ESET Mobile Security

Business Edition для Windows Mobile

Инструкция по установке и руководство пользователя

ESET Mobile Security

Версия 2.5.2011

Содержание

1. Установка ESET Mobile Security

1.1 Минимальные требования к системе

Установить приложение ESET Mobile Security для Windows Mobile на мобильном устройстве можно, если оно соответствует указанным ниже требованиям к системе.

	Минимальные требования к системе
Операционная система	Windows Mobile 5.0 или более поздней версии
Тактовая частота процессора	200 МГц
Объем памяти	16 МБ
Объем свободного места на диске	2,5 МБ

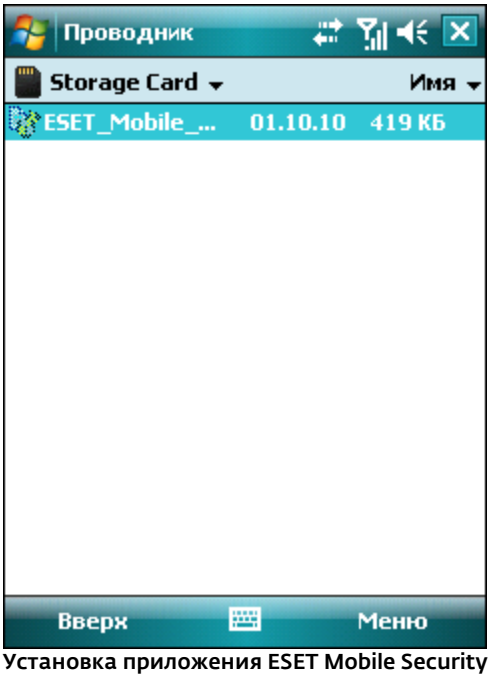
1.2 Установка

Перед установкой сохраните все открытые документы и закройте все запущенные приложения. Приложение ESET Mobile Security можно установить непосредственно на устройство или с помощью компьютера.

После установки активируйте ESET Mobile Security в соответствии с инструкциями, приведенными в разделе Активация приложения 5.

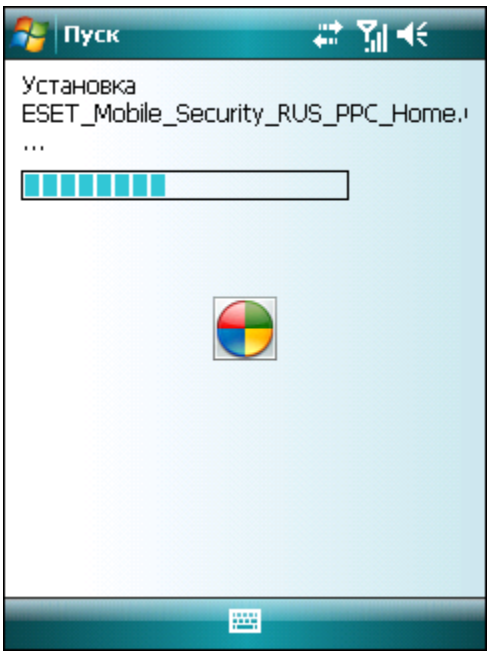
1.2.1 Установка на мобильное устройство

Чтобы установить приложение ESET Mobile Security непосредственно на устройство, загрузите на него установочный файл *.cab* с использованием технологии Wi-Fi или Bluetooth, через USB либо как вложение в сообщение электронной почты. Выберите команду **«Пуск» > «Программы» > «Проводник»**, чтобы найти файл. Выберите файл, чтобы запустить программу установки, и следуйте указаниям мастера установки.



Установка приложения ESET Mobile Security

ПРИМЕЧАНИЕ. Интерфейс пользователя Windows Mobile зависит от модели устройства. На вашем устройстве установочный файл может находиться в другом меню или другой папке.



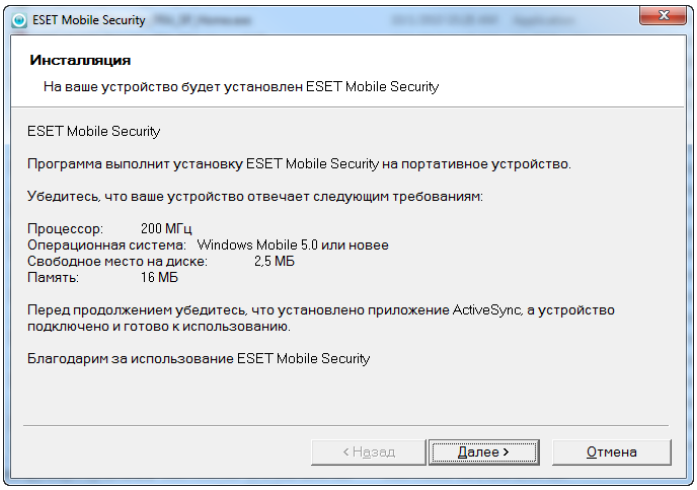
Процесс установки

После установки приложения его параметры можно изменить. Имейте, однако, в виду, что конфигурация по умолчанию обеспечивает максимальный уровень защиты от вредоносных программ.

1.2.2 Установка с помощью компьютера

Чтобы установить приложение ESET Mobile Security с помощью компьютера, подключите мобильное устройство к компьютеру, используя службу ActiveSync (в Windows XP) или центра устройств Windows Mobile (в Windows 7 и Windows Vista). После распознавания устройства запустите загруженный установочный пакет (файл *exe*) и

следуйте указаниям мастера установки.



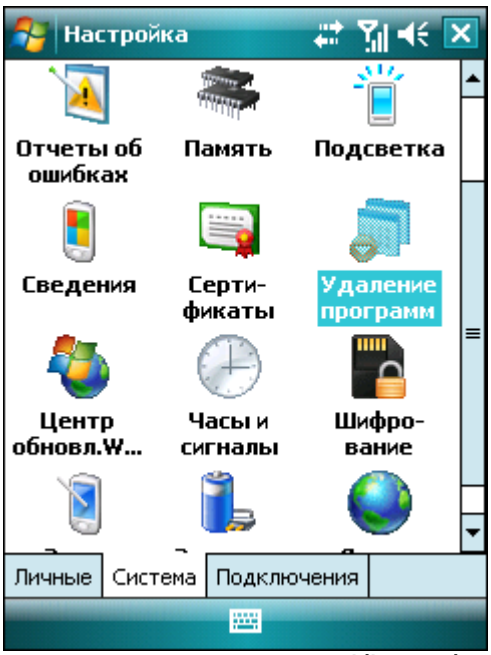
Запуск программы установки на компьютере

Затем следуйте указаниям на экране мобильного устройства.

1.3 Удаление приложения

Чтобы удалить приложение ESET Mobile Security с мобильного устройства, выберите пункт **«Пуск» > «Настройки»**, откройте вкладку **«Система»** и выберите значок **«Удаление программ»**.

ПРИМЕЧАНИЕ. Интерфейс пользователя Windows Mobile зависит от модели устройства. На разных устройствах эти параметры могут немного различаться.



Удаление приложения ESET Mobile Security

Выделите пункт ESET Mobile Security и выберите команду **«Удалить»**. В ответ на предложение подтвердить удаление выберите вариант **«Да»**.

