Dr.WEB

Security Space для Android

Руководство пользователя

Dr.Web Security Space для Android
Версия 12.3.1
Руководство пользователя
28.01.2019

«Доктор Веб», Центральный офис в России

125040, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

Наименование и местонахождение уполномоченного представителя изготовителя:

ЧП «АнтиВирус», 220140, Минск, ул. Притыцкого, д.83, оф.37

Импортер: ЧП «АнтиВирус», 220140, Минск, ул. Притыцкого, д.83, оф.37

Сайт: http://www.drweb.by/

Телефон: +375 (25) 670-10-12

Факс: +375 (17) 253-53-53

Адрес электронной почты: info@drweb.by

«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 Security Space для Android (далее – Dr.Web) защищает мобильные устройства, работающие под управлением операционной системы Android™, а также телевизоры, медиапроигрыватели и игровые консоли, работающие на платформе Android TV™, 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 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 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.
- Фильтрует входящие звонки и SMS-сообщения на основе черных и белых списков.
- Регулярно обновляет вирусные базы Dr.Web через Интернет.
- Ведет статистику обнаруженных угроз и действий приложения, а также журнал событий.
- Ищет и удаленно блокирует устройство при его потере или краже.
- Ограничивает доступ к выбранным веб-сайтам, а также категориям интернет-ресурсов в стандартном браузере Android, Google Chrome, Яндекс.Браузер, Microsoft Edge, Firefox, Opera, Adblock Browser, Dolphin Browser, Спутник и Boat Browser.
- Проверяет и сокращает URL.
- Находит и помогает устранить проблемы безопасности и уязвимости.
- Контролирует интернет-подключения, защищает устройство от несанкционированного доступа извне и предотвращает утечки важных данных по сети.
- Помогает ограничить доступ к приложениям, установленным на устройстве.
- Дает возможность включить семейный поиск для большинства популярных поисковых систем.

Некоторые из перечисленных функций недоступны при работе с приложением на платформе Android TV.

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.

  Dr.Web также работает на телевизорах, медиаплеерах и игровых консолях на платформе Android TV.
- Для загрузки обновлений вирусных баз требуется интернет-соединение.
- Для совместной работы с приложениями, которые блокируют запуск других приложений, требуется, чтобы эти приложения-блокировщики не ограничивали запуск Dr.Web.
- Если вы используете планшетный компьютер, для фильтрации звонков и сообщений и работы Антивора Dr.Web требуется возможность установить и использовать SIM-карту.
- URL-фильтр работает во встроенном браузере Android, в Google Chrome, Яндекс.Браузер, Microsoft Edge, Firefox, Opera, Adblock Browser, Dolphin Browser, Спутник и Boat Browser.
- На устройствах с Android 5.1 или более ранними версиями для корректной работы URL-фильтра необходимо, чтобы для используемого браузера была включена функция сохранения истории.

На устройствах с кастомными прошивками или открытым root-доступом (так называемых рутованных устройствах) корректная работа Dr.Web не гарантируется. Для подобных устройств не предусмотрено оказание технической поддержки.

По умолчанию установка приложения осуществляется во внутреннюю память устройства. Для корректной работы Dr.Web и, в частности, Антивора Dr.Web не следует переносить установленное приложение на съемные носители.

3. Установка Dr.Web

Установить Dr.Web можно одним из следующих способов:

- Установка из Google Play.
- Установка с сайта «Доктор Веб».
- Установка с помощью программы синхронизации с компьютером.

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 и нажмите кнопку **Установить** или **Купить** (при выборе версии приложения с неограниченной лицензией Dr.Web Security Space Life).

   

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

2. Если вы выбрали версию Dr.Web Security Space Life, для продолжения установки вам необходимо выполнить оплату.
3. Далее откроется экран с информацией о функциях устройства, к которым требуется доступ для работы приложения.

   Ознакомьтесь со списком необходимых разрешений и нажмите **Принять**.
4. Для начала работы с приложением нажмите кнопку **Открыть**.

Для дальнейшей работы с приложением необходимо активировать коммерческую или демонстрационную лицензию (за исключением версии Dr.Web Security Space Life).

Установка с сайта «Доктор Веб»

Чтобы установить приложение с сайта «Доктор Веб», включите следующую системную настройку:

- На устройствах с Android 7.1 или более ранними версиями:
  1. В настройках устройства откройте экран **Безопасность**.
  2. Установите флажок **Неизвестные источники**.

- На устройствах с Android 8.0 или более поздними версиями:
  1. В настройках устройства откройте экран **Установка неизвестных приложений**.
  2. Разрешите установку приложений из выбранного источника.

Загрузить установочный файл Dr.Web можно на сайте компании «Доктор Веб» по адресу https://download.drweb.com/android/.

Запуск установочного файла на устройстве

1. Скопируйте установочный файл на устройство.
2. При помощи файлового менеджера найдите и запустите установочный файл.
3. В открывшемся окне нажмите кнопку **Установить**.
4. Нажмите **Открыть**, чтобы начать работу с приложением.

   Нажмите **Готово**, чтобы закрыть окно установки и начать работу с приложением позже.

Для дальнейшей работы с приложением необходимо активировать коммерческую или демонстрационную лицензию.

После установки приложения:

- На устройствах с Android 7.1 или более ранними версиями в настройках устройства отключите настройку **Неизвестные источники**.
- На устройствах с Android 8.0 или более поздними версиями в настройках устройства отключите настройку **Установка неизвестных приложений**.

Установка с помощью программы синхронизации

Установка с помощью программы синхронизации мобильного устройства с компьютером (например, HTC Sync™ и др.).

1. Синхронизируйте мобильное устройство с компьютером.
2. Запустите мастер установки приложений, входящий в пакет программы синхронизации.
3. Укажите путь, по которому установочный файл расположен на компьютере, далее следуйте инструкциям мастера установки.
4. Приложение будет перенесено на мобильное устройство, где вы можете просмотреть информацию о нем и подтвердить установку. После подтверждения приложение будет установлено автоматически.
5. Закройте мастер установки программы синхронизации.

Dr.Web установлен и готов к использованию.

Для дальнейшей работы с приложением необходимо активировать коммерческую или демонстрационную лицензию.

4. Обновление и удаление Dr.Web

Обновление Dr.Web

Настройка автоматического обновления для версии с сайта «Доктор Веб»

Если вы загрузили и установили Dr.Web с сайта компании «Доктор Веб», вы можете настроить проверку доступности новой версии приложения при каждом обновлении вирусных баз. Для этого:

1. На главном экране нажмите **Меню** и выберите пункт **Настройки**.
2. На экране **Настройки** выберите **Обновление вирусных баз**.
3. На экране **Обновление вирусных баз** установите флажок **Новая версия**.

При появлении новой версии приложения вы получите стандартное уведомление и сможете ее оперативно загрузить и установить.

Обновление через Google Play вручную

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 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

> Антивор Dr.Web затрудняет удаление приложения Dr.Web с устройства. Если у вас настроен Антивор, отключите его перед тем, как удалять приложение.

Чтобы удалить Dr.Web:

1. В настройках устройства выберите **Приложения** или **Диспетчер приложений**.

2. В списке установленных приложений выберите **Dr.Web** 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. Лицензирование

Для работы Dr.Web требуется лицензия. Лицензия позволяет использовать все функции приложения на протяжении всего срока действия и регулирует права пользователя, установленные в соответствии с пользовательским договором.

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, вы можете активировать демонстрационную лицензию.

Если у вас есть действующая лицензия на программные продукты Dr.Web Security Space или Антивирус Dr.Web (поставка в коробке или в виде электронной лицензии), вы можете использовать имеющуюся лицензию для работы Dr.Web.

Если вы приобрели версию приложения с неограниченной лицензией (Dr.Web Security Space Life) из Google Play, процедура получения и регистрации лицензии происходит автоматически.

При включении режима централизованной защиты лицензия автоматически загружается с сервера централизованной защиты.

Лицензионный ключевой файл

Права пользователя на использование Dr.Web хранятся в специальном файле, называемом *лицензионным ключевым файлом*.

Лицензионный ключевой файл имеет расширение .key и содержит, в частности, следующую информацию:

- Период, в течение которого разрешено использование продукта.
- Перечень компонентов, разрешенных к использованию.
- Другие ограничения.

Лицензионный ключевой файл является действительным при одновременном выполнении следующих условий:

- Срок действия лицензии не истек.
- Лицензия распространяется на все используемые приложением модули.
- Целостность лицензионного ключевого файла не нарушена.

При нарушении любого из условий лицензионный ключевой файл становится недействительным, при этом антивирус перестает обезвреживать вредоносные программы.

Редактирование лицензионного ключевого файла делает его недействительным. Поэтому не рекомендуется открывать его без крайней необходимости в текстовых редакторах во избежание его случайной порчи.

5.1. Экран Лицензия

На экране **Лицензия** (см. Рисунок 1) вы можете купить или активировать коммерческую лицензию, а также получить демонстрационную лицензию.

Чтобы перейти на экран **Лицензия**, запустите приложение и выполните одно из следующих действий:

- Нажмите **Подробнее** в уведомлении об отсутствии лицензии в верхней части главного экрана приложения.
- На главном экране приложения нажмите **Меню** и выберите пункт **Лицензия**.

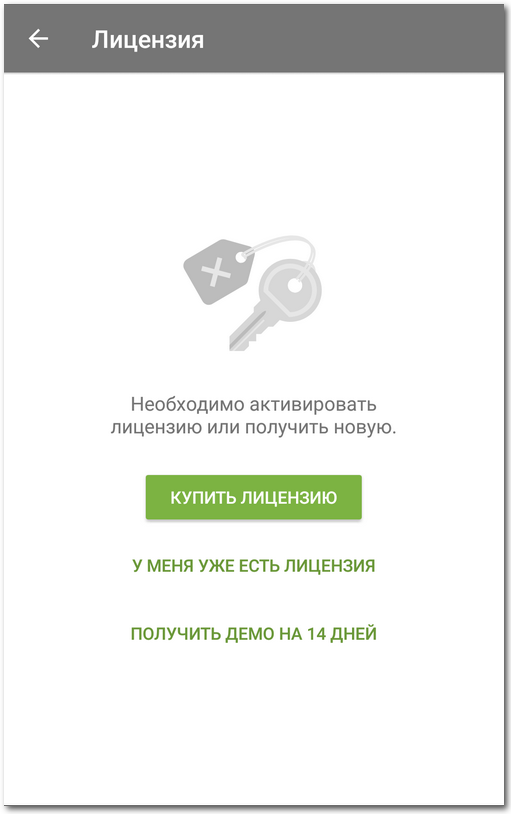

Рисунок 1. Экран Лицензия

5.2. Активация демонстрационной лицензии

Если вы хотите ознакомиться с функциями приложения перед покупкой лицензии, вы можете активировать демонстрационную лицензию на 14 дней. Для этого:

1. Запустите приложение.

2. Перейдите на экран Лицензия.
3. Выберите **Получить демо на 14 дней**.
4. Укажите ваши личные данные (см. Рисунок 2):
   - Имя и фамилию.
   - Действительный адрес электронной почты.
   - Страну.
5. По желанию установите флажок **Получать новости по электронной почте**.

