Dr.WEB

Light для Android

Руководство пользователя

Dr.Web Light для Android
Версия 11.2
Руководство пользователя
04.07.2018

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

«Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности.

«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение

Dr.Web Light защищает мобильные устройства, работающие под управлением операционной системы Android™ от вирусных угроз, созданных специально для этих устройств.

В приложении применены разработки и технологии «Доктор Веб» по обнаружению и обезвреживанию вредоносных объектов, которые представляют угрозу информационной безопасности устройства и могут повлиять на его работу.

Dr.Web Light использует технологию Origins Tracing™ for Android, которая находит вредоносные программы для платформы Android. Эта технология позволяет определять новые семейства вирусов на основе базы знаний об уже найденных и изученных угрозах. Origins Tracing for Android способна распознавать как перекомпилированные вирусы, такие как Android.SmsSend, Spy, так и приложения, зараженные Android.ADRD, Android.Geinimi, Android.DreamExploid. Названия угроз, обнаруженных при помощи Origins Tracing for Android, имеют вид «Android.*VirusName*.origin».

О руководстве

Руководство призвано помочь пользователям устройств под управлением ОС Android установить и настроить приложение, а также ознакомиться с его основными функциями.

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`Internal storage\Android\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

1.1. Функции Dr.Web

Dr.Web Light выполняет следующие функции:

- Защищает файловую систему устройства в режиме реального времени (проверяет сохраняемые файлы, устанавливаемые приложения и т.д.).
- Проверяет все файлы в памяти или отдельные файлы и папки по запросу пользователя.
- Проверяет архивы.
- Проверяет SD-карту или другой съемный носитель.
- Находит угрозы в файлах LNK, которые Dr.Web определяет как Exploit.CplInk.
- Удаляет обнаруженные угрозы безопасности или перемещает их в карантин.
- Разблокирует устройство, если его заблокировала программа-вымогатель.
- Регулярно обновляет вирусные базы Dr.Web через Интернет.
- Ведет статистику обнаруженных угроз и действий приложения, а также журнал событий.
- Находит и помогает устранить проблемы безопасности и уязвимости.

Dr.Web Light поддерживает работу в режиме Multi-Window, позволяющем запуск нескольких приложений в отдельных окнах. Работа в данном режиме возможна только на устройствах Samsung Galaxy S III и выше, Samsung Galaxy Note 2 и выше.

2. Системные требования

Перед установкой проверьте, что ваше устройство соответствует следующим требованиям и рекомендациям:

- Операционная система Android версии 4.4/5.0/5.1/6.0/7.0/7.1/8.0/8.1.
- Для загрузки обновлений вирусных баз требуется интернет-соединение.

На устройствах с кастомными прошивками или открытым root-доступом (так называемых рутованных устройствах) корректная работа Dr.Web Light не гарантируется.

По умолчанию установка приложения осуществляется во внутреннюю память устройства. Для корректной работы Dr.Web Light не следует переносить установленное приложение на съемные носители.

3. Установка Dr.Web

Установка из Google Play

Чтобы установить Dr.Web из Google Play, убедитесь, что:

- У вас есть учетная запись Google.
- Ваше устройство привязано к учетной записи Google.
- На устройстве есть доступ к Интернету.
- Устройство удовлетворяет системным требованиям.

Чтобы установить приложение, выполните следующие действия:

1. Откройте Google Play на устройстве, найдите в списке приложений Dr.Web Light и нажмите кнопку **Установить**.

   

   Если Dr.Web Light не отображается в Google Play, значит ваше устройство не удовлетворяет системным требованиям.

2. Далее откроется экран с информацией о функциях устройства, к которым требуется доступ для работы приложения.

   Ознакомьтесь со списком необходимых разрешений и нажмите **Принять**.

3. Для начала работы с приложением нажмите кнопку **Открыть**.

4. Обновление и удаление Dr.Web

Обновление Dr.Web

Если для приложений из Google Play не настроено автоматическое обновление, вы можете запустить обновление вручную:

1. Запустите приложение **Play Маркет** и выберите пункт **Мои приложения и игры**.
2. В списке установленных приложений найдите Dr.Web Light и нажмите **Обновить**.

   Кнопка **Обновить** доступна, если новая версия приложения уже вышла.

3. При обновлении приложению могут потребоваться новые разрешения. В этом случае откроется окно для подтверждения.

   Нажмите кнопку **Принять**, чтобы разрешить доступ к необходимым для приложения функциям устройства.

   Для начала работы с приложением нажмите кнопку **Открыть**.

Удаление Dr.Web

Чтобы удалить Dr.Web:

1. В настройках устройства выберите **Приложения** или **Диспетчер приложений**.
2. В списке установленных приложений выберите **Dr.Web Light** и нажмите **Удалить**.

Карантин и сохраненный журнал событий приложения не удаляются по умолчанию. Вы можете удалить их вручную из папки **Android/data/com.drweb/files** во внутренней памяти устройства.

5. Приступая к работе

После установки Dr.Web Light вы можете ознакомиться с интерфейсом и главным меню приложения, настроить панель уведомлений и установить виджет Dr.Web на главном экране устройства.

5.1. Лицензионное соглашение

При первом запуске приложения откроется Лицензионное соглашение, которое необходимо принять для дальнейшей работы.

В этом же экране вам предлагается принять положение об отправке статистики работы приложения и найденных угроз на серверы компании «Доктор Веб», а также на серверы Google и Яндекс. Возможность отказа от отправки статистики существует в расширенной версии Dr.Web.

5.2. Разрешения

Начиная с версии 6.0, в ОС Android появилась возможность разрешать или запрещать приложениям доступ к функциям устройства и личным данным пользователя.

После установки и принятия Лицензионного соглашения откроется окно, в котором Dr.Web Light попросит предоставить приложению доступ к данным на устройстве. Если вы не предоставите приложению необходимые разрешения, оно не сможет работать.

Dr.Web Light запрашивает доступ к фото, мультимедиа, и файлам на устройстве при первом запуске приложения. Это разрешение необходимо для работы приложения.

