ESET MOBILE SECURITY

ДЛЯ ANDROID

Инструкция по установке и руководство пользователя

Щелкните здесь, чтобы загрузить актуальную версию этого документа

Содержание

ESET **MOBILE SECURITY**

Приложение ESET Mobile Security разработано компанией ESET, spol. s r.o..
Для получения дополнительных сведений посетите веб-сайт www.eset.com.

Служба поддержки клиентов: www.eset.com/support

Версия 20. 10. 2011

1. Установка ESET Mobile Security

Установить ESET Mobile Security для Android на мобильном устройстве можно, если оно соответствует указанным ниже системным требованиям.

	Минимальные системные требования
Операционная система	Android 2.0/2.1 (Éclair) и более поздних версий
CPU	600 МГц
RAM	256 МБ
Свободный объем внутренней памяти телефона	5 МБ

Android 3.0 (Honeycomb) не поддерживается.

1.1 Установка

Для установки ESET Mobile Security воспользуйтесь одним из следующих вариантов действий.

- Найдите **ESET Mobile Security** (или просто **Eset**) в Android Market. Данное приложение находится в разделе **Приложения** > **Инструменты**.
- Загрузите установочный файл ESET Mobile Security *(ems.apk)* на компьютер с веб-сайта ESET. Подключите мобильное устройство к этому компьютеру по USB или Bluetooth и скопируйте данный файл в нужное место.
- Загрузите файл *ems.apk*, просканировав показанный ниже QR-код с помощью своего мобильного устройства и специального приложения, такого как QR Droid или Barcode Scanner.

ESET Mobile Security **QR-код**

Если ESET Mobile Security устанавливается вручную, нажмите значок Launcher на главном экране Android (или перейдите на экран **Главная** > **Меню**), перейдите в раздел **Настройки** > **Приложения** и выберите вариант **Неизвестные источники**. Найдите файл *ems.apk* с помощью такого приложения, как ASTRO File Manager или ES File Explorer. Откройте этот файл и нажмите **Установить** . После завершения установки приложения нажмите **Открыть**.

После установки активируйте ESET Mobile Security в соответствии с инструкциями, приведенными в разделе Активация приложения 4.

1.2 Удаление приложения

Если нужно удалить ESET Mobile Security с устройства, выполните следующие действия.

1. Нажмите значок Launcher на главном экране Android (или перейдите на экран **Главная** > **Меню**), воспользуйтесь командами **Настройки** > **Местоположение и защита** > **Выбрать администраторов**, отмените выбор **EMS** и нажмите **Отключить**. Введите свой пароль ESET Mobile Security по запросу. (Если вы не выбирали ESET Mobile Security в качестве администратора устройства, переходите сразу к следующему действию.)
2. Вернитесь к окну **Настройки** и нажмите **Приложения** > **Управление приложениями** > **ESET Security** > **Удалить**.

ESET Mobile Security и папка карантина будут удалены с мобильного устройства без возможности восстановления.

2. Активация программы

После успешного выполнения установки нужно активировать ESET Mobile Security. Нажмите **Активировать сейчас** на главном экране ESET Mobile Security.

Существует три способа активации. Выбор конкретного способа зависит от того, каким образом было приобретено приложение ESET Mobile Security.

- Выберите вариант **Активировать пробную лицензию**, если у вас нет лицензии, но вы хотите оценить ESET Mobile Security в деле, прежде чем совершать покупку. Укажите свой адрес электронной почты в поле **Почта**, чтобы активировать ESET Mobile Security на ограниченный период времени. После успешной активации программного продукта вы получите по электронной почте подтверждение. Пробную лицензию можно активировать для любого мобильного устройства только один раз.
- **Активация с помощью ключа активации**: если приложение ESET Mobile Security было приобретено с новым устройством или как коробочная версия, вместе с покупкой был предоставлен ключ активации. Введите полученную информацию в поле **Ключ активации**, а свой текущий адрес электронной почты в поле **Почта**. Новые данные для аутентификации (имя пользователя и пароль) автоматически заменят ключ активации и будут отправлены на указанный адрес электронной почты.
- **Активировать с помощью имени пользователя и пароля**: если приложение было приобретено у дистрибьютора, имя пользователя и пароль были предоставлены при покупке. Введите полученную информацию в поля **Имя пользователя** и **Пароль**. В поле **Почта** введите свой текущий адрес электронной почты.
- **Купить**: выберите этот вариант, если у вас нет лицензии, но вы хотите приобрести ее.

