KASPERSKY lab

Kaspersky Endpoint Security 10 для Android

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 10.8.0.43

Уважаемый пользователь!

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

Дата редакции документа: 30.08.2018

Обозначение документа: 643.46856491.00080-03 90 01

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

Содержание

Об этом документе

Этот документ содержит описание подготовительных процедур и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security 10 для Android" (далее также "Kaspersky Endpoint Security для Android", "приложение").

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка Kaspersky Endpoint Security для Android", "Установка плагина Kaspersky Endpoint Security", "Удаление Kaspersky Endpoint Security для Android", "Подготовка программы к работе" и "Процедура приемки". Эти разделы содержат инструкции по безопасной установке и первоначальной настройке программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки программы.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Endpoint Security для Android, поддержка организаций, использующих Kaspersky Endpoint Security для Android, а также специалистам, которые имеют опыт работы с системой удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center.

Источники информации о программе

Приведенные ниже источники не являются эквивалентом настоящего документа и могут отличаться. Для корректной работы с программой рекомендуется использовать настоящее руководство.

Страница Kaspersky Endpoint Security для Android на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security для Android (http://www.kaspersky.ru/business-security/mobile#tab=frame-1) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security для Android содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Endpoint Security для Android в Базе знаний

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

На странице Kaspersky Endpoint Security для Android 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 Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security для Android, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

В состав электронной справки программы входят файлы справки.

В контекстной справке для плагина управления Kaspersky Endpoint Security для мобильных устройств вы можете найти информацию об окнах в Kaspersky Security Center: описание параметров Kaspersky Endpoint Security для Android и ссылки на описания задач, в которых используются эти параметры.

В полной справке для Kaspersky Endpoint Security для Android вы можете найти информацию о настройке и использовании мобильных приложений.

Обсуждение программ "Лаборатории Касперского" на форуме

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

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

О программе

Программное изделие "Kaspersky Endpoint Security 10 для Android" представляет собой средство антивирусной защиты типа "В" четвертого класса защиты и предназначено для применения на мобильных автоматизированных рабочих местах информационных систем.

Основными угрозами, для противостояния которым используется программное изделие, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия.

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования

В этом разделе содержатся аппаратные и программные требования к компьютеру администратора, который используется для развертывания приложения Kaspersky Endpoint Security для Android на мобильных устройствах, а также требования к мобильному устройству для работы приложения.

Аппаратные и программные требования к компьютеру администратора

Для развертывания Kaspersky Endpoint Security для Android компьютер администратора должен соответствовать аппаратным требованиям Kaspersky Security Center версии 10.0 Service Pack 3. Подробную информацию об аппаратных требованиях Kaspersky Security Center см. в *Руководстве администратора Kaspersky Security Center*.

Аппаратные и программные требования к мобильному устройству пользователя для Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android имеет следующие аппаратные и программные требования:

- смартфон или планшет с разрешением экрана от 320x480 пикселей;
- 65 МБ свободного места в основной памяти устройства;

- операционная система Android™ следующих версий:
  - Android 4.2;
  - Android 4.3;
  - Android 4.4;
  - Android 5.0;
  - Android 5.1;
  - Android 6.0;
  - Android 7.0;
  - Android 7.1;
  - Android 8.0;
  - Android 9.0.
- архитектура процессора Intel® Atom x86, ARM5, ARM6 или ARM7.

Приложение устанавливается только в основную память устройства.

Указания по эксплуатации и требования к среде

Для работы Kaspersky Endpoint Security для Android должны быть выполнены следующие условия:

1. Установка, конфигурирование и управление приложением должны осуществляться в соответствии с эксплуатационной документацией.
2. Приложение должно эксплуатироваться на мобильных устройствах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".

3. Приложение должно эксплуатироваться на мобильных устройствах, на которых у пользователей отсутствуют root-права.

4. Перед установкой и началом эксплуатации приложения необходимо установить все доступные обновления для используемых версий ПО среды функционирования.

5. Должен быть обеспечен доступ приложения ко всем объектам информационной системы, которые необходимы приложению для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).

6. Должна быть обеспечена совместимость приложения с контролируемыми ресурсами информационной системы.

7. Должна быть обеспечена возможность корректной совместной работы приложения со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.

8. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлено приложение.

9. Должна быть обеспечена синхронизация по времени между компонентами приложения, а также между приложением и средой ее функционирования.

10. Персонал, ответственный за функционирование приложения, должен обеспечивать надлежащее функционирование приложения, руководствуясь эксплуатационной документацией.

11. Должна быть обеспечена доверенная связь между приложением и уполномоченными субъектами информационной системы (администраторами безопасности).

12. Функционирование приложения должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности приложения.

13. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.

14. Должна быть обеспечена защищенная область для выполнения функций безопасности приложения.

15. Управление атрибутами безопасности, связанными с доступом к функциям и данным приложения, должно предоставляться только уполномоченным ролям (администраторам приложения и информационной системы).

16. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.

17. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Подготовка к установке программы

Перед установкой программы убедитесь, что программные и аппаратные ресурсы компьютера, на который будет произведена установка, удовлетворяют требованиям, приведенным в разделе "Аппаратные и программные требования".

Также нужно убедиться, что для операционной системы и программных средств, необходимых для установки (если таковые имеются), установлены самые последние пакеты обновлений, выпускаемые производителями операционной системы и программного обеспечения.

В этом разделе

Настройка параметров Сервера администрирования для подключения мобильных устройств

Чтобы мобильные устройства могли подключиться к Kaspersky Security Center, перед установкой мобильного приложения Kaspersky Endpoint Security для Android следует настроить в свойствах Сервера администрирования параметры подключения мобильных устройств.

► *Чтобы настроить параметры Сервера администрирования для подключения мобильных устройств, выполните следующие действия:*

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. Выберите раздел **Параметры**.

3. В блоке **Параметры подключения к Серверу администрирования** установите флажок **Открывать порт для мобильных устройств**.

4. В поле **Порт для мобильных устройств** укажите порт, по которому к Серверу администрирования будут подключаться мобильные устройства.

   По умолчанию используется порт 13292. Если флажок **Открывать порт для мобильных устройств** снят или порт для подключения указан неверно, мобильные устройства не смогут подключаться к Серверу администрирования.

5. Нажмите на кнопку **ОК**.

Отображение папки Управление мобильными устройствами в Консоли администрирования

Отображение папки **Управление мобильными устройствами** в Консоли администрирования позволяет просматривать перечень мобильных устройств, находящихся под управлением Сервера администрирования, настраивать параметры управления мобильными устройствами и устанавливать сертификаты на мобильные устройства пользователей.

► *Чтобы включить отображение папки **Управление мобильными устройствами** в Консоли администрирования, выполните следующие действия:*

1. В контекстном меню Сервера администрирования выберите пункт **Вид** → **Настройка интерфейса**.

2. В открывшемся окне установите флажок **Отображать Управление мобильными устройствами**.

3. Нажмите на кнопку **ОК**.

Папка **Управление мобильными устройствами** будет отображаться в дереве Консоли администрирования после перезапуска Консоли администрирования.

Создание группы администрирования

Централизованная настройка параметров приложения Kaspersky Endpoint Security для Android, установленного на мобильных устройствах пользователей, выполняется через применение к этим устройствам групповых политик (см. раздел "Групповые политики для управления мобильными устройствами" на стр. 34).

Для того чтобы применить политику к группе устройств, перед установкой мобильного приложения на устройства пользователей рекомендуется создать для этих устройств отдельную группу администрирования в папке **Управляемые устройства**.

После создания группы администрирования рекомендуется настроить автоматическое перемещение в эту группу устройств (см. раздел "Создание правила автоматического переноса устройств в группу администрирования" на стр. 17), на которые вы хотите установить приложение. Затем необходимо задать общие для всех устройств параметры с помощью групповой политики.

► *Чтобы создать группу администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** или вложенной папки выберите закладку **Устройства**.
3. Нажмите на кнопку **Создать группу**.

