



MOBILE SECURITY

для Android

Руководство пользователя

(для версии 3.5 и более поздних версий продукта)

[Щелкните здесь, чтобы загрузить актуальную версию этого документа.](#)

MOBILE SECURITY

© ESET, spol. s r.o.

Продукт ESET Mobile Security разработан компанией ESET, spol. s r.o. Дополнительные сведения см. на веб-сайте www.eset.com.

Все права защищены. Запрещается воспроизведение, сохранение в информационных системах и передача данного документа или любой его части в любой форме и любыми средствами, в том числе электронными, механическими способами, посредством фотокопирования, записи, сканирования, а также любыми другими способами без соответствующего письменного разрешения автора. ESET, spol. s r.o. оставляет за собой право изменять любые программные продукты, описанные в данной документации, без предварительного уведомления.

Служба поддержки клиентов: <http://support.eset.com/>

Версия от 30. 1. 2017

Содержание

1. Введение	4
1.1 Новые возможности в версии 3.5	4
1.2 Минимальные требования к системе	4
2. Установка	5
2.1 Загрузка из интернет-магазина Google Play	5
2.2 Загрузка с веб-сайта ESET	5
2.3 Мастер начальной настройки	6
3. Удаление	9
4. Активация программы	9
5. Антивирус	10
5.1 Автоматическое сканирование	12
5.2 Журналы сканирования	13
5.3 Дополнительные настройки	14
6. Антивор	15
6.1 Веб-портал	16
6.1.1 Оптимизация	17
6.1.2 Проактивная защита	17
6.2 Защита SIM-карты	17
6.2.1 Доверенные SIM-карты	18
6.2.2 Надежные номера	18
6.3 SMS-команды	19
6.4 Настройки	20
6.4.1 Защитный пароль	20
6.4.2 Контактная информация	20
7. Антифишинг	21
8. Фильтрация вызовов и SMS	22
8.1 Правила	22
8.1.1 Добавление нового правила	23
8.2 Журнал	23
9. Проверка безопасности	23
9.1 Отслеживание местоположения устройства	24
9.2 Аудит приложения	25
10. Отчет по безопасности	26
11. Настройки	27
12. Служба поддержки	28

1. Введение

ESET Mobile Security представляет собой комплексное решение для безопасности, которое предохраняет ваше устройство от возникающих угроз и фишинговых страниц, фильтрует нежелательные вызовы и сообщения, а также позволяет управлять устройством удаленно в случае потери или кражи.

К основным возможностям решения относятся:

- [Защита от вирусов](#)
- [Антивор](#)
- [Защита от фишинга](#)
- [Интеграция с порталом My Eset](#)
- [Фильтрация вызовов и SMS](#)
- [Аудит безопасности](#)
- [Отчет по безопасности](#)

1.1 Новые возможности в версии 3.5

В ESET Mobile Security 3.5 представлены следующие обновления и улучшения:

- [Проактивная защита](#)
- [Улучшенная защита от фишинга](#)
- [Отчет по безопасности](#)
- Системные разрешения легко доступны из ESET Mobile Security
- Последнее известное местоположение устройства, сохраняемое в компоненте ESET Антивор перед исчерпанием заряда аккумулятора устройства

1.2 Минимальные требования к системе

Чтобы установить ESET Mobile Security на устройство под управлением Android, оно должно соответствовать следующим минимальным требованиям к системе.

- Операционная система:  Android 4 (Ice Cream Sandwich) или более новая версия
- Разрешение сенсорного экрана: минимум 480 x 800 пкс
- Процессор: ARM с набором инструкций ARMv7+, x86 Intel Atom
- ОЗУ: 128 МБ
- Свободное место во внутреннем хранилище: 20 МБ
- Подключение к Интернету

ПРИМЕЧАНИЕ. Не поддерживаются устройства с двумя SIM-картами и устройства, на которых выполнен рутинг. Модуль Антивор и фильтр вызовов и SMS недоступны на планшетах, которые не поддерживают телефонные звонки и обмен сообщениями.

2. Установка

Программа ESET Mobile Security доступна для загрузки по следующим каналам распространения:



[Google Play](#) — это приложение получает регулярные обновления через Google Play.



[Веб-сайт ESET](#) — это приложение получает обновления из системы проверки обновления версии ESET.



[Amazon Appstore.](#)

Для защиты ваших личных данных и ресурсов устройства Android программе ESET Mobile Security потребуется доступ к функциям устройства, а в некоторых случаях и контроль над ними. Подробное описание каждого типа разрешения и его использования см. в таблице в следующей статье базы знаний:

<http://support.eset.com/kb2711/#PrivacyPolicy>

(Статья доступна не на всех языках.)

2.1 Загрузка из интернет-магазина Google Play

Откройте на своем устройстве Android приложение Google Play и найдите программу ESET Mobile Security (или просто ESET).

Другой способ загрузки — открыть ссылку или просканировать приведенный ниже QR-код с помощью мобильного устройства и приложения для сканирования QR-кодов:



<https://play.google.com/store/apps/details?id=com.eset.ems2.gp>



2.2 Загрузка с веб-сайта ESET

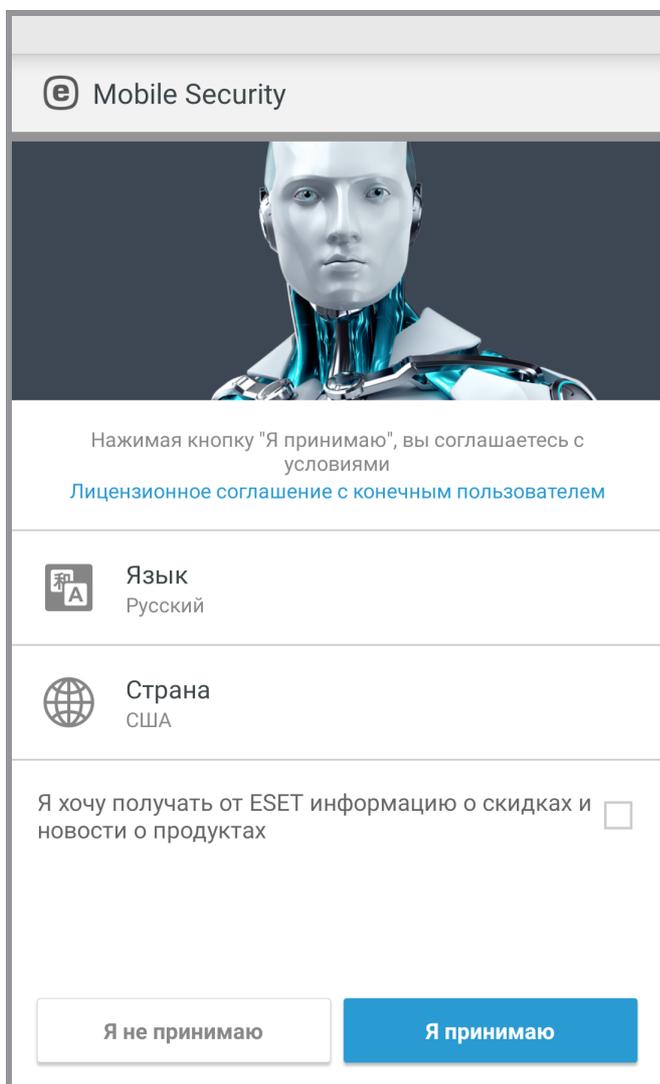
Доступность веб-версии зависит от вашего региона.

1. Загрузите установочный файл APK с [веб-сайта ESET](#).
2. На устройстве должны быть разрешены приложения из неизвестных источников. Для этого коснитесь значка запуска  на главном экране Android или выберите «Главная» > «Меню»). Нажмите **Настройки** > **Безопасность**. Флажок рядом с параметром **Неизвестные источники** должен быть установлен.
3. Откройте файл из области уведомлений Android или найдите его с помощью обозревателя файлов. Обычно файл сохраняется в папку загрузок.
4. Нажмите **Установить**, а затем **Открыть**.