Если вы отклоните запрос на предоставление доступа, вам будет предложено перейти на экран настроек:

1. Нажмите **Перейти в Настройки** и выберите раздел **Разрешения**.
2. Разрешите приложению доступ к необходимым функциям и данным, переместив переключатель вправо.

Просмотр списка необходимых разрешений

1. Откройте настройки устройства  .
2. Нажмите **Приложения** или **Диспетчер приложений**.
3. Найдите в списке установленных приложений Dr.Web Light и нажмите на него.
4. На экране **О приложении** выберите пункт **Разрешения**.
5. В меню, расположенном в верхнем правом углу, выберите **Все разрешения**.

5.3. Интерфейс

Главный экран

На главном экране (см. Рисунок 1) располагается список основных компонентов Dr.Web, а также информация о полной версии приложения.

Меню в правом верхнем углу главного экрана позволяет:

- Выполнить обновление вирусных баз.
- Перейти к настройкам приложения.
- Открыть справку.
- Открыть экран с информацией о приложении.

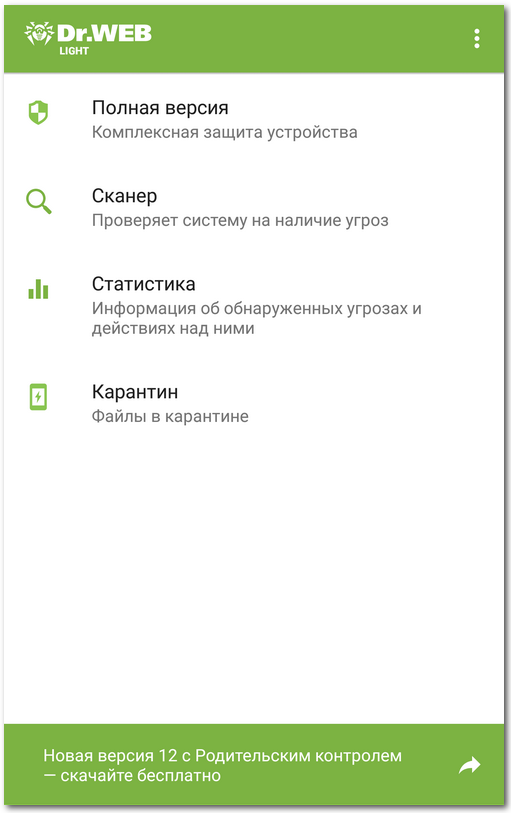

Рисунок 1. Главный экран приложения

Панель состояния

В верхней части главного экрана приложения находится панель состояния с индикатором, который отображает текущее состояние защиты устройства (см. Рисунок 2).

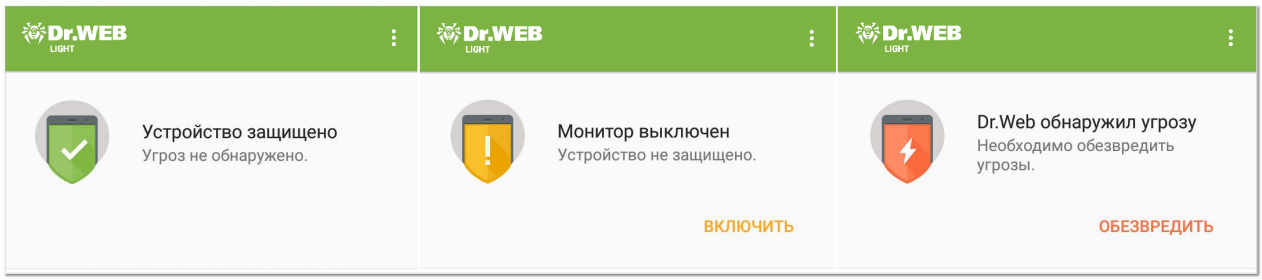

Рисунок 2. Панель состояния

- Индикатор зеленого цвета означает, что устройство защищено. Дополнительных действий не требуется.
- Индикатор желтого цвета означает, что Dr.Web обнаружил проблемы безопасности.
- Индикатор красного цвета означает, что Dr.Web обнаружил угрозы.

Нажмите на предложенное действие на панели, чтобы повысить защиту устройства и обезвредить угрозы.

5.4. Панель уведомлений

Панель уведомлений Dr.Web (см. Рисунок 3) используется для быстрого доступа к основным функциям приложения. Кроме того, она оперативно отображает предупреждения о найденных угрозах.

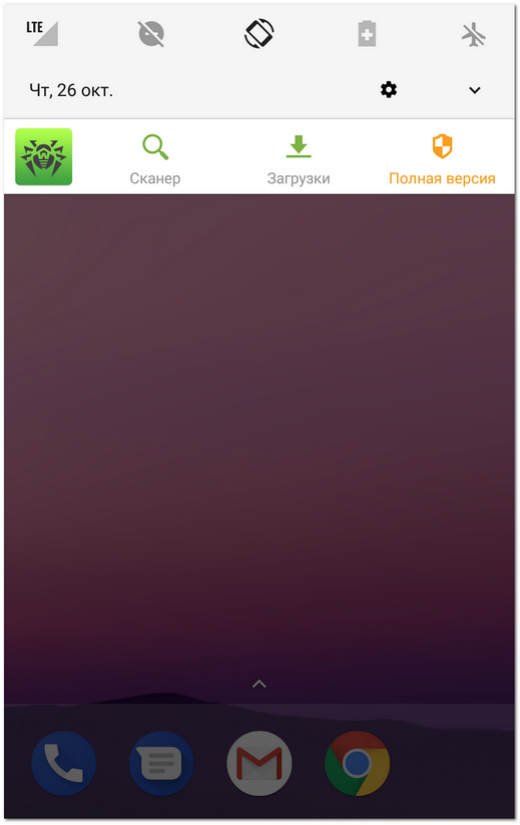

Рисунок 3. Панель уведомлений

Панель уведомлений Dr.Web можно включить или отключить с помощью опции **Панель уведомлений** на экране **Общие настройки**.