   Откроется окно создания новой группы.
4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем. Подробные сведения о работе с группами администрирования см. в *Руководстве администратора Kaspersky Security Center*.

Создание общего сертификата

Для идентификации пользователя мобильного устройства в Консоли администрирования необходимо создать общий сертификат.

► *Чтобы создать общий сертификат, выполните следующие действия:*

1. В дереве консоли выберите папку **Дополнительно** → **Управление мобильными устройствами** → **Сертификаты**.

2. В рабочей области папки **Сертификаты** по ссылке **Добавить сертификат** запустите мастер установки сертификатов.

3. В окне мастера **Выбор пользователя** укажите пользователей, для которых вы хотите создать общий сертификат.

4. В окне мастера **Тип сертификата** выберите вариант **Общий сертификат**.

5. В окне мастера **Источник сертификата** укажите способ создания общего сертификата.

   - Чтобы создать общий сертификат автоматически средствами Сервера администрирования автоматически, выберите вариант **Задать сертификат средствами Сервера администрирования**.

   - Чтобы назначить пользователю сертификат, созданный ранее, выберите вариант **Указать файл сертификата**. По кнопке **Задать** откройте окно **Сертификат** и укажите в нем файл сертификата.

     Снимите флажок **Опубликовать сертификат**, если вы не хотите указывать тип мобильного устройства и способ уведомления пользователя о создании сертификата.

6. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте.

7. В окне мастера **Информация о сертификате** нажмите на кнопку **Готово для** завершения работы мастера установки сертификатов.

В результате работы мастера установки сертификатов будет создан общий сертификат, который пользователь сможет установить на мобильное устройство. Для получения сертификата необходимо запустить синхронизацию мобильного устройства с Сервером администрирования. Подробную информацию о создании сертификатов и настройке правил их выпуска см. в *Руководстве администратора Kaspersky Security Center*.

Создание правила автоматического переноса устройств в группу администрирования

Централизованное управление параметрами приложения Kaspersky Endpoint Security для Android, установленного на мобильных устройствах пользователей, возможно только тогда, когда эти устройства находятся в созданной заранее группе администрирования, для которой назначена групповая политика (см. раздел "Создание группы администрирования" на стр. 15).

Если правило автоматического перемещения обнаруженных в сети мобильных устройств в группу администрирования не задано, то при первой синхронизации устройства с Сервером администрирования устройство автоматически попадает в Консоль администрирования в папку **Дополнительно** → **Опрос сети** → **Домены** → **KES10**. Групповая политика к этому устройству не применяется.

► *Чтобы создать правило автоматического перемещения мобильных устройств в группу администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Нераспределенные устройства**.
3. В разделе **Перемещение устройств** нажмите на кнопку **Добавить**, чтобы запустить процесс создания правила автоматического перемещения устройств в группу администрирования.

   Откроется окно **Новое правило**.

4. Введите имя правила.

5. Укажите группу администрирования, в которую должны помещаться устройства после установки на них мобильного приложения Kaspersky Endpoint Security для Android. Для этого нажмите на кнопку **Обзор** справа от поля **Группа, в которую следует перемещать устройства** и в открывшемся окне выберите группу.

6. В блоке **Выполнение правила** выберите вариант **Выполняется один раз для каждого устройства**.

7. Установите флажок **Перемещать только устройства, не размещенные в группах администрирования**, для того чтобы в результате применения правила мобильные устройства, уже распределенные в другие группы администрирования, не были перемещены в выбранную группу.

8. Установите флажок **Включить правило**, чтобы правило применялось для только что обнаруженных устройств.

9. Откройте раздел **Программы** и выполните следующие действия:

   a. Установите флажок **Версия операционной системы**.

   b. Выберите операционную систему Android для устройств, которые будут перемещаться в указанную группу.

10. Нажмите на кнопку **ОК**.

Созданное правило отображается в списке правил перемещения устройств в разделе **Перемещение устройств** окна свойств папки **Нераспределенные устройства**.

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

Установка Kaspersky Endpoint Security для Android

В этом разделе описаны способы развертывания Kaspersky Endpoint Security для Android в сети организации.

В этом разделе

Разрешения

Для работы всех функций приложений Kaspersky Endpoint Security для Android запрашивает у пользователя необходимые разрешения. Kaspersky Endpoint Security для Android запрашивает обязательные разрешения во время прохождения мастера установки, а также после установки перед использованием отдельных функций приложений. Без предоставления обязательных разрешений Kaspersky Endpoint Security для Android установить невозможно.

На некоторых устройствах (например, Huawei, Meizu, Xiaomi) требуется вручную добавить Kaspersky Endpoint Security для Android в список приложений, запускаемых при загрузке операционной системы (**Безопасность** → **Разрешения** → **Автозапуск**). Если приложение не добавлено в список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства.

Таблица 1. Обязательные разрешения для работы Kaspersky Endpoint Security для Android

Разрешение	Функция приложения
Управление вызовами	Подключение к Kaspersky Security Center (идентификатор устройства)
Доступ к памяти	Антивирус
Администратор устройства	Защита приложения от удаления
	Установка сертификатов безопасности

Установка через Kaspersky Security Center

Установка Kaspersky Endpoint Security для Android выполняется на мобильные устройства пользователей, учетные записи которых добавлены в Kaspersky Security Center. Подробнее о работе с учетными записями пользователей в Kaspersky Security Center см. в *Руководстве администратора Kaspersky Security Center, раздел "Управление учетными записями пользователей"*.

Для установки Kaspersky Endpoint Security для Android требуется выполнить следующие действия:

1. Создать инсталляционный пакет (см. раздел "Создание инсталляционного пакета" на стр. 23).

   Инсталляционный пакет – набор файлов, формируемый для дистанционной установки приложения "Лаборатории Касперского" при помощи Kaspersky Security Center.

2. Настроить параметры инсталляционного пакета (см. раздел "Настройка параметров инсталляционного пакета" на стр. 24).
3. Создать автономный пакет установки (см. раздел "Создание автономного пакета установки" на стр. 25).

   Автономный пакет установки – установочный файл мобильного приложения, содержащий параметры подключения приложения к Серверу администрирования. Создается на основе инсталляционного пакета для Kaspersky Endpoint Security для Android. Автономный пакет установки является частным случаем пакета мобильных приложений.

Пользователь получит ссылку на Веб-сервер, на котором расположен автономный пакет установки Kaspersky Endpoint Security для Android. Для установки приложения пользователю необходимо запустить apk-файл. Дополнительной настройки Kaspersky Endpoint Security для Android после установки не требуется.

Для установки Kaspersky Endpoint Security для Android на мобильном устройстве пользователя должна быть разрешена установка приложений из неизвестных источников (**Настройки Android** → **Безопасность** → **Неизвестные источники**).

► *Чтобы установить Kaspersky Endpoint Security для Android через Kaspersky Security Center, выполните следующие действия:*

1. В дереве консоли выберите папку **Дополнительно** → **Управление мобильными устройствами** → **Мобильные устройства**.
2. В рабочей области папки **Мобильные устройства** нажмите на кнопку **Добавить мобильное устройство**.

   Запустится мастер подключения нового мобильного устройства. Следуйте его указаниям.

3. В окне мастера **Операционная система** выберите **Android**.
4. В окне мастера **Способ установки Kaspersky Endpoint Security для Android** выберите **По ссылке на собственный Веб-сервер**.
5. В окне мастера **Выбор пользователей** выберите одного или нескольких пользователей для установки Kaspersky Endpoint Security для Android на их мобильные устройства.

   Если пользователя нет в списке, вы можете добавить новую учетную запись, не выходя из мастера подключения нового мобильного устройства.

6. В окне мастера **Источник сертификата** выберите источник сертификата для защиты обмена данными между Kaspersky Endpoint Security для Android и Kaspersky Security Center:

   - **Выписать сертификат средствами Сервера администрирования.** В этом случае сертификат будет создан автоматически.
   - **Указать файл сертификата**. В этом случае требуется предварительно подготовить собственный сертификат и выбрать его в окне мастера. Этот вариант невозможно использовать, если вы хотите установить Kaspersky Endpoint Security для Android на несколько мобильных устройств. Для каждого пользователя должен быть создан отдельный сертификат.