2.3 Мастер начальной настройки

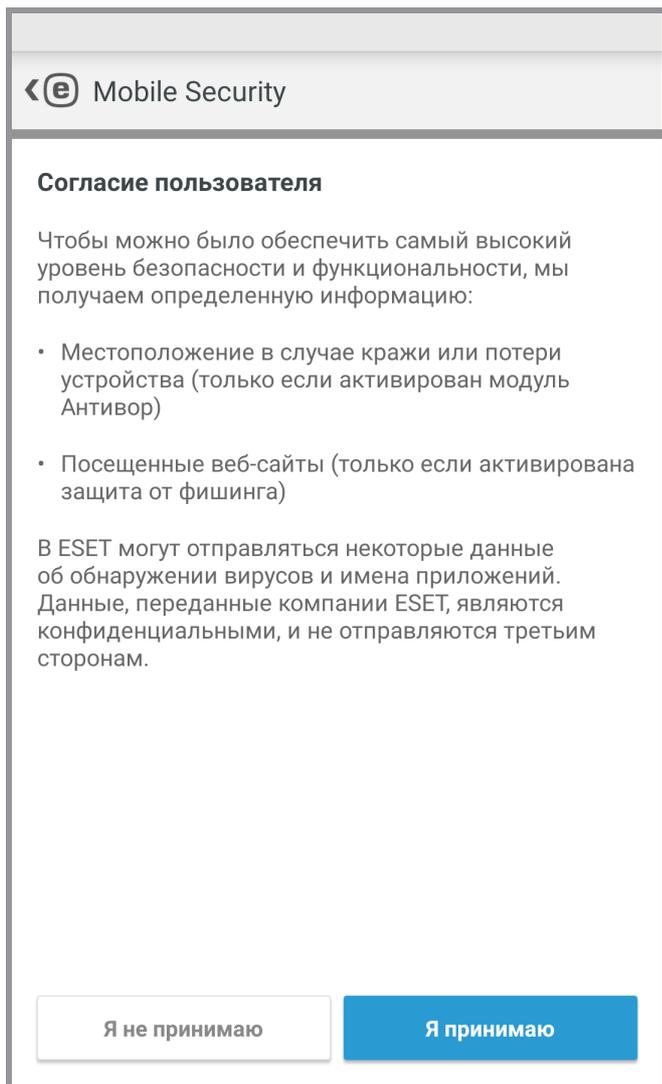
После установки приложения следуйте запросам на экране мастера начальной настройки:

1. Нажмите **Язык** для выбора языка, который следует использовать в ESET Mobile Security. В дальнейшем этот выбор можно изменить в настройках программы.



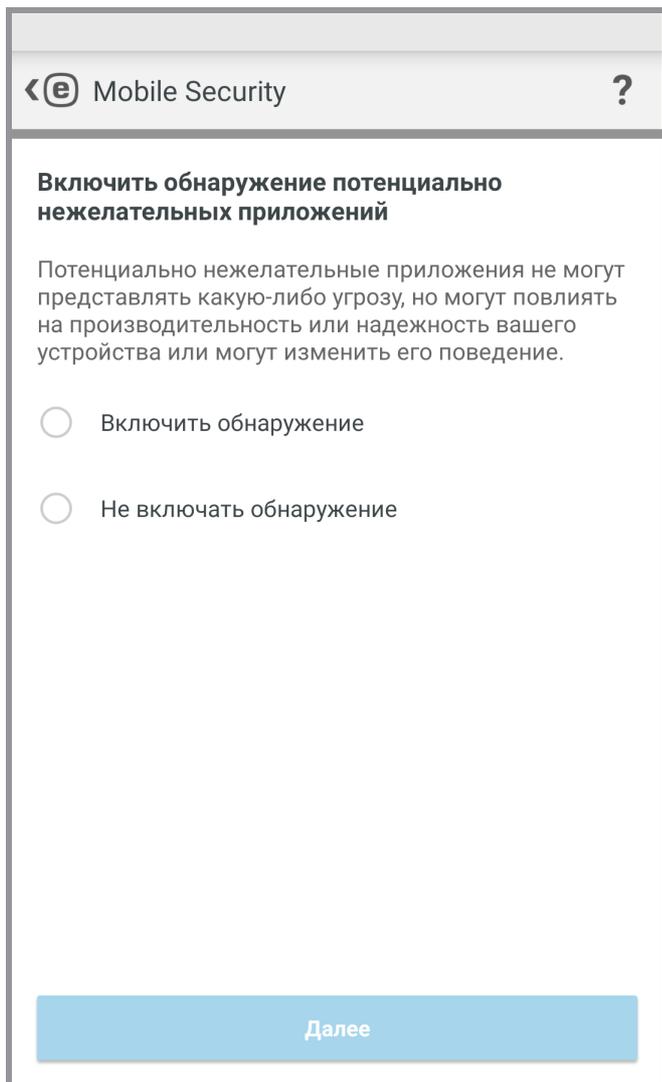
2. Нажмите **Страна**, чтобы выбрать страну, в которой вы находитесь.
3. Нажмите **Принять**, чтобы согласиться с условиями лицензионного соглашения.

4. Нажмите **Принять** на экране **Согласие пользователя**. Некоторая информация, например местоположение устройства и посещенные веб-сайты, может предоставляться компании ESET.



5. Нажмите **Далее**, если вы хотите участвовать в **ESET Live Grid**. В дальнейшем этот выбор можно изменить в настройках программы. Дополнительные сведения [см. в этом разделе](#).

6. Выберите **Включить обнаружение** или **Не включать обнаружение**, чтобы определить, будет ли ESET Mobile Security обнаруживать потенциально нежелательные приложения, затем нажмите **Далее**. В дальнейшем этот выбор можно изменить в настройках программы. Дополнительные сведения о потенциально нежелательных приложениях [см. в этом разделе](#).



7. На следующем этапе будет показан список всех доступных на устройстве учетных записей электронной почты. Выберите учетную запись, которую следует использовать для связи с ESET по вопросам регистрации лицензии на продукт, получения информации о сбросе пароля безопасности и связи со службой поддержки клиентов ESET. Если в списке нет ни одной учетной записи электронной почты, нажмите **Добавить учетную запись** > **ОК** > **Существующая** для входа в существующую учетную запись электронной почты или **Новая** для создания новой.
8. Нажмите **Активировать**, чтобы активировать расширенные функции продукта, или **Пропустить**, чтобы начать использование бесплатной версии.

3. Удаление

Программу ESET Mobile Security можно удалить с помощью мастера удаления, доступного в главном меню программы. Коснитесь «Меню»  > **Настройки** > **Удалить**. Вам будет предложено ввести пароль безопасности.

В качестве альтернативы выполните указанные ниже действия для удаления продукта вручную.

1. На главном экране ОС Android коснитесь значка запуска  (или откройте Главный экран > Меню и коснитесь **Настройки** > **Безопасность** > **Администраторы устройства**). Выберите ESET Mobile Security и нажмите **Деактивировать**. Нажмите **Разблокировать** и введите свой пароль безопасности. Этот шаг можно пропустить, если приложение больше не задано в качестве администратора устройства.
2. Вернитесь на экран **Настройки** и нажмите **Управление приложениями** > ESET Mobile Security > **Удалить**.

4. Активация программы

ESET Mobile Security поставляется в трех версиях:

- Бесплатная — базовые возможности доступны бесплатно в течение неограниченного времени.
- Пробная — расширенные функции активируются на ограниченное время (по умолчанию 30 дней).
- Расширенная — расширенные функции активируются до окончания срока действия вашей лицензии.

В следующей таблице показано, какие возможности доступны в бесплатной, пробной и расширенной версиях.

	Бесплатная	Пробная и расширенная
Защита от вирусов	✓	
Защита от вирусов — автоматическое сканирование		✓
Автоматическое обновление базы данных вирусов		✓
Антивор — SMS-команды (за исключением очистки)	✓	
Антивор — веб-портал		✓
Антивор — защита SIM-карты		✓
Защита от фишинга		✓
Фильтрация вызовов и SMS		✓
Аудит безопасности		✓
Отчет по безопасности	✓	