> На устройствах с Android 6.0 или более поздними версиями, если опция **Панель уведомлений** отключена, компонент SpIDer Guard не показывает всплывающие уведомления о проверке файлов. Подробнее см. в разделе Общие настройки.

Если Dr.Web обнаружит угрозы, на панели уведомлений появится значок  .

С помощью панели уведомлений можно выполнить следующие действия:

- Перейти на экран Dr.Web Light. Для этого нажмите на значок Dr.Web.
- Запустить быструю, полную или выборочную проверку с помощью опции **Сканер**.
- Запустить проверку объектов, загруженных на устройство, выбрав опцию **Загрузки**.
- Ознакомиться с информацией о приложении Dr.Web Security Space для Android и загрузить его на бесплатный период 14 дней.

5.5. Виджет

Для удобства работы с Dr.Web Light вы можете добавить на главный экран вашего устройства специальный виджет, позволяющий включать и отключать постоянную антивирусную защиту SpIDer Guard.

Добавление виджета Dr.Web

Добавление виджета осуществляется стандартным способом операционной системы:

1. Откройте список виджетов, доступных на вашем устройстве.
2. В списке выберите виджет **Dr.Web 1×1 (маленький)**.

Он показывает текущее состояние защиты и позволяет включить или отключить SpIDer Guard (см. Рисунок 4).

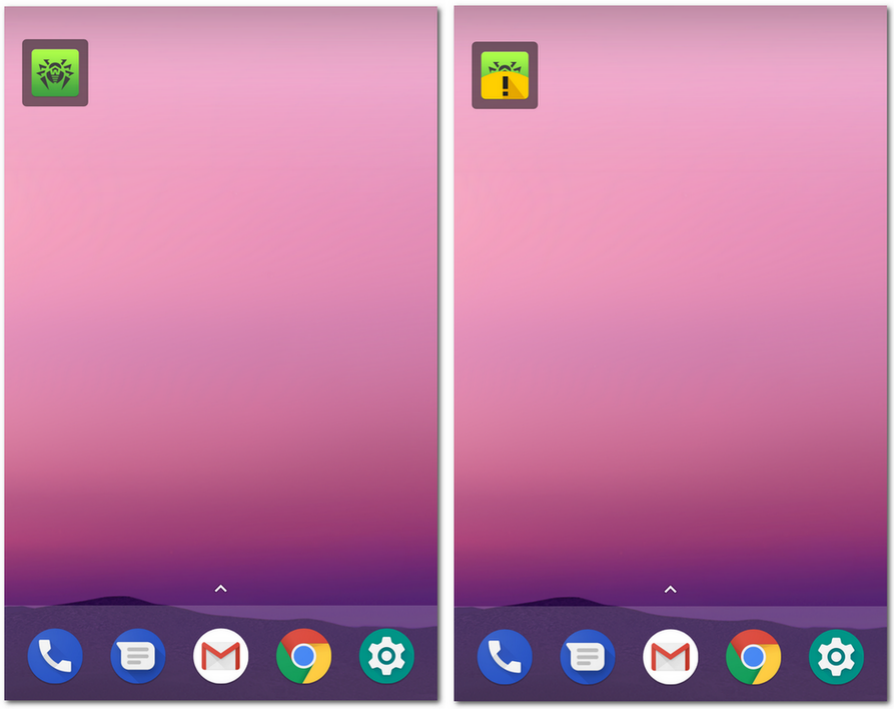

Рисунок 4. Виджет Dr.Web

6. Компоненты Dr.Web

На главном экране приложения находится список компонентов и их текущее состояние (включен или отключен). В состав Dr.Web входят следующие компоненты:

- **Полная версия**. Позволяет ознакомиться с информацией об антивирусе Dr.Web Security Space и загрузить его из Google Play.
- Сканер. Проверяет систему по запросу пользователя. Возможны 3 типа проверки: быстрая, полная, выборочная.
- Статистика. Позволяет просмотреть статистику обнаруженных угроз и действий приложения над ними.
- Карантин. Позволяет просмотреть и обработать угрозы, перемещенные в карантин.

6.1. Антивирусная защита

Компонент SpIDer Guard проверяет файловую систему в режиме реального времени.

Компонент Сканер Dr.Web позволяет запустить сканирование вручную в любой момент.

Если любой из компонентов обнаружит угрозу на устройстве, вы сможете выбрать действие для ее обезвреживания.

6.1.1. SpIDer Guard: постоянная антивирусная защита

Включение постоянной защиты

При первом запуске Dr.Web Light постоянная защита автоматически включается после принятия Лицензионного соглашения. Чтобы отключить или снова включить SpIDer Guard, выберите **SpIDer Guard** на экране Настройки.

SpIDer Guard работает независимо от того, запущено приложение или нет.

При обнаружении угроз безопасности на панели уведомлений в верхней части экрана появится предупреждающий значок  (для Android 5.0 и ниже – ) и всплывающее уведомление о найденных угрозах. С панели уведомлений вы можете открыть список угроз для применения к ним действий по обезвреживанию.

Работа SpIDer Guard будет остановлена в случае полной очистки внутренней памяти вашего устройства с помощью встроенного Диспетчера задач. В этом случае для восстановления постоянной антивирусной защиты требуется заново открыть Dr.Web Light.

Настройки SpIDer Guard

Чтобы открыть настройки SpIDer Guard:

1. На главном экране нажмите **Меню** и выберите пункт **Настройки**.
2. На экране **Настройки** нажмите **SpIDer Guard**.

- Чтобы включить проверку файлов в архивах, установите флажок **Файлы в архивах**.

> По умолчанию проверка архивов отключена. Включение проверки архивов может сказаться на быстродействии системы и увеличить расход заряда батареи. При этом, отключение проверки архивов не сказывается на уровне защиты, поскольку SpIDer Guard проверяет установочные файлы APK, независимо от установленного значения параметра **Файлы в архивах**.