7. В окне мастера **Способ уведомления пользователей** выберите канал передачи ссылки для установки приложения:

   - Для передачи ссылки по электронной почте выберите **Отправить ссылку на Kaspersky Endpoint Security** и настройте параметры в блоке По **электронной почте**. Убедитесь, что в параметрах учетных записей пользователей указан адрес электронной почты.
   - Для передачи ссылки с помощью SMS-сообщения выберите **Отправить ссылку на Kaspersky Endpoint Security** и настройте параметры в блоке С **помощью SMS**. Убедитесь, что в параметрах учетных записей пользователей указан номер телефона.
   - Для установки Kaspersky Endpoint Security для Android с помощью QR-кода выберите **Показать ссылку на инсталляционный пакет** и выполните сканирование QR-кода с помощью камеры мобильного устройства.
   - Если вам не подошел ни один из перечисленных способов, выберите **Показать ссылку на инсталляционный пакет** → **Скопировать**, чтобы сохранить ссылку для установки Kaspersky Endpoint Security для Android в буфер обмена. Передайте ссылку для установки приложения любым доступным способом.

8. Завершите работу мастера подключения нового мобильного устройства.

После установки Kaspersky Endpoint Security для Android на мобильные устройства пользователей вы сможете настраивать параметры устройств и приложений с помощью групповых политик (см. раздел "Групповые политики для управления мобильными устройствами" на стр. 34).

Создание инсталляционного пакета

Инсталляционный пакет Kaspersky Endpoint Security для Android представляет собой самораспаковывающийся архив `ak_package.exe`. В состав архива входят файлы, необходимые для установки мобильного приложения на устройства:

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` – набор файлов, необходимый для установки мобильного приложения Kaspersky Endpoint Security для Android;
- `installer.ini` – конфигурационный файл с параметрами подключения к Серверу администрирования;
- `KES10_xx_xx_xxx.apk` – установочный файл мобильного приложения Kaspersky Endpoint Security для Android;
- `kmlisten.exe` – утилита доставки инсталляционного пакета на мобильное устройство через рабочую станцию;
- `kmlisten.ini` – конфигурационный файл с параметрами для утилиты доставки инсталляционного пакета;
- `kmlisten.kpd` – файл с описанием программы.

► *Чтобы создать инсталляционный пакет Kaspersky Endpoint Security для Android, выполните следующие действия:*

1. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. В рабочей области папки **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.

   Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.
3. В окне мастера **Выберите тип инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
4. В окне мастера **Выбор дистрибутива программы для установки** выберите самораспаковывающийся архив `ak_package.exe`, который входит в комплект поставки.

   Если архив был распакован ранее, то вы можете выбрать входящий в состав архива файл с описанием приложения `kmlisten.kpd`. В результате в поле ввода отобразится название приложения 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.

Настройка параметров инсталляционного пакета

► *Чтобы настроить параметры инсталляционного пакета, выполните следующие действия:*

1. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Kaspersky Endpoint Security для Android выберите пункт **Свойства**.
3. На закладке **Параметры** укажите параметры подключения мобильных устройств к Серверу администрирования и имя группы администрирования, 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.

     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, открытого 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 **KES10**).

     Указанная группа будет создана автоматически в папке **Дополнительно** → **Опрос сети** → **Домены**.

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

  Адрес электронной почты пользователя используется для формирования имени мобильных устройств при добавлении их в группу администрирования.

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

Создание автономного пакета установки

► *Чтобы создать автономный пакет установки, выполните следующие действия:*

1. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. Выберите инсталляционный пакет приложения Kaspersky Endpoint Security для Android.
3. В контекстном меню инсталляционного пакета выберите пункт **Создать автономный пакет установки**.

   В результате запустится мастер создания автономного пакета установки. Следуйте его указаниям.
4. Настройте способы распространения автономного пакета установки:

   - Чтобы распространить путь к сформированному автономному пакету установки среди пользователей по электронной почте, в блоке **Дальнейшие действия** перейдите по ссылке **Разослать ссылку на автономный пакет установки по электронной почте**.

     Откроется окно создания сообщения, текст которого содержит путь к папке общего доступа с автономным пакетом установки.

   - Чтобы разместить ссылку на сформированный автономный пакет установки на веб-сайте своей компании, перейдите по ссылке **Пример HTML-кода для размещения ссылки на веб-сайте**.

     Откроется tmp-файл, содержащий HTML_RJL ссылки.
5. Чтобы опубликовать сформированный автономный пакет установки на Веб-сервере Kaspersky Security Center, а также просмотреть весь список автономных пакетов для выбранного инсталляционного пакета, в окне мастера **Мастер создания автономного пакета установки успешно завершил работу** установите флажок **Открыть список автономных пакетов**.

После завершения работы мастера откроется окно **Список автономных пакетов для инсталляционного пакета <Имя инсталляционного пакета>**.

Окно **Список автономных пакетов для инсталляционного пакета <Имя инсталляционного пакета>** содержит следующую информацию:

- список автономных пакетов установки;
- сетевой путь к папке общего доступа в поле **Путь**;
- адрес автономного пакета на Веб-сервере Kaspersky Security Center в поле **Веб-адрес**.

При рассылке по электронной почте вы можете указать в качестве ресурса для загрузки пользователями установочного файла приложения как адрес, содержащийся в поле **Веб-адрес**, так и адрес, указанный в поле **Путь**. При рассылке SMS-сообщений пользователям следует указать ссылку для загрузки, содержащуюся в поле **Веб-адрес**.

Рекомендуется скопировать адрес подготовленного автономного пакета в буфер обмена, чтобы затем добавить ссылку для загрузки нужного установочного файла в сообщение электронной почты или SMS-сообщение для пользователей.

Настройка параметров синхронизации

Для применения групповой политики на мобильных устройствах пользователей следует настроить периодичность запуска синхронизации с Kaspersky Security Center.

По умолчанию мобильные устройства автоматически синхронизируются с Kaspersky Security Center каждые шесть часов. Автоматическая синхронизация в зоне роуминга включена.

► *Чтобы настроить параметры синхронизации мобильных устройств с Kaspersky Security Center, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.
2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.
3. Откройте окно свойств политики двойным щелчком мыши.

4. В окне **Свойства: <Название политики>** выберите раздел **Синхронизация**.

5. Выберите периодичность запуска синхронизации в раскрывающемся списке **Запускать синхронизацию**.

6. Чтобы запретить синхронизацию устройства с Kaspersky Security Center в роуминге, установите флажок **Выключить синхронизацию в роуминге**.

   Пользователь устройства может выполнять синхронизацию вручную в настройках приложения (→ **Настройки** → **Синхронизация** → **Синхронизировать**).

7. Чтобы скрыть от пользователя параметры синхронизации (адрес сервера, порт и группа администрирования) в настройках приложения, снимите флажок **Показывать параметры синхронизации на устройстве**. Изменить скрытые параметры невозможно.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Установка плагина Kaspersky Endpoint Security

Для управления мобильными устройствами на рабочее место администратора необходимо установить плагин управления Kaspersky Endpoint Security. Плагин управления Kaspersky Endpoint Security обеспечивает интерфейс управления мобильными устройствами и установленными на них мобильными приложениями через Консоль администрирования Kaspersky Security Center.

► *Чтобы установить плагин управления Kaspersky Endpoint Security,*

скопируйте из дистрибутива комплексного решения установочный файл плагина `klcfinst.exe` и запустите его на рабочем месте администратора.

Установка сопровождается мастером и не требует настройки параметров.

Вы можете убедиться, что плагин управления установлен, просмотрев список установленных плагинов управления программами в окне свойств Сервера администрирования в разделе **Дополнительно → Информация об установленных плагинах управления программами**.