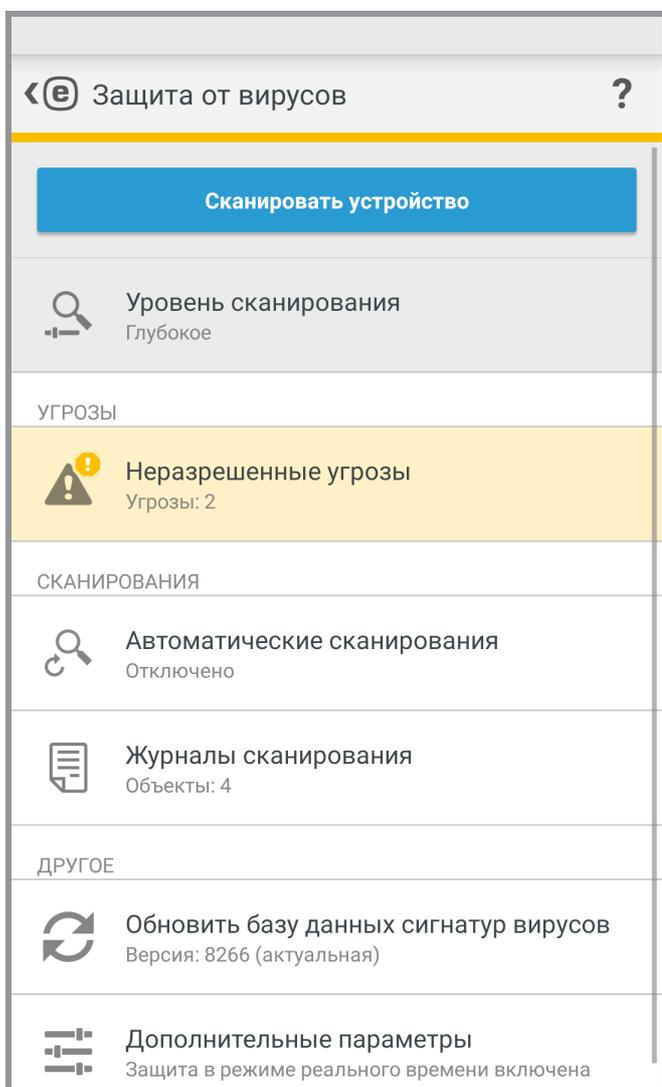
Чтобы активировать ESET Mobile Security непосредственно на устройстве Android, коснитесь «Меню»  на главном экране ESET Mobile Security (или нажмите кнопку **МЕНЮ** на устройстве), а затем — элемента **Лицензия**.

Есть несколько способов активации ESET Mobile Security. Доступность того или иного способа зависит от страны и того, как продукт был получен (с веб-страницы ESET, из Google Play или Amazon Appstore).

- **Купить расширенную версию** — выберите этот параметр, если у вас нет лицензии и вы хотите ее приобрести через Google Play.
- **Ввести лицензионный ключ** — выберите этот параметр, если у вас уже есть лицензионный ключ. Лицензионный ключ — это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца лицензии. Его можно найти в сообщении электронной почты, полученном от компании ESET, или на лицензионной карте в упаковке продукта.
- **Активация бесплатной версии** — выберите этот параметр, если вы хотите ознакомиться с программой ESET Mobile Security до покупки. Для каждой учетной записи Google это можно сделать только один раз.
- **У меня есть имя пользователя и пароль. Что мне делать?** — выберите этот параметр, чтобы преобразовать ваши имя пользователя и пароль в лицензионный ключ на сайте <https://my.eset.com/convert>.

5. Антивирус

Модуль защиты от вирусов защищает устройство от вредоносного кода, блокируя входящие угрозы и удаляя их.



Сканирование устройства

Файлы некоторых predetermined типов сканируются по умолчанию. Во время сканирования устройства проверяются память, запущенные процессы, зависящие от них динамические библиотеки, а также файлы, находящиеся на съемных носителях и во внутреннем хранилище. Сводные данные о результатах сканирования сохраняются в файл журнала в разделе [Журналы сканирования](#). Чтобы прервать запущенное сканирование, нажмите .

Уровень сканирования

Доступны два уровня сканирования.

- **Сканирование Smart.** Во время сканирования Smart проверяются установленные приложения, DEX-файлы (исполняемые файлы для ОС Android), SO-файлы (библиотеки), архивы (максимальная глубина сканирования — три уровня вложения в архиве) и содержимое SD-карт.
- **Тщательное сканирование.** В этом режиме проверяются файлы всех типов с любыми расширениями, находящиеся во внутреннем хранилище и на SD-карте.

Обновление базы данных сигнатур вирусов

По умолчанию программа ESET Mobile Security регулярно загружает и устанавливает обновления. Это происходит автоматически. Чтобы обновить ее вручную, коснитесь элемента **Обновить базу данных сигнатур вирусов**.

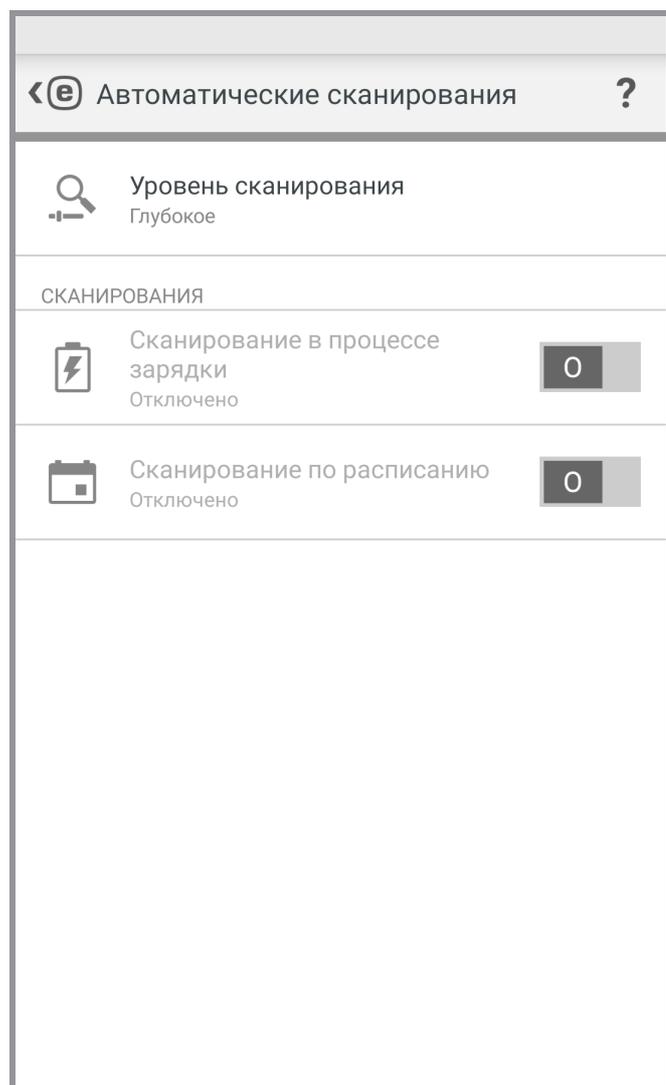
ПРИМЕЧАНИЕ. Чтобы предотвратить ненужное использование пропускной способности сети, обновления выпускаются по мере необходимости при появлении новых угроз. Обновления предоставляются бесплатно, но за передачу данных в мобильной сети может взиматься плата.

Дополнительную информацию о сканировании см. по следующим ссылкам:

- [Автоматическое сканирование](#)
- [Журналы сканирования](#)
- [Дополнительные параметры](#)

5.1 Автоматическое сканирование

Кроме запускаемого вручную сканирования устройства, приложение ESET Mobile Security может выполнять автоматическое сканирование.



Уровень сканирования

Доступны два уровня сканирования. Этот параметр применяется во время сканирования в процессе зарядки и сканирования по расписанию.

- **Сканирование Smart.** Во время сканирования Smart проверяются установленные приложения, DEX-файлы (исполняемые файлы для ОС Android), SO-файлы (библиотеки), архивы (максимальная глубина сканирования — три уровня вложения в архиве) и содержимое SD-карт.
- **Тщательное сканирование.** В этом режиме проверяются файлы всех типов с любыми расширениями, находящиеся во внутреннем хранилище и на SD-карте.

Сканирование в процессе зарядки

Если выбран этот параметр, сканирование начинается автоматически, когда устройство находится в состоянии простоя, полностью заряжено и подключено к зарядному устройству.

Сканирование по расписанию

Этот параметр позволяет запланировать время, когда устройство будет сканироваться автоматически. Чтобы запланировать сканирование, коснитесь переключателя  рядом с элементом **Сканирование по расписанию** и укажите значения дат и времени начала сканирования.

