМ РАЗДЕЛЕ

Удаление программы с устройства под управлением Android	52
ЗАО «Лаборатория Касперского»	54
Удаление программы с устройства под управлением BlackBerry, Symbian и Windows Mobile.....	54
Удаление программы с устройства под управлением iOS	55

УДАЛЕНИЕ ПРОГРАММЫ С УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ ANDROID

Возможность самостоятельного удаления пользователем программы Kaspersky Security 10 со своего устройства под управлением Android зависит от того, разрешено ли это в политике, применяемой к группе, в которую входит данное устройство.

Если политикой предусмотрена возможность удаления программы, то пользователь может самостоятельно удалить Kaspersky Security с устройства, используя интерфейс программы или возможности управления Android-устройством.

Если политикой запрещено удалять программу Kaspersky Security с устройства, пользователю следует обратиться к администратору. Администратор может либо дистанционно удалить программу с устройства средствами Kaspersky Security Center (см. раздел «Удаление программы с устройства без участия пользователя» на стр. [53](#)) без участия пользователя, либо разрешить удаление программы (см. раздел «Разрешение пользователям удалять программу» на стр. [52](#)) с устройства через политику, применяемую к этому устройству.

РАЗРЕШЕНИЕ ПОЛЬЗОВАТЕЛЯМ УДАЛЯТЬ ПРОГРАММУ

Вы можете разрешить или запретить пользователям удалять программу Kaspersky Security 10 для мобильных устройств со своих мобильных устройств, используя групповую политику, которая применяется к устройствам. Если вы не возражаете против возможности удаления программы для всех устройств из группы, вы можете разрешить это действие в свойствах созданной ранее политики для этой группы.

Если вы хотите разрешить удаление программы только на некоторых устройствах, вам следует создать особую групповую политику и применить ее к нужным устройствам. При следующей синхронизации мобильных устройств с Сервером администрирования программа станет доступной для самостоятельного удаления.

► Чтобы разрешить пользователям удалять программу Kaspersky Security со своих мобильных устройств, выполните следующие действия:

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли откройте папку **Управляемые компьютеры**.

3. В папке **Управляемые компьютеры** выберите группу, устройствам в составе которой вы планируете разрешить удаление программы.
4. Создайте новую подгруппу 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**.
5. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.
6. Запустите процедуру добавления в эту группу устройств, которым необходимо разрешить удаление программы, одним из следующих способов:
 - по ссылке **Добавить компьютеры в группу**, расположенной в рабочей области главного окна программы на закладке **Группы**;
 - по ссылке **Добавить компьютеры**, расположенной в рабочей области главного окна программы на закладке **Компьютеры**.

В результате запускается мастер добавления клиентских компьютеров. Следуйте его указаниям.

7. В рабочей области созданной группы выберите закладку **Политики** и запустите мастер создания политики по ссылке **Создать политику**.

Следуйте указаниям мастера. Измените значения параметров на следующих шагах:

- На шаге **Выбор программы** для создания групповой политики выберите Kaspersky Security для мобильных устройств.
- На шаге **Дополнительные параметры** в блоке **Управление программой** установите флажок **Разрешить удаление с устройства Kaspersky Security 10 для мобильных устройств**.
- На шаге **Создание групповой политики** для программы в блоке параметров **Состояние политики** выберите вариант **Активная политика**.

В результате созданная политика будет активной для выбранной группы и при следующей синхронизации мобильных устройств из этой группы с Сервером администрирования программа Kaspersky Security станет доступной для самостоятельного удаления пользователями.

УДАЛЕНИЕ ПРОГРАММЫ С УСТРОЙСТВА БЕЗ УЧАСТИЯ ПОЛЬЗОВАТЕЛЯ

Вы можете дистанционно удалить Kaspersky Security 10 для мобильных устройств с мобильных устройств пользователей, подключенных к Серверу администрирования Kaspersky Security Center. Для этого вы должны создать специальную групповую политику и применить ее к нужным устройствам. При следующей синхронизации мобильных устройств с Сервером администрирования программа будет автоматически удалена с них.

- ➡ *Чтобы удалить программу Kaspersky Security с мобильных устройств без участия пользователей, выполните следующие действия:*

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.
2. В дереве консоли откройте папку **Управляемые компьютеры**.
3. В папке **Управляемые компьютеры** выберите группу, с устройств в составе которой вы планируете удалить программу.