   На этом шаге приложение может запросить у вас доступ к контактам. Если вы разрешите доступ, поля **Адрес электронной почты** и **Страна** будут заполнены автоматически. Если вы отклоните запрос, то поля потребуется заполнить вручную.
6. Нажмите **Получить демо**. Демонстрационная лицензия будет активирована.

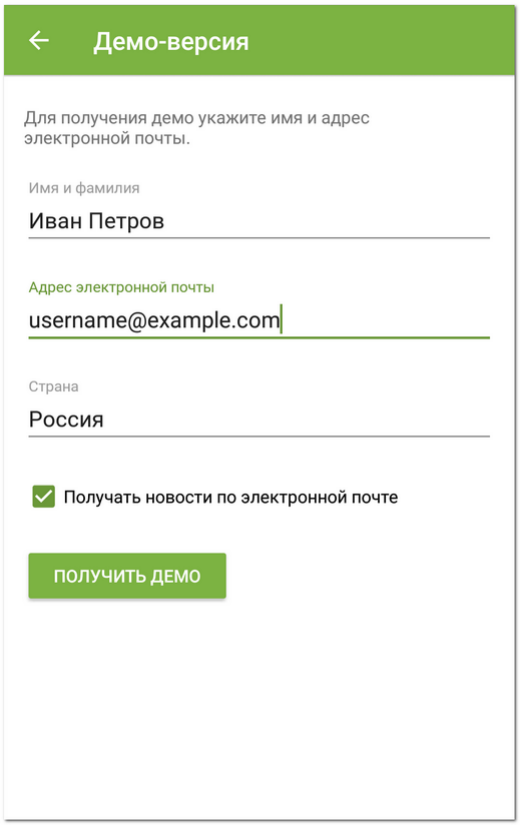

Рисунок 2. Получение демонстрационной лицензии

5.3. Покупка лицензии

Если приложение установлено из Google Play

1. Запустите приложение.
2. Перейдите на экран Лицензия.
3. Выберите **Купить лицензию**.

Если у вас нет учетной записи Google, укажите адрес электронной почты, на который будет зарегистрирована лицензия. При переустановке приложения или его установке на другом устройстве вы можете восстановить лицензию, используя этот адрес.

На этом шаге приложение может запросить доступ к контактам. Если вы разрешите доступ, поле с адресом электронной почты заполнится автоматически. Если вы запретите доступ, вам нужно будет ввести адрес вручную.

4. На экране **Покупка лицензии** (см. Рисунок 3) выберите один из следующих вариантов:

   - **Лицензия на 1 год**
   - **Лицензия на 2 года**

   При выборе любого из вариантов откроется экран покупки лицензии. Через некоторое время после совершения оплаты лицензия активируется автоматически. Если из-за возможных технических сбоев при покупке загрузка ключевого файла не началась, обратитесь в службу технической поддержки: https://support.drweb.com/.

   - **Бессрочная лицензия**

   При выборе лицензии с неограниченным сроком действия откроется экран покупки в Google Play.

   После выполнения оплаты новая версия приложения будет скачена и установлена на устройство. Лицензия будет активирована автоматически.

   При первом запуске приложения вам предлагается удалить старую версию Dr.Web. Если вы хотите сохранить текущие настройки для их дальнейшего использования с Dr.Web Security Space Life, экспортируйте их в файл перед удалением.

   Нажмите кнопку **ОК**, чтобы подтвердить удаление.

Антивор Dr.Web затрудняет удаление приложения Dr.Web с устройства. Если у вас настроен Антивор, отключите его перед удалением приложения.

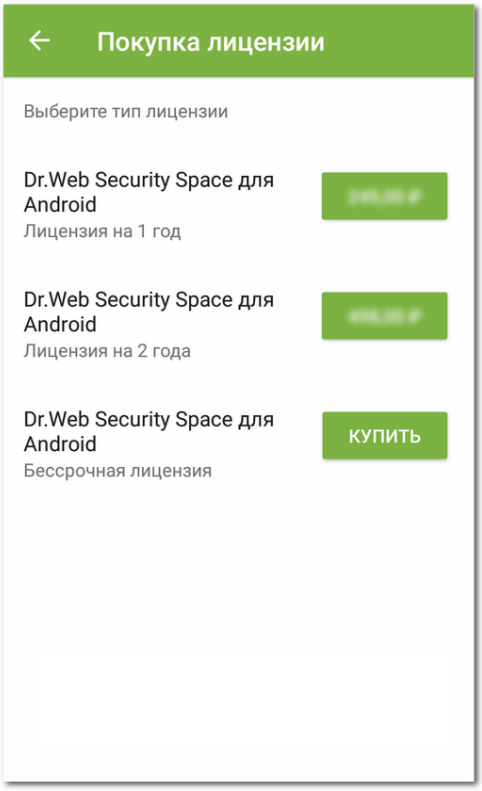

Рисунок 3. Покупка лицензии

Если приложение установлено с сайта компании «Доктор Веб»

Если вы установили Dr.Web с сайта компании, вы можете приобрести лицензию следующим образом:

1. Запустите приложение.
2. Перейдите на экран Лицензия.
3. Выберите вариант **Купить лицензию**. Будет открыта страница интернет-магазина «Доктор Веб».

   Вы также можете зайти в интернет-магазин, перейдя по ссылке https://estore.drweb.com/mobile/.
4. Выберите срок действия лицензии и количество защищаемых устройств.
5. Нажмите **Купить**.
6. Заполните форму покупки и нажмите **Сделать заказ**.

   После оформления заказа серийный номер будет выслан на указанный вами адрес электронной почты. Кроме того, вы можете выбрать вариант получения серийного номера в виде SMS-сообщения на указанный номер мобильного телефона.
7. Далее вам необходимо зарегистрировать серийный номер или скопировать ключевой файл на мобильное устройство.

5.4. Активация лицензии

Активация лицензии требуется, если вы установили приложение с сайта компании «Доктор Веб». Вам также может понадобиться активация, если вы уже являетесь владельцем действующей лицензии на программные продукты Dr.Web, в состав которой входит Dr.Web Security Space для Android.

Чтобы активировать лицензию, вам нужно зарегистрировать серийный номер. Это можно сделать двумя способами:

- Зарегистрировать серийный номер в приложении. В этом случае на устройстве с установленным приложением должно быть активное интернет-соединение.
- Зарегистрировать серийный номер на сайте «Доктор Веб». Если на устройстве с установленным приложением нет интернет-соединения, вы можете зарегистрировать серийный номер с помощью компьютера или другого устройства с активным интернет-соединением. В этом случае вам будет выслан лицензионный ключевой файл, который нужно скопировать на устройство, чтобы активировать лицензию.

Регистрация серийного номера и активация лицензии в приложении

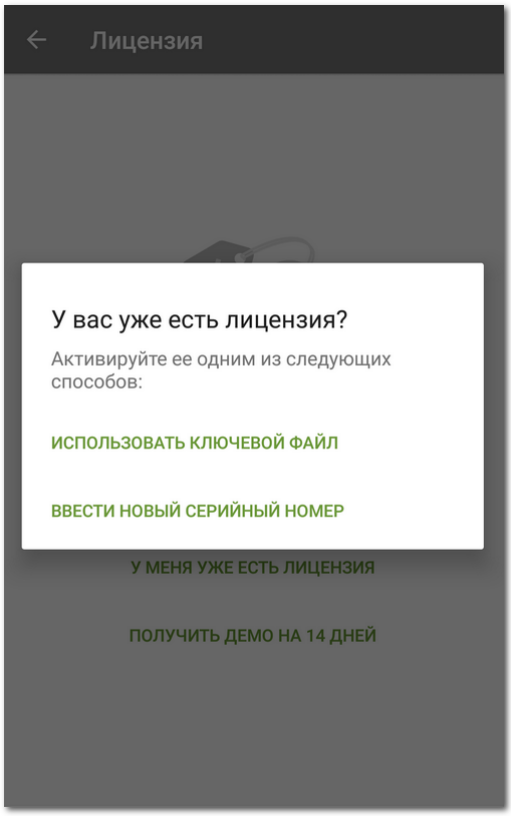

Рисунок 4. Активация лицензии

Чтобы зарегистрировать серийный номер и активировать лицензию в приложении, выполните следующие действия:

1. Запустите приложение.
2. Перейдите на экран Лицензия.
3. Выберите пункт **У меня уже есть лицензия**.
4. В следующем окне (см. Рисунок 4) нажмите **Ввести новый серийный номер**.
5. На экране **Активация лицензии** (см. Рисунок 5) введите серийный номер, который вы получили после покупки.
6. Нажмите кнопку **Активировать**.

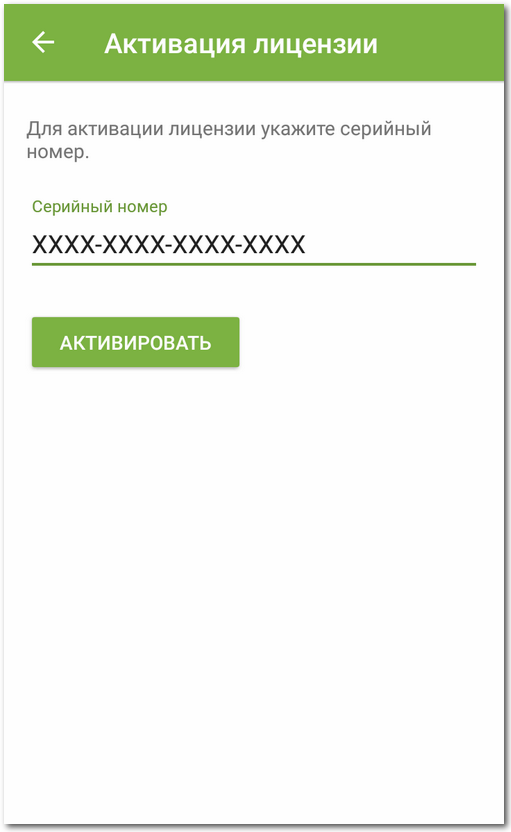

Рисунок 5. Регистрация серийного номера

7. Укажите ваши личные данные:
   - Имя и фамилию.
   - Страну.
   - Действительный адрес электронной почты.
8. По желанию установите флажок **Получать новости по электронной почте**.
9. Нажмите кнопку **Активировать**.

Откроется главный экран приложения. Внизу экрана появится сообщение о том, что лицензия активирована.

Регистрация серийного номера на сайте

Чтобы зарегистрировать серийный номер и получить ключевой файл, выполните следующие действия:

1. Зайдите на сайт https://products.drweb.com/register/.
2. Введите регистрационный серийный номер, полученный при покупке Dr.Web.
3. Заполните форму со сведениями о покупателе.
4. Ключевой файл с расширением .key будет выслан по указанному вами адресу электронной почты в виде ZIP-архива.

Использование ключевого файла

1. Скопируйте ключевой файл в папку во внутренней памяти устройства.

   Вы можете распаковать архив и скопировать только файл с расширением .key или перенести на устройство весь ZIP-архив целиком.
2. На экране Лицензия выберите пункт **У меня уже есть лицензия**.
3. Выберите пункт **Использовать ключевой файл** (см. Рисунок 4).
4. Найдите папку, в которой лежит ключевой файл или ZIP-архив с файлом и выберите его.

Ключевой файл будет установлен и готов к использованию. Откроется главный экран приложения. Внизу экрана появится сообщение о том, что лицензия активирована.