Удаление Kaspersky Endpoint Security для Android

Вы можете дистанционно удалить Kaspersky Endpoint Security для Android с мобильных устройств пользователя следующими способами:

- С помощью групповой политики. Этот способ удобен, если вы хотите удалить приложение с нескольких устройств одновременно.
- С помощью настройки локальных параметров приложения. Этот способ удобен, если вы хотите удалить приложение с отдельного устройства.

► *Чтобы удалить приложение с помощью применения групповой политики, выполните следующие действия:*

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят мобильные устройства, на которых вы хотите удалить Kaspersky Endpoint Security для Android.
2. В рабочей области группы выберите закладку **Политики**.
3. В списке политик выберите политику для программы Kaspersky Endpoint Security для мобильных устройств.

   Если требуется, вы можете создать новую групповую политику.
4. Откройте окно свойств политики двойным щелчком мыши.
5. Выберите раздел **Дополнительно**.
6. В блоке **Удаление Kaspersky Endpoint Security для Android** установите флажок **Удалить с устройства Kaspersky Endpoint Security для Android**.
7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате после синхронизации с Сервером администрирования приложение Kaspersky Endpoint Security для Android будет удалено с мобильных устройств. Пользователи мобильных устройств получат уведомление об удалении приложения.

► *Чтобы удалить приложение с помощью настройки локальных параметров, выполните следующие действия:*

1. В дереве консоли выберите **Дополнительно** → **Управление мобильными устройствами** → **Мобильные устройства**.
2. В списке устройств выберите устройство, на котором вы хотите удалить приложение.
3. Откройте окно свойств устройства двойным щелчком мыши.
4. Выберите раздел **Программы** → **Kaspersky Endpoint Security для мобильных устройств <версия>**.
5. Откройте окно свойств приложения Kaspersky Endpoint Security двойным щелчком мыши.
6. Выберите раздел **Дополнительно**.
7. В блоке **Удаление Kaspersky Endpoint Security для Android** установите флажок **Удалить с устройства Kaspersky Endpoint Security для Android**.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате после синхронизации с Сервером администрирования приложение Kaspersky Endpoint Security будет удалено с мобильного устройства. Пользователь устройства получит уведомление об удалении приложения.

Подготовка программы к работе

После установки программы требуется выполнить следующие действия:

1. Создать отдельную группу администрирования для мобильных устройств.
2. Создать политику для мобильных устройств.
3. Активировать мобильное приложение Kaspersky Endpoint Security для Android.

В этом разделе

Создание группы администрирования

Централизованная настройка параметров приложения Kaspersky Endpoint Security для Android, установленного на мобильных устройствах пользователей, выполняется через применение к этим устройствам групповых политик (см. раздел "Групповые политики для управления мобильными устройствами" на стр. 34).

Для того чтобы применить политику к группе устройств, перед установкой мобильного приложения на устройства пользователей рекомендуется создать для этих устройств отдельную группу администрирования в папке **Управляемые устройства**.

После создания группы администрирования рекомендуется настроить автоматическое перемещение в эту группу устройств (см. раздел "Создание правила автоматического переноса устройств в группу администрирования" на стр. 17), на которые вы хотите установить приложение. Затем необходимо задать общие для всех устройств параметры с помощью групповой политики.

► *Чтобы создать группу администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** или вложенной папки выберите закладку **Устройства**.
3. Нажмите на кнопку **Создать группу**.

   Откроется окно создания новой группы.
4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем. Подробные сведения о работе с группами администрирования см. в *Руководстве администратора Kaspersky Security Center*.

Групповые политики для управления мобильными устройствами

Этот раздел содержит информацию о групповой политике для управления мобильными устройствами, создании и удалении групповой политики.

В этом разделе

О групповой политике

Групповая политика – это единый набор параметров для управления мобильными устройствами, входящими в группу администрирования, а также установленными на устройствах мобильными приложениями. Вы можете создать групповую политику с помощью мастера создания политики.

С помощью политики вы можете настраивать параметры как отдельных устройств, так и группы. Для группы устройств параметры управления можно настроить в окне свойств групповой политики, для одного устройства – в окне локальных параметров программы. Параметры управления, заданные индивидуально для одного устройства, могут отличаться от значений параметров, установленных в политике для группы, в которую входит это устройство.

Каждый параметр, представленный в политике, имеет атрибут – "замок", который показывает, наложен ли запрет на изменение параметра в политиках вложенного уровня иерархии (для вложенных групп и подчиненных Серверов администрирования) и в локальных параметрах программы.

Значения параметров, заданные в политике и в локальных параметрах программы, сохраняются на Сервере администрирования, распространяются на мобильные устройства в ходе синхронизации и сохраняются на устройствах в качестве действующих параметров.

Если пользователь установит на своем устройстве другие значения параметров, которые не были зафиксированы "замком", то при очередной синхронизации устройства с Сервером администрирования новые значения параметров будут переданы на Сервер администрирования и сохранены в локальных параметрах программы вместо значений, которые были установлены ранее администратором.

Подробную информацию о работе с политиками и группами администрирования в Консоли администрирования Kaspersky Security Center см. в *Руководстве администратора Kaspersky Security Center*.

Создание групповой политики

Политики, сформированные для группы администрирования, отображаются в рабочей области группы в Консоли администрирования Kaspersky Security Center на закладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус (активна / неактивна). В одной группе можно создать несколько политик для разных приложений. Активной может быть только одна политика для каждого приложения. При создании новой активной политики предыдущая активная политика становится неактивной.

Вы можете изменять политику после ее создания.

► *Чтобы создать политику для управления мобильными устройствами, выполните следующие действия:*

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

Следуйте указаниям мастера создания политики. Для перехода между окнами мастера используйте кнопку **Далее**. Чтобы прекратить работу мастера, нажмите на кнопку **Отмена** в окне мастера. В этом случае политика не будет создана.

Шаг 1. Определение названия групповой политики

На этом шаге в поле **Имя** укажите имя новой политики. Если вы укажете имя уже существующей политики, к нему автоматически будет добавлено окончание (1).

Перейдите к следующему шагу мастера создания политики.

Шаг 2. Выбор программы для создания групповой политики

На этом шаге в списке программ выберите **Kaspersky Endpoint Security для мобильных устройств <версия>**.

Создание политики для мобильных устройств возможно, если на рабочем месте администратора установлен плагин управления Kaspersky Endpoint Security. Если плагин не установлен, название соответствующей программы будет отсутствовать в списке программ.

Перейдите к следующему шагу мастера создания политики.

Шаг 3. Выбор состояния политики

На этом шаге мастер предлагает выбрать состояние политики:

- **Активная политика**. Мастер сохраняет созданную политику на Сервере администрирования. При следующей синхронизации мобильного устройства с Сервером администрирования политика будет использоваться на устройстве в качестве действующей.
- **Неактивная политика**. Мастер сохраняет созданную политику на Сервере администрирования как резервную. В дальнейшем политика может быть активирована по событию. При необходимости неактивную политику можно сделать активной.

> Для одной программы в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика автоматически становится неактивной.

Завершите работу мастера.

Удаление групповой политики

► *Чтобы удалить групповую политику, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно удалить политику.
2. В рабочей области группы администрирования на закладке **Политики** выберите политику, которую вы хотите удалить.

3. В контекстном меню политики выберите пункт **Удалить**.

В результате групповая политика будет удалена. До применения новой групповой политики мобильные устройства, входящие в группу администрирования, продолжат работу с параметрами, заданными в удаленной политике.

Активация приложения

В Kaspersky Security Center лицензия может распространяться на различные группы функциональности. Для полноценного функционирования Kaspersky Endpoint Security для Android необходимо, чтобы приобретенная организацией лицензия на Kaspersky Security Center распространялась на функциональность **Управление мобильными устройствами**. Функциональность **Управление мобильными устройствами** предназначена для подключения мобильных устройств к Kaspersky Security Center и управления ими.

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

Особенность активации приложения Kaspersky Endpoint Security для Android состоит в том, что информация о лицензии передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.