Активация действительна на определенный период времени. По истечении срока действия активации необходимо продлить лицензию (приложение предупреждает об этом заранее).

ПРИМЕЧАНИЕ. Во время активации устройство должно быть подключено к Интернету. При этом на устройство будет загружен небольшой объем данных. Такая передача данных оплачивается в соответствии с текущим тарифом поставщика услуг.

3. Антивирус

Полное сканирование

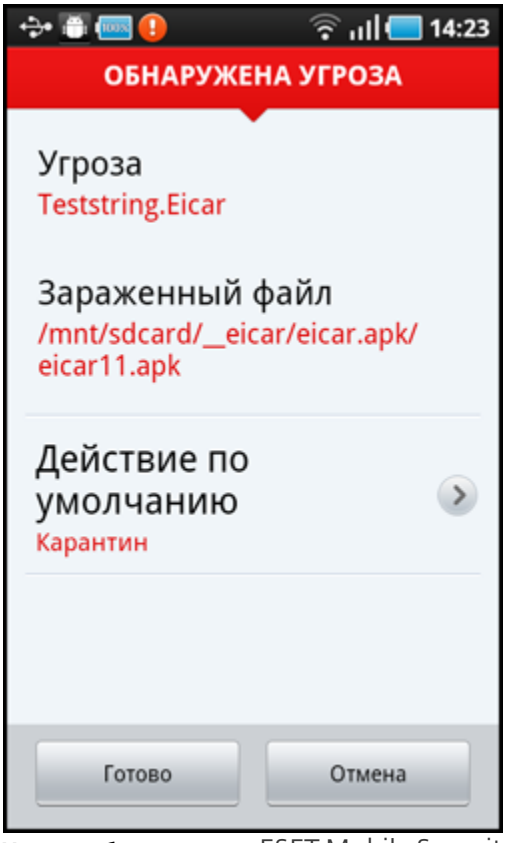
Функция **Полное сканирование** позволяет проверить мобильное устройство на наличие заражений.

Файлы некоторых предопределенных типов сканируются по умолчанию. В ходе полного сканирования устройства выполняется проверка памяти, запущенных процессов, связанных с ними динамических библиотек и файлов во внутренней памяти и на съемных носителях. После окончания сканирования на экран будет выведена краткая сводка о его результатах (например, о количестве зараженных файлов, количестве просканированных файлов, длительности сканирования и т. д.).

Если нужно прервать выполняемый процесс сканирования, нажмите **Отмена**.

Сканирование папки

Для проверки определенных папок на устройстве выберите команду **Сканирование папки**. Найдите папки, которые нужно сканировать, установите для них флажки в правом столбце и нажмите **Сканировать**.



Угроза, обнаруженная ESET Mobile Security

Журналы сканирования

Раздел **Журналы сканирования** содержит подробные данные о выполненных задачах сканирования. Журналы создаются после каждого запускаемого вручную (по запросу) сканирования или при обнаружении заражения в процессе сканирования в режиме реального времени.

В каждом журнале содержится следующая информация:

- дата и время события;
- количество просканированных файлов;
- количество зараженных файлов;
- имя и полный путь для зараженных файлов;
- длительность сканирования;
- действия, выполненные в ходе сканирования, и возникшие ошибки.

Карантин

Карантин предназначен в первую очередь для безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя очистить или безопасно удалить, а также если они отнесены ESET Mobile Security к зараженным по ошибке.

Информация о файлах, помещенных на карантин, записывается в журнал. Она включает имя и исходное местоположение зараженного файла, дату и время помещения файла на карантин.

Если нужно восстановить помещенный на карантин файл в исходное местоположение, нажмите его и выберите команду **Восстановить**. Этой возможностью пользоваться не рекомендуется.

Для удаления помещенного на карантин файла с устройства без возможности восстановления нажмите его и выберите команду **Удалить**. Для удаления всех помещенных на карантин файлов нажмите кнопку **МЕНЮ** и выберите команду **Удалить все**.

Настройки

Настройки в разделе **По запросу** позволяют изменить параметры запускаемого вручную (по запросу) сканирования.

