Dr.WEB

Light для Android

Руководство пользователя

Dr.Web Light для Android
Версия 12.2
Руководство пользователя
16.04.2024

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «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».

Dr.Web Light использует Dr.Web Mobile Engine SDK — инструментарий создания приложений для Android с высоким уровнем безопасности. Благодаря разнообразию методик обнаружения угроз он обеспечивает защиту как от известных, так и от новых угроз для мобильных платформ.

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.

Обозначение	Комментарий
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

1.1. Функции Dr.Web

Dr.Web Light выполняет следующие функции:

- Отслеживает изменения в файловой системе устройства в режиме реального времени (сохраняемые файлы, устанавливаемые приложения и т. д.).
- Проверяет все файлы в памяти или отдельные файлы и папки по запросу пользователя.
- Проверяет архивы.
- Отслеживает изменения в системной области.
- Удаляет обнаруженные угрозы безопасности или перемещает их в карантин.
- Разблокирует устройство, если его заблокировала программа-вымогатель.
- Помогает разблокировать устройство друга.
- Регулярно обновляет вирусные базы Dr.Web через интернет.
- Ведет статистику обнаруженных угроз и действий приложения, а также журнал событий.

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 более поздних версий, Samsung Galaxy Note 2 и более поздних версий.

2. Системные требования

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

Параметр	Требование
Операционная система	Android версии 4.4–14.0
Процессор	x86/x86-64/ARMv7/ARMv8
Свободная оперативная память	Не менее 512 МБ
Свободная основная память	Не менее 35 МБ (для хранения данных)
Разрешение экрана	Не менее 800×480
Прочее	Интернет-соединение (для обновления вирусных баз)

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

По умолчанию приложение устанавливается 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

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

Установка из Xiaomi GetApps

Чтобы установить Dr.Web из Xiaomi GetApps, убедитесь, что:

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

Чтобы установить приложение

1. Откройте Xiaomi GetApps на устройстве, найдите в списке приложений Dr.Web Light и нажмите кнопку **Скачать**.

   Если Dr.Web Light не отображается в Xiaomi GetApps, значит, ваше устройство не удовлетворяет системным требованиям.

2. 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. Откройте приложение **Play Маркет**.
2. Нажмите на иконку вашего профиля Google.
3. Выберите пункт **Управление приложениями и устройством**.
4. Перейдите на вкладку **Управление**.
5. Нажмите на список **Доступны обновления** и выполните одно из действий:
   - Выберите **Dr.Web Light** и нажмите **Обновить**.
   - Установите флажок напротив **Dr.Web Light** и нажмите значок .

   Приложение находится в списке **Доступны обновления**, если новая версия приложения уже вышла.
6. 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**.

Папка карантина и файлы журнала не удаляются автоматически. Вы можете удалить их вручную из папки `Android/data/com.drweb/files` во внутренней памяти устройства.

На устройствах с Android 11 и более поздними версиями журналы сохраняются в папке `Download/DrWeb`.

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.

На 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.

После установки Dr.Web Light и принятия Лицензионного соглашения предоставьте приложению необходимые разрешения. Dr.Web Light запрашивает следующие обязательные разрешения:

- На устройствах с Android 10.0 или более ранними версиями: доступ к фото, мультимедиа и файлам.
- На устройствах с Android 11.0 или более поздними версиями: доступ ко всем файлам.

Без предоставления обязательных разрешений работа с Dr.Web Light невозможна. Запрос разрешений будет отображаться каждый раз при заходе в приложение, пока вы не предоставите разрешения, следуя инструкциям, приведенным ниже или отображающимся на экране запроса.

На устройствах с Android 13.0 или более поздними версиями Dr.Web Light запрашивает разрешение на отправку уведомлений. Разрешение требуется для того, чтобы Dr.Web Light мог использовать панель уведомлений для сообщений о состоянии защиты устройства. Если разрешение не будет предоставлено, Dr.Web Light не сможет сообщить вам об обнаружении угроз и необходимости проверки подозрительных файлов, пока вы не откроете приложение.

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

- На устройствах с Android 9.0 или более ранними версиями:
  1. Нажмите **Перейти в Настройки** и выберите раздел **Разрешения**.
  2. Выберите пункт **Память** или **Хранилище** и предоставьте разрешение, используя переключатель.
- На устройствах с Android 10.0:
  1. Нажмите **Перейти в Настройки** и выберите раздел **Разрешения**.
  2. Выберите пункт **Память** или **Хранилище** в категории **Запрещено** и выберите опцию **Разрешить**.
- На устройствах с Android 11.0 или более поздними версиями:
  1. Нажмите **Перейти в Настройки** и выберите раздел **Разрешения**.
  2. Выберите пункт **Файлы и медиаконтент** или **Хранилище** в категории **Запрещено** и выберите опцию **Разрешить управление всеми файлами**. С помощью этой опции вы предоставляете доступ к фото и мультимедиа, а также доступ ко всем файлам.

Чтобы открыть список всех разрешений для Dr.Web Light

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

При первоначальном входе в приложение на экране располагается панель состояния, информация о полной версии приложения, меню Сканера Dr.Web, а также панель навигации Dr.Web (см. Рисунок 1).