Если активация приложения не произошла в течение трех дней с момента установки на мобильное устройство, то приложение автоматически переключается в режим работы с ограниченной функциональностью. В этом режиме работы большинство компонентов приложения не работает. При переходе в режим работы с ограниченной функциональностью приложение прекращает выполнять автоматическую синхронизацию с Kaspersky Security Center. Поэтому, если по каким-то причинам активация приложения не произошла в течение трех дней с момента установки, пользователю необходимо вручную выполнить синхронизацию с Kaspersky Security Center.

► *Чтобы активировать приложение Kaspersky Endpoint Security для Android, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.

2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В окне **Свойства: <Название политики>** выберите раздел **Лицензирование**.

5. В блоке **Лицензия** в раскрывающемся списке **Ключ** выберите ключ для активации приложения, размещенный в хранилище ключей Сервера администрирования Kaspersky Security Center.

   В поле ниже отобразится информация о приложении, для которого приобретена лицензия, срок окончания действия лицензии, ее тип.

6. Установите флажок **Активировать ключом из хранилища Kaspersky Security Center**.

   Если приложение активировано без помощи ключа, размещенного в хранилище Kaspersky Security Center, Kaspersky Security для мобильных устройств заменит этот ключ на ключ активации выбранный в списке **Ключ**.

7. Чтобы активировать приложение на мобильном устройстве пользователя, заблокируйте изменение параметров.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Приложение Kaspersky Endpoint Security для Android активировано на всех мобильных устройствах.
- На главном окне Kaspersky Endpoint Security для Android отображается сообщение **Устройство защищено** (см. рис. ниже).
- Антивирусные базы приложения обновлены на всех мобильных устройствах.
- Настроена активная политика, которая применяется на всех мобильных устройствах.
- Настроено расписание антивирусной проверки всей файловой системы мобильного устройства.

- Параметры приложения находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Сертифицированное состояние программы" на стр. 71).

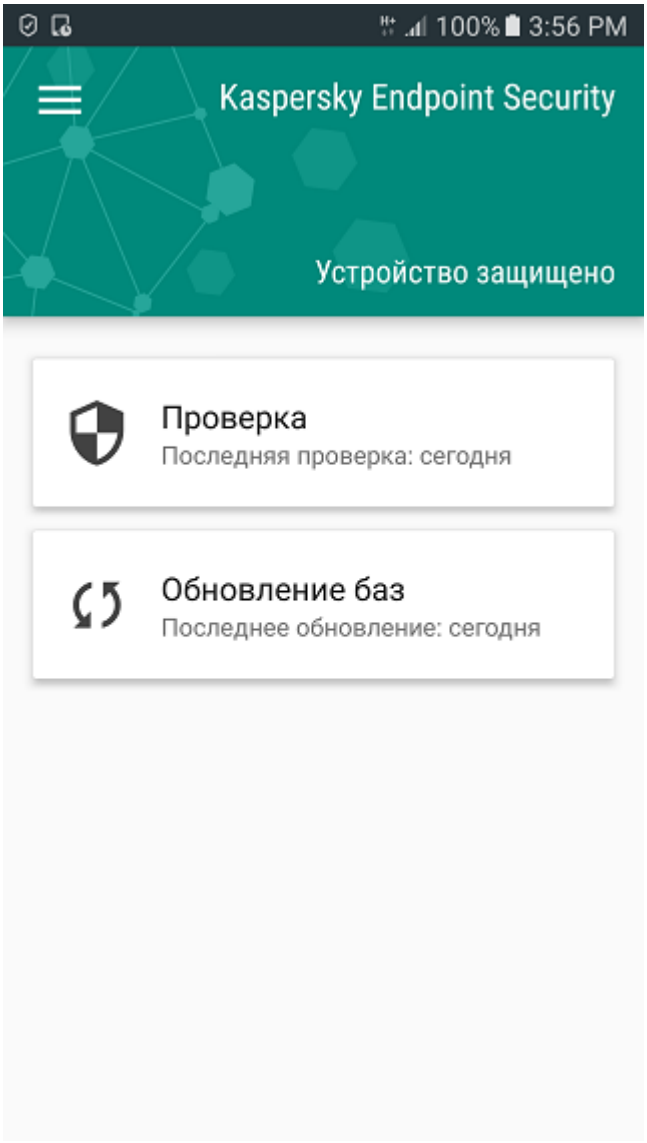

Рисунок 1. Интерфейс приложения в безопасном состоянии

Проверка работоспособности. EICAR

Чтобы проверить работоспособность Антивируса, вы можете использовать тестовый "вирус" EICAR.

Тестовый вирус предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый вирус не является вирусом и не содержит программного кода, который может нанести вред вашему мобильному устройству, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Файл, который содержит тестовый вирус, называется eicar.com. Вы можете загрузить его со страницы сайта **EICAR** http://www.eicar.org/anti_virus_test_file.htm.

Перед сохранением файла на мобильном устройстве убедитесь, что постоянная защита файлов в этой папке отключена.

Проверка работоспособности Антивируса состоит из следующих этапов.

1. Проверка работоспособности при установке вредоносного приложения.
2. Проверка работоспособности при загрузке вредоносного файла во внутреннюю память мобильного устройства.

► *Чтобы проверить работоспособность Антивируса при установке вредоносного приложения, выполните следующие действия:*

1. Запустите приложение Google Play™ на устройстве.
2. Найдите приложение Test Virus. Для этого в строке поиска Google Play введите название приложения и нажмите **ENTER**.
3. Выберите Test Virus в списке результатов поиска. Test Virus разработан организацией Itus Mobile Security.

   Откроется страница с подробными сведениями о Test Virus.
4. На странице подробных сведений о приложении нажмите **Установить**.
5. Ознакомьтесь со списком прав, которые нужны приложению Test Virus.
6. Нажмите **Принять**.

Начнется загрузка и установка приложения Test Virus. Kaspersky Endpoint Security для Android обнаружит вредоносное приложение и предложит его удалить. Установка Test Virus будет прекращена. Вы можете просмотреть результаты работы Kaspersky Endpoint Security для Android в отчетах (→ **Отчеты**).

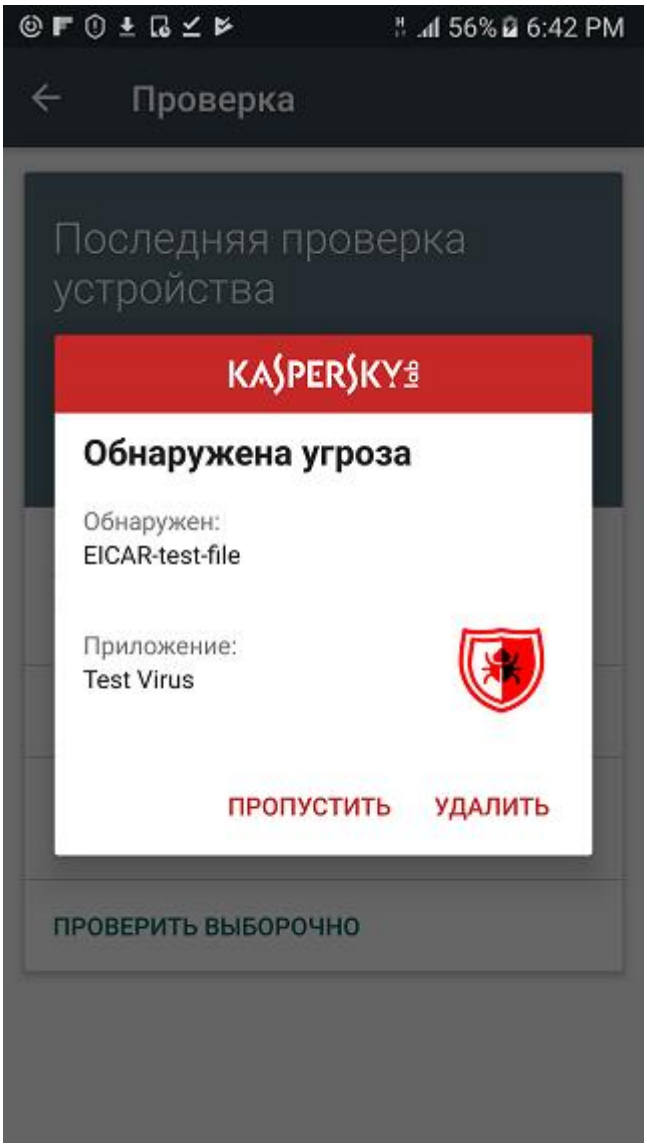

Рисунок 2. Обнаружение вредоносного приложения

► *Чтобы проверить работоспособность Антивируса при загрузке вредоносного файла, выполните следующие действия:*

1. Откройте в браузере сайт **EICAR** http://www.eicar.org/anti_virus_test_file.htm на устройстве.