Ключевой файл программ Dr.Web Security Space или Антивирус Dr.Web может быть использован для работы Dr.Web, если он поддерживает использование компонентов DrWebGUI и Update.

Чтобы проверить возможность использования ключевого файла:

1. Откройте ключевой файл в текстовом редакторе (например, в «Блокноте»).
2. Проверьте, присутствуют ли компоненты DrWebGUI и Update в списке значений параметра Applications в группе [Key]: если эти компоненты есть в списке, ключевой файл может быть использован для работы Dr.Web.

Ключевой файл имеет формат, защищенный от редактирования. Редактирование файла делает его недействительным. Чтобы избежать порчи ключевого файла, не следует сохранять его при закрытии текстового редактора.

5.5. Восстановление лицензии

Восстановление лицензии может понадобиться, если вы переустановили приложение или хотите использовать Dr.Web на другом устройстве.

Если приложение установлено из Google Play

1. Запустите приложение.
2. Перейдите на экран Лицензия.
3. На экране **Лицензия** выберите **У меня уже есть лицензия**.
4. Нажмите **Восстановить покупку в Google Play**.
5. Укажите адрес электронной почты, который вы использовали для регистрации лицензии, и ваши личные данные.

   Лицензия, зарегистрированная для указанного адреса электронной почты, будет активирована автоматически.

Если приложение установлено с сайта «Доктор Веб»

Если вы приобрели приложение на сайте компании, вы можете восстановить лицензию двумя способами:

- Ввести новый серийный номер.
- Использовать ключевой файл.

Восстановление демонстрационной лицензии

Чтобы восстановить демонстрационную лицензию, выполните следующие действия:

1. Запустите приложение.
2. Перейдите на экран Лицензия.
3. На экране **Лицензия** выберите **Получить демо на 14 дней**.
4. Укажите адрес электронной почты, который вы использовали во время активации демонстрационной лицензии, и ваши личные данные.
5. Нажмите **Получить демо**.

5.6. Продление лицензии

Чтобы просмотреть информацию об используемой лицензии:

- **На Android**. На главном экране (см. Рисунок 7) нажмите **Меню** и выберите пункт **Лицензия**.
- **На Android TV**. На главном экране перейдите в раздел **Разное** -> **Лицензия**.

На экране **Лицензия** вы можете просмотреть серийный номер, имя владельца лицензии и даты начала и окончания срока действия лицензии.

Если Dr.Web работает в режиме централизованной защиты в рамках предоставления антивирусной услуги Dr.Web AV-Desk, на экране **Лицензия** также показывается дата окончания подписки на услугу.

Продление лицензии

Чтобы продлить лицензию Dr.Web, вам не нужно переустанавливать или прерывать работу приложения.

Вы можете продлить лицензию одним из следующих способов:

- Если у вас уже есть новый серийный номер, просто зарегистрируйте его.
- Если вы приобрели вашу текущую лицензию на сайте «Доктор Веб», вы можете:
  - Купить лицензию.
  - Использовать ключевой файл.
  - Продлить лицензию на вашей персональной странице на сайте «Доктор Веб».

    Чтобы перейти на эту страницу, нажмите **Меню** , выберите пункт **О программе** и перейдите по ссылке **Мой Dr.Web**.
- Если вы приобрели вашу текущую лицензию в Google Play:
  1. На главном экране нажмите **Меню** и выберите пункт **Лицензия**.
  2. На экране **Лицензия** (см. Рисунок 6) нажмите **Продлить лицензию из Google Play**.

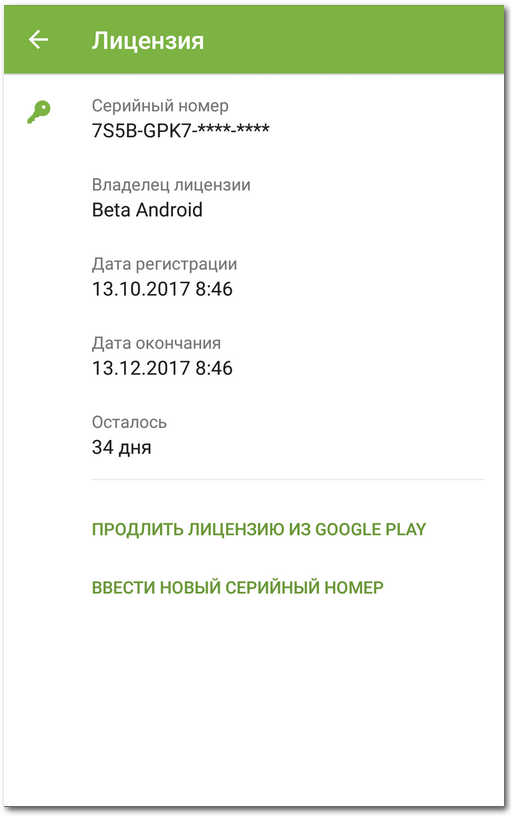

Рисунок 6. Продление лицензии

  3. На экране **Покупка лицензии** (см. Рисунок 3) выберите один из следующих вариантов:
     - **Лицензия на 1 год**

- **Лицензия на 2 года**
- **Бессрочная лицензия**

При выборе любого из вариантов откроется экран покупки лицензии. Через некоторое время после совершения оплаты лицензия активируется автоматически. Если из-за возможных технических сбоев при покупке загрузка ключевого файла не началась, обратитесь в службу технической поддержки: https://support.drweb.com/.

5.7. Настройка уведомлений об окончании срока действия лицензии

На мобильных устройствах вы можете включить и отключить использование уведомлений о скором окончании срока действия лицензии (кроме версии приложения с бессрочной лицензией Dr.Web Security Space Life). Для этого:

1. На главном экране нажмите **Меню** и выберите **Настройки** (см. Настройки).
2. Выберите пункт **Лицензия**.
3. Снимите флажок **Уведомления**, чтобы отключить уведомления. Чтобы получать уведомления, установите флажок.

6. Приступая к работе

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

6.1. 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.

Вы можете в любой момент отказаться от отправки статистики в настройках приложения, сняв флажок **Отправка статистики** в разделе **Общие настройки**.

Если Dr.Web был установлен при помощи установщика, предоставленного администратором антивирусной сети компании, Лицензионное соглашение открыто не будет.

6.2. 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 попросит предоставить приложению доступ к данным на устройстве. Разрешения требуются и компонентам приложения. Для каждого компонента приложение запрашивает свой набор разрешений при первом запуске. Если вы не предоставите приложению необходимые разрешения, оно не сможет работать.

- Dr.Web запрашивает доступ к фото, мультимедиа и файлам на устройстве при первом запуске приложения. Это разрешение необходимо для работы приложения.
- Фильтр звонков и SMS запрашивает разрешения:
  - Осуществлять телефонные звонки и управлять ими.
  - Отправлять и просматривать SMS-сообщения.
  - Доступ к контактам.
- URL-фильтр запрашивает доступ к специальным возможностям Android для работы в поддерживаемых браузерах.

- Антивор Dr.Web запрашивает:
  - Доступ к телефонным звонкам и управлению ими.
  - Возможность отправлять и просматривать SMS-сообщения.
  - Доступ к контактам.
  - Доступ к данным о местоположении устройства.
  - Доступ к специальным возможностям Android.
  - Разрешение назначить Dr.Web администратором устройства.
- Брандмауэр Dr.Web запрашивает разрешение подключиться к сети VPN для отслеживания трафика.
- Dr.Web на Android TV запрашивает:
  - Доступ к контактам.
  - Доступ к фото, мультимедиа, и файлам на устройстве.

Если вы отклоните один или несколько запросов 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 для каждого пункта вправо.

Просмотр списка необходимых разрешений

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

6.3. Интерфейс

Главный экран

На главном экране (см. Рисунок 7) располагается список основных компонентов Dr.Web.

Меню в правом верхнем углу главного экрана позволяет:

- Открыть экран с информацией о лицензии.
- Посмотреть статистику.
- Посмотреть список файлов, перемещенных в карантин.
- Запустить обновление вирусных баз вручную.
- Перейти к настройкам приложения.

- Открыть справку.
- Перейти к управлению учетной записью.
- Открыть экран с информацией о приложении.

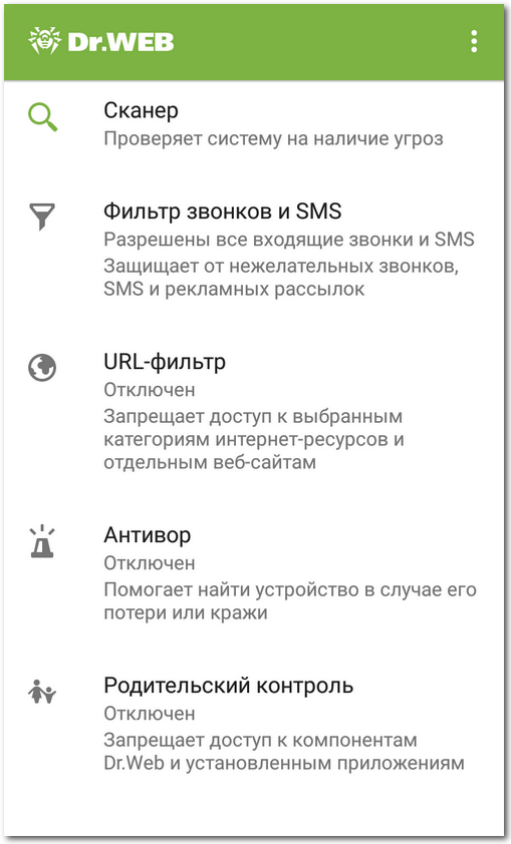

Рисунок 7. Главный экран приложения

Панель состояния

В верхней части главного экрана приложения находится панель состояния с индикатором, который отображает текущее состояние защиты устройства (см. Рисунок 8).

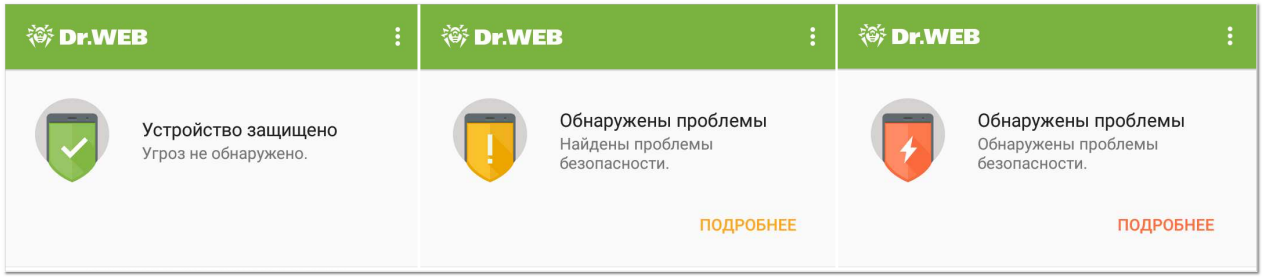

Рисунок 8. Панель состояния

- Индикатор зеленого цвета означает, что устройство защищено. Дополнительных действий не требуется.

- Индикатор желтого цвета означает, что Dr.Web обнаружил проблемы безопасности, отсутствие лицензии и т.д. Чтобы узнать больше о найденных угрозах и устранить их, нажмите **Подробнее** на панели.
- Индикатор красного цвета означает, что Dr.Web обнаружил угрозы. Чтобы обезвредить угрозы, нажмите **Подробнее**.