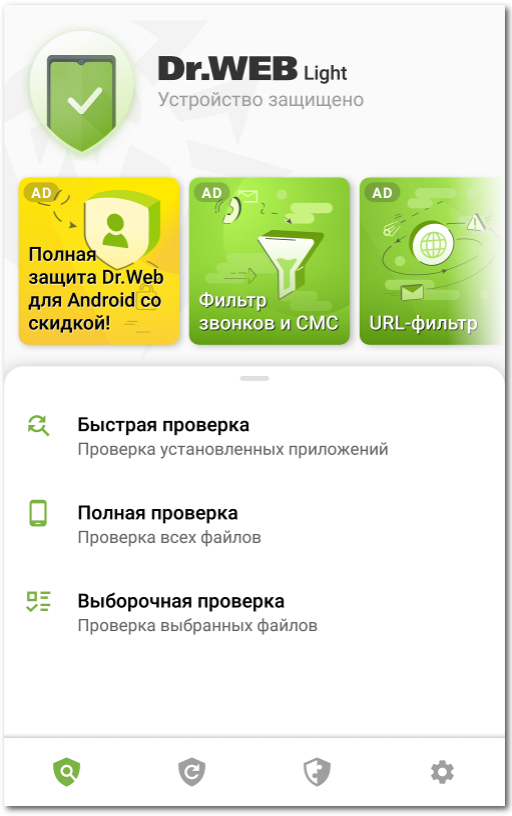

Рисунок 1. Главный экран Dr.Web

Панель состояния

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

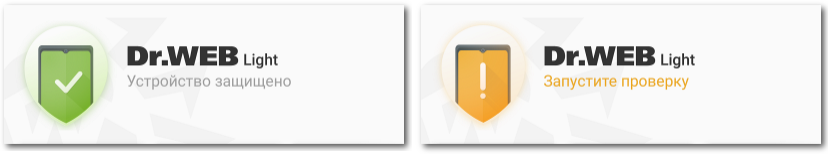

Рисунок 2. Панель состояния

- Зеленый индикатор означает, что устройство защищено. Дополнительных действий не требуется.
- Желтый индикатор означает, что Dr.Web обнаружил проблемы безопасности, например, на устройство были добавлены новые файлы или вирусные базы устарели. Нажмите на панель, чтобы запустить выборочную проверку устройства.

Информация о полной версии приложения

Ниже панели состояния расположены слайды о возможностях полной версии приложения. Слайды позволяют ознакомиться с информацией об антивирусе Dr.Web Security Space для Android и загрузить его из Google Play.

Нажмите на первый слайд, чтобы открыть страницу Dr.Web Security Space для Android в Google Play. Нажмите на любой из следующих слайдов, чтобы ознакомиться с возможностями одного из компонентов, доступных в Dr.Web Security Space для Android. Кнопка **Подробнее** на слайде позволяет открыть страницу Dr.Web Security Space для Android на сайте компании «Доктор Веб». Смахните слайд влево, чтобы перейти к следующему слайду.

Панель навигации

В нижней части экрана расположена панель навигации Dr.Web, с помощью которой вы можете переключаться между вкладками компонентов.

- Вкладка  Сканер позволяет запустить проверку системы по запросу пользователя. Возможны 3 типа проверки: быстрая, полная и выборочная.
- Вкладка  Вирусные базы информирует о текущем статусе вирусных баз и позволяет запустить обновление вирусных баз вручную.
- Вкладка  **Инструменты** включает в себя следующие компоненты:
  - Статистика позволяет просмотреть статистику обнаруженных угроз и действий приложения над ними.
  - Карантин позволяет просмотреть и обработать угрозы, перемещенные в карантин.
  - Помощь другу помогает разблокировать устройство друга, которое заблокировано Антивором Dr.Web.
- Вкладка  Настройки позволяет управлять настройками компонентов и приложения Dr.Web.

5.4. Уведомления

На устройствах с Android 7.0 или более поздними версиями все уведомления Dr.Web группируются в одно разворачивающееся уведомление.

На устройствах с Android 8.0 или более поздними версиями уведомления Dr.Web разделены на категории, или каналы. В настройках устройства вы можете управлять поведением каждой категории уведомлений отдельно. Если вы отключите одну из категорий, вы перестанете получать все уведомления из этой категории. По умолчанию все категории включены.

Категории уведомлений

Категория	Уведомления
Обнаружение угрозы	Уведомления об угрозах, обнаруженных Сканером Dr.Web.
Статус антивирусной защиты	Если панель уведомлений отключена, эта категория содержит следующие уведомления: • **Устройство защищено**. Показывается, если не запущена проверка Сканера Dr.Web. • Уведомление о типе проверки Сканера Dr.Web. Показывается, если запущена одна из проверок: быстрая, полная или выборочная. Если панель уведомлений включена, на ней отображается сообщение о том, что идет проверка, если запущена одна из проверок Сканера Dr.Web.
Уведомления от друзей	Уведомления, полученные от друзей.
Другое	• **Требуются разрешения**. Показывается при открытии приложения, если ранее был отклонен запрос на доступ к фото, мультимедиа и файлам.
Группировать уведомления	Эта категория не содержит конкретных уведомлений, но она позволяет сгруппировать все уведомления Dr.Web в одно разворачивающееся уведомление.

Панель уведомлений

Панель уведомлений Dr.Web (см. Рисунок 3) оперативно отображает предупреждения о подозрительных изменениях в системной области и потенциальных угрозах.

На панели уведомлений отображается индикатор текущего состояния защиты: — на устройствах с Android 11.0 и более ранних версий, — на устройствах с Android 12.0 и более поздних версий. Если Dr.Web обнаружит новые файлы на устройстве или подозрительные изменения в системной области, индикатор сменит цвет на желтый. Если Dr.Web обнаружит угрозы, индикатор сменит цвет на красный.

Рисунок 3. Панель уведомлений на Android 11.0 (слева) и Android 12.0 (справа)

Чтобы включить панель уведомлений Dr.Web

1. Нажмите значок на панели навигации Dr.Web.
2. Выберите **Общие настройки**.

3. Включите опцию **Панель уведомлений**.

> На Android 5.0 и 5.1, если Dr.Web обнаружит подозрительные изменения в системной области или угрозы, панель уведомлений отображается поверх всех приложений до тех пор, пока к обнаруженному объекту не будет применено какое-либо действие или пока вы не смахнете уведомление с панели уведомлений.