2. Выберите раздел Download.

3. Найдите файл тестового "вируса" eicar.com.txt и загрузите файл на устройство.

Начнется загрузка "вируса". Kaspersky Endpoint Security для Android обнаружит вредоносный файл и удалит его. Вы можете просмотреть результаты работы Kaspersky Endpoint Security для Android в отчетах (→ **Отчеты**).

Разделение доступа к функциям программы по пользовательским ролям

В Kaspersky Endpoint Security для Android предусмотрены следующие учетные записи:

- Учетная запись администратора Kaspersky Security Center.
- Учетная запись пользователя мобильного устройства.

Администратор Kaspersky Security Center

Учетная запись администратора служит для управления мобильным устройством. Администратор управляет мобильным устройством с помощью Консоли администрирования Kaspersky Security Center. Администратор создает групповые политики, в которых может настроить параметры работы Kaspersky Endpoint Security для Android. У администратора есть возможность заблокировать пользователю мобильного устройства доступ к настройкам Kaspersky Endpoint Security для Android с помощью атрибута "замок"  в групповой политике. Администратор также имеет возможность дистанционно удалить Kaspersky Endpoint Security для Android. Таким образом мобильное устройство перестает быть управляемым.

Администраторы Kaspersky Security Center могут настраивать права доступа пользователей Консоли администрирования к различным функциям программы в зависимости от служебных обязанностей пользователей.

В интерфейсе Консоли администрирования настройка прав доступа выполняется в окне свойств Сервера администрирования на закладках **Безопасность** и **Роли пользователей**. На закладке **Роли пользователей** можно добавлять типовые роли пользователей с настроенным набором прав. В разделе **Безопасность** можно настраивать права для одного пользователя или для группы пользователей, а также назначать роли одному пользователю или группе пользователей. Права пользователей для каждой программы настраиваются по *функциональным областям*.

Для каждой функциональной области администратор может назначать следующие права доступа:

- **Разрешить изменение**. Пользователю Консоли администрирования разрешено изменять параметры политики в окне ее свойств.
- **Запретить изменение**. Пользователю Консоли администрирования запрещено изменять параметры политики в окне ее свойств. Закладки политики, входящие в функциональную область, для которой назначено это право, не отображаются в интерфейсе.

Соответствие функциональных областей и разделов политики приведено в таблице ниже.

Таблица 2. Права доступа к разделам плагина управления Kaspersky Endpoint Security

Функциональная область	Раздел политики
Android for Work	Управление Android for Work
Анти-Вор	Анти-Вор
Контроль приложений	Контроль приложений, Сторонние приложения
Защита	Защита, Проверка, Обновление
Контроль соответствия	Контроль соответствия
Контейнеры	Контейнеры
Параметры устройства	Управление устройством, Синхронизация
Управление устройствами Samsung	Общие параметры, Параметры для KNOX 1, Параметры для KNOX 2
Управление системой	Дополнительно, Wi-Fi
Веб-Фильтр	Веб-Фильтр

Пользователь мобильного устройства

Учетная запись пользователя мобильного устройства служит для управления мобильным устройством и Kaspersky Endpoint Security для Android. Пользователь мобильного устройства может запускать антивирусную проверку и обновлять антивирусные базы без ограничений. Администратор Kaspersky Security Center может ограничить пользователю мобильного устройства доступ к настройками Kaspersky Endpoint Security для Android, расписанию антивирусных проверок, удалению приложения.

Настройка антивирусной защиты Android-устройств

Для своевременного обнаружения угроз, поиска вирусов, а также других вредоносных приложений следует настроить параметры постоянной защиты и автоматический запуск антивирусной проверки.

Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.

► *Чтобы настроить параметры постоянной защиты мобильного устройства, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.
2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В окне **Свойства: <Название политики>** выберите раздел **Защита**.
5. В блоке **Защита** настройте параметры защиты файловой системы мобильного устройства:
   - Установите флажок **Включить защиту**.

     Kaspersky Endpoint Security для Android будет проверять только новые приложения и файлы из папки Загрузки.
   - Установите флажок **Расширенный режим защиты**.

     Kaspersky Endpoint Security для Android будет проверять все файлы, которые пользователь открывает, изменяет, перемещает, копирует, запускает и сохраняет на устройстве, а также мобильные приложения сразу после их установки.

- Снимите флажок **Использовать Kaspersky Security Network**.

  Kaspersky Endpoint Security для Android не будет выполнять дополнительную проверку новых приложений до их первого запуска на устройстве пользователя при помощи облачной службы Kaspersky Security Network.

- Установите флажок **Защита от рекламы и автодозвона**.

  Kaspersky Endpoint Security для Android будет блокировать рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя.

6. В списке **Действие, если лечение невозможно** выберите вариант **Удалить** или **На карантин**.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

► *Чтобы настроить автоматический запуск антивирусной проверки мобильного устройства, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.

2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В окне **Свойства: <Название политики>** выберите раздел **Проверка**.

5. В блоке **Параметры проверки устройства** настройте параметры проверки:

   - Снимите флажок **Проверять только исполняемые файлы**.

     Kaspersky Endpoint Security для Android будет проверять все файлы, сохраненные на устройстве и на карте расширения памяти.

   - Установите флажок **Проверять архивы с распаковкой**.

     Kaspersky Endpoint Security для Android будет проверять содержимое архивов размером до 2 Гб.

- Установите флажок **Лечить файлы, если это возможно**.

  Если лечение невозможно, приложение выполняет действие, выбранное для невылеченных объектов в списке **Действие, если лечение невозможно**. Если флажок снят, Kaspersky Endpoint Security для Android при обнаружении угрозы выполняет действие, выбранное в списке **Действие при обнаружении угрозы**.

  Вариант **Запросить действие** позволяет пользователю устройства при обнаружении нескольких угроз применить выбранное действие к каждому файлу с помощью флажка **Применить ко всем угрозам**.

6. В блоке **Проверка по расписанию** настройте параметры автоматического запуска полной проверки файловой системы устройства. Для этого нажмите на кнопку **Расписание** и в открывшемся окне **Расписание** задайте периодичность и время запуска полной проверки.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Для поддержания защиты мобильного устройства в актуальном состоянии следует настроить параметры обновления антивирусных баз.

По умолчанию обновление антивирусных баз приложения в зоне роуминга выключено. Обновление антивирусных баз приложения по расписанию не выполняется.

► *Чтобы настроить параметры обновления антивирусных баз приложения, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.

2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В окне **Свойства: <Название политики>** выберите раздел **Обновление баз**.

5. Чтобы Kaspersky Endpoint Security загружал обновления баз по сформированному расписанию, когда устройство находится в зоне роуминга, в блоке **Обновление баз в роуминге** установите флажок **Разрешать обновление баз в роуминге**.

   Даже если флажок снят, пользователь может запустить обновление антивирусных баз в роуминге вручную.

6. В блоке **Источник обновлений баз** укажите источник обновлений, из которого Kaspersky Endpoint Security будет получать и устанавливать обновления антивирусных баз приложения, **Сервер администрирования**.