- Чтобы включить проверку встроенной SD-карты и съемных носителей при каждом подключении, установите флажок **Встроенная SD-карта и съемные носители**. Если эта настройка включена, проверка запускается при каждом включении компонента SpIDer Guard.
- Чтобы включить/отключить проверку системы на наличие рекламных программ и потенциально опасных программ (в том числе, программ взлома и программ-шуток), выберите пункт **Дополнительные опции** и установите/снимите флажки **Рекламные программы** и **Потенциально опасные программы** соответственно.

Статистика

Приложение регистрирует события, связанные с работой SpIDer Guard (включение/отключение, результаты проверки памяти устройства, устанавливаемых приложений, обнаружение угроз безопасности).

Действия приложения отображаются в разделе **Действия** на вкладке **Статистика**, отсортированные по дате (см. раздел Статистика).

Проверка работы SpIDer Guard

Вы можете проверить работоспособность SpIDer Guard с помощью тестового файла EICAR. Этот файл обычно используется, чтобы:

- Проверить правильность установки антивируса.
- Продемонстрировать поведение антивируса при вирусной угрозе.
- Проверить корпоративный регламент при обнаружении угрозы.

Файл не является вирусом и не содержит фрагментов вирусного кода, поэтому совершенно безопасен для вашего устройства. Файл определяется Dr.Web как «EICAR Test File (NOT a Virus!)».

Вы можете скачать файл из Интернета или создать файл самостоятельно:

1. В любом текстовом редакторе создайте новый файл, состоящий из одной строки:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

2. Сохраните файл с расширением .com.

Как только вы сохраните файл EICAR на вашем устройстве, вы сразу же услышите характерный звук и увидите предупреждающее сообщение от SpIDer Guard: «Обнаружена угроза! EICAR Test File (NOT a Virus!)». Кроме того, появится индикатор красного цвета на панели состояния в верхней части главного экрана, и на панели уведомлений Dr.Web появится значок  (см. Рисунок 5).

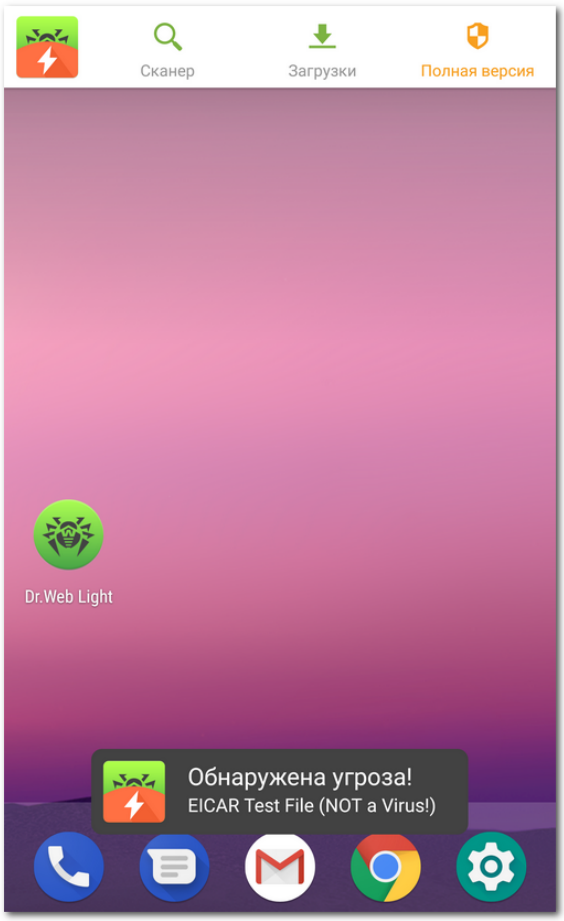

Рисунок 5. Обнаружение тестового файла EICAR

6.1.2. Сканер Dr.Web: проверка по запросу пользователя

Проверка системы по запросу пользователя осуществляется компонентом Сканер Dr.Web. Он позволяет производить быстрое или полное сканирование файловой системы, а также проверять отдельные файлы и папки.

Рекомендуется периодически сканировать файловую систему, если компонент SpIDer Guard какое-то время был неактивен. Обычно при этом достаточно проводить быструю проверку системы.

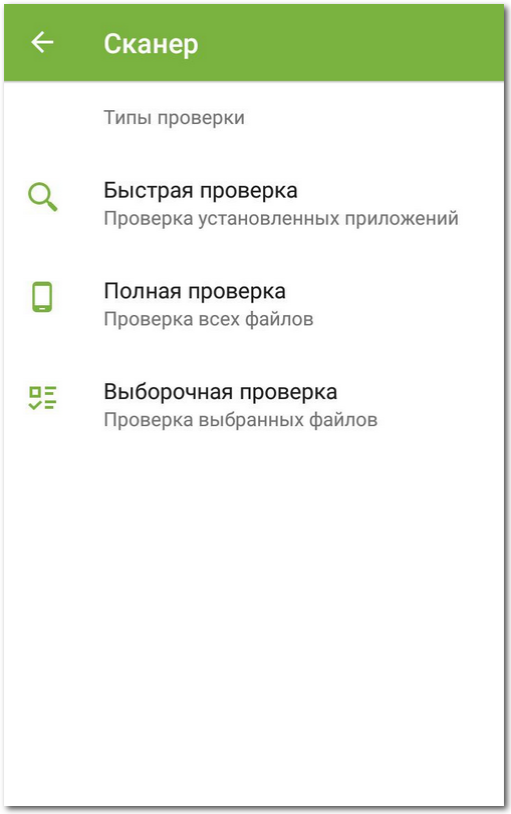

Рисунок 6. Сканер Dr.Web

Проверка

Чтобы проверить систему, на главном экране Dr. Web выберите пункт **Сканер**, затем на экране **Сканер** (см. Рисунок 6) выполните одно из следующих действий:

- Чтобы запустить сканирование только установленных приложений, выберите пункт **Быстрая проверка**.
- Чтобы запустить сканирование всех файлов, выберите пункт **Полная проверка**.
- Чтобы проверить отдельные файлы и папки, выберите пункт **Выборочная проверка**, затем выберите необходимые объекты в появившемся списке объектов файловой системы (см. Рисунок 7). Чтобы выбрать все объекты, установите флажок в правом верхнем углу экрана. Затем нажмите **Проверить**.