Параметр **Показывать предупреждения** позволяет выводить на экран уведомления при обнаружении новой угрозы модулем сканирования по запросу.

Если нужно просканировать все приложения (файлы *.apk*), установленные на устройстве, выберите вариант **Сканировать приложения**.

Проактивная защита — это алгоритмический метод обнаружения, основанный на анализе кода и поиске типичных признаков поведения вирусов. Основным преимуществом этого метода является возможность обнаружения вредоносных программ, не распознаваемых с использованием текущей версии базы данных сигнатур вирусов. При активации проактивной защиты время сканирования будет увеличено.

Параметр **Глубина сканирования архивов** позволяет задать уровень вложенности архивов (файлов с расширением *.zip*), подлежащих сканированию. Чем больше это число, тем глубже сканирование.

Параметр **История проверок** позволяет задать максимальное количество журналов, сохраняемых в разделе **Журналы сканирования** 5.

В соответствующем поле можно указать действие по умолчанию, автоматически выполняемое при обнаружении зараженных файлов. Доступны указанные ниже варианты.

- **Игнорировать**: с зараженным файлом не будут выполняться никакие действия (этот вариант использовать не рекомендуется).
- **Удалить**: зараженный файл будет удален.
- **Карантин** (вариант по умолчанию): зараженный файл будет помещен на **карантин** 5.

Настройки раздела **Расширения** показывают наиболее распространенные типы файлов, подвергаемые заражениям на платформе Android. Выберите типы файлов, которые нужно сканировать, или отмените выбор расширений, если выполнять сканирование файлов соответствующих типов не нужно. Эти настройки применяются и к сканированию по запросу, и к сканированию в режиме реального времени.

- **Сканирование с исключениями**: если снять этот флажок, будут сканироваться файлы всех типов. Файлы также будут проверяться, если они не выдавались за файлы другого типа. При этом сканирование займет более длительное время.
- **DEX (системные файлы)** — формат исполняемых файлов, которые содержат компилированный код, написанный для ОС Android.
- **SO (библиотеки)** — общие библиотеки, сохраненные в указанных местоположениях в файловой системе и связанные с программами, которым нужны их функции.
- **Архивы (сжатые файлы)** — сжатые файлы Zip.
- **Другие** — другие известные типы файлов.

В разделе настроек **Реальное время** можно сконфигурировать параметры сканирования для модуля сканирования при доступе. Модуль сканирования при доступе проверяет файлы, к которым обращается пользователь, в режиме реального времени. Он автоматически сканирует папку *Загрузка* на карте памяти, файлы из числа установочных файлов с разрешением *.apk* и файлы на карте памяти после ее подключения (если активирован параметр **Сканировать карту памяти**). Модуль сканирования при доступе автоматически запускается при загрузке системы.

- **Защита в режиме реального времени**: если этот параметр активирован (по умолчанию), модуль сканирования при доступе работает в фоновом режиме.
- Параметр **Показывать предупреждения** позволяет выводить на экран уведомления при обнаружении новой угрозы модулем сканирования при доступе.
- **Сканировать карту памяти**: файлы сканируются до их открытия или сохранения на карту памяти.
- **Проактивная защита**: если выбрать этот параметр, будут использоваться методы эвристического анализа. Эвристический анализ позволяет в упреждающем режиме обнаруживать новые вредоносные программы, еще не обнаруживаемые с помощью базы данных сигнатур вирусов, путем анализа кода и распознавания типичного для вирусов поведения. При активации проактивной защиты время сканирования увеличивается.
- Параметр **Глубина сканирования архивов** позволяет задать уровень вложенности архивов (файлов с расширением *.zip*), подлежащих сканированию. Чем больше это число, тем глубже сканирование.
- **Действие по умолчанию**: этот параметр позволяет указать действие по умолчанию, которое будет выполняться автоматически при обнаружении зараженных файлов модулем сканирования при доступе. Если выбрать вариант **Игнорировать**, то с зараженным файлом не будут выполняться никакие действия (этот вариант использовать не рекомендуется). Вариант **Удалить** позволяет удалить зараженный файл. Если же остановиться на возможности **Карантин**, то зараженный файл будет помещен на **карантин** 5.