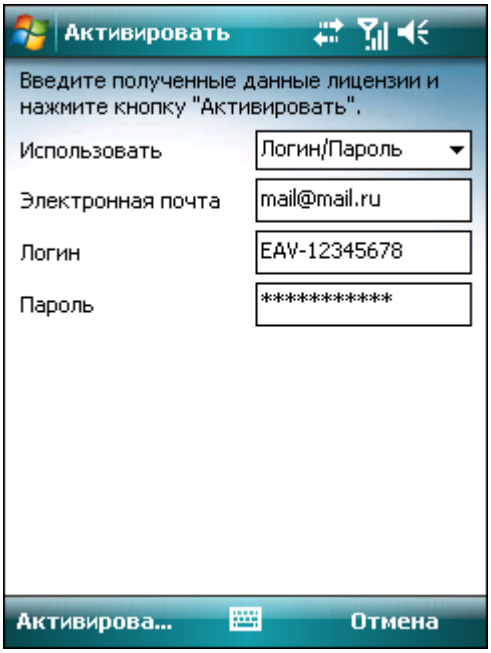
Удаление приложения ESET Mobile Security

2. Активация приложения

Выполнение инструкций, приведенных в данном руководстве, начинается в главном окне приложения ESET Mobile Security (**«Пуск» > «Программы» > ESET Mobile Security**).

Главное окно приложения ESET Mobile Security

После установки приложения ESET Mobile Security его необходимо активировать. Если предложение активировать продукт не отобразилось автоматически, выберите команду **«Меню» > «Активировать»**.



Активация программы

Есть два способа активации; выбор того или иного зависит от способа приобретения приложения ESET Mobile Security.

2.1 Активация с помощью имени пользователя и пароля

Если продукт был приобретен в виде электронной лицензии, имя пользователя и пароль были предоставлены вместе с покупкой. Выберите параметр **«Логин/пароль»** и введите полученную информацию в поля **«Логин»** и **«Пароль»**. В поле **«Электронная почта»** введите свой текущий адрес. Выберите команду **«Активировать»**, чтобы завершить активацию. По электронной почте будет отправлено подтверждение об успешной активации продукта.

2.2 Активация с помощью ключа регистрации

Если продукт ESET Mobile Security был приобретен с новым устройством или как коробочная версия, вместе с покупкой был предоставлен ключ регистрации. Выберите параметр **«Ключ регистрации»** и введите в поле **«Электронная почта»** свой текущий адрес электронной почты, а в поле **«Ключ регистрации»** - полученные сведения. Выберите команду **«Активировать»**, чтобы завершить активацию. Новые учетные данные (имя пользователя и пароль) автоматически заменят ключ регистрации и будут отправлены на указанный адрес электронной почты.

Активация действительна на определенный период времени. По истечении срока действия активации необходимо обновить 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. Эта операция оплачивается в соответствии с текущим тарифом поставщика услуг.

3. Обновление приложения

По умолчанию вместе с приложением ESET Mobile Security устанавливается задача обновления, гарантирующая регулярное выполнение этой процедуры. Кроме того, обновление можно выполнять вручную.

После установки приложения рекомендуется запустить вручную первое обновление. Для этого выберите команду **«Действие» > «Обновить»**.

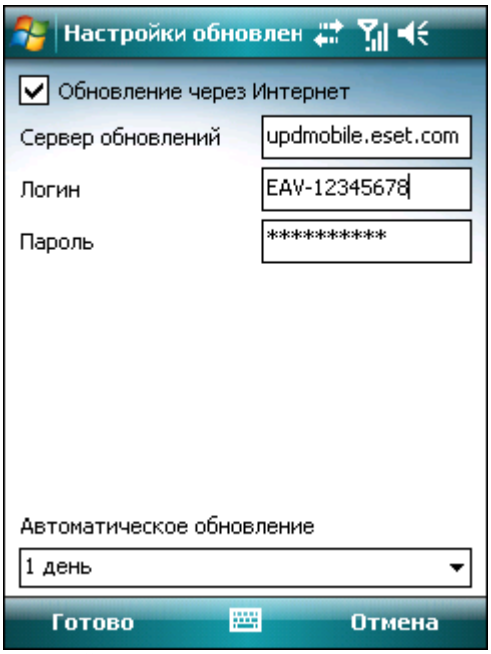
3.1 Настройки

Чтобы настроить параметры обновления, выберите команду **«Меню» > «Настройки» > «Обновление»**.

Параметр **«Обновление через Интернет»** включает и отключает автоматическое обновление.

Можно указать **сервер обновлений**, с которого будут загружаться обновления (рекомендуется оставить значение по умолчанию *updmobile.eset.com*).

Выбрать интервал автоматического обновления можно с помощью параметра **«Автоматическое обновление»**.



Настройки обновления

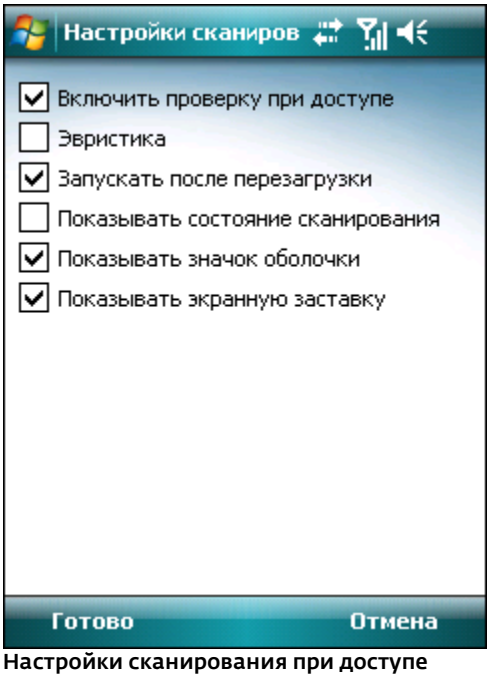
ПРИМЕЧАНИЕ. Чтобы снизить использование пропускной способности сети, обновления базы данных сигнатур вирусов выпускаются по мере необходимости при появлении новых угроз. Несмотря на то, что обновления базы данных сигнатур вирусов бесплатны при активной лицензии, поставщик услуг мобильной связи может взимать плату за передачу данных.

4. Модуль сканирования при доступе

Модуль сканирования при доступе проверяет файлы, к которым обращается пользователь, в реальном времени. Все запускаемые, открываемые и сохраняемые файлы автоматически проверяются на наличие угроз. Сканирование осуществляется еще до того, как с файлом выполняется какое-либо действие, что обеспечивает максимальный уровень защиты. Модуль сканирования при доступе автоматически запускается при загрузке системы.

4.1 Настройки

Чтобы включить или отключить указанные ниже параметры, выберите команду **«Меню» > «Настройки» > «При доступе»**.



Настройки сканирования при доступе

- **«Включить проверку в режиме "по доступу"»**: если этот параметр включен, модуль сканирования при доступе работает в фоновом режиме.
- **«Эвристика»**: если выбрать этот параметр, будет использоваться технология эвристического анализа. Эвристические методы позволяют сразу обнаруживать новые вредоносные программы, сигнатуры которых пока отсутствуют в базе данных, путем анализа кода и распознавания типичного для вирусов поведения. Недостатком этих методов является увеличение времени сканирования.
- **«Запускать после перезагрузки»**: если выбрать этот параметр, после перезагрузки устройства автоматически будет запускаться модуль сканирования при доступе.
- **«Показывать состояние сканирования»**: если выбрать этот параметр, в правом нижнем углу будет отображаться состояние выполняемого сканирования.
- **«Показывать значок оболочки»**: этот параметр включает показ значка быстрого доступа к настройкам модуля сканирования при доступе в правом нижнем углу начального экрана Windows Mobile.
- **«Показывать экранную заставку»**: этот параметр позволяет включить или отключить отображение заставки приложения ESET Mobile Security при запуске устройства.

5. Модуль сканирования по требованию

С помощью модуля сканирования по требованию можно проверить, не заражено ли мобильное устройство. Файлы некоторых предопределенных типов сканируются по умолчанию.

5.1 Проверка всего устройства

В ходе проверки всего устройства выполняется проверка памяти, запущенных процессов, связанных с ними динамических библиотек (DLL) и файлов во внутренней и съемной памяти.