С помощью панели уведомлений можно выполнить следующие действия:

- Открыть главный экран приложения при зеленом индикаторе и текущем состоянии защиты **Устройство защищено**. Для этого нажмите на индикатор.
- Запустить выборочную проверку при желтом индикаторе и текущем состоянии защиты **Запустите проверку**. Для этого нажмите на индикатор.
- Открыть результаты проверки при красном индикаторе и текущем состоянии защиты **Устраните проблемы**. Для этого нажмите на индикатор.
- Ознакомиться с информацией о приложении Dr.Web Security Space для Android и загрузить его на бесплатный период 14 дней. Для этого нажмите на текст **Полная версия**.

Чтобы просмотреть состояние защиты, текущие и рекомендуемые действия на устройствах с Android 12.0 и более поздних версий, нажмите ⌄.

5.5. Виджет

Для удобства работы с Dr.Web Light вы можете добавить на главный экран вашего устройства специальный виджет, позволяющий контролировать состояние защиты устройства.

Чтобы добавить виджет Dr.Web

1. Откройте список виджетов, доступных на вашем устройстве.
2. В этом списке выберите виджет Dr.Web.

Виджет показывает текущее состояние защиты (см. Рисунок 4).

- Виджет без индикатора сообщает об отсутствии угроз. Дополнительных действий не требуется.
- Виджет с желтым индикатором сообщает об обнаружении новых файлов или приложений на устройстве. Нажмите на виджет, чтобы запустить проверку новых объектов.
- Виджет с красным индикатором сообщает о необходимости обезвредить обнаруженные угрозы. Нажмите на виджет, чтобы открыть экран результатов проверки и выбрать действия для обнаруженных угроз.

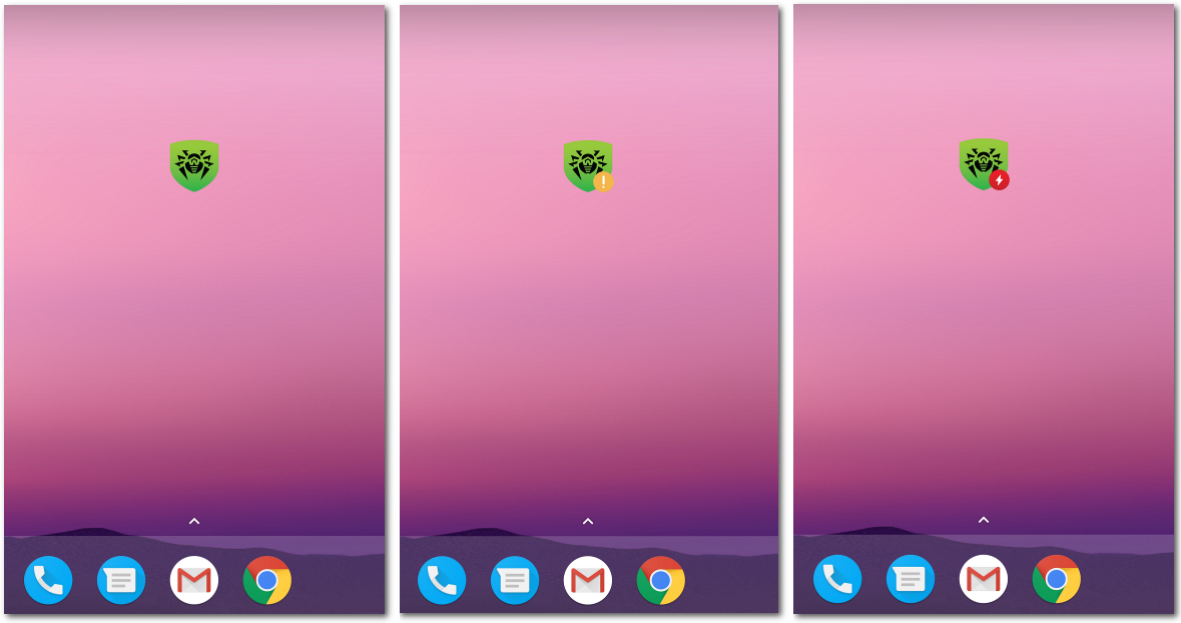

Рисунок 4. Виджет Dr.Web

6. Компоненты Dr.Web

Вы можете перейти к компоненту Dr.Web с помощью панели навигации в нижней части экрана.

- Сканер: позволяет запустить проверку системы по запросу пользователя. Возможны 3 типа проверки: быстрая, полная и выборочная.
- Вирусные базы: информирует о текущем статусе вирусных баз и позволяет запустить обновление вирусных баз вручную.
- Статистика: позволяет просмотреть статистику обнаруженных угроз и действий приложения над ними.
- Карантин: позволяет просмотреть и обработать угрозы, перемещенные в карантин.
- Помощь другу: помогает разблокировать устройство друга, которое заблокировано Антивором Dr.Web.
- Настройки: позволяет управлять настройками компонентов и приложения Dr.Web.

6.1. Антивирусная защита

- Сканер Dr.Web позволяет запустить проверку на наличие угроз.
- На экране Результаты проверки вы можете выбрать действия, чтобы обезвредить обнаруженные угрозы безопасности.

6.1.1. 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. Обычно при этом достаточно проводить быструю проверку системы.