Если приложение обнаружило несколько событий, требующих внимания пользователя, кнопка **Подробнее** откроет раздел **События**, в котором будут отображены все важные сообщения.

6.4. Панель уведомлений

Панель уведомлений Dr.Web (см. Рисунок 9) используется для быстрого доступа к основным функциям приложения. Кроме того, она оперативно отображает предупреждения о найденных угрозах.

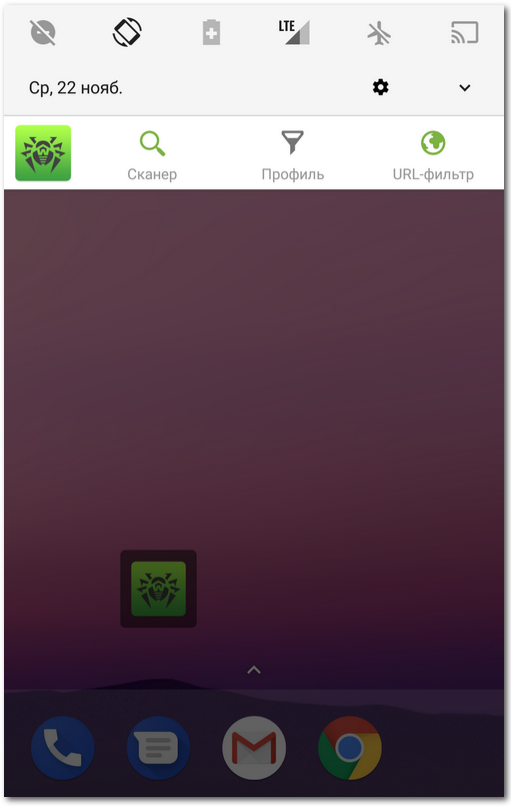

Рисунок 9. Панель уведомлений

На устройствах, работающих на платформе Android TV, панель уведомлений недоступна.

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 (см. раздел Общие настройки).

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

Если ваше устройство не поддерживает использование SIM-карт, вместо опции **Профиль** на панели уведомлений появится опция **Загрузки**, позволяющая запустить проверку объектов, загруженных на устройство.

Если Dr.Web работает в режиме централизованной защиты и при этом у вас отсутствуют права на изменение настроек фильтрации звонков и сообщений и/или URL-фильтра, опции **Профиль** и/или **URL-фильтр** будут недоступны на панели уведомлений.

С помощью панели уведомлений можно выполнить следующие действия:

- Перейти на экран Dr.Web. Для этого нажмите на значок Dr.Web.
- Запустить быструю, полную или выборочную проверку с помощью опции **Сканер**.
- Выбрать профиль фильтрации звонков и сообщений с помощью опции **Профиль**.
- Выбрать категории веб-сайтов, к которым вы хотите ограничить доступ, с помощью опции **URL-фильтр**.

6.5. Виджет

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

На устройствах, работающих на платформе Android TV, виджет недоступен.

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 10).

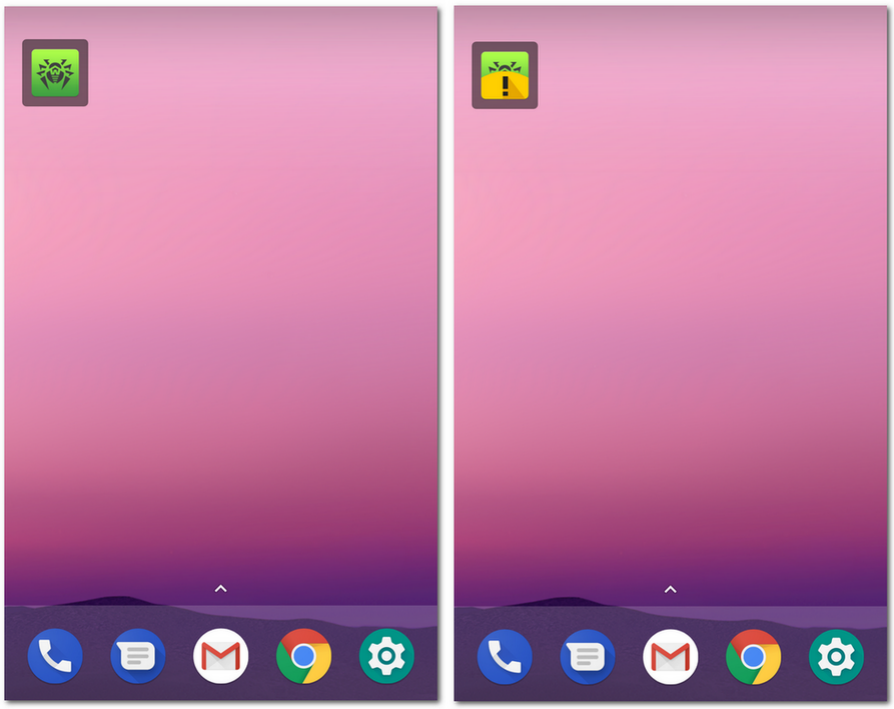

Рисунок 10. Виджет Dr.Web

6.6. Мой Dr.Web

Онлайн-сервис Мой Dr.Web – это ваша персональная страница на сайте компании «Доктор Веб». На этой странице вы можете получить информацию о вашей лицензии (срок действия, серийный номер), продлить срок ее действия, просмотреть дату и время последнего обновления, а также количество записей в вирусных базах, ознакомиться с новостями и специальными предложениями, задать вопрос службе поддержки и многое другое.

Чтобы открыть онлайн-сервис Мой Dr.Web:

1. На главном экране нажмите **Меню** и выберите пункт **О программе**.
2. Нажмите **Мой Dr.Web**.

7. Учетная запись Dr.Web

Учетная запись Dr.Web позволяет защитить паролем доступ к компонентам Dr.Web и настройкам устройства.

По умолчанию пароль от учетной записи потребуется:

- Для доступа к компонентам Dr.Web:
  - Антивор Dr.Web.
  - Родительский контроль.
- Если у вас включен Антивор Dr.Web, для доступа к опциям приложения:
  - **Сброс настроек**.
  - **Резервная копия**.
  - **Администрирование**.
- Если у вас включен Антивор Dr.Web, для доступа к настройкам на вашем устройстве:
  - **Настройки** - > **Приложения** или **Диспетчер приложений** - > **Dr.Web Security Space** (на Android 6.0 и выше).
  - **Настройки** - > **Специальные возможности** (на Android 6.0 и выше).
  - **Настройки** - > **Безопасность** - > **Местоположение** (на Android 6.0 и выше).
  - **Настройки** - > **Безопасность** - > **Администраторы устройства**. Если вы исключите Dr.Web из списка администраторов устройства, устройство будет заблокировано. Для разблокировки потребуется ввести пароль от учетной записи.

Вы можете защитить паролем доступ к Фильтру звонков и SMS, URL-фильтру, а также к настройкам приложения (см. раздел Родительский контроль).

Создание учетной записи

Чтобы создать учетную запись Dr.Web:

1. На главном экране приложения нажмите **Меню** в правом верхнем углу.
2. Выберите пункт **Учетная запись**.
3. На экране **Учетная запись** укажите адрес электронной почты.

   Адрес необходим, чтобы восстановить забытый пароль от учетной записи. Укажите действительный адрес электронной почты и нажмите кнопку **Продолжить**.

   Обратите внимание, что после регистрации учетной записи адрес электронной почты нельзя будет изменить. Если вы захотите использовать другой адрес, вам понадобится удалить учетную запись и заново зарегистрировать ее на новый адрес.

Для регистрации адреса электронной почты требуется активное интернет-соединение.

4. Придумайте пароль. Пароль должен содержать не менее 4 символов.
5. Повторите пароль и нажмите **Продолжить**.

   На следующем экране вы увидите подтверждение того, что учетная запись успешно создана и зарегистрирована.
6. Нажмите **Продолжить**.

Управление учетной записью

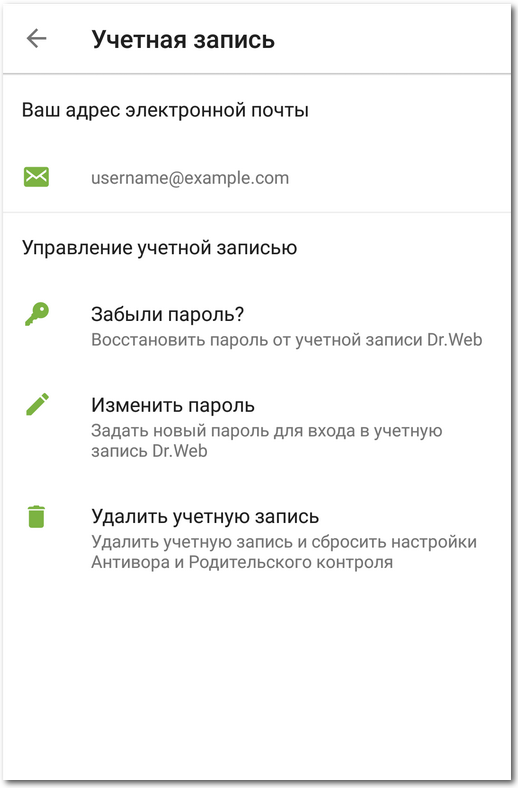

Рисунок 11. Учетная запись

На экране **Учетная запись** в разделе **Управление учетной записью** (см. Рисунок 11) вы можете выполнить следующие действия:

- Если забыли пароль, задать новый пароль.
- Изменить пароль.
- Удалить учетную запись.

При удалении учетной записи компоненты Антивор и Родительский контроль будут отключены, их настройки будут сброшены.

8. Компоненты Dr.Web

На главном экране приложения находится список компонентов и их текущее состояние (включен или отключен):

- Сканер проверяет систему по запросу пользователя. Возможны 3 типа проверки: быстрая, полная и выборочная.
- Фильтр звонков и SMS блокирует нежелательные звонки и SMS-сообщения.
- URL-фильтр ограничивает доступ пользователя к ресурсам сети Интернет.
- Антивор помогает найти и заблокировать устройство в случае его потери или кражи.
- Родительский контроль задает ограничения на использование устройства.
- Брандмауэр контролирует интернет-подключения и передачу данных по сети.
- Аудитор безопасности выполняет анализ системы и устраняет обнаруженные проблемы безопасности и уязвимости.

На устройствах, для которых не предусмотрено использование SIM-карт (отсутствует слот для SIM-карт), **Фильтр звонков и SMS** и **Антивор Dr.Web** недоступны.

8.1. Антивирусная защита

Компонент SplDer 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.

8.1.1. SplDer Guard: постоянная антивирусная защита

Включение постоянной защиты

При первом запуске Dr.Web постоянная защита автоматически включается после принятия Лицензионного соглашения. Чтобы отключить или снова включить SplDer Guard, выберите **SplDer Guard** на экране Настройки. SplDer Guard работает независимо от того, запущено приложение или нет.

В режиме централизованной защиты настройки компонента SplDer Guard могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг.

При обнаружении угроз безопасности в строке состояния 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.

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 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, обнаружение угроз безопасности и результаты проверки памяти устройства и устанавливаемых приложений. Статистика SpIDer Guard отображается в разделе **Действия** на вкладке **Статистика** и отсортирована по дате (см. раздел Статистика).