Чтобы запустить проверку всего устройства, выберите команду **«Действие» > «Сканирование » > «Все устройство»**.

ПРИМЕЧАНИЕ. По умолчанию проверка памяти не выполняется. Его можно включить в разделе **«Меню» > «Настройки» > «Общие»**.

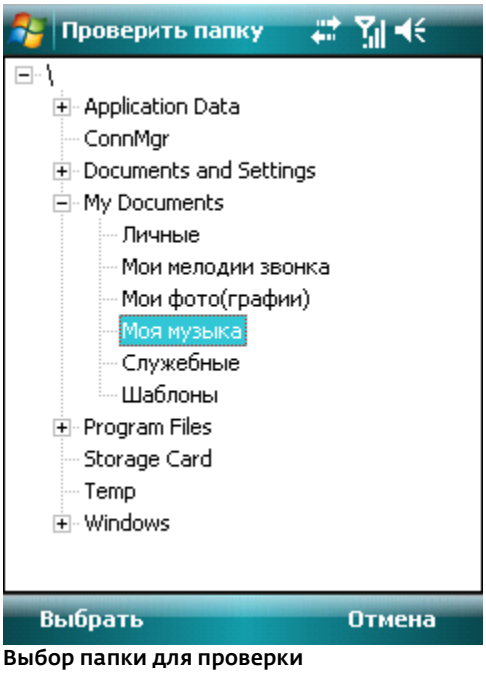
Программа проверяет сначала системную память (включая запущенные процессы и связанные с ними библиотеки DLL), а затем файлы и папки. При сканировании в течение короткого времени отображаются путь к файлу и его имя.

ПРИМЕЧАНИЕ. Чтобы прервать запущенное сканирование, выберите команду **«Действие» > «Проверка» > «Остановить»**.

5.2 Проверка папки

Для проверки определенной папки на устройстве выберите команду **«Меню» > «Проверка» > «Папка»** .

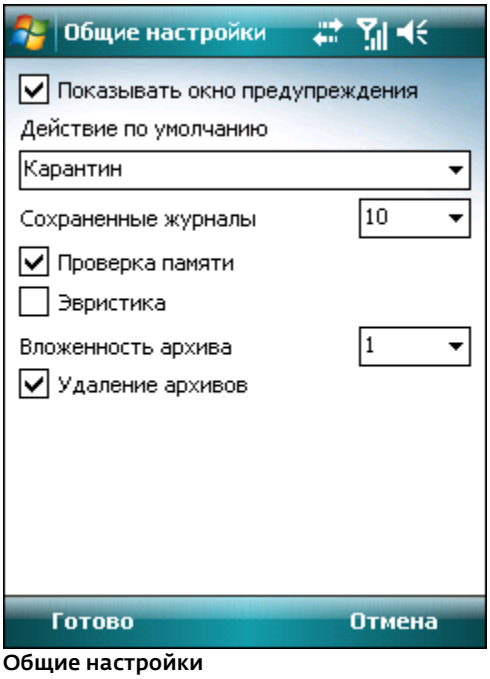
Выделите папку, которую необходимо проверить, а затем выберите команду **«Выбрать»**.



Выбор папки для проверки

5.3 Общие настройки

Чтобы изменить параметры проверки, выберите команду **«Меню» > «Настройки» > «Общие»**.



Общие настройки

Установите флажок **«Показывать окно предупреждения»**, если нужно, чтобы отображались уведомления.

Можно выбрать действие по умолчанию, автоматически выполняемое при обнаружении зараженных файлов. Доступны указанные ниже варианты.

- **Карантин**
- **Удалить,**
- **Ничего не предпринимать (не рекомендуется).**

Параметр **«Сохраненные журналы»** позволяет задать максимальное количество журналов,

сохраняемых в разделе **«Меню» > «Журналы» > «Проверка»**.

Если включена функция **«Проверка памяти»**, перед проверкой файлов будет автоматически проверяться на наличие вредоносных программ память устройства.

Если включен параметр **«Эвристика»**, приложение ESET Mobile Security будет использовать эвристические методы сканирования. Эвристический анализ - это алгоритмический способ обнаружения вредоносных программ, основанный на анализе кода в поисках типичных признаков вирусов. Основным преимуществом этого способа является возможность обнаружения вредоносных программ, не распознаваемых с использованием текущей версии базы данных сигнатур вирусов, недостатком - увеличение времени сканирования.

Параметр **«Вложенность архива»** позволяет задать уровень вложенности архивов, подлежащих сканированию. Чем больше это число, тем глубже сканирование.

Если включен параметр **«Удаление архивов»**, файлы архивов (*zip*, *rar* и *jar*), содержащие зараженные объекты, будут автоматически удаляться.

Настройки расширений

5.4 Настройки расширений

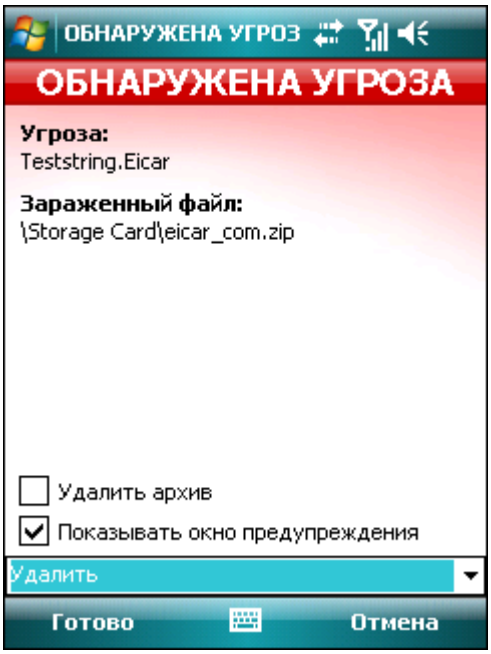
Чтобы выбрать на мобильном устройстве типы файлов, которые нужно проверить, выберите команду **«Меню» > «Настройки» > «Расширения»**.

Появится окно **«Расширения»** со списком типов файлов, наиболее подверженных заражению. Выберите типы файлов, которые нужно проверить, или отмените их выбор, если выполнять их проверку не нужно. Если включить параметр **«Архивы»**, будут проверены архивы всех поддерживаемых типов (*zip*, *rar* и *jar*).

Чтобы проверить все файлы, снимите флажок **«С учетом расширений»**.

6. Обнаружена угроза

При обнаружении угрозы приложение ESET Mobile Security предлагает выполнить то или иное действие.



Окно предупреждения об угрозе

Рекомендуется выбрать команду **«Удалить»**. Если выбрать вариант **«Карантин»**, файл будет перемещен из исходного местоположения в папку карантина. Если выбрать команду **«Игнорировать»**, никакие действия предприняты не будут, а зараженный файл останется на мобильном устройстве.

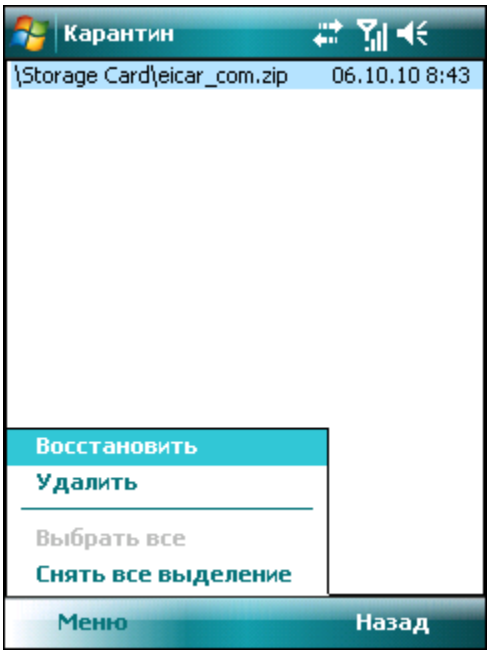
Если обнаружен зараженный файл в архиве (например, *.zip*), в окне предупреждения будет доступно действие **«Удалить архив»**. Выбрав его и действие **«Удалить»**, можно удалить все файлы в архиве.