ESET Mobile Security выводит на экран значок уведомления  в левом верхнем углу (строка состояния Android). Если этот значок отображать не следует, на главном экране ESET Mobile Security нажмите кнопку **МЕНЮ**, выберите **Настройки уведомлений** и снимите флажок **Включить виджет** . Имейте в виду, что при этом не будет отключен значок предупреждения красного цвета с

восклицательным знаком, который уведомляет пользователя об угрозе безопасности (например, об отключении сканирования на наличие вирусов в режиме реального времени, согласования SIM и т. д.).

4. Защита от спама

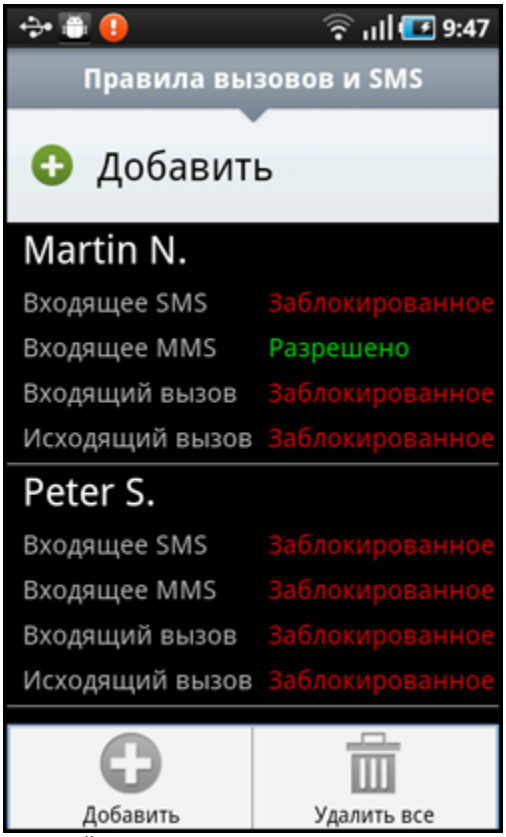
Модуль **Защита от спама** блокирует входящие сообщения SMS и MMS, а также входящие и исходящие вызовы на основе ваших правил.

Как правило, нежелательные сообщения содержат рекламные объявления от операторов мобильной связи либо послания от неизвестных или неуказанных пользователей. Под термином *блокировать контакты* понимается автоматическое перемещение входящих сообщений в раздел **Журналы спама** 7. При блокировании входящего сообщения уведомление на экран не выводится. Преимуществом такого подхода является то, что вы не будете отвлекаться на ненужную информацию, но все же всегда сможете проверить журналы на предмет наличия сообщений, которые могли быть заблокированы по ошибке.

Для создания нового правила Защита от спама нажмите **Правила вызовов и SMS** > **Добавить**. Введите номер телефона, который следует заблокировать, или же нажмите кнопку **+**, чтобы выбрать нужный номер из адресной книги. Настройте правило, разрешив или заблокировав сообщения и вызовы, и нажмите **Готово**.

Для изменения или удаления существующего правила нажмите и удерживайте соответствующий элемент, после чего выберите нужное действие. Если следует удалить все правила Защита от спама, нажмите кнопку **МЕНЮ** и выберите пункт **Удалить все**.

ПРИМЕЧАНИЕ. Номер телефона должен включать международный код и собственно номер (например, +761020020000).



Настройка Защита от спама

Настройки

Блокировать скрытые номера: установите этот флажок, если следует блокировать вызовы от абонентов, намеренно скрывающих свои номера с помощью функции запрета определения телефонного номера.

Блокировать известные контакты: этот параметр позволяет блокировать сообщения и вызовы от контактов из адресной книги.

Блокировать неизвестные контакты: блокируются сообщения и вызовы от контактов, отсутствующих в адресной книге. Этот параметр можно использовать, чтобы блокировать нежелательные телефонные звонки (например, рекламные) или предотвращать набор детьми неизвестных номеров. (Для предотвращения этого рекомендуется защитить настройки Защита от спама **паролем** 10.)

В разделе **Журналы спама** можно просмотреть вызовы и сообщения, заблокированные модулем защиты от спама. В каждом журнале содержатся имя события, соответствующий номер телефона, дата и время события. Для заблокированных SMS-сообщений также приводится тело сообщения.

5. БлокВор

Функция **БлокВор** предотвращает несанкционированный доступ к мобильному телефону.