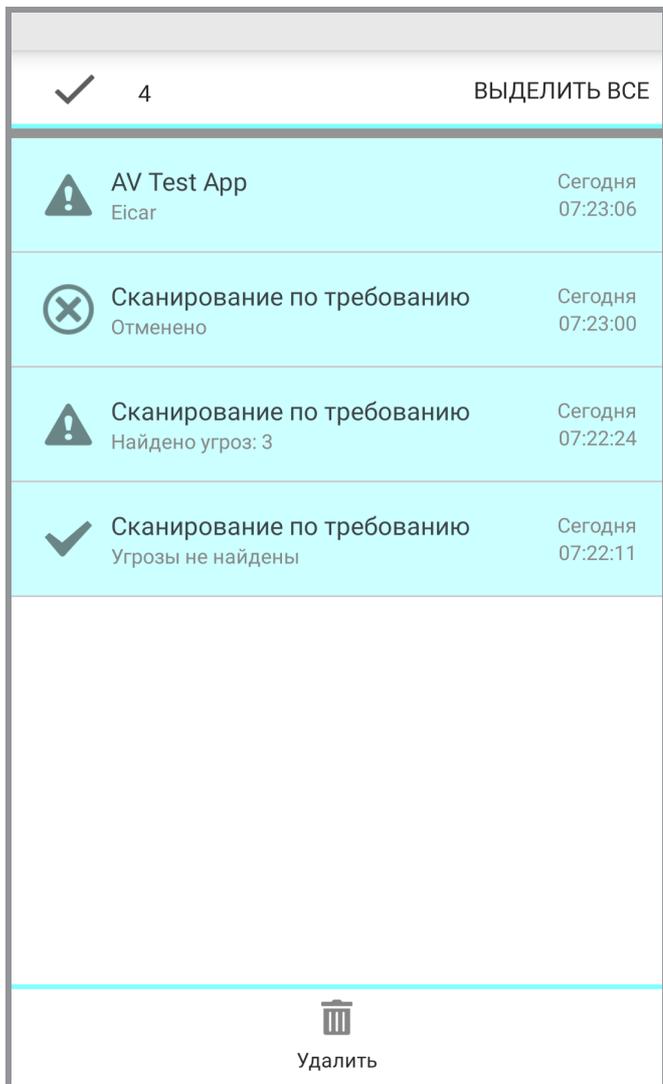
5.2 Журналы сканирования

В разделе «Журналы сканирования» содержатся комплексные данные о каждом запланированном или запущенном вручную сканировании устройства.

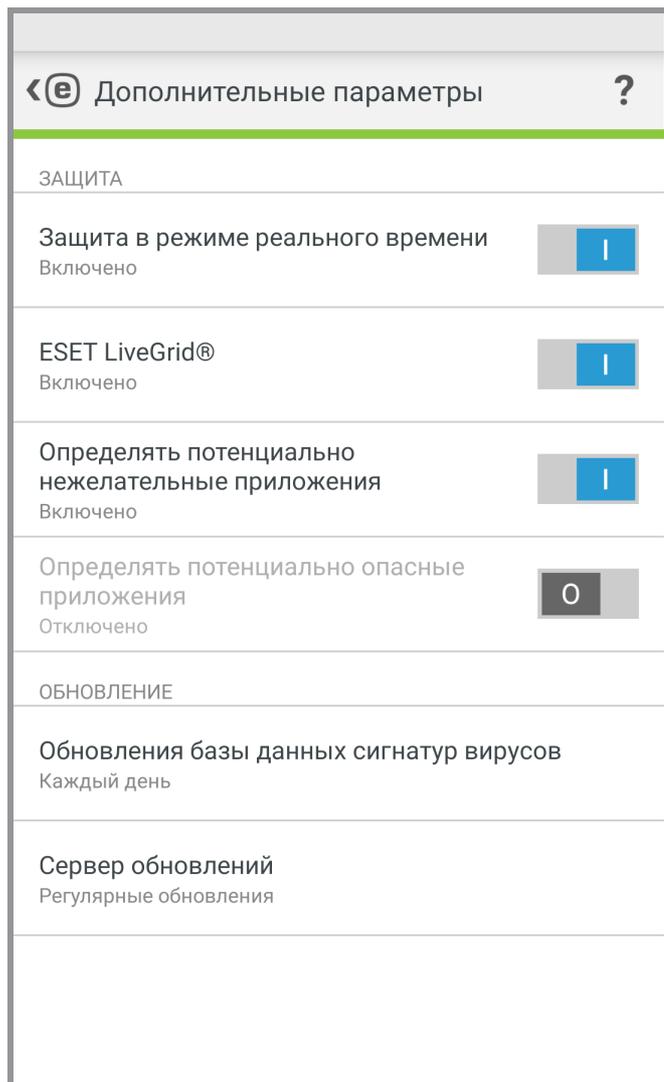
Каждый журнал содержит такие сведения:

- дата и время сканирования;
- уровень сканирования (Smart или тщательное);
- продолжительность сканирования;
- количество просканированных файлов;
- результаты сканирования или ошибки, обнаруженные во время сканирования.

Чтобы удалить журнал из списка, коснитесь журнала и задержите на нем палец, чтобы выбрать его, а затем нажмите «Удалить» .



5.3 Дополнительные настройки



Защита в режиме реального времени

Модуль сканирования в реальном времени запускается автоматически при запуске системы и сканирует файлы, с которыми работает пользователь. Он автоматически сканирует папку *Download* и установленные или обновленные приложения.

ESET Live Grid

Построенное на основе передовой системы раннего предупреждения *ThreatSense.Net* решение ESET Live Grid предназначено для обеспечения более высокого уровня безопасности вашего устройства. Оно непрерывно отслеживает запущенные в системе программы и процессы и сравнивает их с новейшими сведениями, полученными от миллионов пользователей ESET по всему миру. Кроме того, сканирование выполняется быстрее и точнее по мере роста базы данных ESET Live Grid. Это позволяет обеспечивать более качественную упреждающую защиту и более высокую скорость сканирования для всех пользователей ESET. Рекомендуется включить эту функцию. Благодарим за поддержку.

Определять потенциально нежелательные приложения

Потенциально нежелательное приложение отличается тем, что содержит рекламу, устанавливает панели инструментов, отслеживает результаты поиска или выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого приложения перевешивают риски. Поэтому компания ESET помещает эти приложения, в отличие от других вредоносных программ, в категорию незначительного риска.

Определять потенциально опасные приложения

Существует множество надежных программ, которые упрощают администрирование подключенных к сети устройств. Однако злоумышленники могут использовать их для причинения вреда. Включив параметр **Определять потенциально опасные приложения**, можно отслеживать и, если нужно, блокировать такие приложения. Потенциально опасными приложениями считаются нормальные коммерческие программы. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы.

Обновления базы данных сигнатур вирусов

Этот параметр позволяет задать период времени для автоматической загрузки баз данных угроз. Эти обновления выпускаются, когда в базу данных добавляется новая угроза. Рекомендуется оставить значение по умолчанию (ежедневно).

Сервер обновлений

Этот параметр позволяет выбрать обновление устройства с **сервера тестовых обновлений**. Тестовые обновления — это обновления, которые уже прошли полное внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Преимущество в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако иногда такие обновления могут быть недостаточно стабильны. Чтобы проверить версии имеющихся программных модулей, коснитесь «Меню»  на главном экране ESET Mobile Security, а затем выберите **О программе > ESET Mobile Security**. Неопытным пользователям рекомендуется для параметра **Регулярные обновления** оставить значение по умолчанию.

6. Антивор

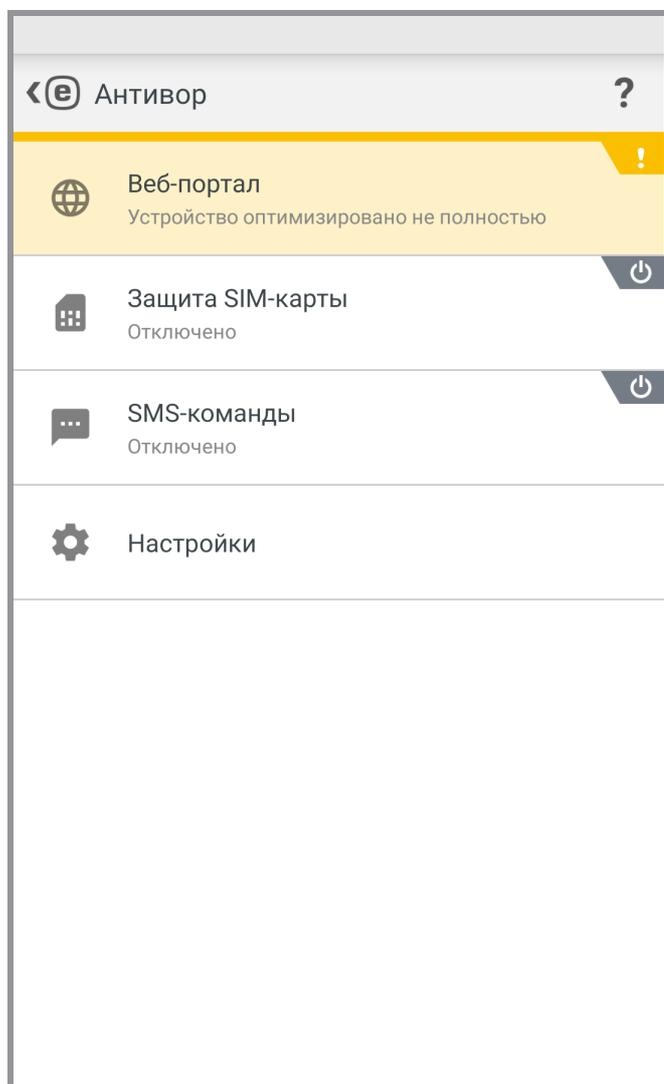
Компонент **Антивор** защищает мобильное устройство от несанкционированного доступа.