Если параметр **«Показывать окно предупреждения»** отключен, во время сканирования предупреждения не отображаются (сведения о том, как отключить предупреждения для последующего сканирования, см. в разделе «Общие настройки» 8).

6.1 Карантин

Карантин предназначен в первую очередь для изоляции и безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя вылечить или безопасно удалить либо если они отнесены к зараженным по ошибке.

Информация о файлах, помещенных на карантин, записывается в журнал. Она включает дату и время помещения файла на карантин и путь к его исходному местоположению в системе. Чтобы открыть папку карантина, выберите команду **«Меню» > «Вид» > «Карантин»**.



Список карантина

Чтобы восстановить файлы из карантина, выберите команду **«Меню» > «Восстановить»** (каждый файл будет восстановлен в своем исходном местоположении). Чтобы удалить файлы, выберите команду **«Меню» > «Удалить»**.

7. Anti-Theft

Функция Anti-Theft предотвращает несанкционированный доступ к устройству.

Если после потери или кражи телефона в него вставлена новая недоверенная SIM-карта, то 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 папки «Отправлено».

Для удаления всех данных (контактов, сообщений и приложений), сохраненных на устройстве и подключенных к нему съемных носителях, можно отправить на телефонный номер неавторизованного пользователя SMS-сообщение с запросом удаленной очистки устройства в следующем формате:
#RC# DS пароль
где *пароль* - это пароль, заданный в разделе **«Меню» > «Настройки» > «Пароль»**.

7.1 Настройки

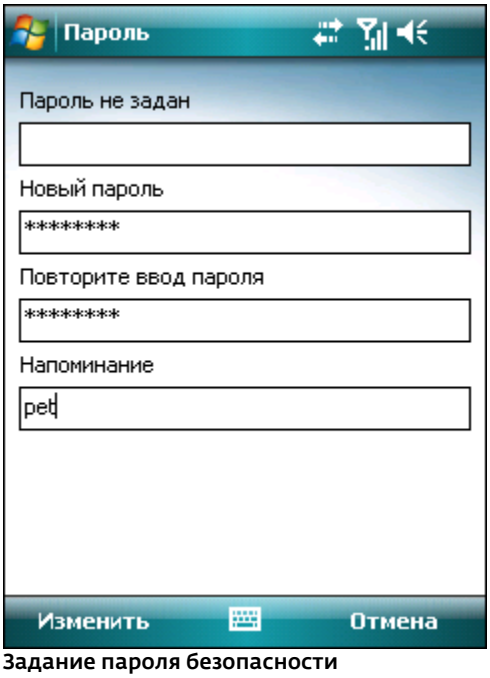
Сначала задайте пароль в разделе **«Меню» > «Настройки» > «Пароль»**. Пароль требуется для выполнения указанных ниже действий.

- Отправка SMS-сообщения с запросом на удаленную очистку устройства.
- Доступ к параметрам Anti-Theft на устройстве.
- Удаление приложения ESET Mobile Security с устройства.

Чтобы задать новый пароль, введите его в поля **«Новый пароль»** и **«Повторите ввод пароля»**. Функция **«Напоминание»** (если она включена) позволяет получить подсказку, если не удается вспомнить пароль.

Чтобы изменить существующий пароль, введите его в поле **«Введите текущий пароль»**, а затем задайте новый пароль.

ВНИМАНИЕ! Пароль следует выбирать тщательно, поскольку он требуется для удаления приложения ESET Mobile Security с устройства.



Задание пароля безопасности

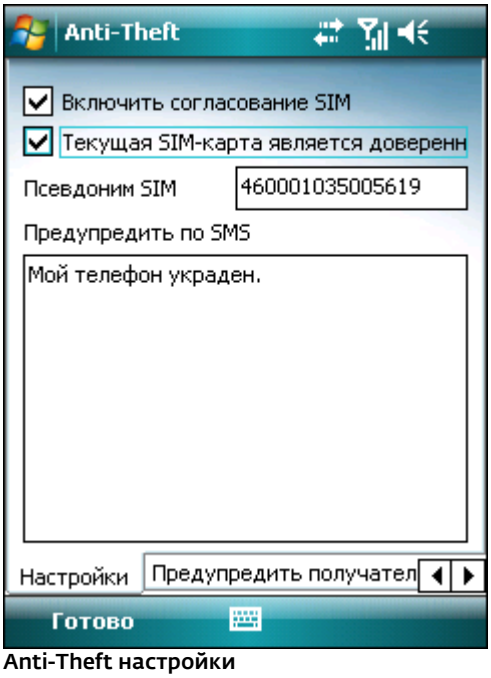
Чтобы открыть настройки функции Anti-Theft, выберите команду **«Меню» > «Настройки» > Anti-Theft** и введите пароль.

Чтобы отключить автоматическую проверку вставляемых SIM-карт (и отправку SMS-сообщений с предупреждением), снимите флажок **«Включить согласование SIM»**.

Если текущую SIM-карту нужно сохранить как доверенную, установите флажок **«Текущая SIM-карта является доверенной»**, после чего она будет внесена в список **доверенных SIM-карт** на одноименной вкладке. В поле **«Псевдоним SIM»** будет автоматически введен номер IMSI.

Если используются несколько SIM-карт, можно выбрать отдельный **псевдоним SIM** для каждой из них (назвав их, например, *«Рабочая»*, *«Домашняя»* и т. д.).

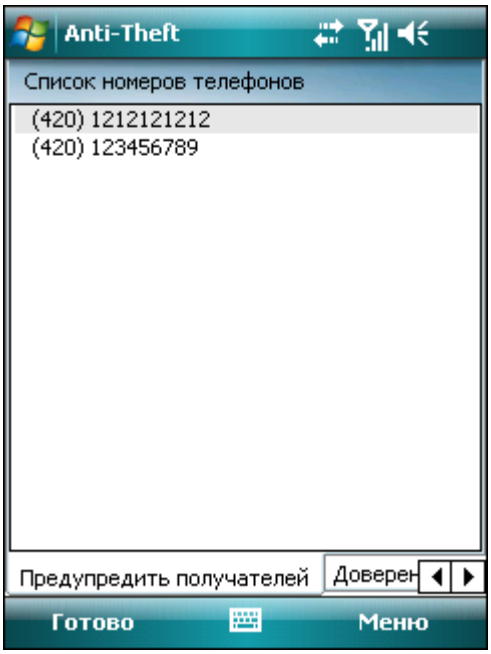
В поле **«Предупредить по SMS»** можно изменить текстовое сообщение, отправляемое на указанные номера после вставки недоверенной SIM-карты в устройство.



Anti-Theft настройки

На вкладке **«Предупредить получателей»** отображается список номеров, на которые будет отправляться SMS-сообщение с предупреждением о вставке недоверенной SIM-карты в устройство. Чтобы добавить номер в этот список, выберите команду **«Меню» > «Добавить»**. Чтобы добавить номер из адресной книги, выберите команду **«Меню» > «Добавить контакт»**.