Если в ходе проверки Сканер Dr.Web обнаружил угрозы, внизу экрана сканирования появится значок . Нажмите на него, чтобы перейти к списку обнаруженных угроз и обезвредить их. Если вы закрыли экран сканирования или закрыли приложение, вы можете перейти к списку найденных угроз, нажав на значок на панели уведомлений.

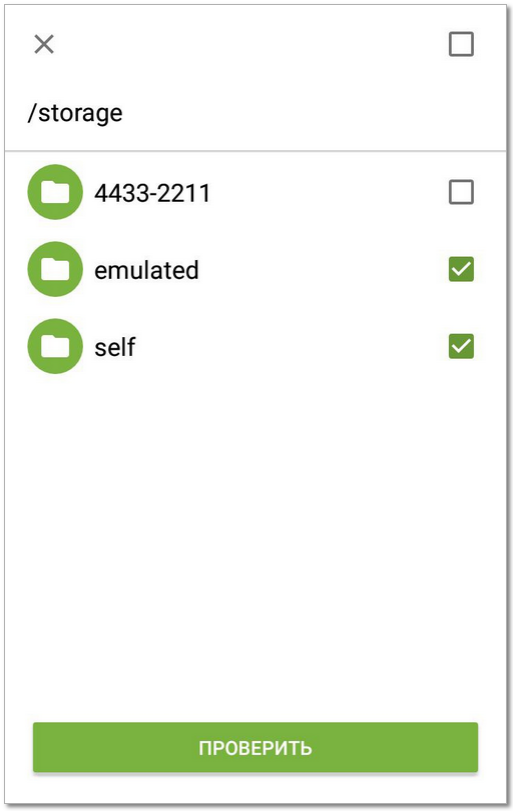

Рисунок 7. Выборочная проверка

Отправка подозрительных файлов в антивирусную лабораторию «Доктор Веб»

Вы можете отправить в антивирусную лабораторию «Доктор Веб» подозрительные ZIP-архивы (файлы с расширением .jar, .apk), предположительно содержащие вирусы, файлы с расширением .odex, .dex, .so, или заведомо чистые ZIP-архивы, которые вызывают так называемое ложное срабатывание:

1. Нажмите и удерживайте файл в списке объектов файловой системы (см. Рисунок 7), затем нажмите кнопку **Отправить в лабораторию**.
2. На следующем экране введите адрес вашей электронной почты, если вы хотите получить результаты анализа отправленного файла.
3. Выберите одну из категорий для вашего запроса:
   - **Подозрение на вирус**, если вы считаете, что файл представляет угрозу.
   - **Ложное срабатывание** или **Ложное срабатывание Origins Tracing**, если вы считаете, что файл был ошибочно отнесен к угрозам.

   Выбор одной из представленных категорий в случае ложного срабатывания осуществляется на основании имени угрозы, предположительно содержащейся в отправляемом файле: если в названии присутствует постфикс «.origin», следует выбирать категорию **Ложное срабатывание Origins Tracing**, в остальных случаях – категорию **Ложное срабатывание**.
4. Нажмите кнопку **Отправить**.

В антивирусную лабораторию «Доктор Веб» могут быть отправлены файлы, размер которых не превышает 50 МБ.

Настройки Сканера Dr.Web

Для доступа к настройкам Сканера Dr.Web перейдите на экран Настройки и выберите пункт **Сканер**.

- Чтобы включить проверку файлов в архивах, установите флажок **Файлы в архивах** в разделе **Сканер**.

  По умолчанию проверка архивов отключена. Включение проверки архивов может сказаться на быстродействии системы и увеличить расход заряда батареи. При этом, отключение проверки архивов не сказывается на уровне защиты, поскольку Сканер Dr.Web проверяет установочные файлы APK, независимо от установленного значения параметра **Файлы в архивах**.

- Чтобы включить/отключить проверку системы на наличие рекламных программ и потенциально опасных программ (в том числе, программ взлома и программ-шуток), выберите пункт **Дополнительные опции** в разделе **Сканер** и установите/снимите флажки **Рекламные программы** и **Потенциально опасные программы** соответственно.

Статистика

Приложение регистрирует события, связанные с работой Сканера Dr.Web (тип и результаты проверки, обнаружение угроз безопасности). Действия приложения отображаются в разделе **Действия** на вкладке **Статистика**, отсортированные по дате (см. раздел Статистика).

6.1.3. Обезвреживание угроз

Просмотр списка угроз

В случае обнаружения угроз безопасности компонентом SplDer Guard в строке состояния в верхней части экрана появляется предупреждающий значок (для Android 5.0 и ниже –) и сообщение о найденных угрозах.

Если угрозы были обнаружены Сканером Dr.Web в ходе запущенной вами проверки, внизу экрана сканирования появится значок . Нажмите на него, чтобы перейти к списку обнаруженных угроз и обезвредить их.

С панели уведомлений вы также можете открыть список угроз и обезвредить их.

Для каждой угрозы в списке показывается:

- Имя угрозы.
- Путь к файлу, содержащему угрозу.

Для найденных угроз, не являющихся вирусами, в скобках указывается тип: рекламная программа, потенциально опасная программа, программа-шутка или программа взлома.

На Android 5.0 и выше при обнаружении угрозы панель уведомлений будет отображаться поверх всех приложений до тех пор, пока к угрозе не будет применено какое-либо действие или пока вы не смахнете уведомление об угрозе с панели уведомлений. Кроме того, на Android 5.0 и выше уведомление об угрозе также появится на экране блокировки устройства, откуда вы можете перейти к списку обнаруженных угроз.

Применение действий к угрозам

Выберите угрозу в списке и примените к ней одно из доступных действий:

- **Удалить**, чтобы полностью удалить угрозу из памяти устройства.
- **В карантин**, чтобы переместить угрозу в специальную папку, где она изолируется от остальной системы.

Если угроза была обнаружена в установленном приложении, то перемещение в карантин для нее невозможно. В этом случае действие **В карантин** в списке будет отсутствовать.