4. Создайте новую подгруппу 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**.
5. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.
6. Запустите процедуру добавления в эту группу устройств, с которых вы планируете удалить программу, одним из следующих способов:
 - по ссылке **Добавить компьютеры в группу**, расположенной в рабочей области главного окна программы на закладке **Группы**;
 - по ссылке **Добавить компьютеры**, расположенной в рабочей области главного окна программы на закладке **Компьютеры**.

В результате запускается мастер добавления клиентских компьютеров. Следуйте его указаниям.

7. В рабочей области группы выберите закладку **Политики** и запустите мастер создания политики по ссылке **Создать политику**.

В результате запускается мастер создания политики. Следуйте его указаниям. Для политики, предназначенной для удаления программы, измените параметры на следующих шагах:

- На шаге **Выбор программы для создания групповой политики** выберите Kaspersky Security для мобильных устройств.
- На шаге **Дополнительные параметры** в блоке **Управление программой** установите флажок **Удалить с устройства Kaspersky Security 10 для мобильных устройств**.

Откроется диалоговое окно с предупреждением о невозможности отмены этой операции. Подтвердите удаление.

- На шаге **Создание групповой политики для программы** в блоке параметров **Состояние политики** выберите вариант **Активная политика**.

В результате созданная политика будет активной для выбранной группы и при следующей синхронизации мобильных устройств из этой группы с Сервером администрирования программа Kaspersky Security на устройствах будет удалена.

УДАЛЕНИЕ ПРОГРАММЫ С УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ BLACKBERRY, SYMBIAN И WINDOWS MOBILE

На устройствах под управлением операционных систем BlackBerry, Symbian и Windows Mobile удаление программы Kaspersky Security 10 для мобильных устройств выполняется пользователями самостоятельно путем стандартной процедуры для соответствующей платформы.

Перед удалением программы с устройств под управлением Windows Mobile и Symbian скрытие конфиденциальной информации будет автоматически отключено, а вся ранее зашифрованная информация расшифрована. Перед удалением программы с устройств под управлением BlackBerry пользователю необходимо вручную отключить скрытие конфиденциальной информации.

Для удаления программы на устройствах под управлением Symbian и Windows Mobile пользователю потребуется ввести секретный код программы, установленный при ее первом запуске. Если пользователь забыл этот код, администратору следует обратиться в Службу технической поддержки, чтобы получить специальную утилиту для удаления программы без ввода секретного кода.

Окончательное удаление программы происходит после перезагрузки устройства.

УДАЛЕНИЕ ПРОГРАММЫ С УСТРОЙСТВА ПОД УПРАВЛЕНИЕМ iOS

Удаление программы Kaspersky Security 10 выполняется пользователем вручную на своем мобильном устройстве обычным для платформы iOS образом.

➡ Чтобы удалить программу Kaspersky Security на устройстве под управлением iOS,

нажмите и удерживайте значок программы на экране, пока он не начнет покачиваться, затем нажмите крестик.

ОБМЕН ИНФОРМАЦИЕЙ С KASPERSKY SECURITY NETWORK

Облачный сервис Kaspersky Security Network – это специальный онлайн-сервис «Лаборатории Касперского», который содержит информацию о надежности файлов, программ и интернет-ресурсов. Kaspersky Security использует облачный сервис Kaspersky Security Network в работе следующих компонентов:

- Проверка. Программа выполняет дополнительную проверку устанавливаемых программ до их первого запуска. Проверка производится на новые угрозы, информация о которых еще не вошла в антивирусные базы.
- Веб-Фильтр. Программа выполняет дополнительную проверку веб-сайтов до их открытия.

О том, какие данные передаются в «Лабораторию Касперского» при использовании облачного сервиса во время работы Kaspersky Security на мобильных устройствах пользователей, вы можете прочитать в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать перечисленную ниже информацию:

- о контрольных суммах обрабатываемых файлов (MD5);
- о количестве установок программ;
- о веб-адресе, посещаемом в текущий момент пользователем, для определения репутации этого веб-адреса;
- статистические данные об обнаруженных угрозах.

Вся информация, передаваемая в облачный сервис, не содержит персональных данных и иной конфиденциальной информации пользователя. Информация, полученная облачным сервисом Kaspersky Security Network, защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями. Вы можете получить более подробную информацию на веб-сайте <http://support.kaspersky.ru>.

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.....	57
Техническая поддержка по телефону.....	57
Получение технической поддержки через Kaspersky CompanyAccount	57

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/international>).