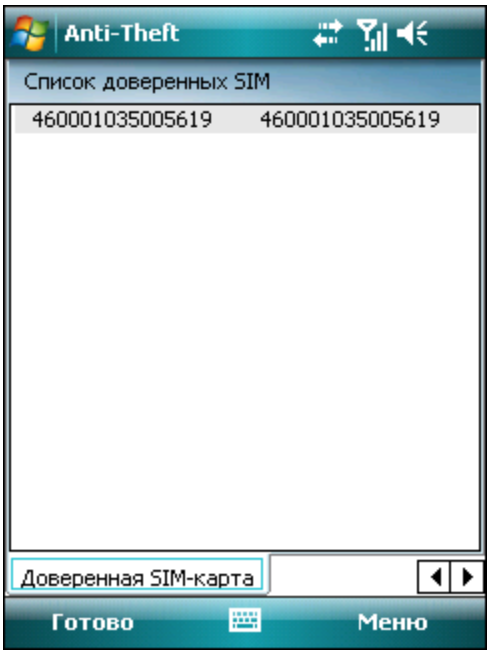
ПРИМЕЧАНИЕ. Номер телефона должен включать международный код и собственно номер (например, *+76102002000*).



Предопределенный список номеров телефонов

На вкладке **«Доверенная SIM-карта»** выводится список доверенных SIM-карт. Каждая запись содержит псевдоним SIM (левый столбец) и номер IMSI (правый столбец).

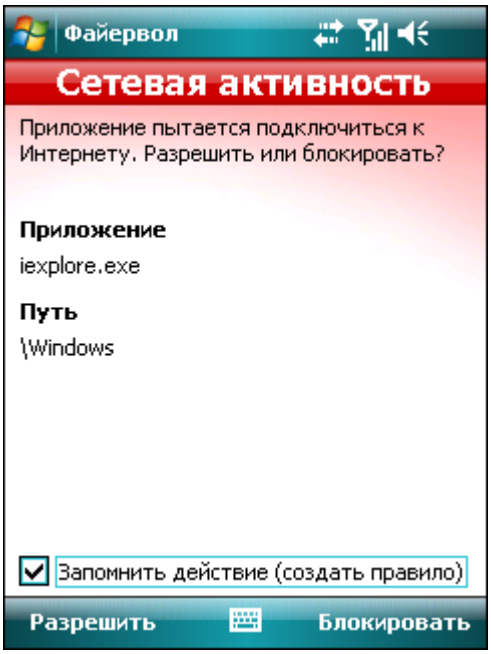
Чтобы удалить SIM-карту из списка, выделите ее и выберите команду **«Меню» > «Удалить»**.



Список доверенных SIM-карт

8. Файервол

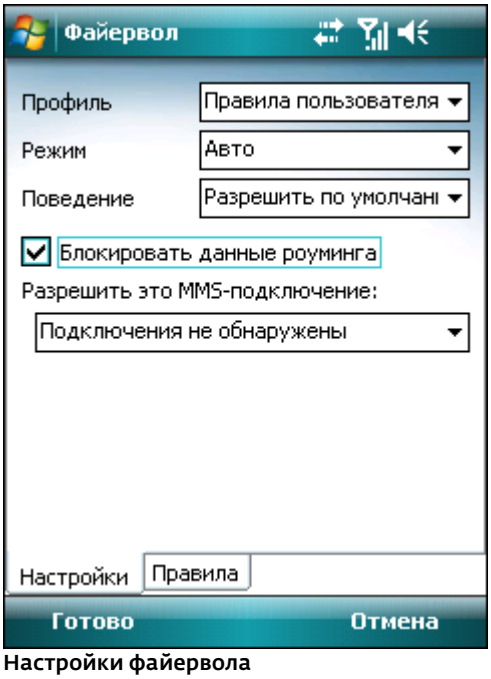
Файервол контролирует входящий и исходящий сетевой трафик, разрешая или блокируя отдельные соединения на основе правил фильтрации.



Предупреждение файервола

8.1 Настройки

Чтобы открыть настройки файервола, выберите команду **«Меню» > «Настройки» > «Файервол»**.



Настройки файервола

Доступны указанные ниже профили.

- **«Разрешить все»**: разрешена передача всего сетевого трафика.
- **«Блокировать все»**: блокируется весь сетевой трафик.
- **«Пользовательские правила»**: пользователь может задать свои правила фильтрации.

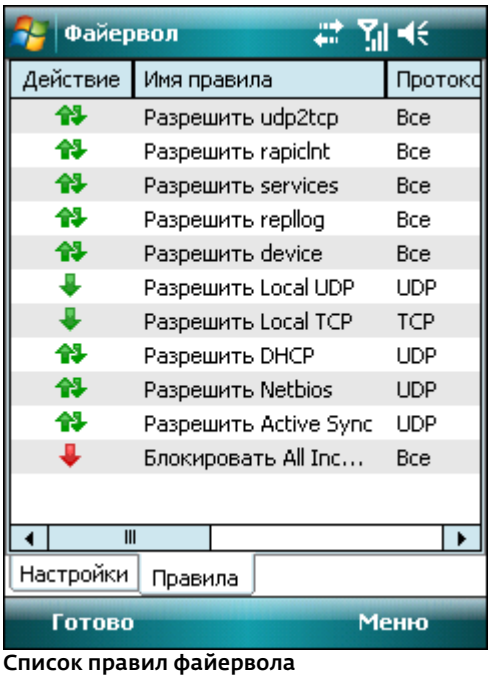
В профиле **«Пользовательские правила»** можно выбрать один из двух режимов фильтрации, которые указаны ниже.

- **«Авто»**: данный режим подходит для пользователей, которым важны простота и удобство и которые не собираются создавать правила. В этом режиме разрешена отправка всего исходящего трафика. В разделе **«Поведение»** можно выбрать действие по умолчанию для входящего трафика (**«Разрешить по умолчанию»** или **«Блокировать по умолчанию»**).
- **«Интерактивный»**: этот режим позволяет настроить параметры персонального файервола. При обнаружении соединения, для которого не определено правило, появляется диалоговое окно с сообщением об этом. В нем можно разрешить или заблокировать соединение и создать правило. После создания правила все подобные соединения будут разрешаться или блокироваться в соответствии с ним. Если приложение, для которого определено правило, было изменено, в диалоговом окне можно принять или отклонить изменение. Существующее правило будет изменено в соответствии с выбранным ответным действием.

«Блокировать данные роуминга»: если этот флажок установлен, приложение ESET Mobile Security автоматически обнаруживает подключение к роуминговой сети устройства и блокирует входящий и исходящий трафик. Данные, получаемые через подключение Wi-Fi или GPRS, при этом не блокируются.

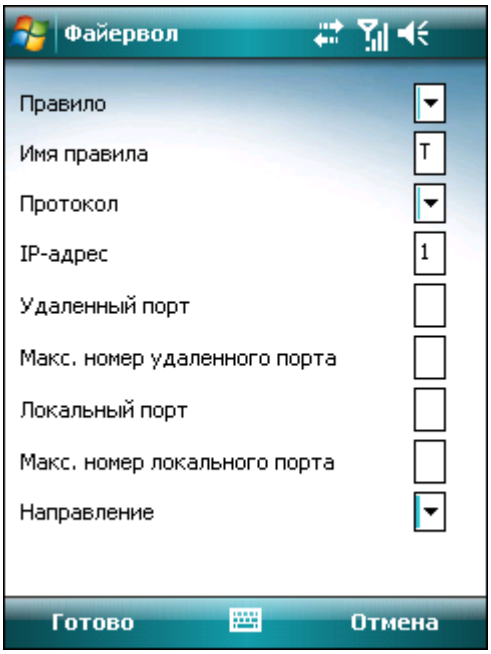
«Разрешить это MMS-подключение»: установите этот флажок, чтобы получать MMS-сообщения в роуминговой сети. MMS-сообщения, получаемые по другим подключениям, будут блокироваться приложением ESET Mobile Security.

На вкладке **«Правила»** можно изменять и удалять правила фильтрации.



Список правил файервола

Чтобы создать правило, выберите команду **«Меню» > «Добавить»**, заполните необходимые поля и выберите пункт **«Готово»**.