7. В блоке **Обновление баз по расписанию** настройте параметры автоматического запуска обновлений антивирусных баз на устройстве пользователя. Для этого нажмите на кнопку **Расписание** и в открывшемся окне **Расписание** задайте периодичность и время запуска обновления.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Защита Kaspersky Endpoint Security для Android от удаления

Для защиты мобильного устройства и выполнения требований корпоративной безопасности вы можете включить защиту Kaspersky Endpoint Security для Android от удаления. В этом случае пользователю недоступно удаление приложения с помощью интерфейса Kaspersky Endpoint Security для Android. При удалении приложения с помощью инструментов операционной системы Android появится запрос на выключение прав администратора для Kaspersky Endpoint Security для Android. После выключения прав мобильное устройство будет заблокировано.

На некоторых Samsung-устройствах под управлением операционной системы Android 7.0 и выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) устройство может быть заблокировано, если выполнены следующие условия: включена защита Kaspersky Endpoint Security для Android от удаления (см. стр. 50) и заданы требования к надежности пароля разблокировки экрана. Для разблокировки устройства требуется отправить на устройство специальную команду.

► *Чтобы включить защиту Kaspersky Endpoint Security для Android от удаления, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.
2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В окне **Свойства: <Название политики>** выберите раздел **Дополнительно**.
5. В блоке **Удаление Kaspersky Endpoint Security для Android** снимите флажок **Разрешить удаление Kaspersky Endpoint Security для Android**.

На устройствах под управлением операционной системы Android версии 7.0 и выше для защиты приложения от удаления Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android предлагает пользователю предоставить приложению необходимые права. Пользователь может пропустить эти шаги или выключить права в параметрах устройства позднее. В этом случае защита приложения от удаления не работает.

6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. При попытке удаления приложения мобильное устройство будет заблокировано.

Обнаружение взлома устройства (root)

Kaspersky Endpoint Security для Android позволяет обнаруживать взлом устройства (root). На взломанном устройстве системные файлы не защищены и доступны для изменения. Также на взломанном устройстве доступна установка сторонних приложений из неизвестных источников. После обнаружения взлома рекомендуется восстановить нормальную работу устройства.

При взломе устройства вы получите уведомление после синхронизации мобильного устройства с Kaspersky Security Center. Вы можете просмотреть уведомления о взломе в рабочей области Сервера администрирования на закладке **Мониторинг**. Вы также можете выключить уведомление о взломе в параметрах уведомлений о событиях.

Настройка отображения Android-устройств в Kaspersky Security Center

Для удобства работы со списком мобильных устройств следует настроить параметры отображения устройства в Kaspersky Security Center. По умолчанию список мобильных устройств отображается в дереве консоли **Дополнительно** → **Управление мобильными устройствами** → **Мобильные устройства**. Информация об устройстве обновляется автоматически. Вы также можете обновить список мобильных устройств вручную по кнопке **Обновить** в правом верхнем углу.

Вы можете настроить формат имени устройства, а также выбрать статус устройства. Статус устройства информирует вас о работе компонентов Kaspersky Endpoint Security для Android на мобильном устройстве пользователя. Компоненты Kaspersky Endpoint Security для Android могут не работать по следующим причинам:

- Пользователь выключил компонент в настройках устройства.
- Пользователь не предоставил приложению необходимые права для работы компонента (например, отсутствует разрешение на определение местоположения устройства для выполнения соответствующей команды Анти-Вора).

Для отображения статуса устройства необходимо включить условие **Определяемый программой** в свойствах группы администрирования (**Свойства** → **Статус устройства** → **Условия для статуса устройства "Критический"** и **Условия для статуса устройства "Предупреждение"**). В свойствах группы администрирования вы также можете выбрать другие критерии для формирования статуса мобильного устройства.

► *Чтобы настроить отображение Android-устройств в Kaspersky Security Center, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.
2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.

3. Откройте окно свойств политики двойным щелчком мыши.
4. В окне **Свойства: <Название политики>** выберите раздел **Информация об устройстве**.
5. В блоке **Имя устройства в Kaspersky Security Center** выберите формат имени устройства:
   - `<Модель устройства / Электронная почта / IMEI>`;
   - `<Модель устройства / Электронная почта (если есть) или IMEI>`.

   В списке мобильных устройств в графе **Имя устройства** устройство будет отображаться в виде выбранного формата.
6. Установите атрибут "замок" в закрытое положение.
7. В блоке **Статус устройства в Kaspersky Security Center** выберите статус устройства, если не работает компонент Kaspersky Endpoint Security для Android: (**Критический**), (**Предупреждение**) или (**ОК**).

   В списке мобильных устройств статус устройства будет изменен в соответствии с выбранным статусом.
8. Установите атрибут "замок" в закрытое положение.
9. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка уведомлений Kaspersky Endpoint Security

Если вы хотите, чтобы пользователь мобильного устройства не отвлекался на уведомления Kaspersky Endpoint Security для Android, вы можете выключить некоторые уведомления.

По умолчанию все уведомления Kaspersky Endpoint Security включены.

► *Чтобы настроить отображение уведомлений о работе Kaspersky Endpoint Security для Android, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую добавлены мобильные устройства.
2. В рабочей области группы администрирования на закладке **Политики** выберите политику для управления мобильными устройствами.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В окне **Свойства: <Название политики>** выберите раздел **Дополнительно**.
5. В блоке **Уведомление пользователя** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры уведомлений на устройстве**.
6. Выберите уведомления Kaspersky Endpoint Security, которые вы хотите показывать на мобильном устройстве пользователя.

   > Некоторые уведомления Kaspersky Endpoint Security являются обязательными и их невозможно выключить (например, уведомления об истечении срока действия лицензии).
7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. На мобильном устройстве пользователя не будут отображаться уведомления Kaspersky Endpoint Security, которые вы выключили.

Участие в Kaspersky Security Network

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

Использование KSN приводит к выходу программы из сертифицированного состояния.

► *Чтобы выключить использование Kaspersky Security Network, выполните следующие действия:*

1. Откройте окно настройки параметров политики управления мобильными устройствами, на которых установлено Kaspersky Endpoint Security для Android.
2. В окне **Свойства: <Название политики>** выберите раздел **Дополнительно**.
3. В блоке **Параметры Kaspersky Security Network** снимите флажок **Использовать Kaspersky Security Network** чтобы выключить использование Kaspersky Security Network.
4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. После применения политики компоненты, использующие Kaspersky Security Network, будут выключены и настройка компонентов будет недоступна.

Предоставление данных в сервисы Google

Чтобы повысить качество работы Kaspersky Endpoint Security для Android, приложение использует сервисы Google™: Google Cloud Messaging и Google Analytics™. Схему взаимодействия Kaspersky Endpoint Security для Android и сервисов Google см. на рис. ниже.