Если вы потеряете свое устройство или кто-то украдет его и заменит вашу SIM-карту на новую (недоверенную), устройство будет автоматически заблокировано ESET Mobile Security, и на указанные вами номера будет отправлено SMS-сообщение. Оно будет включать телефонный номер новой вставленной 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 можете запросить GPS-координаты потерянного устройства или удаленно уничтожить все сохраненные на устройстве данные.

ПРИМЕЧАНИЕ. Некоторые возможности компонента «Антивор» (доверенные SIM-карты и текстовые команды через SMS) недоступны на устройствах, которые не поддерживают обмен сообщениями.

6.1 Веб-портал

Версия 3 программы ESET Mobile Security полностью интегрируется с компонентом защиты ESET Антивор через [портал My Eset](#). На портале можно отслеживать активность устройства, блокировать устройство, отправлять настраиваемые сообщения лицу, нашедшему устройство, включать громкую сирену и дистанционно стирать данные с устройства.



Чтобы создать учетную запись My ESET, нажмите **Создать учетную запись** и заполните форму регистрации. Откройте в своем почтовом ящике письмо с подтверждением учетной записи и перейдите по ссылке, чтобы активировать свою учетную запись. Теперь вам доступно управление функциями безопасности модуля Антивор с сайта my.eset.com. Если у вас уже есть учетная запись My ESET, нажмите **Войти** и введите свои электронную почту и пароль. После завершения этих шагов вы можете связать устройство со своей учетной записью My ESET.

Для получения дальнейших рекомендаций по использованию компонента Антивор на [портале My ESET](#) откройте [интернет-справку по модулю Антивор](#) или нажмите **Справка** в правом верхнем углу экрана.

Последнее известное местоположение — эта функция сохраняет местоположение устройства в компоненте ESET Антивор перед исчерпанием заряда аккумулятора устройства.

6.1.1 Оптимизация

Оптимизация модуля ESET Антивор — это измеримая техническая оценка состояния безопасности устройства. Модуль Антивор изучит вашу систему на наличие проблем, перечисленных ниже.

Для каждой проблемы безопасности можно нажать кнопку **Изменить параметры** для перехода к экрану, на котором можно разрешить данную конкретную проблему. Если вы не желаете, чтобы ошибка отображалась в приложении ESET Mobile Security как проблема, выберите вариант **Пропустить эту ошибку**.

- **Выключена служба определения местоположения** — чтобы включить ее, в настройках Android выберите пункт **Службы определения местоположения** и установите флажок **Использовать беспроводные сети**
- **Не используются спутники GPS** — для доступа к этому параметру в настройках Android выберите **Местоположение > Режим > Высокая точность**
- **Не защищена блокировка экрана** — чтобы защитить устройство с помощью кода блокировки экрана, пароля, PIN-кода или графического ключа, необходимо в настройках Android перейти к пункту **Блокировать экран > Блокировка экрана**, а затем выбрать один из доступных параметров. На большинстве устройств под управлением Android доступны следующие варианты разблокировки: перетаскивание значка блокировки, движение, распознавание лица, распознавание лица и голоса, графический ключ, PIN-код и пароль. Если кто-либо попытается разблокировать ваше устройство с помощью неправильного кода, модуль ESET Антивор сообщит вам о подозрительных действиях на портале My Eset.
- **Выключена передача мобильных данных** — для доступа к этому параметру в настройках Android выберите **Беспроводной доступ и сети > Мобильные сети > Данные**.
- **Отсутствуют службы Google Play** — ESET Антивор использует службы Google Play для доставки команд на устройство в режиме реального времени и отображения push-уведомлений. Если эти службы отключены или отсутствуют на вашем устройстве, функции модуля ESET Антивор, управление которыми осуществляется с помощью сайта My Eset, будут ограничены. В такой ситуации вместо портала My Eset рекомендуем использовать SMS-команды.

6.1.2 Проактивная защита

Этот компонент позволяет настроить предупреждения и действия, срабатывающие в подозрительном режиме, в котором ESET Mobile Security регулярно сохраняет местоположение устройства, фотографии с камеры и IP-адреса WiFi. Можно задать следующие параметры.

- **Активировать при неудачной попытке разблокировки** — по умолчанию этот параметр включен и блокирует устройство при вводе неверного кода разблокировки экрана.
- **Максимальное количество неудачных попыток разблокировки** — количество разрешенных неудачных попыток разблокировки.
- **Время на исправление** — по умолчанию у вас есть 15 секунд, чтобы ввести правильный код разблокировки.
- **Сохранять фотографии в устройстве** — сохраняет фотографии с задней и передней камер в галерею устройства и на портале «Антивор» в случае неудачной попытки разблокировки или извлечения SIM-карты.

6.2 Защита SIM-карты

Чтобы включить защиту SIM-карты, нажмите **Антивор > Защита SIM-карты** в главном меню программы, после чего коснитесь переключателя  для включения данного компонента. Простой мастер поможет вам настроить параметры. Доступ к этим шагам можно также получить с помощью мастера настройки текстовых SMS-команд:

- Ввод [пароля безопасности](#)
- Добавление [контактной информации](#)
- Включение защиты от удаления
- Сохранение текущей [SIM-карты в качестве доверенной](#)
- Добавление [надежного друга](#)

6.2.1 Доверенные SIM-карты

В области интерфейса **Доверенные SIM-карты** отображается список SIM-карт, которые будут приниматься приложением ESET Mobile Security. Если вставить SIM-карту, которой в списке нет, экран будет заблокирован и надежным друзьям будет отправлено SMS-предупреждение.

Чтобы добавить новую SIM-карту, нажмите . Введите **имя SIM-карты** (например, «Дом» или «Работа») и ее идентификатор IMSI (International Mobile Subscriber Identity — международный идентификатор абонента мобильной связи). Идентификатор IMSI обычно нанесен на SIM-карту и состоит из 15 цифр. Иногда он может быть короче.

Чтобы удалить SIM-карту из списка, выберите ее и нажмите .

ПРИМЕЧАНИЕ. Функция «Доверенные SIM-карты» недоступна на устройствах CDMA и WCDMA, а также на устройствах, в которых используется только WiFi.

6.2.2 Надежные номера

В разделе «Надежные друзья» можно добавить или удалить номера телефонов ваших друзей и членов семьи, которые смогут:

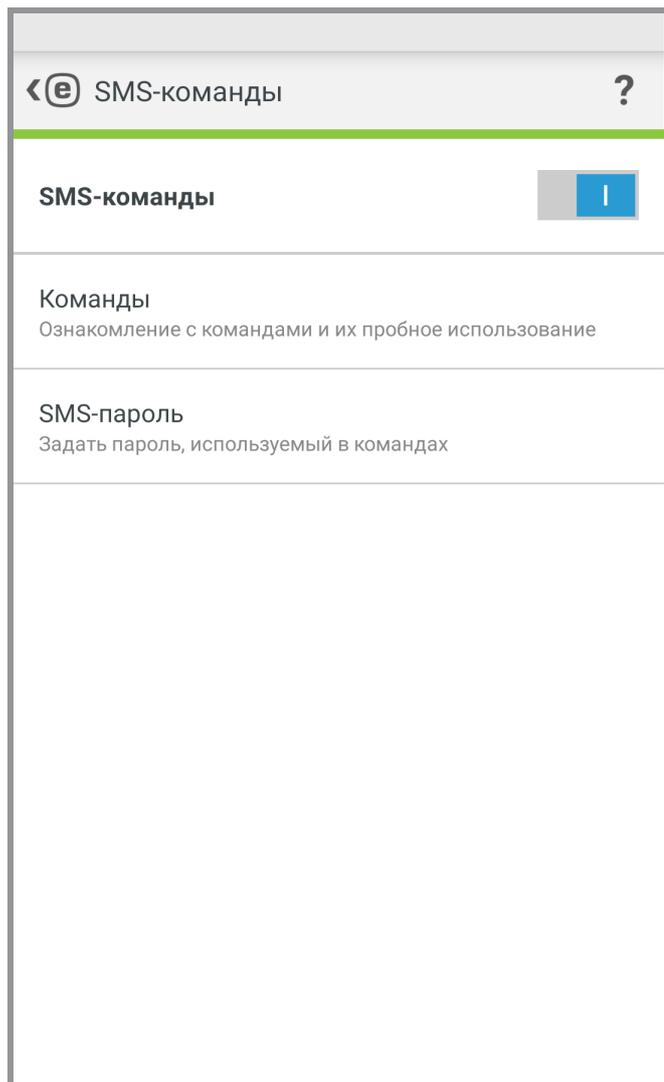
- Получать SMS-предупреждение после обнаружения неавторизованной SIM-карты в вашем устройстве.
- Сбрасывать ваш пароль безопасности (при условии, что для данного контакта включен параметр **Разрешить удаленный сброс пароля безопасности**).