Проверка работы SpIDer Guard

Вы можете проверить работу 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 появится значок  (см. Рисунок 12).

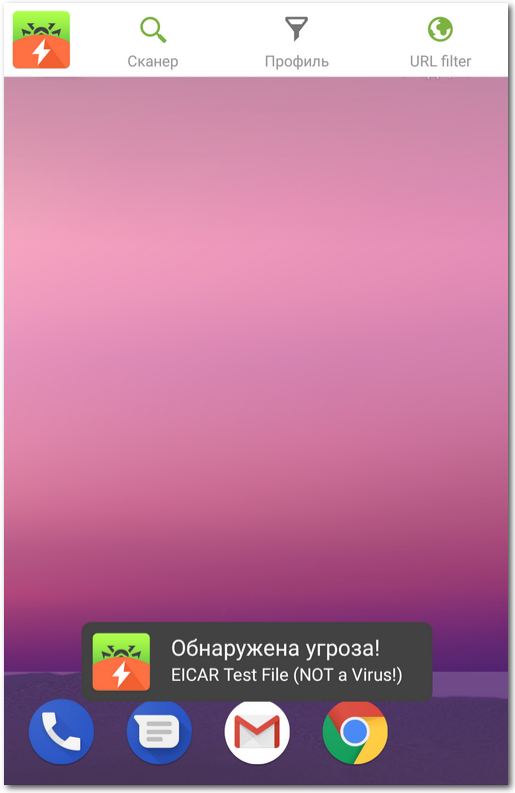

Рисунок 12. Обнаружение тестового файла EICAR

8.1.2. 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.

> В режиме централизованной защиты настройки Сканера Dr.Web могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг. Проверка может запускаться по расписанию, заданному на сервере централизованной защиты.

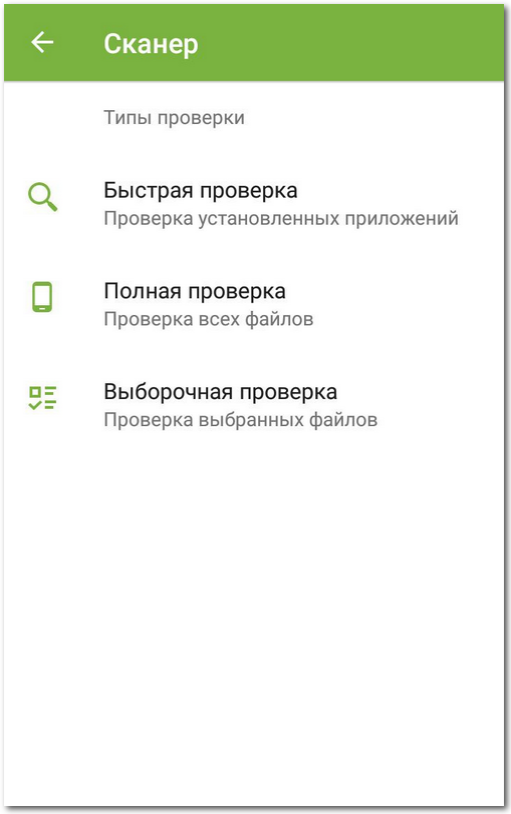

Рисунок 13. Сканер Dr.Web

Проверка

Чтобы проверить систему, на главном экране Dr. Web выберите пункт **Сканер**, затем на экране **Сканер** (см. Рисунок 13) 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 14). Чтобы выбрать все объекты, установите флажок в правом верхнем углу экрана. Затем нажмите **Проверить**.

Если на вашем устройстве открыт root-доступ, вы можете выбрать для проверки папки `/sbin` и `/data`, расположенные в корневой папке.

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.

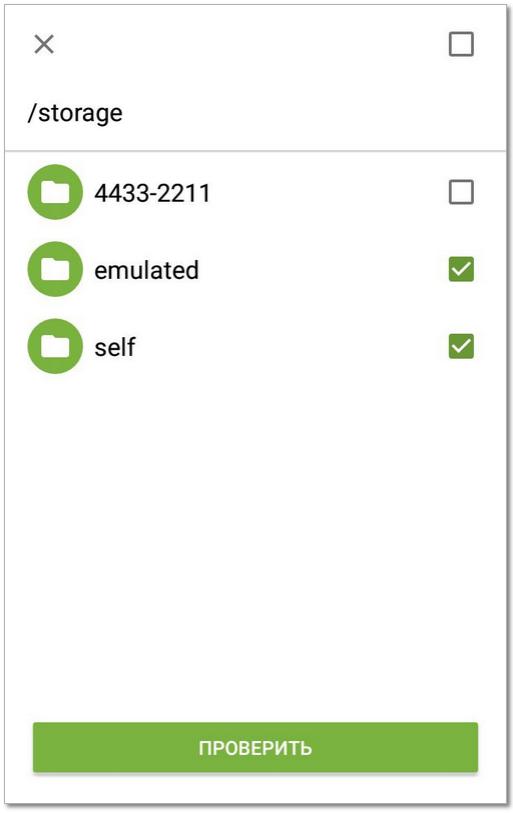

Рисунок 14. Выборочная проверка

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 14), 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).

8.1.3. 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.

Обезвреживание угроз, использующих уязвимость Stagefright

Обезвреживание угроз, использующих уязвимость Stagefright осуществляется Брандмауэром Dr.Web. Включите его, чтобы обеспечить защиту от Stagefright эксплойтов.

Уязвимость Stagefright позволяет взломать устройство с помощью мультимедиа файла с вредоносным кодом.

Брандмауэр Dr.Web анализирует содержимое мультимедиа файлов, которые вы загружаете на устройство, в реальном времени. Если Dr.Web обнаружит вредоносный код в файле, который вы скачиваете на устройство:

- Загрузка файла будет прервана.
- В нижней части экрана вы увидите уведомление со значком  . Имя обнаруженной угрозы будет иметь постфикс <*имя.угрозы*>.Stagefright.
- Запись об обнаруженной угрозе будет занесена в статистику работы приложения.

8.1.4. 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 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 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**.

8.1.5. Обработка приложений-блокировщиков устройства

Dr.Web 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 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 SplDer 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 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.

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.

8.2. Фильтр звонков и SMS

Dr.Web фильтрует SMS-сообщения и телефонные звонки, позволяя блокировать нежелательные сообщения и звонки, например, рекламные рассылки, а также звонки и сообщения с неизвестных номеров.

Вы можете выбрать режим фильтрации звонков и сообщений из предопределенных профилей или создать пользовательский профиль и задать собственные настройки фильтрации.

Вы в любой момент можете посмотреть список заблокированных звонков и SMS-сообщений.

Фильтр звонков и SMS может работать некорректно на устройствах с двумя SIM-картами.

SMS-фильтр может работать некорректно из-за технических ограничений Android.

В режиме централизованной защиты настройки фильтрации могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг.

Включение Фильтра звонков и SMS

При первом включении Фильтр звонков и SMS может запросить следующие разрешения:

- Доступ к контактам.
- Осуществлять телефонные звонки и управлять ими.
- Отправлять и просматривать SMS-сообщения.

Нажмите **Разрешить** в каждом окне.

Кроме того, на устройствах с Android 7.0 или более поздними версиями установите Dr.Web приложением для звонков по умолчанию:

1. В окне **Настройка доступа** нажмите **Предоставить доступ**. Откроется экран настроек устройства **Приложения по умолчанию**.
2. На экране **Приложения по умолчанию** нажмите **Приложение для звонков**.
3. На экране **Приложение для звонков** выберите Dr.Web.

Без необходимых разрешений компонент не будет работать.

8.2.1. Режимы фильтрации

Фильтрация звонков и SMS-сообщений может осуществляться в одном из следующих режимов:

- **Принимать все** – принимать все входящие звонки и SMS-сообщения. Фильтрация отключена.
- **Блокировать все** – блокировать все входящие звонки и SMS-сообщения.
- **Список контактов** – принимать входящие звонки и SMS-сообщения только с номеров из списка контактов.
- **Черный список** – блокировать звонки и SMS-сообщения с номеров, внесенных в черный список.

Кроме того, вы можете выбрать пользовательский режим фильтрации, который определяется настраиваемым профилем. Dr.Web предусматривает создание неограниченного числа профилей, для каждого из которых можно сформировать список номеров и определить действие (принимать/блокировать) для звонков и сообщений с номеров из этого списка.

При выборе пользовательского режима фильтрации будут дополнительно блокироваться контакты из черного списка.

8.2.2. Черный список

В черный список могут быть добавлены номера, с которых вы не хотите получать входящие звонки и SMS-сообщения. Звонки и SMS-сообщения с номеров из черного списка блокируются как при выборе режима фильтрации **Черный список**, так и при выборе любого пользовательского профиля фильтрации.

Звонки и SMS с номеров, добавленных в черный список, могут приниматься, если:

- Эти номера входят в список пользовательского профиля и для них выбрано действие **Разрешить только контакты из списка**.
- Включен режим **Принимать все**.

Создание черного списка

Чтобы создать черный список, выполните следующие действия:

1. Выберите раздел **Фильтр звонков и SMS** на главном экране приложения, затем в появившемся меню выберите **Настроить**.
2. На вкладке **Черный список** нажмите на значок  .

   Для настройки черного списка вы можете использовать:

   - Список контактов.
   - Журналы звонков и сообщений.
   - Ручной ввод телефонных номеров и информации о них.
   - Ключевые слова.

   В черный список можно добавить телефонные номера по одному или добавить несколько телефонных номеров сразу.
3. Чтобы добавить выбранные номера в список, нажмите **Добавить контакт**.
4. Чтобы блокировать все SMS-сообщения по ключевым словам, выберите пункт **Ключевое слово**. Введите ключевое слово и нажмите **Сохранить**.

   Приложение будет искать в сообщениях все слово или словосочетание, которое вы добавите. Если вы хотите, чтобы приложение блокировало сообщения, в которых встречается несколько слов, не стоящих рядом, добавьте их по одному.

Редактирование контакта в черном списке

По умолчанию для каждого контакта, добавленного в черный список, блокируются звонки и SMS-сообщения. При желании вы можете изменить эти настройки. Вы также можете изменить имя и номер телефона.

Чтобы отредактировать контакт:

1. Откройте вкладку **Черный список** и нажмите на контакт.
2. В появившемся окне внесите необходимые изменения и нажмите **Сохранить**.

Очистка черного списка

Чтобы удалить один номер из черного списка, смахните его влево.

Чтобы удалить несколько номеров из списка, нажмите и удерживайте сначала один контакт. После вибросигнала выберите другие контакты, которые хотите удалить. Затем нажмите на значок в правом верхнем углу.

Если вы случайно удалите не тот контакт из списка, вы можете отменить удаление, нажав на опцию **Отменить**.

Чтобы удалить все контакты из черного списка, на вкладке **Черный список** нажмите **Меню** и выберите пункт **Очистить список**.

8.2.3. Профили фильтрации

Dr.Web позволяет создавать пользовательские профили фильтрации звонков и сообщений.