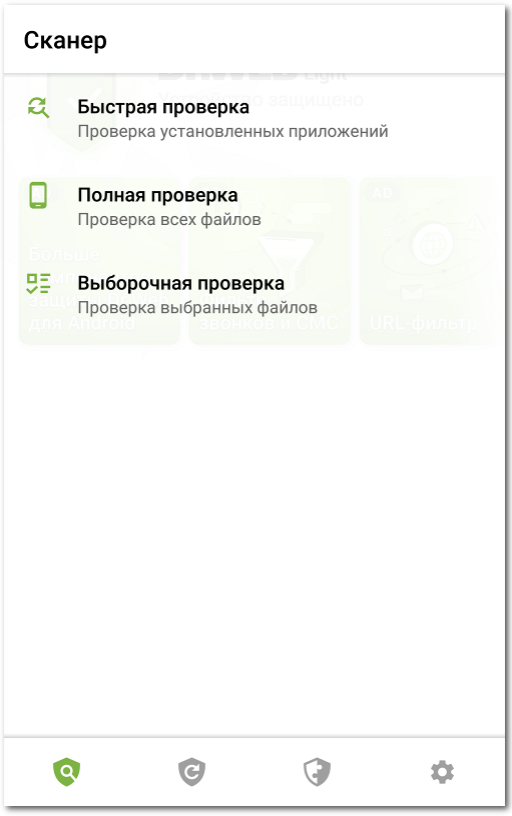

Рисунок 5. Сканер Dr.Web

Проверка

Чтобы проверить систему, на панели навигации Dr.Web нажмите значок , затем на экране **Сканер** (см. Рисунок 5) 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 6). Чтобы выбрать все объекты, установите флажок в правом верхнем углу экрана. Затем нажмите **Проверить**.

> На устройствах с Android 11.0 и более поздних версий папки `/Android/data` и `/Android/obb` защищены системой и недоступны для проверки.

Если в ходе любой проверки Сканер Dr.Web обнаружит угрозы, индикатор в центре экрана проверки станет красным. Нажмите на индикатор или на число найденных угроз, чтобы открыть результаты проверки (см. Рисунок 7) и обезвредить угрозы. Если вы закрыли экран сканирования или закрыли приложение, вы можете открыть результаты проверки, нажав значок на панели уведомлений.

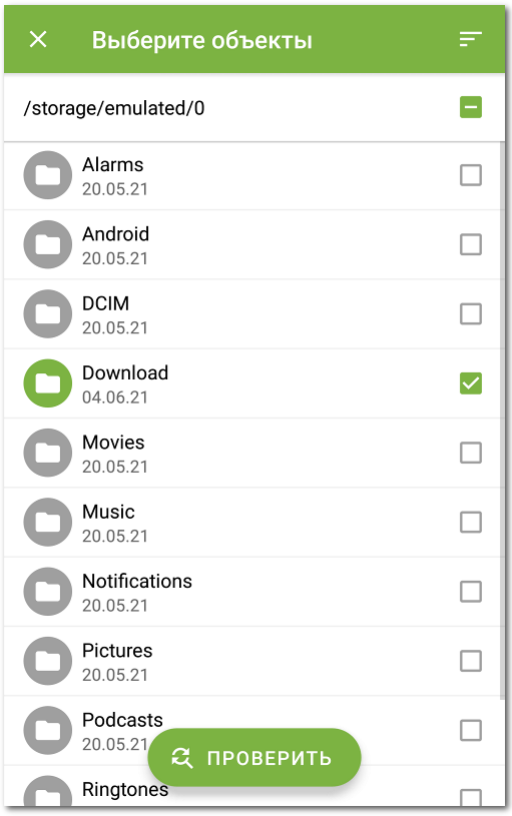

Рисунок 6. Выборочная проверка

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.

Чтобы отправить файл в лабораторию

1. Нажмите и удерживайте файл в списке объектов файловой системы (см. Рисунок 6), 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**, если вы считаете, что файл ошибочно отнесен к угрозам.
4. Нажмите кнопку **Отправить**.

В антивирусную лабораторию «Доктор Веб» могут быть отправлены файлы, размер которых не превышает 250 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**.

  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 APK-файлы независимо от установленного значения параметра **Файлы в архивах**.

- Чтобы отслеживать изменения в системной области, установите флажки **Системная область** и **Любые файлы системной области**. Если эти настройки включены, компонент отслеживает изменения (добавление, изменение и удаление файлов) и уведомляет о добавлении и изменении исполняемых файлов: `.jar`, `.odex`, `.so`, файлов формата APK, ELF, и др.
- Чтобы включить/отключить проверку системы на наличие файлов, которые могут представлять угрозу, установите/снимите соответствующие флажки:
  - Подозрительные объекты,
  - Рекламные программы,
  - Программы дозвона,
  - Программы-шутки,
  - Потенциально опасные программы,
  - Программы взлома,
  - Уязвимые программы.

Статистика

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

6.1.2. Результаты проверки

Если Сканер Dr.Web обнаружит угрозы, на экране появятся:

- Значок в строке состояния Android в левом верхнем углу экрана:

- — на Android 4.4,
- — на Android 5.0–11.0,
- — на Android 12.0 и более поздних версий.

- Всплывающее уведомление в верхней части экрана.
- Красный индикатор на экране проверки.

Чтобы открыть результаты проверки, нажмите на крестик в левом верхнем углу экрана завершенной проверки или на индикатор в уведомлении или на панели состояния.

На Android 5.0 и более поздних версиях уведомление об угрозе также появится на экране блокировки устройства, откуда вы можете перейти к результатам проверки.

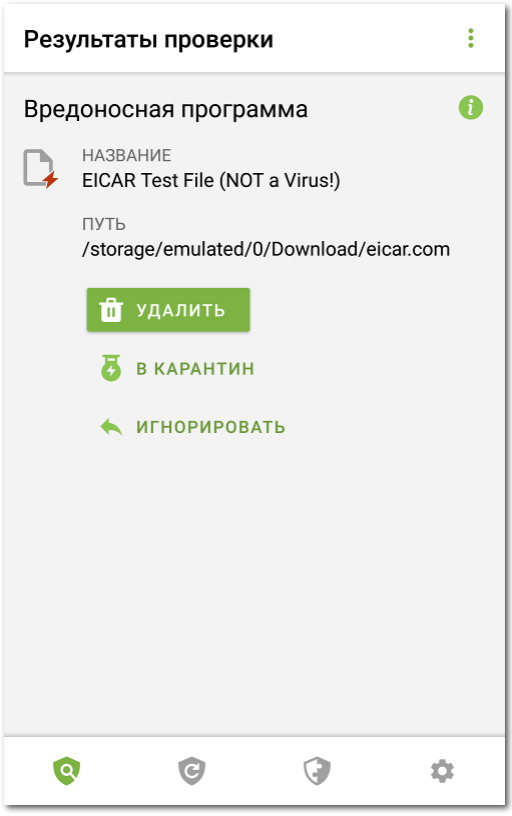

Рисунок 7. Результаты проверки

Обезвреживание угроз

На экране **Результаты проверки** вы можете ознакомиться со списком угроз и подозрительных изменений в системной области. Для каждого объекта указаны его тип и название.