Если вы потеряете телефон или кто-то украдет его и заменит вашу SIM-карту на новую (не являющуюся доверенной), ESET Mobile Security автоматически заблокирует телефон. На указанные пользователем телефонные номера будет тайно отправлено SMS-сообщение с предупреждением. Оно будет включать телефонный номер текущей SIM-карты, номер IMSI и номер IMEI телефона. Неавторизованный пользователь не узнает об отправке сообщения, поскольку оно будет автоматически удалено из диалогов раздела **Сообщения**. Кроме того, вы также можете запросить координаты GPS своего потерянного мобильного телефона или удаленно очистить все данные, имеющиеся на устройстве.

Доверенные SIM-карты

Если текущую SIM-карту следует запомнить в качестве доверенной, нажмите **Добавить > Добавить текущую**. Если используется несколько SIM-карт, можно воспользоваться пунктом **Введите имя SIM-карты**, указав имя для каждой из них (например, *Рабочая*, *Домашняя* и т. д.).

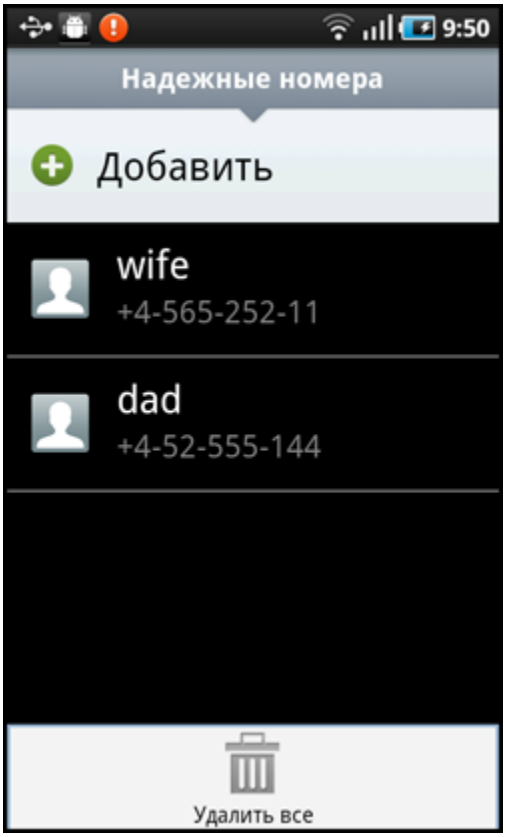
Для изменения или удаления существующей SIM-карты нажмите и удерживайте ее, после чего выберите соответствующую команду. Если следует удалить все пункты из списка, нажмите кнопку **МЕНЮ** и выберите пункт **Удалить все**.

Надежные номера

В списке **Надежные номера** нажмите **Добавить**, чтобы указать номера телефонов, на которые будет отправлено SMS-сообщение с предупреждением после вставки в устройство SIM-карты, не являющейся доверенной. Введите имя в поле **Имя друга** и заполните поле **Номер телефона** или нажмите кнопку **+**, чтобы выбрать контакт из адресной книги. Если у контакта несколько номеров телефона, SMS-сообщение с предупреждением будет отправлено на все эти номера.

Для изменения или удаления существующего пункта списка нажмите и удерживайте его, после чего выберите нужное действие. Если следует удалить все пункты из списка, нажмите кнопку **МЕНЮ** и выберите пункт **Удалить все**.

ПРИМЕЧАНИЕ. Номер телефона должен включать международный код и собственно номер (например, +761020020000).



Список «Надежные номера»

Настройки

Если в вашем устройстве не используется SIM-карта (например, это планшетный компьютер или телефон стандарта CDMA), выберите вариант **Не определять SIM-карту**. При этом будут отключены обозначенные красным цветом предупреждения *Угроза безопасности!* (*Согласование SIM отключено* и *Не задана доверенная SIM-карта*) на главном экране ESET Mobile Security. (Обратите внимание, что параметр «Не определять SIM-карту» будет неактивен на устройствах стандарта CDMA.)

Чтобы включить автоматическую проверку вставляемых SIM-карт (и отправку SMS-сообщений с предупреждением), установите флажок **Определять SIM-карту**.

В поле **Текст SMS-оповещения** можно изменить текстовое сообщение, отправляемое на указанные телефонные номера после вставки в устройство SIM-карты, не являющейся доверенной.