Чтобы добавить нового надежного друга, нажмите  и введите имя и номер мобильного телефона друга, или нажмите , чтобы выбрать контакт из списка контактов телефона. Чтобы удалить надежного друга, выберите соответствующую запись и нажмите «Удалить» .

Если запись надежного друга содержит несколько телефонных номеров, SMS-предупреждение и сброс пароля будут работать со всеми связанными номерами.

ПРИМЕЧАНИЕ. Если вы находитесь за границей, введите все телефонные номера в списке с международным кодом, за которым должен следовать фактический номер (например, +1610100100).

6.3 SMS-команды



Чтобы начать использовать SMS-команды, нажмите **Антивор > SMS-команды** в главном меню программы, после чего коснитесь переключателя  для включения данного компонента. Если мастер [Контроль SIM-карты](#) уже был использован, эта настройка только предложит ввести один дополнительный параметр — SMS-пароль. Для этой цели можно использовать пароль безопасности, однако это не рекомендуется, так как SMS-пароль будет отображаться на экране мобильного устройства во входящих сообщениях.

Можно отправить следующие SMS-команды.

Разблокировать

`eset remote reset`

Отправьте эту команду с устройства надежного друга, чтобы разблокировать экран вашего устройства.

Заблокировать

`eset lock пароль`

Эта команда заблокирует устройство. Впоследствии вы сможете разблокировать его с помощью пароля безопасности.

Сирена

`eset siren пароль`

Громкий звук сирены будет воспроизводиться, даже если на устройстве отключен звук.

Поиск

`eset find пароль`

Вы получите текстовое сообщение, содержащие GPS-координаты целевого устройства и ссылку на его местоположение на картах Google. Через определенное время устройство отправит еще одно сообщение, если появятся более точные координаты местонахождения.

Очистить

eset wipe пароль

С устройства будут безвозвратно удалены контакты, сообщения, электронные письма, учетные записи, содержимое SD-карты, изображения, музыка и видеофайлы, хранящиеся в папках по умолчанию. Приложение ESET Mobile Security останется.

ПРИМЕЧАНИЕ. Несмотря на то что в SMS-командах не учитывается регистр, пароль необходимо вводить точно в таком виде, как он был задан в мастере настройки модуля Антивор.

6.4 Настройки

В разделе настроек модуля Антивор имеется доступ к следующим параметрам.

- [Пароль безопасности](#)
- [Контактная информация](#)

6.4.1 Защитный пароль

Ваш **пароль безопасности** необходим для разблокировки устройства, доступа к модулю Антивор, удаления приложения ESET Mobile Security или отправки текстовых SMS-команд (при условии, что соответствующий параметр был включен при создании SMS-пароля).

Если вы забыли пароль безопасности, попробуйте следующие решения.

- Отправьте текстовое сообщение с [мобильного номера надежного друга](#) на ваш номер. Сообщение должно иметь следующую форму: eset remote reset
- Если устройство подключено к Интернету, запросите код для сброса пароля, нажав **Эл. почта** на заблокированном устройстве. Электронное письмо с кодом проверки будет доставлено в учетную запись электронной почты Google, указанную во время установки. Введите код проверки и новый пароль на заблокированном экране.
- Сбросьте пароль на [портале My Eset](#). После входа выберите устройство, нажмите **Параметры** и введите новый пароль.
- Если устройство не подключено к Интернету, заполните форму в [этой статье базы знаний](#).
- Обратитесь к [службе поддержки клиентов ESET](#), если не удастся отправить вышеупомянутые данные.

ВНИМАНИЕ! Чтобы создать защищенный пароль, который будет труднее подобрать, используйте сочетание цифр, строчных и прописных букв.

6.4.2 Контактная информация

Если вы пометите свое устройство как пропавшее на сайте my.eset.com, на экране заблокированного устройства будут отображаться сведения из раздела **Контактная информация**, помогающие нашедшему связаться с вами.

Эта информация может включать в себя следующее:

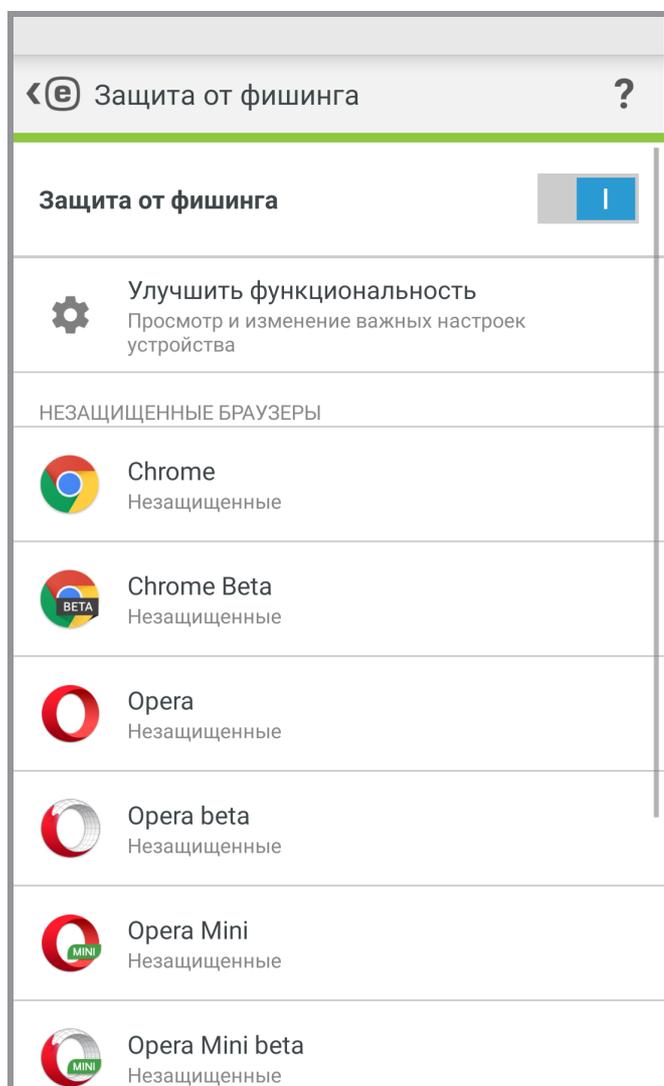
- Ваше имя (необязательно)
- Резервный номер телефона члена семьи или друга
- Описание устройства (необязательно)
- Электронная почта (необязательно)

7. Антифишинг

Термин *фишинг* означает преступную деятельность, которая использует социотехнику (манипуляция пользователями с целью получения конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальной информации, например номерам банковских счетов, номерам кредитных карт, PIN-кодам или именам пользователей и паролям.

Рекомендуется оставить **защиту от фишинга** включенной. Все потенциальные фишинговые атаки с веб-сайтов или доменов, занесенных компанией ESET в базу данных вредоносных объектов, блокируются, а для пользователя отображается уведомление о попытке атаки.

Компонент защиты от фишинга интегрируется с самыми распространенными веб-браузерами, доступными в ОС Android, а именно с браузером Chrome и стандартными браузерами, которые предварительно устанавливаются на устройствах Android (они обычно называются *Интернет* или *Браузер*). Прочие браузеры могут быть указаны как незащищенные, так как они не обеспечивают надлежащую интеграцию модуля защиты от фишинга. Чтобы использовать защиту от фишинга с максимальной эффективностью, рекомендуется не использовать неподдерживаемые веб-браузеры.



Улучшение функциональности — ESET Mobile Security предупреждает вас при необходимости предоставить функции защиты от фишинга дополнительные разрешения в ОС Android. Нажмите **Разрешить**, чтобы открыть настройки доступности системы и рассмотреть имеющиеся параметры для обеспечения поддержки большего числа браузеров и включения защиты при работе с браузером в приватном режиме (инкогнито). Если об этой проблеме не следует сообщать как о неполадке, нажмите **Игнорировать проблему (не рекомендуется)**.