- **Игнорировать**, чтобы временно оставить угрозу нетронутой.
- **Сообщить о ложном срабатывании**, чтобы отправить угрозу в антивирусную лабораторию «Доктор Веб» с сообщением о том, что она не представляет опасности и была ошибочно отнесена антивирусом к подозрительным объектам. Чтобы получить результаты анализа отправленного файла, укажите адрес своей электронной почты в соответствующем поле и нажмите кнопку **Отправить**.

Действие **Сообщить о ложном срабатывании** доступно для модификаций угроз с постфиксом «.origin» и для угроз, обнаруженных в системной области устройства.

6.1.4. Обнаружение угроз в системных приложениях

Приложения, установленные в системной области, в некоторых случаях могут выполнять функции, характерные для вредоносных программ, поэтому при проверке системы Dr.Web Light может определить такие приложения как угрозы. Если данные приложения были установлены производителем устройства, стандартные действия по

обезвреживанию угроз для них неприменимы, но вы можете воспользоваться следующими рекомендациями:

Если системные приложения, определенные как угрозы, не были установлены производителем устройства, стандартные действия по обезвреживанию угроз применимы к ним только в полной версии антивируса при условии, что на устройстве открыт root-доступ.

- Остановите работу приложения через настройки устройства: в списке установленных приложений на экране **Настройки** - > **Приложения** выберите приложение, определенное как угроза, после чего на экране с информацией о нем нажмите кнопку **Остановить**.

Это действие потребуется повторять при каждой перезагрузке устройства.

- Отключите приложение через настройки устройства: в списке установленных приложений на экране **Настройки** - > **Приложения** выберите приложение, определенное как угроза, после чего на экране с информацией о нем нажмите кнопку **Отключить**.
- Если на вашем устройстве установлена пользовательская прошивка, вы можете вернуться к официальному ПО производителя устройства самостоятельно или обратившись в сервисный центр.
- Если вы используете официальное ПО производителя устройства, попробуйте обратиться в компанию-производитель за дополнительной информацией об этом приложении.
- Если на вашем устройстве открыт root-доступ, вы можете попробовать удалить такие приложения с помощью специальных утилит.

Чтобы отключить информирование об обнаружении угроз в известных системных приложениях, установите флажок **Системные приложения** в разделе **Настройки** - > **Общие настройки** - > **Дополнительные опции**.

6.1.5. Обработка приложений-блокировщиков устройства

Dr.Web Light позволяет защитить мобильное устройство от получивших широкое распространение программ-вымогателей для мобильной платформы Android. Такие программы чрезвычайно опасны. Они могут шифровать файлы, хранящиеся во встроенной памяти устройства или на съемных носителях (таких как SD-карта). Эти программы могут блокировать экран и выводить на него сообщения с требованием выкупа за расшифровку файлов и разблокировку устройства.

От действий программ-вымогателей могут пострадать ваши фотографии, видео и документы. Кроме того, они похищают и передают на серверы злоумышленников различную информацию об инфицированном устройстве (в том числе, идентификатор

IMEI), данные из адресной книги (имена контактов, номера телефонов и адреса электронной почты), отслеживают входящие и исходящие вызовы и могут их блокировать. Вся собранная информация, в том числе о телефонных звонках, также передается на управляющий сервер.

Вредоносные программы-вымогатели распознаются и удаляются Dr.Web Light при попытке проникновения на защищаемое устройство. Однако их количество и разнообразие постоянно растет. Поэтому, особенно если вирусные базы Dr.Web не обновлялись в течение некоторого времени и не содержат информации о новых экземплярах, приложение-блокировщик может оказаться установленным на устройстве.

Если мобильное устройство заблокировано программой-вымогателем и на нем включен SpIDer Guard, вы можете разблокировать устройство с помощью следующих манипуляций:

1. В течение 5 секунд подключите и отключите зарядное устройство.
2. В течение следующих 10 секунд подключите наушники.
3. В течение следующих 5 секунд отключите наушники.
4. В течение следующих 10 секунд энергично встряхните мобильное устройство.
5. Dr.Web Light завершит все активные процессы на устройстве, включая процесс, запущенный приложением-блокировщиком, после чего включится короткий вибросигнал (на устройствах, обладающих данной функцией). Далее откроется экран Dr.Web Light.

   

   Обратите внимание, что при завершении активных процессов могут быть потеряны данные других приложений, активных на момент блокировки устройства.

6. После разблокировки устройства рекомендуется обновить вирусные базы Dr.Web и выполнить быструю проверку системы, или же удалить вредоносное приложение.

6.2. Статистика

В Dr.Web Light реализовано ведение статистики обнаруженных угроз и действий приложения.

Для просмотра статистики работы приложения выберите пункт **Статистика** на главном экране приложения.

Просмотр статистики

На вкладке **Статистика** находятся два информационных раздела (см. Рисунок 8):

- **Всего**. Содержит информацию об общем количестве проверенных файлов, обнаруженных и обезвреженных угроз.

- **Действия**. Содержит информацию о результатах проверки Сканером Dr.Web, включении/отключении компонента SpIDer Guard, обнаруженных угрозах и действиях по их обезвреживанию.

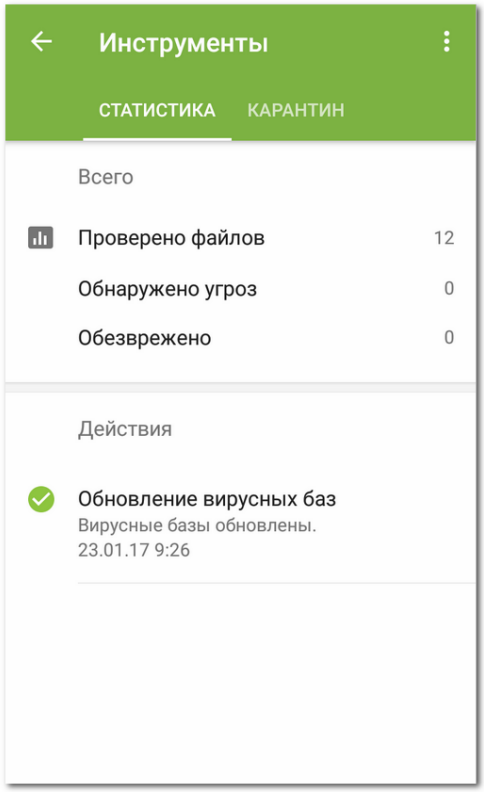

Рисунок 8. Статистика

Очистка статистики

Чтобы удалить всю собранную статистику работы приложения, на вкладке **Статистика** нажмите **Меню** и выберите пункт **Очистить статистику**.