SMS-команды

Удаленные SMS-команды (на очистку, блокирование и поиск) будут работать только в том случае, если установлен флажок **Включить SMS-команды**.

Параметр **Включить SMS-сброс пароля** позволяет осуществить сброс пароля безопасности, отправив SMS-сообщение с номера мобильного телефона, указанного в списке **Надежные номера**, на свой

номер. Такое SMS-сообщение должно быть в следующем формате:
eset remote reset

Если вы потеряли свой телефон и хотели бы заблокировать его, отправьте SMS-сообщение для выполнения удаленной блокировки с любого мобильного устройства на свой номер телефона в таком виде:
eset lock пароль
Замените *пароль* на собственный пароль, заданный в разделе **Пароль** 10. Незаконный пользователь вашего телефона не сможет им воспользоваться, так как нужно будет ввести ваш пароль.

Если нужно запросить координаты GPS своего мобильного устройства, отправьте SMS-сообщение удаленного поиска на свой номер мобильного телефона или номер телефона незаконного пользователя (в зависимости от того, была ли уже заменена SIM-карта):
eset find пароль
Вы получите SMS-сообщение с координатами GPS и ссылкой на карту Google Maps, показывающими точное местонахождение вашего мобильного устройства. Обратите внимание на то, что для получения координат GPS модуль GPS вашего телефона должен быть активирован заранее.

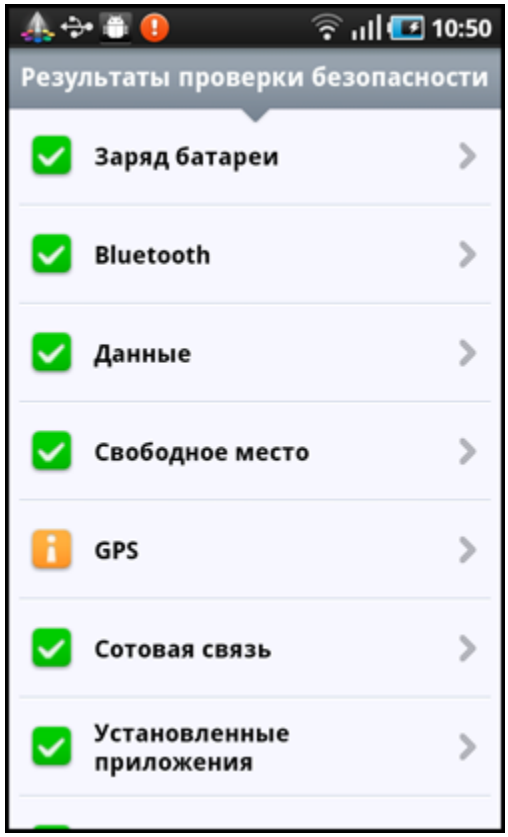
Если нужно удалить все данные на устройстве и подключенных к нему в настоящий момент съемных носителях, отправьте SMS-сообщение для удаленной очистки:
eset wipe пароль
Все контакты, сообщения, электронная почта, установленные приложения, учетная запись Google и содержимое карты памяти будут удалены с устройства без возможности восстановления. Если приложение ESET Mobile Security не выбрано в качестве администратора устройства, удалены будут только контакты, сообщения и содержимое карты памяти.

ПРИМЕЧАНИЕ. Вводить пароль нужно с учетом регистра. Обязательно нужно вводить пароль именно так, как он указан в разделе «Пароль».

6. Параметры системы

Функция **Параметры системы** позволяет проверять состояние телефона: уровень заряда аккумуляторов, состояние Bluetooth, объем свободного места и т. д.

Чтобы запустить проверку безопасности вручную, выберите команду **Проверка**. На экран будет выведен подробный отчет.



Результаты проверки безопасности

Зеленая отметка рядом с элементом указывает, что его значение выше порогового или он не представляет угрозы для безопасности.

Желтый значок является признаком того, что хотя бы у одного элемента значение ниже порогового или он может угрожать безопасности. Нажмите соответствующий элемент, чтобы просмотреть подробные результаты.

Красный восклицательный знак показывает, что значение элемента ниже порогового или он представляет угрозу для безопасности и должен быть исправлен.

Если вы хотите исправить состояние выделенного красным элемента, нажмите его и подтвердите свое решение, выбрав **Да**.