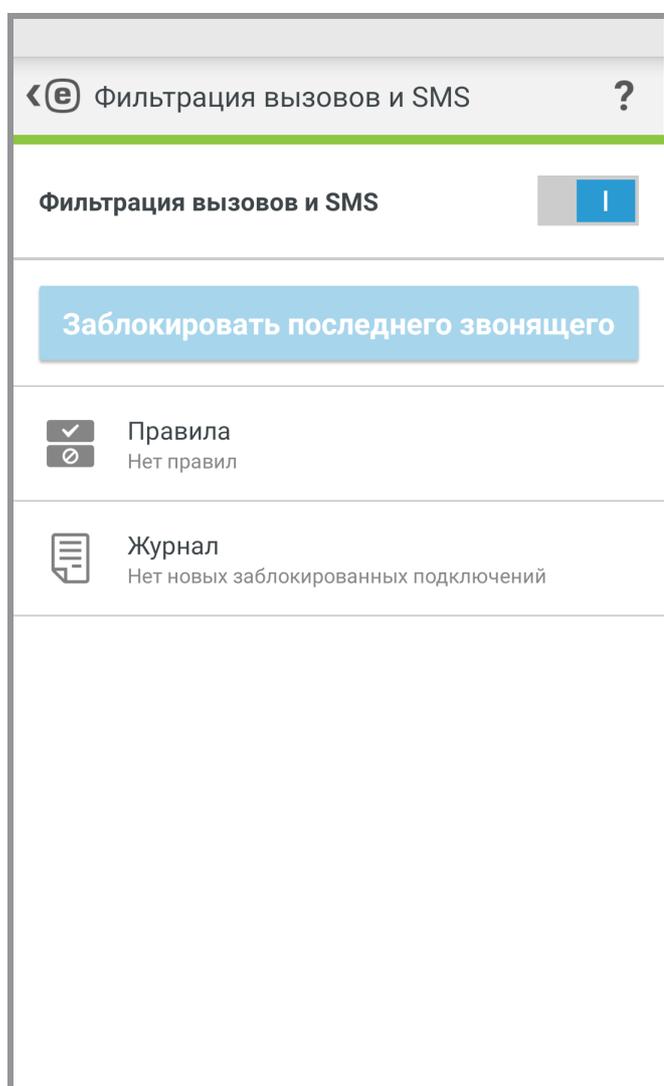
8. Фильтрация вызовов и SMS

Фильтрация вызовов и SMS блокирует входящие SMS- и MMS-сообщения, а также входящие и исходящие вызовы в соответствии с пользовательскими правилами.

К нежелательным сообщениям обычно относятся рекламные объявления от поставщиков услуг мобильной связи или сообщения от неизвестных либо неустановленных пользователей. При блокировке сообщений или вызовов уведомления не отображаются. Просмотрите [раздел «Журнал»](#) для проверки вызовов или сообщений, которые могли быть заблокированы по ошибке.

ПРИМЕЧАНИЕ. Фильтрация вызовов и SMS не работает на планшетах, которые не поддерживают телефонные звонки и обмен сообщениями. Фильтрация SMS- и MMS-сообщений не работает на устройствах под управлением ОС Android 4.4 и более поздних версий и будет отключена на устройствах, где основным приложением для обмена SMS является Google Hangouts.

8.1 Правила



Заблокировать последнего звонящего — коснитесь, чтобы заблокировать входящие звонки с последнего полученного номера телефона. В результате этого действия будет создано правило.

Чтобы создать правило, нажмите **Правила > Добавить правило**. Дополнительные сведения см. в [следующей главе](#).

Для изменения существующего правила выберите его и нажмите **Изменить** . Чтобы удалить запись из списка **Правила**, выберите ее и нажмите **Удалить** .

8.1.1 Добавление нового правила

1. В разделе **Действие** выберите **Блокировать** или **Разрешить**, чтобы указать тип правила для звонков и сообщений.
2. В разделе **Кто** выберите параметр для указания телефонных номеров, на которые будет распространяться правило.
 - **Человек**
 - **Группа** — ESET Mobile Security распознает группы контактов, сохраненные в приложении «Контакты» (например, «Семья», «Друзья» или «Коллеги»).
 - Параметр **Все неизвестные номера** относится ко всем телефонным номерам, не сохраненным в списке контактов. С помощью этого параметра можно заблокировать нежелательные телефонные звонки (например, рекламные) или запретить детям звонить на неизвестные номера.
 - Параметр **Все известные номера** относится ко всем телефонным номерам, сохраненным в списке контактов.
 - Параметр **Скрытые номера** относится к абонентам, которые намеренно скрывают свои номера с помощью услуги «антиопределитель номера».
3. В разделе **Что** выберите тип звонка или сообщения, который следует заблокировать или разрешить:
 -  исходящие звонки,
 -  входящие звонки,
 -  входящие текстовые сообщения (SMS),
 -  входящие мультимедийные сообщения (MMS).
4. В разделе **Когда** выберите **Всегда** или **Пользовательский**, чтобы указать интервал времени и дни недели, когда будет действовать правило. По умолчанию выбраны суббота и воскресенье.

ПРИМЕЧАНИЕ. Если вы находитесь за границей, введите все телефонные номера в списке с международным кодом, за которым должен следовать фактический номер (например, +1610100100).

8.2 Журнал

В разделе **Журнал** отображается список всех вызовов и сообщений, заблокированных функцией фильтрации вызовов и SMS. Каждый журнал содержит следующие сведения: имя события, соответствующий номер телефона, дата и время события. Журналы SMS- и MMS-сообщений содержат также тексты сообщений.

Чтобы удалить запись из списка, выберите ее и нажмите «Удалить» .

9. Проверка безопасности

Аудит безопасности помогает отслеживать и изменять важные параметры устройства, а также просматривать разрешения установленных приложений для предотвращения рисков безопасности.

Чтобы включить или отключить функцию «Аудит безопасности» и ее конкретные компоненты, коснитесь

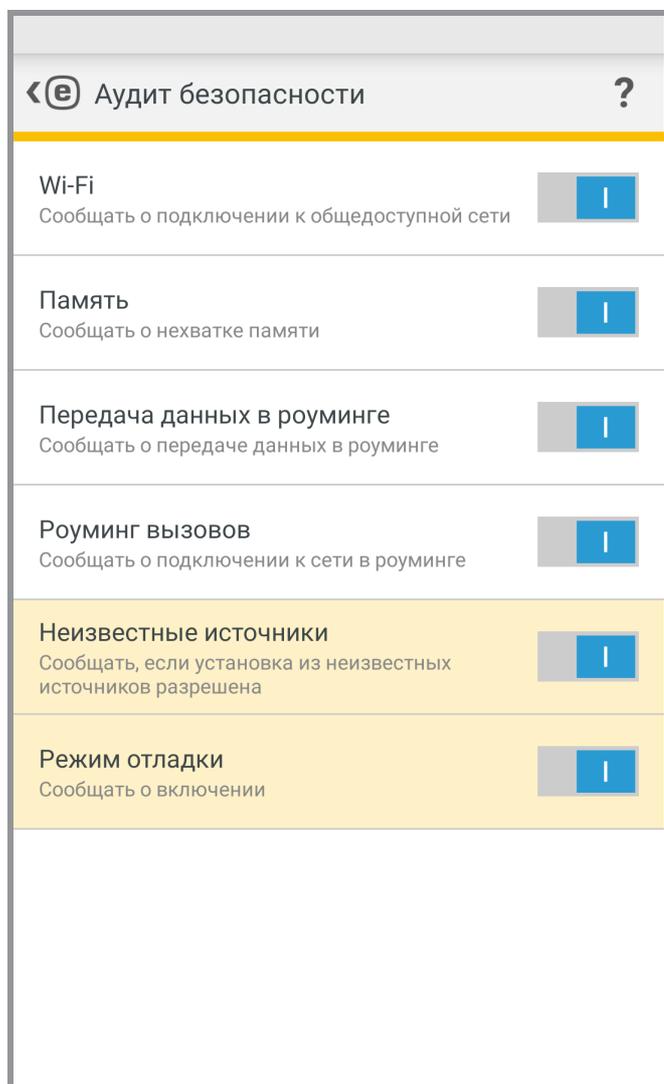


- [Мониторинг устройства](#)
- [Аудит приложения](#)