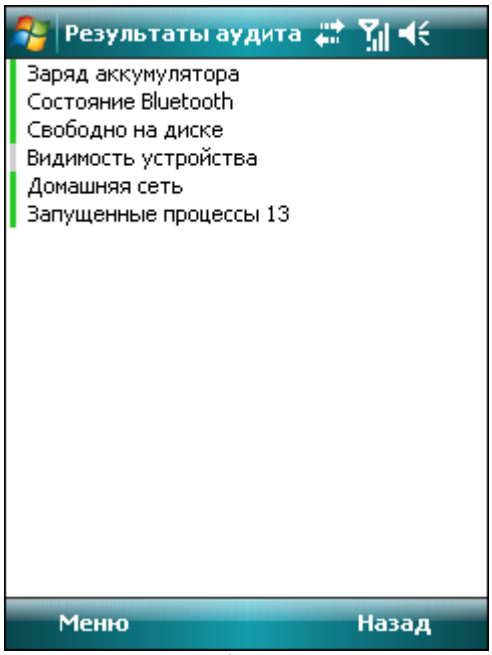


Создание правила

9. Аудит безопасности

Аудит безопасности позволяет проверять состояние телефона: уровень заряда аккумуляторов, состояние Bluetooth, свободное дисковое пространство и т. д.

Чтобы запустить аудит безопасности вручную, выберите команду **«Действие» > «Аудит безопасности»**. Отобразится подробный отчет.

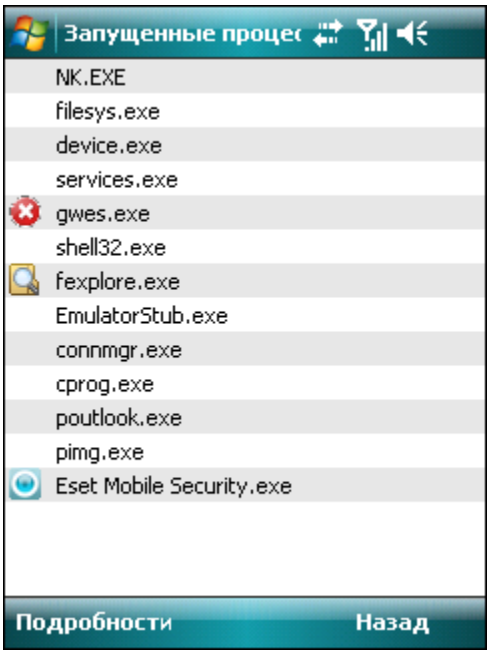


Результаты аудита безопасности

Зеленая отметка рядом с каждым элементом указывает, что значение выше порогового или что элемент не представляет угрозы для безопасности. Красная отметка указывает, что значение ниже порогового или что элемент может угрожать безопасности.

Если элемент **«Состояние Bluetooth»** или **«Видимость устройства»** выделен красным, можно отключить это состояние, выделив элемент и выбрав команду **«Меню» > «Исправить»**.

Чтобы просмотреть подробные сведения об элементе, выделите его и выберите команду **«Меню» > «Подробности»**.



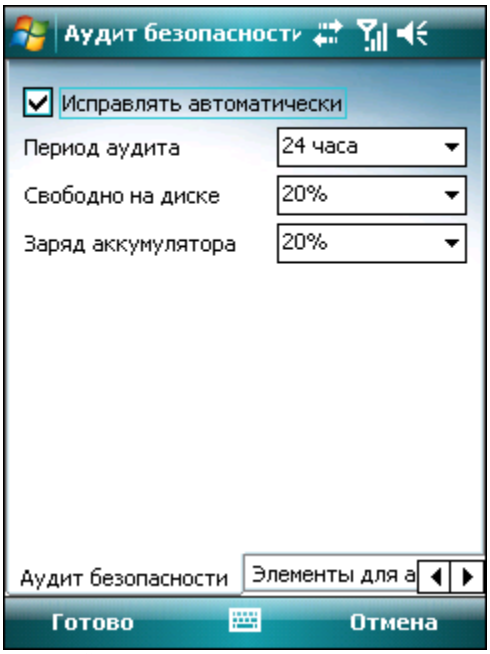
Запущенные процессы

oПараметр **«Запущенные процессы»** отображает список процессов, выполняемых на устройстве.

Чтобы просмотреть подробные сведения о процессе (полный путь к нему и использование памяти), выберите его, а затем выберите команду **«Подробности»**.

9.1 Настройки

Чтобы изменить параметры аудита безопасности, выберите команду **«Меню» > «Настройки» > «Аудит безопасности»**.



Настройки аудита безопасности

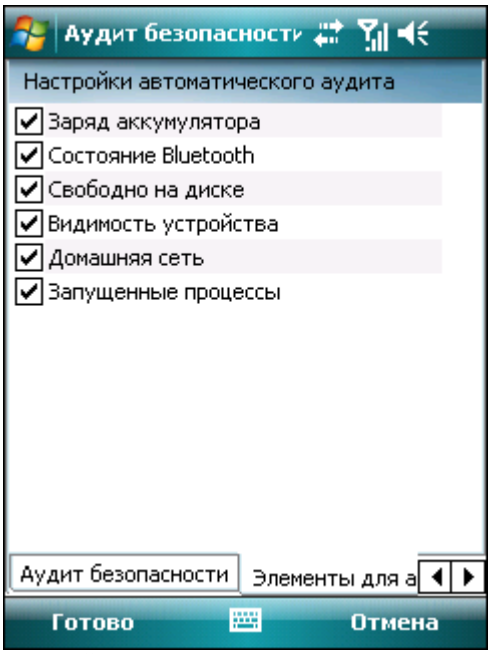
Если параметр **«Исправлять автоматически»** включен, приложение ESET Mobile Security будет

автоматически пытаться устранить факторы риска (связанные, например, с состоянием Bluetooth, видимостью устройства) без вмешательства пользователя. Этот параметр используется только в автоматическом (запланированном) режиме аудита.

Параметр **«Период аудита»** позволяет указать частоту выполнения автоматического аудита. Чтобы отключить автоматический аудит, установите флажок **«Никогда»**.

Ниже можно настроить пороговые значения параметров **«Свободно на диске»** и **«Заряд аккумулятора»**.

На вкладке **«Элементы для аудита»** можно выбрать элементы, которые будут проверяться во время автоматического (запланированного) аудита безопасности.



Настройки автоматического аудита

10. Антиспам

Модуль антиспама блокирует нежелательные входящие SMS- и MMS-сообщения.

Как правило, нежелательные сообщения содержат рекламу от операторов мобильной связи либо послания от неизвестных или неуказанных пользователей.

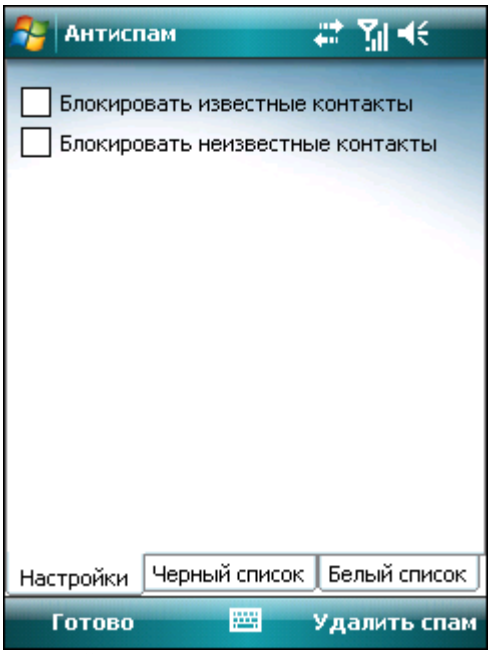
10.1 Настройки

Выберите команду **«Меню» > «Вид» > «Статистика»**, чтобы просмотреть статистические сведения о полученных и заблокированных сообщениях.