Объекты отмечены разными цветами в зависимости от степени опасности. Типы объектов в порядке уменьшения опасности:

1. Вредоносная программа.
2. Модификация. На экране **Результаты проверки** тип объекта отображается как **Вредоносная программа**, но цветовое обозначение отличается.
3. Подозрительный объект.
4. Рекламная программа.
5. Программа дозвона.
6. Программа-шутка.
7. Потенциально опасная программа.
8. Программа взлома.
9. Уязвимая программа.

Наименьшая степень опасности присваивается изменениям в системной области:

- Новые файлы в системной области.
- Изменение системных файлов.
- Удаление системных файлов.

Чтобы посмотреть путь к файлу, выберите соответствующий объект. Для угроз, обнаруженных в приложениях, также указано имя пакета приложения.

В случае обнаружения архива, содержащего несколько угроз, выберите соответствующий объект и нажмите **Раскрыть**, чтобы раскрыть полный список всех угроз в архиве.

Обнаружение угроз в архиве возможно только при включенной опции Файлы в архивах.

Обезвреживание всех угроз

Чтобы удалить сразу все угрозы

- В правом верхнем углу экрана **Результаты проверки** выберите **Меню** > **Удалить все**.

Чтобы переместить в карантин сразу все угрозы

- В правом верхнем углу экрана **Результаты проверки** выберите **Меню** > **Все в карантин**.

Обезвреживание угроз по одной

Для каждого объекта доступен свой набор опций. Чтобы раскрыть список опций, выберите объект. Рекомендуемые опции расположены первыми в списке. Выберите одну из опций:

Удалить, чтобы полностью удалить угрозу из памяти устройства.

В некоторых случаях Dr.Web не может удалить приложения, которые используют специальные возможности Android. Если Dr.Web не удалит приложение после выбора опции **Удалить**, перейдите в безопасный режим и удалите приложение вручную.

Опция недоступна для угроз в системных приложениях.

В карантин, чтобы переместить угрозу в изолированную папку (см. раздел Карантин).

Если угроза обнаружена в установленном приложении, перемещение в карантин для нее невозможно. В этом случае опция **В карантин** недоступна.

Игнорировать, чтобы временно оставить изменение в системной области или угрозу нетронутыми.

Отправить в лабораторию или **Ложное срабатывание**, чтобы отправить файл в антивирусную лабораторию «Доктор Веб» на анализ. Анализ покажет, действительно ли это угроза или ложное срабатывание. Если произошло ложное срабатывание, оно будет исправлено. Чтобы получить результаты анализа, укажите адрес электронной почты.

Если файл отправлен в лабораторию успешно, к объекту автоматически применяется действие **Игнорировать**.

Опция **Отправить в лабораторию** доступна только для добавленных или измененных исполняемых файлов в системной области: `.jar`, `.odex`, `.so`, файлов формата APK, ELF, и др.

Опция **Ложное срабатывание** доступна только для модификаций угроз и для угроз в системной области.

Подробнее в Интернете, чтобы открыть страницу с описанием обнаруженного объекта на сайте «Доктор Веб».

6.1.2.1. Угрозы в системных приложениях

Приложения, установленные в системной области, в некоторых случаях могут выполнять функции, характерные для вредоносных программ, поэтому Dr.Web может определять такие приложения как угрозы.

Для системных приложений, как для любых установленных приложений, опция **В карантин** недоступна.

Если системное приложение может быть удалено без потери работоспособности устройства или вылечено, для него доступна соответствующая опция в полной версии Dr.Web. Для этого на устройстве должен быть разрешен root-доступ.

Если системное приложение не может быть удалено без потери работоспособности устройства, опция **Удалить** недоступна, но вы можете воспользоваться следующими рекомендациями:

- Остановите 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 **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 кастомизированная 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 разрешен root-доступ, вы можете попробовать удалить такие приложения с помощью специальных утилит.

Чтобы отключить информирование об угрозах в системных приложениях, которые не могут быть удалены без потери работоспособности устройства, установите флажок **Системные приложения** в разделе **Настройки** > **Общие настройки**.

6.1.2.2. Изменения в системной области

Системная область — это область памяти, которая используется системными приложениями и содержит критические данные для работы устройства и чувствительные данные пользователей. Если на вашем устройстве не разрешен root-доступ, системная область вам недоступна.

Вредоносные приложения могут получить root-доступ и внести изменения в системную область: удалить, добавить или изменить файлы или папки.

Вы можете включить проверку системной области в настройках Сканера. Если компонент обнаружит подозрительные изменения, он уведомит об этом по итогам проверки.

Изменение	Имя	Тип
Удаление папки с файлами	read-only.area.dir.deleted.threat	Удаление системных файлов
Удаление файла	read-only.area.deleted.threat	Удаление системных файлов
Добавление папки с файлами	read-only.area.dir.added.threat	Новые файлы в системной области
Добавление файла	read-only.area.added.threat	Новые файлы в системной области
Изменение файла	read-only.area.changed.threat	Изменение системных файлов

Если Сканер обнаруживает одно из вышеперечисленных изменений, файлы или папки сами по себе не обязательно вредоносны, но изменение может быть совершено вредоносным приложением.

Для обнаруженных изменений доступны следующие опции:

- Игнорировать.
- Отправить в лабораторию — доступно только при добавлении или изменении исполняемых файлов: `.jar`, `.odex`, `.so`, файлов формата APK, ELF, и др.
- Подробнее в Интернете.