Перед обращением в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами предоставления поддержки (<http://support.kaspersky.ru/support/details>). 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 запросов в «Лабораторию Касперского» и отслеживания их обработки специалистами «Лаборатории Касперского».

Для доступа к Kaspersky CompanyAccount вам потребуется зарегистрироваться (<https://support.kaspersky.com/companyaccount/registration>). Для этого необходимо указать код активации или загрузить файл ключа, а также ввести ваш электронный адрес и название вашей компании. После этого для вашей компании будет создана учетная запись CompanyAccount, в которую автоматически добавлена информация о приобретенной вами лицензии. В дальнейшем на основании этой информации к CompanyAccount вашей организации будут прикреплены все сотрудники вашей организации, которые регистрируются в Kaspersky CompanyAccount.

В Kaspersky CompanyAccount вы можете выполнять следующие действия:

- Работать с запросами:
 - Отправлять запросы в Службу технической поддержки (см. раздел «Электронный запрос в Службу технической поддержки» на стр. [59](#)).
 - Отправлять запросы в Вирусную лабораторию на проверку файлов (см. раздел «Электронный запрос в Антивирусную лабораторию» на стр. [59](#)).
 - Отправлять запросы на подпись сертификатов (например, для подписи APN-сертификатов (см. раздел «Электронный запрос на подпись APN-сертификата» на стр. [59](#))).
 - Отправлять вопросы и отзывы по работе веб-сервиса Kaspersky CompanyAccount.
 - Обмениваться сообщениями со Службой технической поддержки.
 - Отслеживать состояние обработки запросов и просматривать их историю.
- Управлять ключами и кодами активации в организации:
 - Загружать другие файлы ключей и указывать другие коды активации для учетной записи CompanyAccount вашей организации.
 - Удалять ключи и коды активации (только при наличии прав администратора CompanyAccount).
 - Просматривать список программ, на которые распространяется лицензия.
 - Получать копию файла ключа в случае, если файл ключа был утерян или удален.
- Управлять учетными записями CompanyAccount (только при наличии прав администратора CompanyAccount):
 - Добавление и удаление учетных записей.
 - Сброс пароля учетных записей.
 - Просмотр запросов.
 - Управление правами учетных записей.
- Получать уведомления:
 - О статусе обработки запроса.
 - Об истечении срока действия лицензии.
 - О добавлении новых учетных записей в CompanyAccount (при наличии специальных прав).
 - О добавлении нового ключа или кода активации (при наличии специальных прав).

Для администрирования CompanyAccount вашей организации вам необходимо отправить электронный запрос по форме **Вопрос по CompanyAccount**. После получения прав администратора CompanyAccount вы сможете управлять учетными записями вашей организации, а также получать уведомления, например, о присоединении новых пользователей к CompanyAccount вашей организации.

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 АНТИВИРУСНУЮ ЛАБОРАТОРИЮ

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

Вы можете направлять в Антивирусную лабораторию запросы следующих типов:

- *Неизвестная вредоносная программа* – вы подозреваете, что файл содержит вирус, но Kaspersky Security не определяет этот файл как зараженный.

Специалисты Антивирусной лаборатории анализируют присылаемый вредоносный код и при обнаружении неизвестного ранее вируса добавляют его описание в базу данных, доступную при обновлении антивирусных программ.

- *Ложное срабатывание антивируса* – Kaspersky Security определяет файл как зараженный, но вы уверены, что файл не содержит вирусов

Вы также можете направлять запросы в Антивирусную 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.

ЭЛЕКТРОННЫЙ ЗАПРОС НА ПОДПИСЬ APN-СЕРТИФИКАТА

Вы можете отправить в Службу технической поддержки электронный запрос на подпись APN-сертификата.

Для этого в форме электронного запроса вам нужно указать файл запроса APN-сертификата <http://support.kaspersky.ru/9245>.

После автоматической обработки вашего электронного запроса вы получаете файл запроса APN-сертификата, подписанный «Лабораторией Касперского», для дальнейшей отправки в Apple.

Обработанный запрос вы можете посмотреть в списке неактивных запросов вашей учетной записи.

ГЛОССАРИЙ

А

APPLE PUSH NOTIFICATION SERVICE (APNs) СЕРТИФИКАТ

Сертификат, подписываемый компанией Apple, который позволяет рассылать конфигурационные профили iOS в фоновом режиме с помощью iOS MDM-сервера.