Сохранение журнала событий

Вы можете сохранить журнал событий приложения для анализа в случае возникновения проблем при работе с приложением.

1. На вкладке **Статистика** нажмите **Меню** и выберите **Сохранить журнал**.
2. Журнал сохраняется в файлах **DrWeb_Log.txt** и **DrWeb_Err.txt**, расположенных в папке **Android/data/com.drweb/files** во внутренней памяти устройства.

6.3. Карантин

Для обнаруженных угроз в Dr.Web Light реализована функция перемещения в карантин – особую папку, предназначенную для их изоляции и безопасного хранения (см. Рисунок 9).

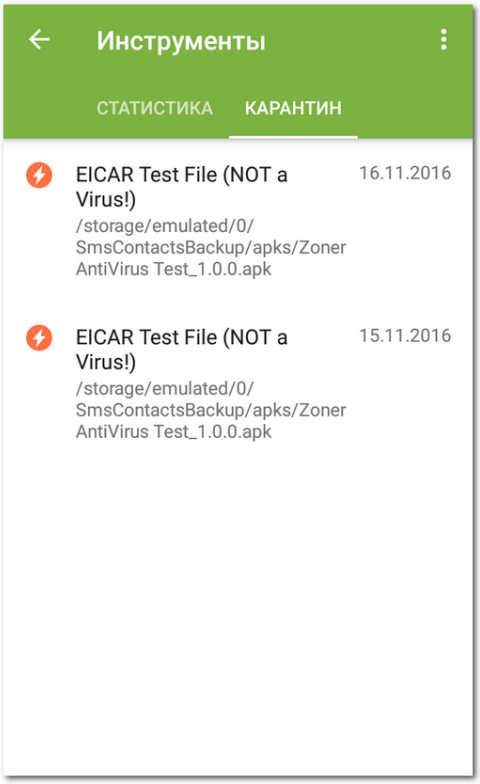

Рисунок 9. Карантин

Просмотр списка объектов в карантине

Чтобы просмотреть список угроз, перемещенных в карантин, выберите пункт Карантин на главном экране приложения.

Просмотр информации об угрозах

Чтобы посмотреть информацию об угрозе, нажмите на нее в списке.

Для каждой угрозы вы можете просмотреть следующую информацию:

- Имя файла.
- Путь к файлу.
- Дата и время перемещения в карантин.

Действия над объектами в карантине

Для каждой угрозы доступны следующие действия:

- **Подробнее в интернете** – для просмотра более подробной информации о подобном типе угроз на сайте компании «Доктор Веб».

- **Восстановить** – для возвращения файла в ту папку, в которой файл находился до перемещения (пользуйтесь данной функцией, только если вы уверены, что файл безопасен).
- **Удалить** – для удаления файла из карантина и из системы.

Удаление всех объектов из карантина

Чтобы удалить все объекты, перемещенные в карантин:

1. Откройте раздел **Карантин**.
2. На экране **Карантин** нажмите **Меню** и выберите пункт **Удалить все**.
3. Нажмите **ОК**, чтобы подтвердить действие.

   Нажмите **Отмена**, чтобы отменить удаление и вернуться в раздел **Карантин**.

Размер карантина

Чтобы просмотреть информацию о размере памяти, занимаемой карантином, и свободном месте во внутренней памяти устройства:

1. Откройте раздел **Карантин**.
2. На экране **Карантин** нажмите **Меню** и выберите пункт **Размер карантина**.
3. Нажмите **ОК**, чтобы вернуться в раздел **Карантин**.

7. Настройки

Чтобы перейти к настройкам приложения (см. Рисунок 10), на главном экране нажмите **Меню** и выберите пункт **Настройки**.

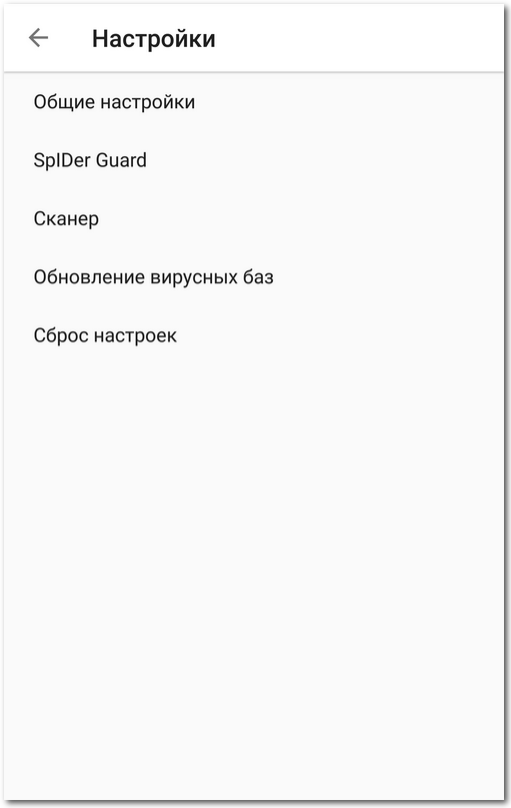

Рисунок 10. Настройки

Если вы установили пароль для доступа к настройкам приложения, вам потребуется ввести пароль от учетной записи.