В разделе «Антиспам» (**«Меню» > «Настройки» > «Антиспам»**) доступны указанные ниже режимы фильтрации.

- **«Блокировать неизвестные контакты»**: установите этот флажок, чтобы принимать сообщения только от отправителей, внесенных в адресную книгу.
- **«Блокировать известные контакты»**: установите этот флажок, чтобы принимать сообщения только от отправителей, не внесенных в адресную книгу.
- Установите оба флажка (**«Блокировать неизвестные контакты»** и **«Блокировать известные контакты»**), чтобы блокировать все входящие сообщения.
- Чтобы отключить защиту от спама, снимите флажки **«Блокировать неизвестные контакты»** и **«Блокировать известные контакты»**. После этого будут приниматься все входящие сообщения.

ПРИМЕЧАНИЕ. Записи в белом и черном списках переопределяют эти параметры (см. раздел «Белый и черный списки» 17).



Настройки модуля антиспама

10.2 Белый список / черный список

«Черный» список - это список телефонных номеров, с которых блокируются все сообщения. Указанные в нем записи имеют более высокий приоритет, чем параметры защиты от спама (вкладка **«Настройки»**).

«Белый» список - это список телефонных номеров, с которых все сообщения всегда принимаются. Указанные в нем записи имеют более высокий приоритет, чем параметры защиты от спама (вкладка **«Настройки»**).

Черный список

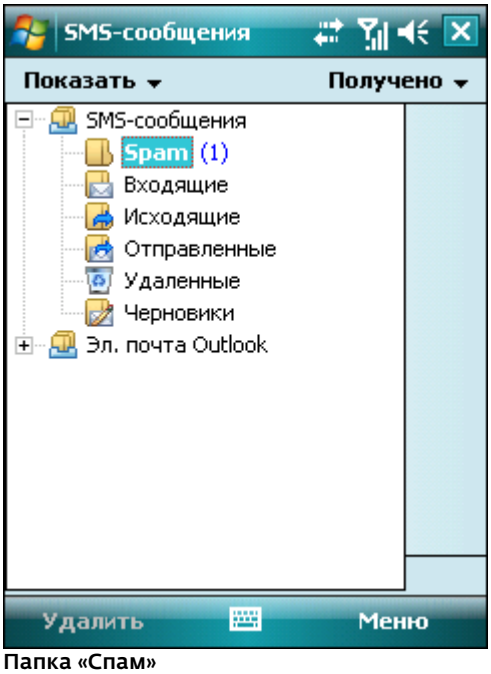
Чтобы добавить номер в белый или черный список, откройте соответствующую вкладку и выберите команду **«Меню» > «Добавить»**. Чтобы добавить номер из адресной книги, выберите команду **«Меню» > «Добавить контакт»**.

Предупреждение. Добавление номера или контакта в черный список приведет к автоматическому перемещению сообщений этого отправителя в папку **«Спам»**.

10.3 Расположение сообщений со спамом

Заблокированные сообщения, квалифицированные как спам в соответствии с настройками модуля антиспама, хранятся в папке **«Спам»**. Это папка автоматически создается при получении первого сообщения со спамом. Чтобы найти папку **«Спам»** и просмотреть заблокированные сообщения, выполните указанные ниже действия.

1. С помощью меню **«Пуск»** откройте используемую на устройстве программу для обмена сообщениями (например, **«Сообщения»**).
2. Выберите пункт **«Текстовые сообщения»** (или **«MMS»**, если нужно найти папку нежелательных MMS-сообщений).
3. Выберите команду **«Меню» > «Перейти к» > «Папки»** (или **«Меню» > «Папки»** на смартфонах).
4. Выберите папку **«Спам»**.

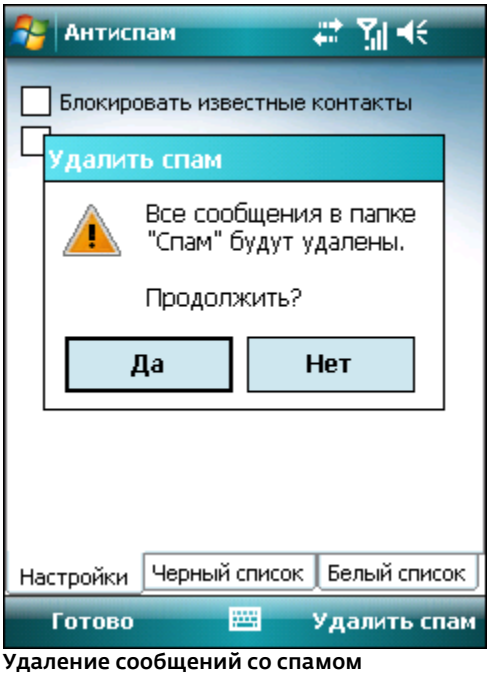


Папка «Спам»

10.4 Удаление сообщений со спамом

Чтобы удалить сообщения со спамом с мобильного устройства, выполните указанные ниже действия.

1. В главном окне приложения ESET Mobile Security выберите пункт **«Меню» > «Настройки» > «Антиспам»**.
2. Выберите команду **«Удалить спам»**.,
3. Нажмите кнопку **«Да»**, чтобы подтвердить удаление всех сообщений со спамом.



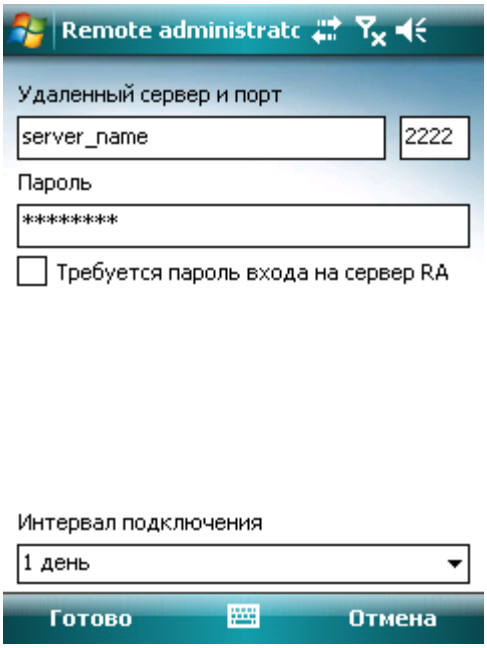
Удаление сообщений со спамом

11. Удаленное администрирование

Средство ESET Remote Administrator (ERA) позволяет централизованно управлять ESET Mobile Security в сетевой среде. С сервера ERA Server можно проверять устройство, устанавливать обновления, проверять файлы журналов, отправлять сообщения и т. д. Приложение ESET Mobile Security Business Edition совместимо со средством ESET Remote Administrator 4.

11.1 Настройки

Для доступа к параметрам средства удаленного администрирования выберите команду **«Меню» > «Настройки» > «Удаленное администрирование»**.



Параметры удаленного администрирования

Введите имя удаленного сервера в поле **«Удаленный сервер и порт»**. В поле «Порт» отображается предопределенный номер порта, используемого для подключения к серверу по сети. Рекомендуется не изменять порт по умолчанию (2222).

Если для ESET Remote Administrator нужна проверка подлинности с помощью пароля, установите флажок **«Требуется пароль для входа на сервер ERA»** и введите пароль в соответствующее поле.

Параметр **«Интервал подключения»** позволяет указать, как часто ESET Mobile Security будет подключаться к серверу ERA Server для отправки данных. Минимальный интервал подключения составляет 1 час. Если нужно подключиться к серверу ERA Server немедленно, выберите команду **«Действие» > «Подключиться к ERA»** в главном окне ESET Mobile Security.