Создание нового профиля

1. В списке доступных режимов фильтрации выберите **Настроить**.
2. Откройте вкладку **Профили** и нажмите на значок .
3. Укажите имя профиля.
4. Выберите действие для входящих звонков и сообщений с номеров из списка данного профиля:
   - **Разрешить только контакты из списка** – принимать звонки и сообщения только с номеров, включенных в список данного профиля. Звонки и SMS от включенных в данный список номеров будут приниматься даже в том случае, если эти номера внесены в черный список.
   - **Запретить контакты из списка** – блокировать звонки и сообщения с номеров, включенных в список данного профиля.
5. Нажмите на значок , чтобы сформировать список контактов. Вы можете выбирать контакты и телефонные номера следующими способами:
   - Из списка контактов.
   - Из журналов звонков и сообщений.
   - Ввести телефонные номера и информацию о них вручную.

   Для поиска контактов в списке контактов и в журналах звонков и сообщений нажмите на значок **Поиск**. В каждом случае вы можете добавить в список один или несколько номеров.

   Чтобы добавить выбранные номера в список, нажмите кнопку **Добавить контакт**.

Количество контактов в списке профиля отображается в скобках справа от его имени.

Список контактов профиля не может быть пустым.

6. Чтобы изменить данные контакта из списка, нажмите на него. В открывшемся окне внесите изменения и нажмите кнопку **Сохранить**.

Возможность редактирования данных не предусмотрена для контактов, добавленных из телефонной книги, а также для скрытых номеров.

7. Чтобы удалить контакт из списка профиля, смахните его влево.

   Чтобы удалить несколько номеров из списка, нажмите и удерживайте сначала один контакт. После вибросигнала выберите другие контакты, которые хотите удалить. Затем нажмите на значок  в правом верхнем углу.

   Если вы случайно удалите не тот контакт из списка, вы можете отменить удаление, нажав на опцию **Отменить**.

При удалении контактов из пользовательского профиля они не удаляются из списка контактов на устройстве.

Редактирование профиля

1. В списке доступных режимов фильтрации выберите **Настроить**.
2. Откройте вкладку **Профили**.
3. Нажмите на профиль, который нужно отредактировать.
4. Внесите изменения.
5. Нажмите кнопку **Сохранить**.

Удаление профиля

1. В списке доступных режимов фильтрации выберите **Настроить**.
2. Откройте вкладку **Профили**.
3. Смахните название профиля влево.

Если вы случайно удалите не тот профиль из списка, вы можете отменить удаление, нажав на опцию **Отменить**.

Чтобы удалить несколько профилей из списка, нажмите и удерживайте сначала один профиль. После вибросигнала выберите другие профили, которые хотите удалить. Затем нажмите на значок  в правом верхнем углу.

8.2.4. Просмотр заблокированных звонков и SMS

Вы можете посмотреть список заблокированных звонков и SMS-сообщений.

Для этого откройте раздел **Фильтр звонков и SMS** на главном экране приложения, затем в появившемся меню профиля выберите **Заблокированные звонки** или **Заблокированные SMS**.

Кроме того, если компонент заблокировал звонки или SMS-сообщения, информация об этом появится на панели состояния. Чтобы посмотреть информацию о заблокированном звонке или сообщении, на панели состояния нажмите **Подробнее**.

Для каждого заблокированного звонка или SMS-сообщения доступна следующая информация:

- Дата и время поступления звонка или сообщения.
- Номер и имя звонившего или отправившего сообщение.
- Текст заблокированного SMS-сообщения.

Действия над заблокированными звонками и SMS

- Чтобы позвонить:
  1. Нажмите на номер в списке заблокированных звонков или сообщений.
  2. Нажмите **Позвонить**.
- Чтобы отправить SMS-сообщение:
  1. Нажмите на номер в списке заблокированных звонков или сообщений.
  2. Нажмите **Отправить SMS**.
- Чтобы удалить звонок или сообщение из списка, смахните его влево.
- Чтобы удалить все звонки или сообщения:
  1. Нажмите **Меню** в правом верхнем углу экрана.
  2. Нажмите **Очистить список**.

8.3. URL-фильтр

Доступ к веб-сайтам контролируется URL-фильтром. URL-фильтр позволяет оградить пользователя от посещения нежелательных интернет-ресурсов. Чтобы настроить URL-фильтр, вы можете выбрать отдельные веб-сайты или категории веб-сайтов.

При попытке открыть веб-сайт из списка запрещенных, вы увидите страницу блокировки.

URL-фильтр поддерживает встроенный браузер Android, а также браузеры Google Chrome, Яндекс.Браузер, Microsoft Edge, Firefox, Opera, Adblock Browser, Dolphin Browser, Спутник и Boat Browser.

Включение URL-фильтра

На главном экране приложения выберите опцию **URL-фильтр** (см. Рисунок 15).

URL-фильтр может запросить доступ к специальным возможностям Android. Доступ необходим для корректной работы URL-фильтра в установленных браузерах. Без доступа URL-фильтр не сможет работать.

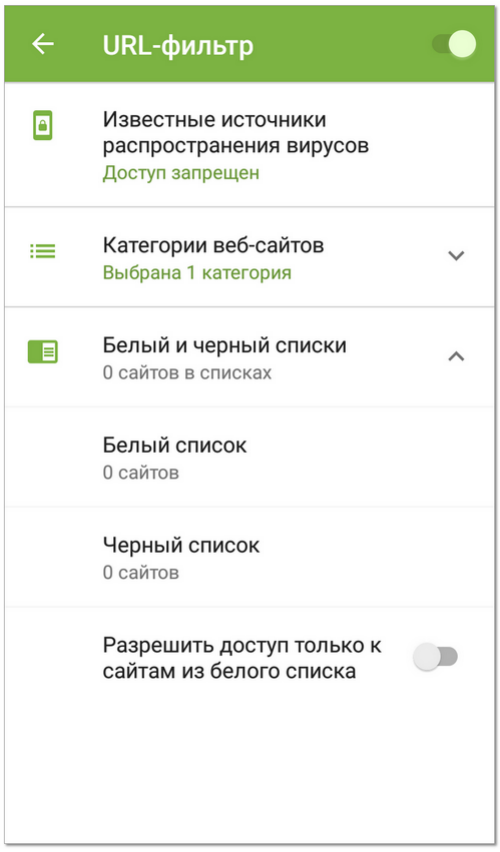

Рисунок 15. Экран URL-фильтр

Категории веб-сайтов

Dr.Web позволяет выбрать определенные категории веб-сайтов, доступ к которым должен быть запрещен. Раскройте список **Категории веб-сайтов** и выберите нужные категории из списка:

- Нерекомендуемые сайты;
- Сайты для взрослых;

Выбирая эту категорию, вы включаете *семейный поиск* в поисковых системах Google, Yandex, Bing, Yahoo и Rambler. Это значит, что из результатов поиска будут полностью исключены материалы «для взрослых».

- Насилие;
- Оружие;
- Азартные игры;
- Наркотики;
- Нецензурная лексика;
- Онлайн-игры;
- Терроризм;
- Электронная почта;
- Социальные сети;
- Чаты;
- URL, добавленные по обращению правообладателя;
- Анонимайзеры.

По умолчанию URL-фильтр запрещает доступ к сайтам, известным как источники распространения вирусов.

Белый и черный списки

Вы можете составить списки веб-сайтов, доступ к которым разрешается или блокируется вне зависимости от остальных настроек URL-фильтра.

По умолчанию списки пусты. Чтобы добавить сайт в белый или черный список:

1. В окне URL-фильтра раскройте раздел **Белый и черный списки**.
2. Выберите список, в который вы хотите добавить адрес.
3. Нажмите на значок  в правом нижнем углу окна.
4. Укажите URL веб-сайта в одном из перечисленных форматов:
   - example.com
   - http://example.com
   - https://www.example.com
   - www.example.com

   

   Вы можете добавить только конкретные URL веб-сайтов, добавление масок или ключевых слов не поддерживается.
5. Нажмите **Добавить URL**.

Если вы попытаетесь добавить URL, который уже есть в противоположном списке, вам будет предложено переместить его.

Разрешить доступ только к сайтам из белого списка

Включите эту опцию, чтобы просматривать только те сайты, которые вы занесли в **Белый список**. Доступ ко всем остальным сайтам будет запрещен.

При работе в режиме централизованной защиты настройки URL-фильтра могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг.

8.4. Антивор Dr.Web

Антивор Dr.Web блокирует ваше устройство и определяет его местоположение в случае потери или кражи. Вы можете управлять Антивором дистанционно с помощью специальных SMS-команд.

SMS-команды можно отправлять с любого номера телефона, либо с номеров, которые вы добавили в список друзей в Антиворе.

Список друзей в Антиворе – это список доверенных номеров, который вы составляете во время первоначальной настройки. С этих номеров можно отправлять SMS-команды для управления Антивором на вашем устройстве без пароля.

Если отправить команду с номера не из списка друзей, в тексте сообщения вместе с командой должен быть указан ваш пароль от учетной записи Dr.Web. Таким образом, если ваше устройство будет украдено, посторонний не сможет его разблокировать.

Для управления всеми функциями Антивора Dr.Web используется пароль от учетной записи Dr.Web. Пароль потребуется:

- Для разблокировки устройства, если оно заблокировано Антивором Dr.Web.
- Для доступа к настройкам Антивора Dr.Web.

При работе в режиме централизованной защиты настройки Антивора Dr.Web могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг.

Включение Антивора Dr.Web

При первом включении Антивор запросит у вас доступ к функциям и данным вашего устройства. Без необходимых разрешений компонент не будет работать. Нажмите

Разрешить в каждом окне и предоставьте Антивору доступ к специальным возможностям Android.

Первоначальная настройка Антивора Dr.Web

1. Добавьте от одного до пяти контактов в список друзей. Чтобы включить Антивор, вам нужно добавить как минимум один контакт. Для этого нажмите на значок  в правом нижнем углу экрана.

   Вы можете добавить контакты следующими способами:

   - Указать телефонные номера и информацию о них вручную.
   - Выбрать номера из журналов звонков и сообщений.
   - Выбрать номера из списка контактов.
2. Нажмите кнопку **Продолжить**.
3. Введите текст, который будет отображаться на экране вашего устройства в случае блокировки. Здесь можно указать, как с вами можно связаться и вернуть потерянное устройство.
4. Нажмите кнопку **Готово**.

При переходе на экран настроек Антивора Dr.Web может появиться сообщение о назначении Dr.Web администратором устройства. Назначьте Dr.Web администратором, чтобы обеспечить полноценную работу Антивора Dr.Web.

На этом первоначальная настройка Антивора Dr.Web завершена. В случае успешной регистрации откроется экран настроек Антивора Dr.Web (см. Рисунок 16). Если при регистрации возникли проблемы, на экране появится описание ошибки. При этом активация Антивора Dr.Web на вашем устройстве не произойдет.

Вход в Антивор Dr.Web

При переходе на версию 12 пароль от Антивора Dr.Web автоматически становится паролем от учетной записи Dr.Web.

Чтобы перейти к настройкам Антивора Dr.Web, введите пароль от учетной записи Dr.Web. Если на вашем устройстве еще не настроена учетная запись, вам будет предложено ее создать.

Если вы введете неправильный пароль 10 раз подряд, поле для ввода пароля будет временно заблокировано. Вы увидите, сколько времени осталось до следующей попытки.

Если на вашем устройстве есть сенсор отпечатков пальцев и ваш отпечаток пальца зарегистрирован на устройстве, вы можете открыть настройки без ввода пароля.