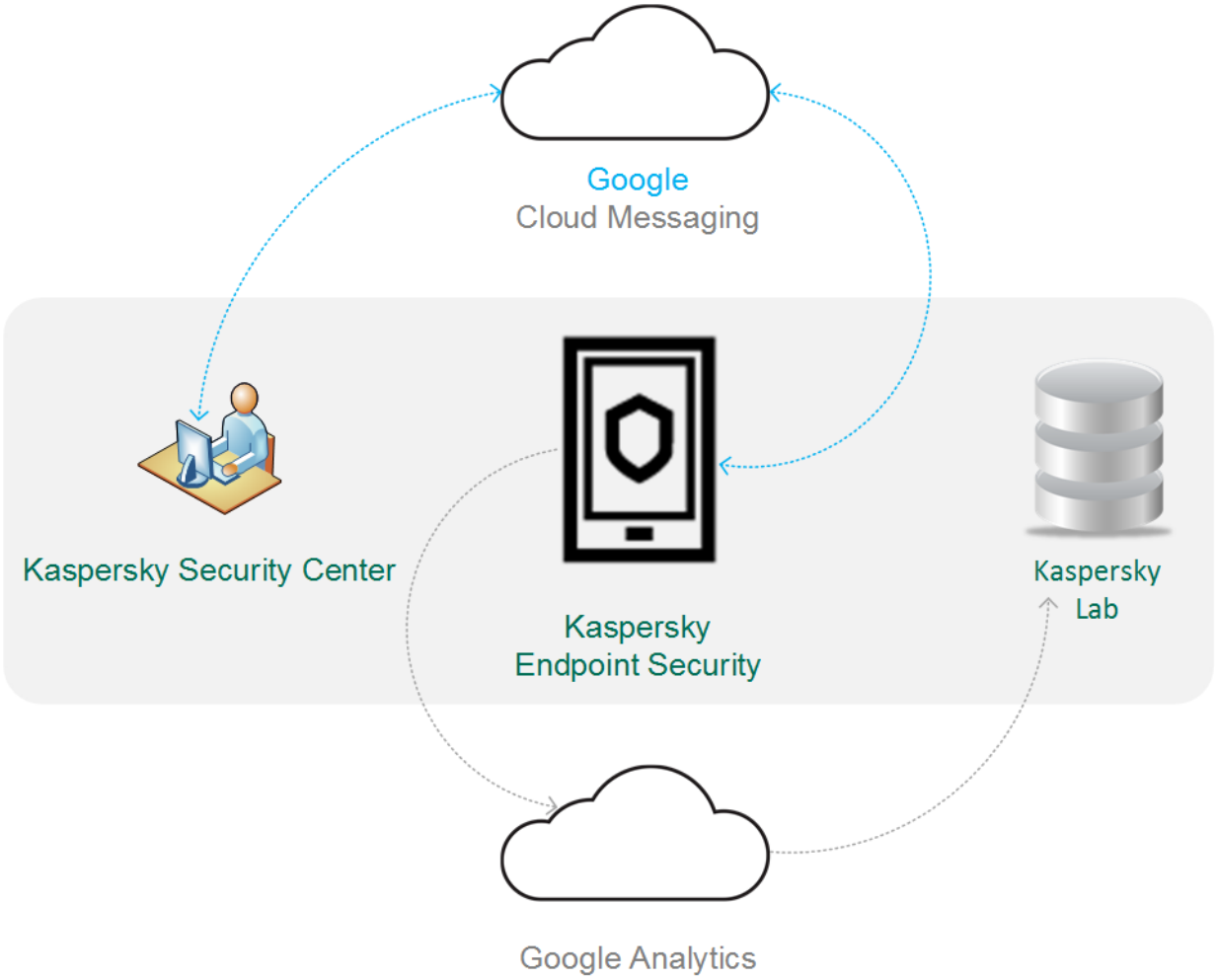

Рисунок 3. Схема взаимодействия Kaspersky Endpoint Security для Android и сервисов Google

В этом разделе

Обмен информацией с Google Cloud Messaging

Kaspersky Endpoint Security для Android использует сервис Google Cloud Messaging для своевременной доставки команд на мобильные устройства. При этом приложение использует механизм push-уведомлений.

Для использования сервиса Google Cloud Messaging необходимо настроить параметры сервиса в Kaspersky Security Center. Подробнее о настройке Google Cloud Messaging в Kaspersky Security Center см. в *Руководстве администратора Kaspersky Security Center, раздел "Управление мобильными устройствами"*. Если параметры Google Cloud Messaging не настроены, команды на мобильном устройстве будут выполняться во время синхронизации устройства с Kaspersky Security Center по расписанию, установленному в политике (например, каждые 24 ч.). Т.е. команды будут выполнены с задержкой.

► *Чтобы запретить обмен информацией с сервисом Google Cloud Messaging, выполните следующие действия:*

1. В дереве консоли выберите **Дополнительно** → **Управление мобильными устройствами** → **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки **Мобильные устройства** выберите раздел **Параметры Google Firebase Cloud Messaging**.
4. Нажмите на кнопку **Сбросить параметры**.

Обмен информацией с Google Analytics

Передача данных в сервис Google Analytics осуществляется по защищенному каналу. Доступ к информации и ее защита регулируются соответствующими условиями использования сервиса Google Analytics.

► *Чтобы запретить обмен данными с сервисом Google Analytics, выполните следующие действия:*

1. Откройте окно настройки параметров политики управления мобильными устройствами, на которых установлено приложение Kaspersky Endpoint Security для Android.
2. В окне **Свойства: <Название политики>** выберите раздел **Дополнительно**.
3. В блоке **Передача данных** снимите флажок **Разрешить передачу данных в Google Analytics**.
4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать срочные пакеты обновлений программного обеспечения, устраняющие уязвимости и ошибки. Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского".

Для сохранения бинарной целостности сертифицированной программы запрещается устанавливать обновления программных модулей, не прошедшие инспекционный контроль. Прошедшие инспекционный контроль обновления программных модулей необходимо получать путем обращения в техническую поддержку АО "Лаборатория Касперского" по телефонам: +7 (495) 663-81-47, 8-800-700-88-11 или из регулярно обновляемых статей об актуальных версиях сертифицированных программ на сайте разработчика-изготовителя (http://support.kaspersky.ru/general/certificates). Информацию об обновлениях следует проверять не реже, чем один раз в месяц.

Программы должны периодически (один раз в полгода) подвергаться анализу уязвимостей: компания, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с сайта разработчика-изготовителя (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- На форуме "Лаборатории Касперского" (http://forum.kaspersky.com).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки.

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2b);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

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

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	http://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	http://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки Kaspersky Endpoint Security для Android.

На Android-устройствах информация о стороннем коде доступна в приложении Kaspersky Endpoint Security для Android по кнопке  → **О приложении**.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Android, Google, Google Play, Google Analytics – товарные знаки Google, Inc.

ARM – товарный знак или зарегистрированный товарный знак ARM Ltd. или дочерних компаний.

Intel, Atom – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 3. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

Приложение. Сертифицированное состояние программы

Этот раздел содержит перечень параметров программы, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии.

Если вы меняете какие-либо из перечисленных параметров с их значений в сертифицированном состоянии на другие значения, вы выводите программу из сертифицированного состояния.

Таблица 4. Параметры и их значения для программы в сертифицированном состоянии

Сущность, к которой относится параметр	**Название параметра**	**Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)**
Kaspersky Security Network (KSN)	Использовать Kaspersky Security Network	Флажок снят.
Сервис Google Analytics	Разрешить передачу данных в Google Analytics	Флажок снят.
Сервис Google Firebase Cloud Messaging (push-уведомления)	Параметры Google Firebase Cloud Messaging	Пусто.
Лицензирование приложения	Способ активации программы	Код активации.
Удаление Kaspersky Endpoint Security для Android пользователем мобильного устройства	Разрешить удаление Kaspersky Endpoint Security для Android	Флажок снят.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Журнал Kaspersky Security Center	Включить аудит	Флажок установлен.
Общие параметры политики	Состояние политики	Активная политика.
	Наследовать параметры политики верхнего уровня	Флажок установлен.
	Форсировать наследование параметров дочерней политики	Флажок снят.
Синхронизация мобильного устройства с Kaspersky Security Center	Запускать синхронизацию	Одно из следующих значений: • Каждые 15 мин. • Каждый час. • Каждые 3 ч. • Каждые 6 ч.
	Выключить синхронизацию в роуминге	Флажок снят.
	Показывать параметры синхронизации на устройстве	Флажок установлен.
Антивирусная проверка	Проверять только исполняемые файлы	Флажок снят.
	Проверять архивы с распаковкой	Флажок установлен.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
	Лечить файлы, если возможно	Флажок установлен.
	Действие если лечение невозможно	Одно из следующих значений: • На карантин. • Удалить.
	Проверка по расписанию	Одно из следующих значений: • После обновления антивирусных баз. • Раз в день.
Защита в реальном времени	Включить защиту	Флажок установлен.
	Расширенный режим защиты	Флажок установлен.
	Использовать KSN	Флажок снят.
	Защиты от рекламы и автодозвона	Флажок установлен.
	Проверять только исполняемые файлы	Флажок снят.
	Действие, если лечение невозможно	Одно из следующих значений: • На карантин. • Удалить.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Обновление антивирусных баз	Разрешить обновление в роуминге	Флажок установлен.
	Источник обновления баз	Сервер администрирования.
	Обновление баз по расписанию	Раз в день в 8:00.