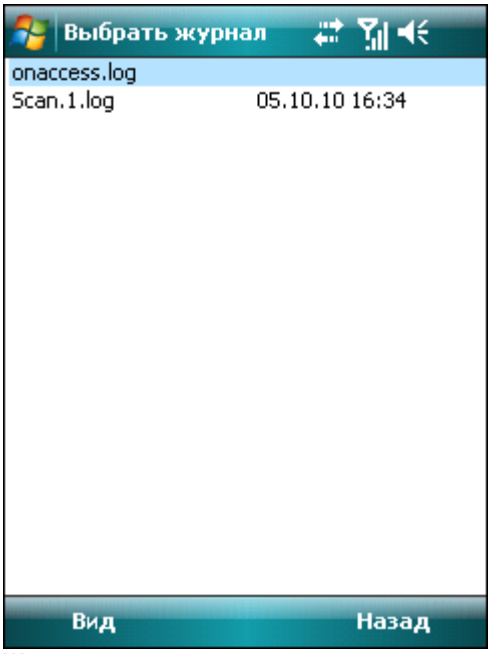
ПРИМЕЧАНИЕ. Для получения дополнительных сведений об управлении сетью с помощью ESET Remote Administrator см. документ «ESET Remote Administrator. Инструкция по установке и руководство пользователя».

12. Просмотр журналов и статистики

Раздел **«Журнал проверки»** (**«Меню» > «Журналы» > «Проверка»**) содержит подробную информацию о выполненных задачах сканирования. Журналы создаются после каждого сканирования по требованию или при обнаружении заражения во время сканирования при доступе. Все зараженные файлы выделяются красным цветом. В конце каждой записи журнала выводится разъяснение, почему файл был включен в журнал.

Журналы **сканирования** содержат следующие данные:

- имя файла журнала (как правило, в формате *Scan. номер.log*);
- дата и время события;
- список проверенных файлов;
- действия, выполненные в ходе сканирования, и возникшие ошибки.



Журнал сканирования

Раздел **«Журнал аудита безопасности»** (**«Меню» > «Журналы» > «Аудит безопасности»**) содержит результаты автоматического (запланированного) аудита и аудита, запущенного вручную.

Журналы **«Аудит безопасности»** содержат следующие сведения:

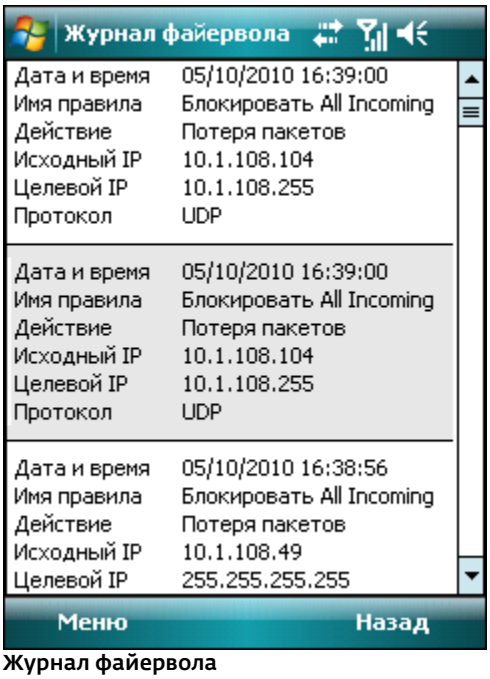
- имя файла журнала (в формате *аудитНомер.log*);
- дата и время аудита;
- подробные результаты.

Журнал аудита безопасности

Раздел **«Журнал файервола»** (**«Меню» > «Журналы» > «Файервол»**) содержит информацию о событиях файервола, заблокированных приложением ESET Mobile Security. Журнал обновляется после каждого сеанса обмена данными через файервол. Новые события отображаются в верхней части журнала.

Журнал файервола содержит следующие сведения:

- дата и время события;
- имя использованного правила;
- действие, выполненное в соответствии с правилом;
- IP-адрес источника;
- IP-адрес назначения;
- использованный протокол.



Журнал файервола

Экран **«Статистика»** (**«Меню» > «Вид» > «Статистика»**) содержит следующую сводную информацию:

- файлы, проверенные модулем сканирования при доступе;
- полученные и заблокированные сообщения;
- файлы, помещенные на карантин;
- данные, полученные и отправленные через файервол.

Чтобы сбросить текущую статистику, выберите команду **«Вид» > «Сбросить счетчики»**.

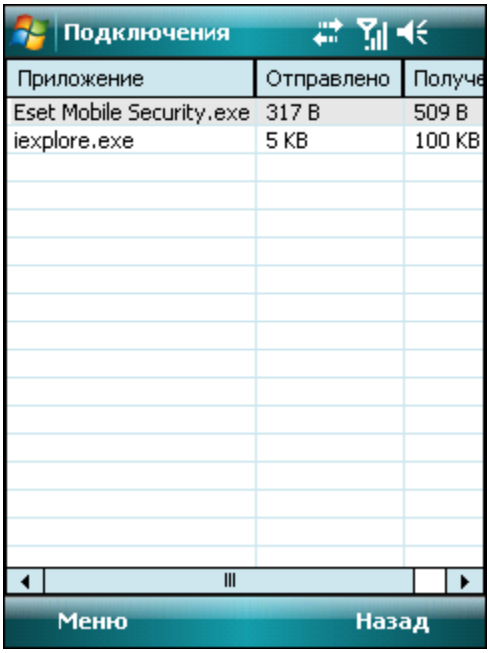
ПРИМЕЧАНИЕ. Статистические данные собираются, начиная с момента последнего перезапуска устройства.

Статистика

Раздел **«Подключения»** (**«Меню» > «Вид» > «Подключения»**) содержит информацию о приложениях, используемых для отправки и получения данных.

Она включает:

- имя процесса;
- объем отправленных данных;
- объем полученных данных.



Подключения

13. Устранение неполадок и поддержка

13.1 Устранение неполадок

В этом разделе приведены ответы на часто задаваемые вопросы о приложении ESET Mobile Security.

13.1.1 Установка завершилась неудачей

Самой распространенной причиной вывода сообщения об ошибке при установке является то, что на устройстве установлена неправильная версия приложения ESET Mobile Security. При загрузке файла установки с *веб-сайта компании ESET* убедитесь, что выбрана версия, подходящая для вашего устройства.

13.1.2 Сбой обновления

Это сообщение об ошибке появляется после неудачной попытки обновления, если программе не удалось подключиться к серверу обновлений.

Выполните действия, описанные ниже.

1. Проверьте подключение к Интернету, для чего попробуйте открыть веб-сайт *http://www.eset.com* в своем веб-браузере.
2. Убедитесь, что программа использует правильный сервер обновлений: выберите команду **«Меню» > «Настройки» > «Обновление»** и проверьте поле **«Сервер обновлений»**. В нем должен быть указан адрес *updmobile.eset.com*.

13.1.3 Истекло время ожидания при загрузке файла

Во время обновления неожиданно снизилась скорость подключения к Интернету или подключение было разорвано. Попробуйте выполнить обновление позже.

13.1.4 Файл обновления отсутствует

При установке новой базы данных сигнатур вирусов из файла обновления (*esetav_wm.upd*) он должен находиться в установочной папке ESET Mobile Security (*\Program Files\ESET\ESET Mobile Security*).

13.1.5 Файл базы данных поврежден

Файл обновления базы данных сигнатур вирусов (*esetav_wm.upd*) поврежден. Необходимо заменить файл и снова запустить обновление.

13.2 Техническая поддержка

По административным и техническим вопросам, связанным с ESET Mobile Security или другими продуктами безопасности ESET, обращайтесь к специалистам нашей службы технической поддержки. Для поиска решения технической проблемы используйте один из способов, описанных ниже.

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, разбитой на категории и дополненной эффективными средствами поиска.

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