Компонент только информирует о вышеперечисленных изменениях. Чтобы обнаружить вредоносное приложение, которое могло внести изменение в системную область, выполните полную проверку устройства.

6.1.3. Приложения-блокировщики устройства

Dr.Web Light позволяет защитить мобильное устройство от программ-вымогателей. 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, вы можете разблокировать устройство.

Чтобы разблокировать устройство

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, имеющих эту функцию). 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. Вирусные базы

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 не обновлялись более 24 часов (например, при отсутствии подключения к интернету), вам нужно запустить обновление вручную.

Чтобы узнать, требуется ли вам выполнить обновление вирусных баз вручную

1. Нажмите  на панели навигации.

2. В открывшемся окне вы увидите статус вирусных баз и дату последнего обновления. Если последнее обновление было более 24 часов назад, вам нужно выполнить обновление вручную.

Чтобы запустить обновление

1. Нажмите на панели навигации.
2. В открывшемся 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 мобильной сети при загрузке обновлений

1. Нажмите на панели навигации (см. Рисунок 12).
2. Выберите раздел **Вирусные базы**.
3. Чтобы не использовать мобильную сеть при загрузке обновлений, 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 мобильной сети 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.

6.3. Статистика

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

Для просмотра статистики работы приложения нажмите значок на панели навигации и выберите пункт **Статистика**.

Просмотр статистики

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

- **Всего**. Содержит информацию об общем количестве проверенных файлов, обнаруженных и обезвреженных угроз.
- **События**. Содержит информацию о результатах проверки Сканером Dr.Web, статусе обновления вирусных баз, обнаруженных угрозах и действиях по их обезвреживанию.

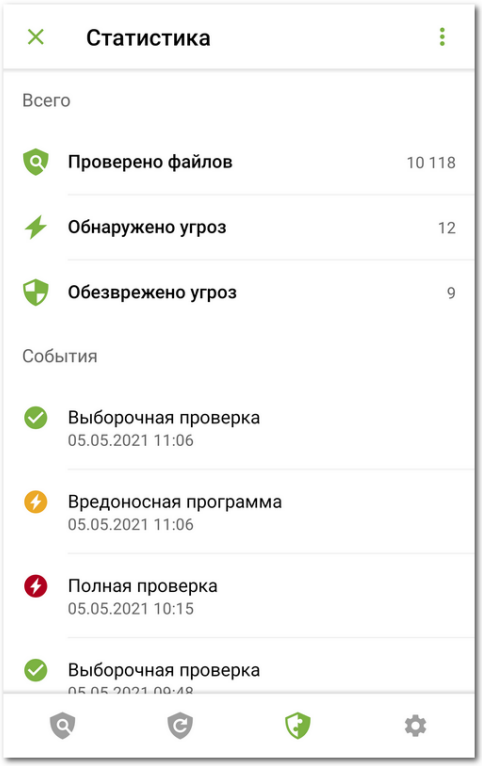

Рисунок 8. Статистика

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 журналы**.
2. Журнал сохраняется в файлах `DrWeb_Log.txt` и `DrWeb_Err.txt`, расположенных в папке `Android/data/com.drweb/files` во внутренней памяти устройства.

На устройствах с Android 11 и более поздними версиями журналы сохраняются в папке `Download/DrWeb`.

6.4. Карантин

Для обнаруженных угроз доступна опция перемещения в карантин — особую папку, предназначенную для их изоляции и безопасного хранения (см. Рисунок 9).

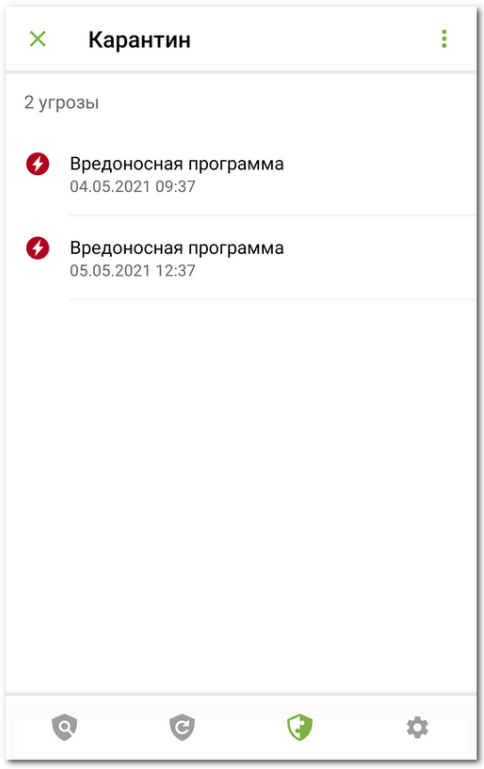

Рисунок 9. Карантин

Просмотр списка объектов в карантине

Чтобы просмотреть список угроз, перемещенных в карантин, нажмите значок на панели навигации и выберите пункт **Карантин**.

Просмотр информации об угрозах

Чтобы посмотреть информацию об угрозе, нажмите ее имя в списке.

Для каждой угрозы вы можете просмотреть следующую информацию:

- имя файла;
- путь к файлу;

- дата и время перемещения в карантин.

Вы можете раскрыть карточку с информацией об угрозе, смахнув ее вверх. Смахните карточку вниз, чтобы свернуть ее.

Чтобы просмотреть список угроз в архиве, содержащем несколько угроз, выберите соответствующий объект и нажмите **Раскрыть** напротив пункта **Угроза**.

Доступные опции

Для каждой угрозы доступны следующие опции:

- **Подробнее в Интернете** — для просмотра описания угрозы на сайте «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.
- **Ложное срабатывание** — для отправки файла в антивирусную лабораторию «Доктор Веб» на анализ. Анализ покажет, действительно ли файл представляет угрозу или это ложное срабатывание. Если произошло ложное срабатывание, оно будет исправлено. Чтобы получить результаты анализа, укажите свой адрес электронной почты.