На экране **Настройки** доступны следующие опции:

- **Общие настройки**. Позволяет настроить панель уведомлений, включить и отключить звуковые оповещения (см. раздел Общие настройки).
- **SplDer Guard**. Позволяет задать настройки для компонента SplDer Guard, который осуществляет постоянную проверку на наличие угроз безопасности (см. раздел Настройки SplDer Guard).
- **Сканер**. Позволяет настроить компонент Сканер, который осуществляет проверку по запросу пользователя (см. раздел Настройки Сканера Dr.Web).
- **Обновление вирусных баз**. Позволяет запретить использовать мобильный Интернет для обновления вирусных баз (см. раздел Обновление вирусных баз).
- **Сброс настроек**. Позволяет сбросить пользовательские настройки и вернуться к настройкам по умолчанию (см. раздел Сброс настроек).

7.1. Общие настройки

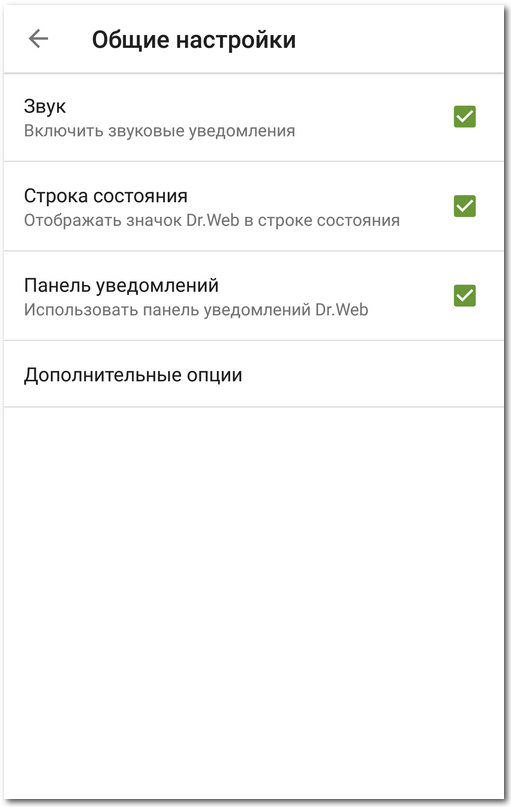

Рисунок 11. Общие настройки

На экране **Общие настройки** (см. Рисунок 11) доступны следующие опции:

- **Звук**. Позволяет настроить звуковые оповещения об обнаружении угроз, их удалении или перемещении в карантин. По умолчанию звуковые уведомления включены.
- **Строка состояния**. Позволяет настроить отображение значка приложения в строке состояния. Эта опция также позволяет отключить отображение панели Dr.Web в области уведомлений. Подробнее см. в разделе Панель уведомлений.

> Настройка недоступна на устройствах с Android 8.0 или более поздними версиями.

- **Панель уведомлений**. Позволяет определить внешний вид панели Dr.Web в области уведомлений. Если опция включена, используется панель Dr.Web. Если опция отключена, панель имеет стандартный вид панели уведомлений Android.

> На устройствах с Android 6.0 или более поздними версиями, если опция **Панель уведомлений** отключена, компонент SpIDer Guard не показывает следующие всплывающие уведомления:
>
> - Идет проверка памяти устройства...
> - Проверка памяти устройства завершена.

- Проверка <*название приложения*> завершена. Угроз не обнаружено.

  Если SplDer Guard обнаружит угрозу, всплывающее уведомление появится, независимо от того, включена опция **Панель уведомлений** или нет.

- **Дополнительные опции**. Содержит дополнительные настройки:
  - **Системные приложения**. Позволяет включить или отключить информирование об обнаружении угроз в известных системных приложениях. По умолчанию эта опция отключена. Подробнее см. в разделе Обнаружение угроз в системных приложениях.

7.2. Обновление вирусных баз

Для обнаружения угроз безопасности Dr.Web Light использует специальные вирусные базы, в которых содержится информация обо всех информационных угрозах для устройств под управлением ОС Android, известных специалистам «Доктор Веб». Базы требуют периодического обновления, поскольку новые вредоносные программы появляются регулярно. Для этого в приложении реализована возможность обновления вирусных баз через Интернет.

Обновление

Вирусные базы обновляются автоматически через интернет несколько раз в сутки. Если вирусные базы долгое время не обновлялись (например, при отсутствии подключения к Интернету), вам нужно запустить обновление вручную.

Чтобы узнать, требуется ли вам выполнить обновление вирусных баз вручную:

1. На главном экране приложения нажмите **Меню** и выберите **Вирусные базы**.
2. В открывшемся окне вы увидите статус вирусных баз и дату последнего обновления. Если вирусные базы устарели, вам нужно выполнить обновление вручную.

Чтобы запустить обновление:

1. На главном экране приложения нажмите **Меню** и выберите **Вирусные базы**.
2. В появившемся окне нажмите **Обновить**.

Сразу после установки приложения рекомендуется выполнить обновление вирусных баз, чтобы Dr.Web Light мог использовать самую свежую информацию об известных угрозах. Сигнатуры вирусов, информация об их признаках и моделях поведения обновляются сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда – до нескольких раз в час.

Настройки обновлений

По умолчанию обновления загружаются автоматически несколько раз в сутки.

Чтобы разрешить или запретить использование мобильных сетей при загрузке обновлений:

1. На главном экране приложения нажмите **Меню** и выберите **Настройки** (см. Рисунок 10).
2. Выберите раздел **Обновление вирусных баз**.
3. Чтобы не использовать при загрузке обновлений мобильные сети, установите флажок **Обновление по Wi-Fi**.

Если активные сети Wi-Fi не будут обнаружены, вам будет предложено использовать мобильный Интернет. Изменение этой настройки не влияет на использование мобильных сетей остальными функциями приложения и мобильного устройства.

При обновлении происходит загрузка данных по сети. За передачу данных может взиматься дополнительная плата. Уточняйте подробности у вашего мобильного оператора.

7.3. Сброс настроек

Вы можете в любой момент сбросить пользовательские настройки приложения и восстановить настройки по умолчанию.

1. На экране настроек (см. Рисунок 10) в разделе **Сброс настроек** выберите пункт **Сброс настроек**.
2. Подтвердите возврат к настройкам по умолчанию.

Предметный указатель

Предметный указатель

П

Р

С

У

Ф