9.1 Отслеживание местоположения устройства

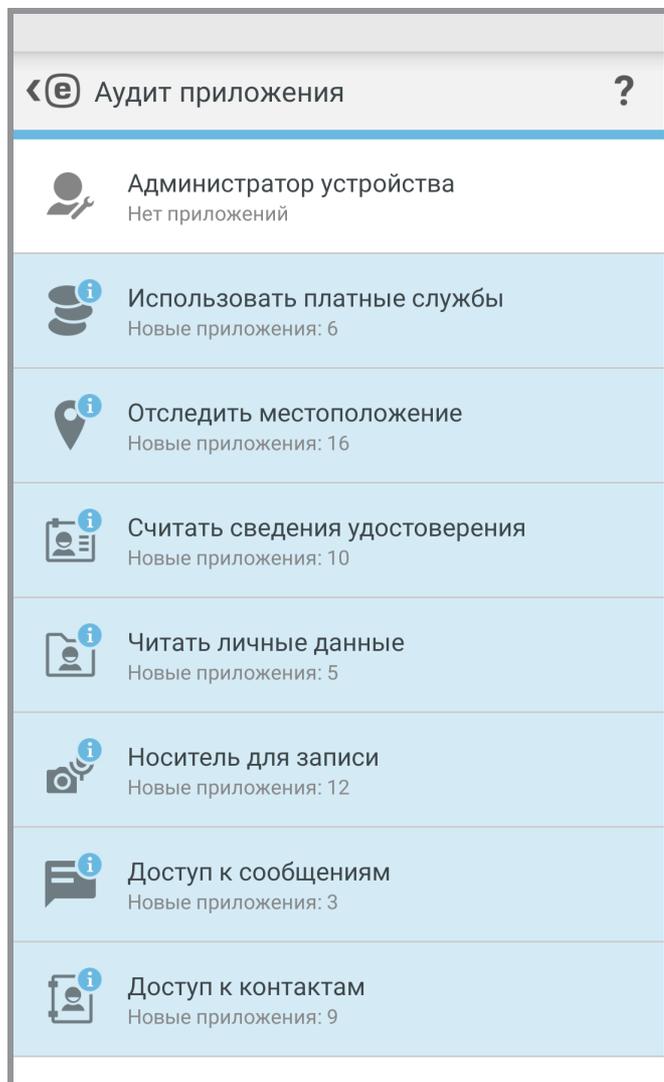
В разделе **Мониторинг устройства** определите, какие компоненты устройства будут отслеживаться программой ESET Mobile Security.

Коснитесь каждого из параметров, чтобы просмотреть его подробное описание и текущее состояние. В параметрах **Неизвестные источники** и **Режим отладки** нажмите **Открыть настройки**, чтобы изменить настройки в разделе параметров ОС Android.

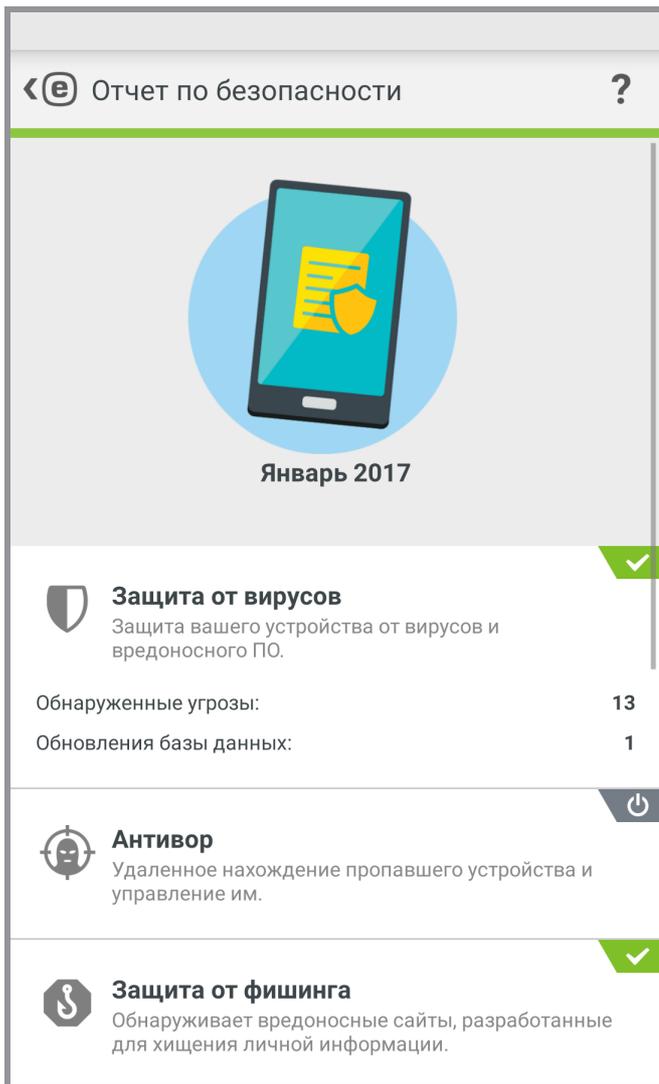


9.2 Аудит приложения

Функция «Аудит приложения» выполняет аудит установленных на вашем устройстве приложений, которые могут иметь доступ к платным услугам, отслеживать ваше местоположение либо считывать ваши идентификационные данные, контакты или текстовые сообщения. ESET Mobile Security предоставляет список таких приложений, отсортированных по категориям. Выберите каждую категорию, чтобы просмотреть подробное описание. Коснитесь того или иного приложения, чтобы просмотреть сведения о его разрешениях.



10. Отчет по безопасности



Отчет по безопасности предоставляет комплексный обзор каждого программного модуля, сведения о его состоянии и статистику. Также на экране «Отчет по безопасности» можно включить модули, которые в настоящее время не используются. Каждый раздел программного модуля содержит следующую информацию.

Защита от вирусов:

- Установленные приложения
- Обновленные приложения
- Просканированные приложения
- Обнаруженные угрозы
- Обновления базы данных сигнатур вирусов

Антивор

Защита от фишинга:

- Просканированные веб-сайты
- Обнаруженные угрозы

Фильтрация вызовов и SMS:

- Исходящие звонки
- Полученные звонки
- Заблокированные звонки

Аудит безопасности:

- Предупреждения о роуминге
- Предупреждения об открытой сети Wi-Fi

Включите параметр **Оповещение о месячном отчете**, чтобы отображать краткое сообщение в строке уведомлений Android. Коснитесь уведомления, чтобы открыть окно **Отчет по безопасности**.

11. Настройки

Для доступа к настройкам программы коснитесь «Меню»  на главном экране ESET Mobile Security (или нажмите кнопку меню на устройстве) и затем коснитесь элемента **Настройки**.

Язык

По умолчанию приложение ESET Mobile Security устанавливается на языке, который выбран в качестве языка системы на устройстве (настройки **Язык и клавиатура** в ОС Android). Чтобы изменить язык интерфейса приложения, коснитесь элемента «Язык» и выберите язык.

Постоянное уведомление

В приложении ESET Mobile Security значок  отображается в левом верхнем углу экрана (в строке состояния Android). Если отображать этот значок не нужно, снимите флажок **Постоянное уведомление** и нажмите **Выключить**.

Специальные предложения

В приложении вы будете получать новости и новейшие предложения от компании ESET.

Обновление

Чтобы обеспечить максимальную защиту, важно использовать самую последнюю версию ESET Mobile Security. Чтобы узнать, доступна ли более новая версия на веб-сайте ESET, коснитесь элемента **Обновление**. Эта возможность недоступна, если программа ESET Mobile Security была загружена из магазина Google Play. В этом случае следует устанавливать обновления, доступные в магазине Google Play.

удаления

Выполнение мастера удаления окончательно удалит программу ESET Mobile Security с устройства. Если перед этим была включена защита от удаления программы, вам будет предложено ввести пароль безопасности. Чтобы удалить продукт вручную, выполните [шаги, описанные в этом разделе](#).

12. Служба поддержки

Сотрудники службы поддержки клиентов ESET с радостью помогут вам в решении административных и технических вопросов, возникающих при работе с приложением ESET Mobile Security или любыми другими продуктами ESET.

Чтобы обратиться в службу поддержки клиентов ESET, [щелкните эту ссылку](#).

Чтобы отправить запрос в службу поддержки со своего устройства, коснитесь «Меню»  на главном экране ESET Mobile Security (или нажмите кнопку меню на устройстве), последовательно щелкните элементы **Служба поддержки клиентов > Служба поддержки клиентов** и заполните все обязательные поля. ESET Mobile Security содержит расширенные функции ведения журнала, помогающие в диагностике потенциальных технических проблем. Для предоставления специалистам ESET подробного журнала приложения убедитесь, что выбран параметр **Отправить журнал приложения** (по умолчанию). Нажмите **Отправить**, чтобы отправить запрос. Специалист службы поддержки клиентов ESET свяжется с вами по указанному адресу электронной почты.