> Опция **Ложное срабатывание** доступна только для модификаций угроз.

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 **Удалить**, 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**.
3. Нажмите **ОК**, чтобы вернуться в раздел **Карантин**.

6.5. Помощь другу

Компонент **Помощь другу** помогает разблокировать устройство друга, которое заблокировано Антивором Dr.Web.

Что такое Антивор Dr.Web

Антивор доступен в приложении Dr.Web Security Space для Android. Если устройство потеряно или украдено, Антивор блокирует устройство. Чтобы его разблокировать, нужно ввести пароль. Если владелец устройства не помнит пароль, вы можете помочь сбросить пароль и разблокировать устройство.

Как работает Помощь другу

При включении компонента **Помощь другу** вы указываете свой адрес электронной почты и сообщаете его пользователям Dr.Web Security Space для Android, которым вы доверяете. Пользователи Dr.Web Security Space для Android добавляют вас в друзья в Антиворе. Вы подтверждаете полученные запросы в друзья.

Если кому-то из друзей требуется помощь в разблокировке устройства, ваш друг отправляет вам уведомление. Получив уведомление, вы связываетесь с другом, узнаете код подтверждения и отправляете запрос на разблокировку устройства друга. При получении запроса на разблокировку Антивор позволяет другу сбросить пароль, после чего друг может продолжить работу на устройстве.

Для взаимодействия с устройством друга оба устройства должны быть подключены к интернету. Доставка уведомлений может занимать до 15 минут.

Чтобы включить Помощь другу

1. На панели навигации нажмите значок  и выберите **Помощь другу**.
2. На экране **Помощь другу** нажмите **Включить**.
3. Введите свой адрес электронной почты и нажмите **Продолжить**.

Чтобы добавить друга

1. Сообщите указанный вами адрес электронной почты пользователю Dr.Web Security Space для Android, чтобы он мог отправить вам запрос в друзья.
2. Дождитесь уведомления о запросе в друзья.
3. Нажмите на уведомление, чтобы перейти на экран **Помощь другу**.
4. Нажмите на строку с адресом электронной почты друга, отправившего запрос.
5. Нажмите **Подтвердить** на карточке друга, чтобы подтвердить запрос в друзья.

Если вы не приняли или отклонили запрос в друзья, пользователь не сможет отправить вам запрос на разблокировку.

Чтобы изменить имя друга

1. На карточке друга (см Рисунок 10) нажмите .
2. Введите новое имя друга.
3. Нажмите , чтобы сохранить изменения.

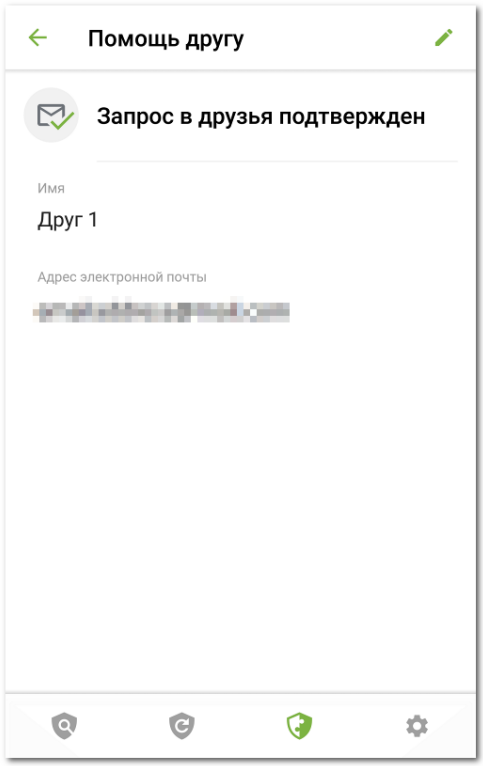

Рисунок 10. Карточка друга

Вы можете редактировать только имя друга. Если адрес электронной почты друга изменился или больше не используется, вы можете удалить друга.

Чтобы удалить друга

- Смахните соответствующий контакт влево.

Если вы случайно удалите контакт друга, запрос в друзья которого вы еще не подтвердили, вы можете отменить удаление, нажав **Отменить**.

Чтобы разблокировать устройство друга

1. Нажмите на уведомление о блокировке, которое вы получили от друга.

2. Свяжитесь с другом. Возможно, устройство потеряно или украдено и уведомление было отправлено посторонним.
3. Если действительно нужна помощь в разблокировке устройства, узнайте у друга код подтверждения. Код подтверждения отображается на экране блокировки на устройстве друга.
4. Введите код подтверждения и нажмите **Разблокировать** (см. Рисунок 11).

Если вы случайно проигнорировали или закрыли уведомление о блокировке, попросите друга отправить уведомление повторно.

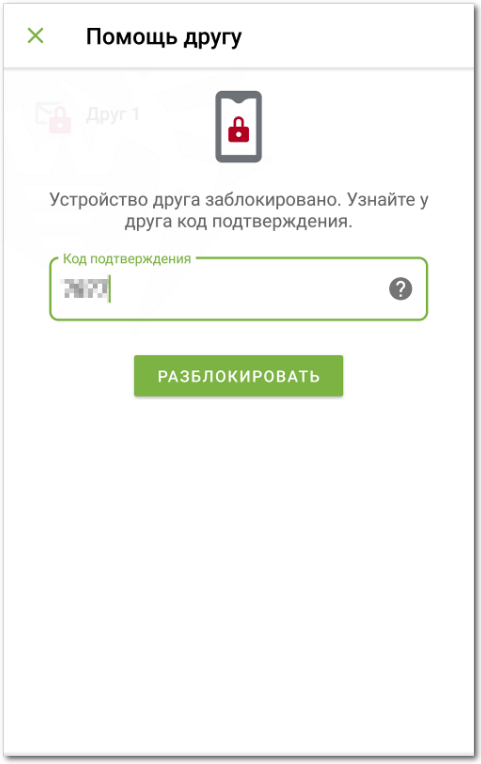

Рисунок 11. Код подтверждения разблокировки

Чтобы отключить Помощь другу

1. На панели навигации нажмите значок и выберите **Помощь другу**.
2. На экране **Помощь другу** нажмите **Меню** и выберите **Отключить**.