И

iOS MDM-ПРОФИЛЬ

Позволяет рассылать конфигурационные профили iOS в фоновом режиме с помощью MDM-сервера, а также получать расширенную диагностическую информацию о мобильных устройствах. iOS MDM-профиль необходимо отправлять пользователю для того, чтобы Сервер администрирования мог обнаружить и подключить его мобильное устройство под управлением iOS.

А

АГЕНТ АДМИНИСТРИРОВАНИЯ

Установочный файл программы Kaspersky Security для операционной системы Android, содержащий настройки подключения программы к Серверу администрирования. Создается на основе инсталляционного пакета для этой программы и является частным случаем пакета мобильных приложений.

Г

ГРУППА АДМИНИСТРИРОВАНИЯ

Набор управляемых устройств, например, мобильных устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ. Управляемые устройства группируются с целью управления ими как единым целым, например, объединяются мобильные устройства под управлением одной операционной системы. В состав группы могут входить другие группы. Для устройств в группах могут быть созданы групповые политики и сформированы групповые задачи.

ГРУППОВАЯ ЗАДАЧА (KSM)

Задача, определенная для группы администрирования и выполняемая на всех входящих в ее состав управляемых устройствах.

И

ИНСТАЛЛЯЦИОННЫЙ ПАКЕТ

Набор файлов, формируемый для удаленной установки программы «Лаборатории Касперского» при помощи системы удаленного администрирования. Инсталляционный пакет создается на основании специальных файлов, входящих в состав дистрибутива программы, и содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию.

К

КОНТЕЙНЕР

Специальная оболочка для мобильных программ, позволяющая контролировать действия содержащейся в контейнере программы, тем самым защищая личные и корпоративные данные на устройстве.

М

МОБИЛЬНОЕ УСТРОЙСТВО iOS MDM

Мобильное устройство на платформе iOS, находящееся под управлением Сервера мобильных устройств iOS MDM.

П**ПАКЕТ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ**

Установочный файл для операционной системы Android (файл с расширением apk), загруженный на Сервер администрирования. Пакеты мобильных приложений хранятся на веб-сервере Kaspersky Security Center или в папке общего доступа администратора Kaspersky Security Center. Пакеты мобильных приложений могут быть созданы для программ сторонних производителей. При создании пакета мобильных приложений можно указать, что программа будет в контейнере.

ПЛАГИН УПРАВЛЕНИЯ ПРОГРАММОЙ

Специализированный компонент, предоставляющий интерфейс для управления работой программы «Лаборатории Касперского» через Консоль администрирования. Для каждой программы существует свой плагин управления. Он входит в состав всех программ «Лаборатории Касперского», управление которыми может осуществляться при помощи Kaspersky Security Center.

ПОЛИТИКА

Набор параметров работы программы для группы администрирования при управлении программой средствами Kaspersky Security Center. Для разных групп параметры работы программы могут быть различны. Политика включает в себя параметры полной настройки всей функциональности программы.

С**СЕРВЕР АДМИНИСТРИРОВАНИЯ**

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах «Лаборатории Касперского» и управления ими.

СЕРВЕР МОБИЛЬНЫХ УСТРОЙСТВ iOS MDM

Компонент системы администрирования Kaspersky Security Center, позволяющий подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью iOS MDM-профилей.

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 ежедневно, 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/>

Антивирусная 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.

На Android-устройствах информация из файла legal_notices.txt отображается в окне **Дополнительно** в разделе **О программе**.

УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apple – зарегистрированный товарный знак Apple Inc.

Android – товарные знаки Google, Inc.

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

Nokia, Series 60 – товарные знаки или зарегистрированные товарные знаки Nokia Corporation.

Blackberry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Правообладателем товарного знака Symbian является Symbian Foundation Ltd.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

А

APN-сертификат 24, 59

А

Автономный пакет 35, 39

Автономный пакет

распространение 36, 40

создание 35, 39

Активация программы 28, 51

Г

Группа администрирования

правило переноса 27

создание 26

З

ЗАО «Лаборатория Касперского» 62

И

Инсталляционный пакет 33, 37, 41

Инсталляционный пакет

настройка параметров 35, 39, 43

распространение 20, 43

создание 33, 37, 41

К

Контейнер 11

Л

Лицензия

активация программы 28, 51

М

Массовая рассылка 24, 25

П

Пакет мобильного приложения 28

Плагин управления

обновление 32

установка 23

У

Установка

Kaspersky Security Center 21

на Android-устройства 15, 33, 37, 41, 46

на BlackBerry-устройства 20

на iOS-устройства 19, 48

на Symbian-устройства 20

на Windows Mobile-устройства 20