Убедитесь, что справа от поля ввода пароля на экране аутентификации Антивора Dr.Web есть значок , затем прикоснитесь к сенсору.

Обратите внимание, что при включенном Родительском контроле нельзя войти в Антивор Dr.Web с помощью отпечатка пальца.

8.4.1. Настройки Антивора Dr.Web

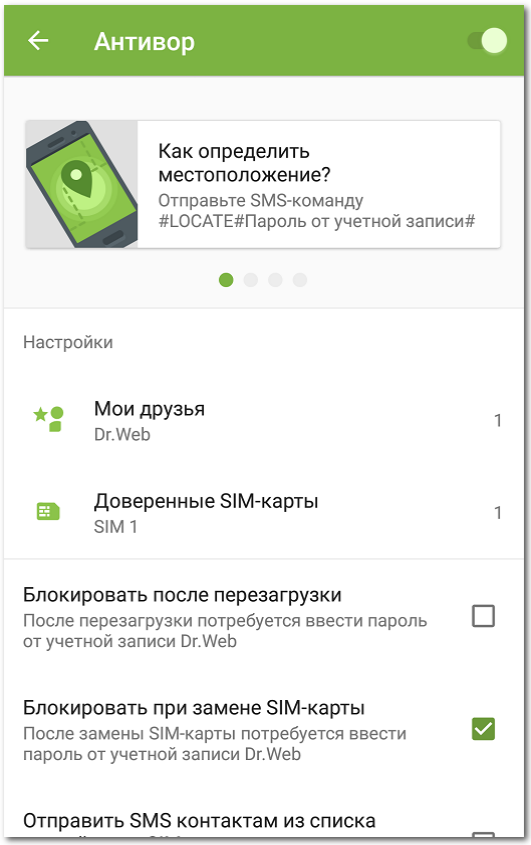

Рисунок 16. Настройки Антивора Dr.Web

Справка

На экране **Антивор** (см. Рисунок 16) можно посмотреть справку – карточки с описанием SMS-команд – и отправить SMS-команду. Нажмите на карточку команды, чтобы перейти на полное описание команды или отправить команду. Листайте карточки вправо, чтобы просмотреть все доступные команды и инструкции к ним (см. раздел Отправка SMS-команд в Антиворе Dr.Web).

Мои друзья

Список друзей в Антиворе – это список доверенных номеров, с которых вы можете отправлять SMS-команды для поиска, блокировки устройства или удаления данных без

указания пароля. В список друзей можно добавить от одного до пяти телефонных номеров. Чтобы просмотреть и отредактировать список друзей, нажмите **Мои друзья**:

- Чтобы добавить друзей, нажмите на значок  в правом нижнем углу экрана. Вы можете выбрать контакты из списка контактов, журнала звонков, журнала SMS или ввести данные вручную.
- Чтобы изменить данные контакта из списка, нажмите на него в списке друзей.

  Внесите необходимые правки и нажмите **Сохранить**.
- Чтобы удалить контакт из списка, смахните его влево.

  Если вы случайно удалите не тот контакт из списка друзей, вы можете отменить удаление, нажав на опцию **Отменить**.

На устройствах с Android 4.4 или более поздними версиями необходимо, чтобы в список друзей был добавлен хотя бы один телефонный номер.

Доверенные SIM-карты

Список доверенных SIM-карт – это список SIM-карт, которые вы используете на устройстве. По умолчанию Антивор настроен блокировать устройство, если обнаружит на нем SIM-карту не из списка доверенных. Даже если ваше устройство украдут и заменят SIM-карту, им нельзя будет воспользоваться. При смене одной доверенной SIM-карты из этого списка на другую Антивор не заблокирует ваше устройство.

Если вы используете сразу две SIM-карты на устройстве с Android 5.1 или более поздними версиями, в список доверенных автоматически добавляются обе SIM-карты. Если на устройстве используется версия Android 5.0 или более ранняя версия, сделать доверенной можно только одну SIM-карту (одновременно добавить обе SIM-карты нельзя).

Добавление новых SIM-карт в список доверенных осуществляется при перезагрузке устройства или при запуске Dr.Web.

Нажмите **Доверенные SIM-карты**, чтобы посмотреть или отредактировать список:

- Чтобы переименовать SIM-карту, нажмите на нее в списке. В открывшемся экране информации о SIM-карте укажите новое имя в поле **Имя** и нажмите **Сохранить**.
- Чтобы удалить SIM-карту из списка доверенных, смахните ее влево.

SIM-карта, используемая в данный момент на вашем устройстве, не может быть удалена из списка доверенных.

Блокировать после перезагрузки

По умолчанию опция отключена.

Если эта опция включена, Антивор Dr.Web будет блокировать устройство после каждой перезагрузки. Чтобы разблокировать устройство, нужно ввести пароль от учетной записи Dr.Web. Без пароля устройство разблокировать нельзя.

Блокировать при замене SIM-карты

По умолчанию опция включена.

Если Антивор Dr.Web обнаружит на устройстве SIM-карту не из списка доверенных, он заблокирует устройство. Чтобы разблокировать устройство, нужно ввести пароль от учетной записи Dr.Web. Без пароля устройство разблокировать нельзя.

Отправить SMS контактам из списка друзей, если SIM-карта заменена

По умолчанию опция отключена.

Если эта опция включена, Антивор Dr.Web отправит SMS-сообщения всем абонентам из списка друзей, как только обнаружит на устройстве SIM-карту не из списка доверенных. Кроме того, Антивор Dr.Web определит номер, привязанный к этой SIM-карте.

При перезагрузке устройства с замененной SIM-картой, Антивор повторно отправит SMS-сообщения абонентам из списка друзей. Антивор может отправить максимум пять таких SMS-рассылок в день.

Удалить данные

По умолчанию опция отключена.

Если ваше устройство украдено и заблокировано, посторонний может попробовать разблокировать его перебором пароля. Чтобы никто не смог получить доступ к вашим данным, активируйте опцию **Удалить данные**.

После того, как пароль будет введен неверно 10 раз на заблокированном устройстве:

- Если Dr.Web активирован в качестве администратора устройства, настройки устройства будут сброшены до заводских (будут удалены все установленные вами приложения, ваши личные данные, фотографии, SMS-сообщения, контакты, будет удалена вся информация с карты памяти). Обратите внимание, что сброс до заводских настроек удалит в том числе Dr.Web.
- Если Dr.Web не активирован в качестве администратора устройства, будут удалены ваши личные данные. Dr.Web не будет удален и продолжит блокировать устройство.

Текст на экране блокировки

Здесь вы можете изменить текст, который будет отображаться на экране заблокированного устройства в случае его потери или кражи. Например, вы можете указать ваш второй номер телефона или адрес электронной почты для связи.

Нажмите **Текст на экране блокировки**, напишите новый текст и нажмите **Сохранить**.

Режим работы без SIM-карты

Режим работы без SIM-карты активируется как при физическом отсутствии SIM-карты, так и в случае, если ваше устройство запрещает установленным приложениям доступ к информации о SIM-карте. Это относится к устройствам, для которых предусмотрено использование SIM-карт.

Как только Антивор Dr.Web обнаружит, что не имеет доступ к SIM-карте, откроется экран с просьбой ввести пароль учетной записи Dr.Web. На панели уведомлений также появится сообщение о том, что SIM-карта не найдена. Введите пароль, чтобы сделать режим без SIM-карты доверенным. Отправка SMS-команд будет недоступна, однако вы сможете использовать остальные функции Антивора Dr.Web.

8.4.2. SMS-команды

Вы можете управлять Антивором Dr.Web удаленно с помощью SMS-команд, которые позволяют получить информацию о местонахождении вашего мобильного устройства, а также заблокировать его функции и удалить вашу персональную информацию.

Таблица SMS-команд

Для управления Антивором Dr.Web используются следующие SMS-команды:

Команда	Действие
#LOCK#*Пароль***#**	Заблокировать устройство. В ответ на команду вы получите SMS-сообщение: «Антивор Dr.Web - Устройство <*название устройства*> заблокировано».
#SIGNAL#*Пароль***#**	Заблокировать устройство и включить на нем звуковой сигнал, который продолжит звучать после перезагрузки устройства. В ответ на команду вы получите SMS-сообщение: «Антивор Dr.Web - Устройство <*название устройства*> заблокировано».
#LOCATE#*Пароль***#**	Получить координаты мобильного устройства в SMS-сообщении.

	В ответ на команду вы получите ссылку с координатами предполагаемого местоположения устройства на карте. Для указания местоположения устройства используется Dr.Web Anti-theft Locator – специальный сервис компании «Доктор Веб», показывающий в окне интернет-браузера карту местности и положение устройства на ней. Точность определения координат устройства зависит от доступности GPS-приемника, видимости окружающих сетей Wi-Fi и ближайших базовых передающих станций GSM. Таким образом, в зависимости от полученных данных, координаты будут определены точно (в виде позиции на карте) или приблизительно (в виде круга определенного радиуса). В верхней части экрана с картой вы можете выбрать наиболее подходящий вам сервис карт.
#UNLOCK#*Пароль***#**	Разблокировать устройство без сброса пароля от учетной записи Dr.Web.
#WIPE#*Пароль***#**	Восстановить заводские настройки мобильного устройства и удалить все данные из внутренней памяти устройства. В ответ на команду вы получите SMS-сообщение: «Антивор Dr.Web - Удаление данных на устройстве *<название устройства>*». Эта команда также будет выполнена, если устройство заблокировано и в настройках Антивора Dr.Web включена опция **Удалить данные**.
#RESETPASSWORD#	Разблокировать устройство и задать новый пароль. Эта команда может быть отправлена только с номера телефона, указанного в списке друзей.

SMS-команды не зависят от регистра. Например, чтобы заблокировать мобильное устройство, вы можете отправить команду **#LOCK#***Пароль***#** в виде **#Lock#***Пароль***#**, **#lock#***Пароль***#**, **#lOck#***Пароль***#** и т.д.

Чтобы результаты, полученные после отправки SMS-команды #LOCATE#, были наиболее точными, разрешите использование беспроводных сетей для определения местоположения в настройках мобильного устройства.

Отправка SMS-команд в Антиворе Dr.Web

Вы можете отправлять SMS-команды непосредственно через интерфейс Антивора Dr.Web на устройства, на которых также функционирует Антивор Dr.Web.

1. На экране настроек Антивора Dr.Web (см. Рисунок 16) нажмите на карточку с SMS-командой.

2. Нажмите **Отправить SMS-команду**.
3. Выберите команду из списка:
   - **Заблокировать** – соответствует команде #LOCK#.
   - **Заблокировать и включить звуковой сигнал** – соответствует команде #SIGNAL#.
   - **Обнаружить местоположение** – соответствует команде #LOCATE#.
   - **Разблокировать** – соответствует команде #UNLOCK#.
   - **Удалить все данные** – соответствует команде #WIPE#.
   - **Разблокировать и задать новый пароль** – соответствует команде #RESETPASSWORD#.
4. Укажите номер, на который вы хотите отправить SMS-команду.
5. Укажите пароль, установленный для учетной записи на устройстве получателя команды. Если ваш номер добавлен в список друзей получателя SMS-команды, пароль указывать не обязательно.
6. Нажмите кнопку **Отправить**.