Настройки

По умолчанию Параметры системы выполняется периодически каждые сутки. Если нужно отключить периодическую проверку, снимите флажок **Проверять периодически**.

Если параметр **Исправлять автоматически** включен, приложение ESET Mobile Security будет автоматически пытаться устранить факторы риска (связанные, например, с состоянием bluetooth) без вмешательства пользователя. Этот параметр распространяется только на периодические (запланированные) проверки.

Параметр **История проверок** позволяет задать максимальное количество журналов, сохраняемых в разделе **Результаты проверки**.

Параметр **Период проверки** дает возможность указать частоту выполнения периодической (запланированной) проверки.

Для изменения пороговых значений, при которых объем свободного места и заряд батареи будут считаться низкими, можно воспользоваться параметрами **Минимальный объем памяти** и **Минимальный заряд батареи**.

На вкладке **Элементы для проверки** можно выбрать элементы, которые будут проверяться в процессе периодических (запланированных) проверок.

В разделе **Результаты проверки** можно найти журналы, в которых содержатся все данные о выполненных по расписанию или запущенных вручную проверках. В каждом таком журнале содержатся дата и время события и подробные результаты для каждого элемента.

Диспетчер задач представляет общие сведения обо всех процессах, службах и задачах, запущенных на устройстве. ESET Mobile Security позволяет остановить процессы, службы и задачи, не выполняемые системой. Такие элементы обозначаются красным значком (**x**).

7. Обновление

По умолчанию при установке приложения ESET Mobile Security настраивается задача обновления, обеспечивающая регулярное выполнение этой процедуры. Для запуска обновления вручную нажмите **Обновление**.

Настройки

В полях **Имя пользователя** и **Пароль** должна содержаться информация, которую вы получили в сообщении электронной почты о лицензии.

Параметр **Автоматическое обновление** позволяет настроить интервал автоматической загрузки обновлений базы данных сигнатур вирусов.

ПРИМЕЧАНИЕ. Чтобы предотвратить ненужное использование пропускной способности сети, обновления выпускаются по мере необходимости при появлении новых угроз. Сами обновления предоставляются при наличии активной лицензии бесплатно, но при этом поставщик услуг мобильной связи может взимать плату за передачу данных.

8. Пароль

Пароль безопасности предотвращает неразрешенное внесение изменений в настройки. Пароль нужен в таких ситуациях:

- доступ к защищенным паролем функциям ESET Mobile Security (антивирус, Защита от спама, БлокВор и Параметры системы);
- доступ к телефону в случае, если он был заблокирован;
- отправка SMS-команд на свое устройство;
- удаление ESET Mobile Security.

ПРИМЕЧАНИЕ. Защита от удаления доступна только для ОС Android 2.2 и более поздних версий.

Для выбора нового пароля безопасности введите его в поля **Пароль** и **Повторите ввод пароля**. Параметр **Подсказка** (если настроен) позволяет получить подсказку, когда не удается вспомнить пароль.

ВНИМАНИЕ! Пароль следует выбирать тщательно, поскольку он понадобится, чтобы разблокировать устройство или удалить ESET Mobile Security.

На вкладке **Применить к** можно указать, какие модули будут защищены паролем.

Если вы забудете пароль, то сможете отправить SMS-сообщение с номера мобильного телефона, сохраненного в списке **Надежные номера**, на номер своего телефона. Такое SMS-сообщение должно быть в следующем формате:
eset remote reset
Пароль будет сброшен.

9. Устранение проблем и поддержка

9.1 Техническая поддержка

По административным и техническим вопросам, связанным с ESET Mobile Security или другими продуктами безопасности ESET, обращайтесь к специалистам нашей службы поддержки клиентов.

Ответы на часто задаваемые вопросы можно найти в базе знаний ESET по адресу *http://kb.eset.com*

База знаний содержит большой объем полезной информации об устранении наиболее распространенных проблем, которую легко найти с помощью категорий и удобных средств поиска.

Для обращения в службу поддержки клиентов ESET можно использовать форму запроса по адресу *http://eset.com/support/contact*

Если вы хотите поделиться с нами своим мнением, перейдите на главный экран ESET Mobile Security, нажмите кнопку **МЕНЮ** и выберите команду **Служба поддержки клиентов**.