При отключении **Помощь другу** все друзья будут удалены. Каждый друг получит уведомление о том, что вы отклонили его запрос в друзья.

7. Настройки

Чтобы перейти к настройкам приложения (см. Рисунок 12), нажмите значок на панели навигации.

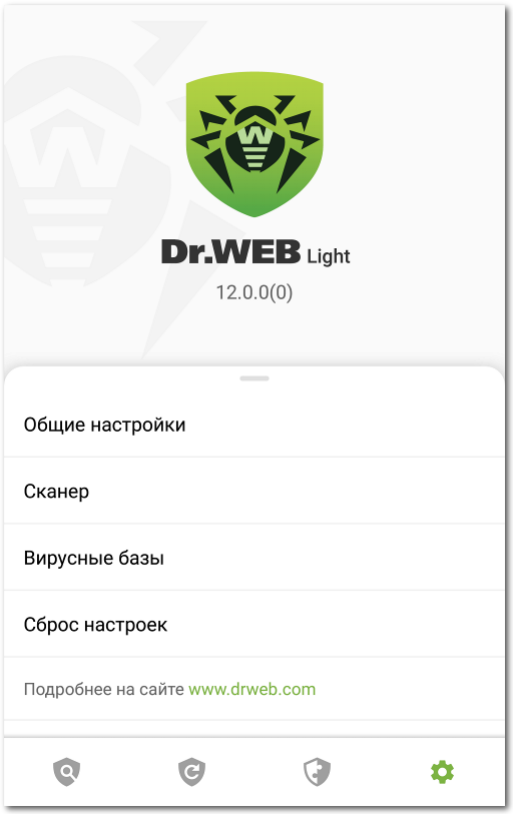

Рисунок 12. Настройки

На экране **Настройки** доступны следующие опции:

- **Общие настройки**. Позволяет включить темную тему приложения, настроить панель уведомлений и информирование об угрозах в системных приложениях, включить и отключить звуковые оповещения (см. раздел Общие настройки).
- **Сканер**. Позволяет настроить компонент Сканер, который осуществляет проверку по запросу пользователя (см. раздел Настройки Сканера Dr.Web).
- **Вирусные базы**. Позволяет запретить использовать мобильный интернет для обновления вирусных баз (см. раздел Вирусные базы).
- **Сброс настроек**. Позволяет сбросить пользовательские настройки и вернуться к настройкам по умолчанию (см. раздел Сброс настроек).
- **Подробнее на сайте www.drweb.com**. Позволяет перейти на сайт компании «Доктор Веб» и ознакомиться с информацией о приложении и других продуктах компании.

Экран **Настройки** также помогает получить информацию о продукте и его производителе. В верхней части экрана под названием продукта отображается

установленная версия приложения. Смахните меню **Настройки** вверх, чтобы раскрыть дополнительные информационные опции:

- **Справка**. Позволяет ознакомиться с документацией к приложению Dr.Web Light.
- **Значки социальных сетей**. Позволяют перейти на страницы компании «Доктор Веб» в различных социальных сетях.

7.1. Общие настройки

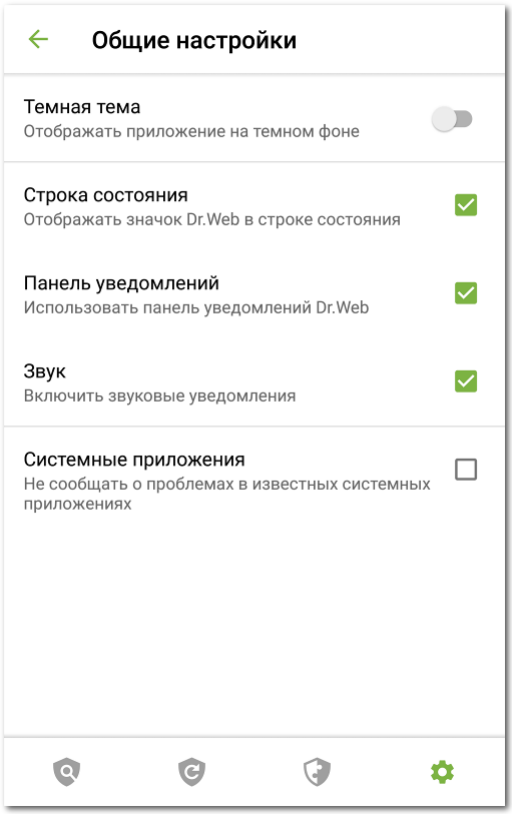

Рисунок 13. Общие настройки

На экране **Общие настройки** (см. Рисунок 13) доступны следующие опции:

- **Темная тема**. Позволяет выбрать темный или светлый фон приложения.
- **Строка состояния**. Позволяет настроить отображение значка приложения в строке состояния. Эта опция также позволяет отключить отображение панели Dr.Web в области уведомлений (см. раздел 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.

- **Звук**. Позволяет настроить звуковые оповещения об обнаружении угроз, их удалении или перемещении в карантин. По умолчанию звуковые уведомления включены.
- **Системные приложения**. Позволяет включить или отключить информирование об угрозах в системных приложениях, которые не могут быть удалены без потери работоспособности устройства. По умолчанию эта опция отключена.

7.2. Сброс настроек

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

Чтобы сбросить настройки

1. На экране настроек (см. Рисунок 12) в разделе **Сброс настроек** выберите пункт **Сброс настроек**.
2. Подтвердите возврат к настройкам по умолчанию.

Предметный указатель

Предметный указатель

Р

С

У

Ф