8.4.3. Отключение Антивора Dr.Web

Чтобы отключить Антивор Dr.Web, выполните следующие действия:

1. На главном экране приложения выберите **Антивор**.
2. Введите пароль от учетной записи Dr.Web.
3. На экране **Антивор** (см. Рисунок 16) переведите переключатель в правом верхнем углу экрана в положение ОТКЛ.
4. В появившемся окне нажмите **ОК**.

> Отключение Антивора Dr.Web значительно снижает уровень защиты вашего устройства.

8.5. Родительский контроль

С помощью Родительского контроля владелец учетной записи Dr.Web может задать настройки доступа для другого пользователя устройства. Владелец учетной записи может запретить доступ к любому установленному приложению и к настройкам компонентов Dr.Web.

Обратите внимание, Родительский контроль запрещает использовать отпечаток пальца вместо пароля от учетной записи Dr.Web, кроме случая, когда ваше устройство заблокировано.

Включение Родительского контроля

Чтобы включить Родительский контроль:

1. Введите пароль от учетной записи Dr.Web. Если вы введете неправильный пароль 10 раз подряд, поле для ввода пароля будет временно заблокировано. Вы увидите сколько времени остается до следующей попытки.

   Если на вашем устройстве еще не настроена учетная запись, вам будет предложено ее создать.
2. Нажмите кнопку **Включить**.

Настройка Родительского контроля

Экран **Родительский контроль** (см. Рисунок 17) содержит две вкладки:

- **Приложения**. Содержит список всех приложений, установленных на устройстве. Выберите приложения, доступ к которым будет запрещен.

  Чтобы снова открыть доступ к приложению, снимите флажок с приложения в настройках Родительского контроля.
- **Компоненты**. Содержит список компонентов Dr.Web, доступ к которым можно запретить:
  - URL-фильтр. Позволяет владельцу учетной записи ограничить доступ к конкретным веб-сайтам, веб-страницам, а также к категориям веб-сайтов (например, «Наркотики», «Оружие», «Терроризм», «Сайты для взрослых» и др.).
  - Фильтр звонков и SMS. Позволяет владельцу учетной записи создавать списки номеров, с которых пользователь устройства может получать звонки и сообщения. Например, можно разрешить входящие звонки и SMS-сообщения только с определенных номеров или номеров из списка контактов.
  - Настройки Dr.Web. Позволяет владельцу учетной записи запретить пользователю устройства заходить в настройки Dr.Web и изменять их. Например, без пароля от учетной записи пользователь не сможет сбросить настройки.

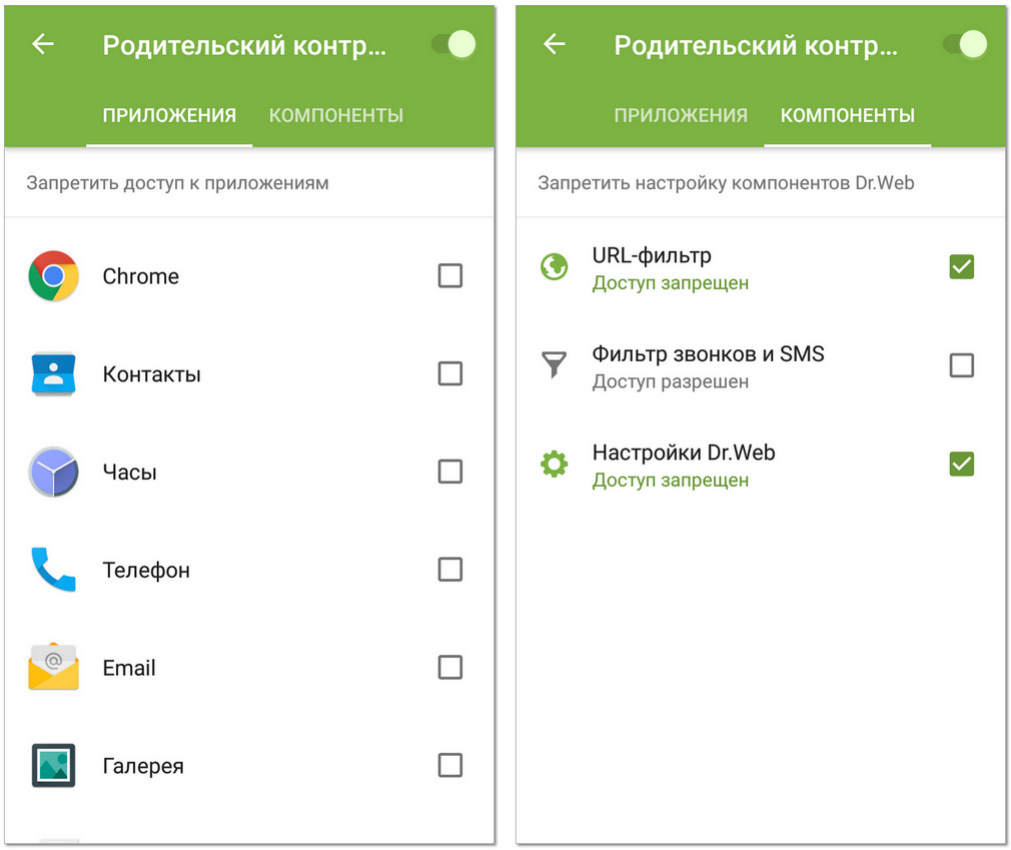

Рисунок 17. Родительский контроль. Вкладки Приложения и Компоненты

Отключение Родительского контроля

Чтобы отключить Родительский контроль, выполните следующие действия:

1. На главном экране приложения выберите **Родительский контроль**.
2. Введите пароль от учетной записи Dr.Web.
3. Переведите переключатель в правом верхнем углу экрана в положение ОТКЛ и нажмите **ОК**.

8.6. Брандмауэр Dr.Web

Брандмауэр Dr.Web защищает мобильное устройство от несанкционированного доступа извне и предотвращает утечку важных данных по сети. Он позволяет контролировать подключения и передачу данных по сети и блокировать подозрительные соединения.

Особенности использования

Брандмауэр Dr.Web реализован на базе технологии VPN для Android, что позволяет ему работать, не требуя получения прав суперпользователя (root) на устройстве. Реализация технологии VPN на Android связана с определенными ограничениями:

- В первую очередь, в каждый момент времени только одно приложение на устройстве может использовать VPN. В результате, когда приложение включает VPN на устройстве, открывается окно с запросом разрешения использования VPN для этого приложения. Если пользователь предоставит такое разрешение, приложение начинает использовать VPN, при этом другое приложение, использовавшее VPN до этого момента, теряет эту возможность. Такой запрос появляется при первом включении Брандмауэра Dr.Web. Кроме того, он может появляться при перезагрузке устройства и тогда, когда другие приложения запрашивают VPN. VPN приходится делить между приложениями во времени, и брандмауэр может работать, только когда он полностью владеет правами на использование VPN.
- Включение Брандмауэра Dr.Web может привести к невозможности подключения устройства, на котором он запущен, к другим устройствам напрямую через Wi-Fi или локальную сеть. Это зависит от модели устройства и используемых для подключения приложений.
- При включенном Брандмауэре Dr.Web устройство не может использоваться в качестве точки доступа Wi-Fi.

Технология VPN для Android используется только для реализации функций брандмауэра, при этом VPN-туннеля не создаётся и интернет-трафик не шифруется.

Включение Брандмауэра Dr.Web

1. На главном экране приложения выберите опцию **Брандмауэр**.
2. Чтобы включить Брандмауэр Dr.Web, нажмите кнопку **Включить** или используйте переключатель в правом верхнем углу экрана. По умолчанию брандмауэр отключен.

   Dr.Web запрашивает разрешение на подключение к VPN. Для работы Брандмауэра необходимо предоставить это разрешение.

   Чтобы включить Брандмауэр Dr.Web после загрузки устройства, откройте приложение Dr.Web.

   На устройствах с Android 7.0 или более поздними версиями вы можете настроить автоматическое включение Брандмауэра Dr.Web после загрузки устройства. Для этого:

   1. В настройках устройства выберите **VPN**.
   2. На экране **VPN** откройте настройки сети Dr.Web Security Space (Dr.Web Security Space Life).
   3. На экране **Dr.Web Security Space** (**Dr.Web Security Space Life**) включите настройку **Постоянная VPN**.

      На устройствах с Android 8.0 или более поздними версиями вы можете заблокировать доступ к Интернету после загрузки устройства, пока не появится подключение к VPN. Для этого включите настройку **Подключаться только через VPN**.

Если в ходе работы права на использование VPN переходят к другому приложению, Брандмауэр Dr.Web будет отключен, о чем будет выведено соответствующее предупреждение в разделе уведомлений. Чтобы снова включить Брандмауэр Dr.Web, достаточно нажать на данное предупреждение.

Если вы работаете с устройством в режиме ограниченного доступа (гостевого профиля), вам недоступны настройки Брандмауэра Dr.Web.

8.6.1. Текущая активность сетевых подключений

Информацию о текущей активности сетевых подключений можно получить на вкладке Трафик (см. Рисунок 18) или из плавающего окна (см. Рисунок 19).

Вкладка Трафик

На вкладке в режиме реального времени показывается список подключений, инициированных установленными на устройстве приложениями. Чтобы просмотреть подробную информацию о подключениях какого-либо приложения (IP-адресов и портов подключений, а также размер исходящего/входящего трафика), нажмите на него в списке.

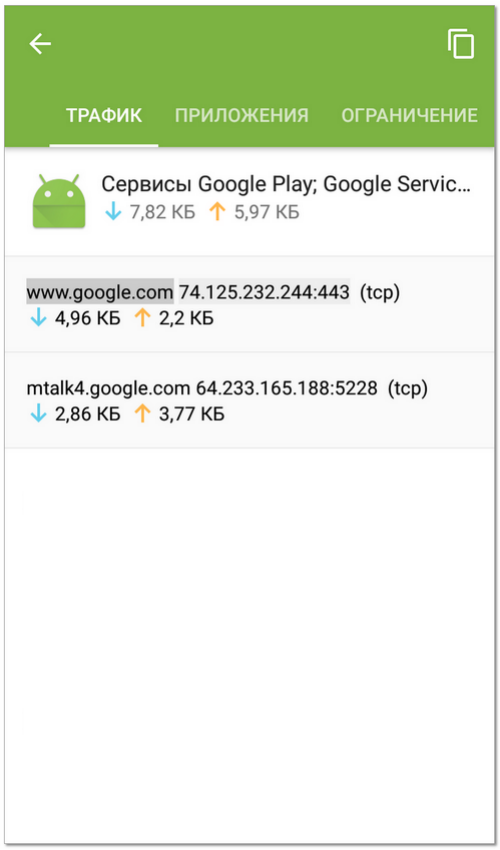

Рисунок 18. Вкладка Трафик

Копирование адреса

Чтобы скопировать адрес в буфер обмена:

1. Нажмите на нужное приложение, чтобы раскрыть подробную информацию о текущем трафике.
2. Нажмите и удерживайте строчку с адресом. Вы перейдете в режим копирования. Доступные для копирования адреса станут подсвечены серым.
3. Нажмите на нужный адрес, а затем нажмите на значок в правом верхнем углу экрана. Адрес будет скопирован в буфер.

Чтобы выйти из режима копирования, нажмите на значок ← в левом верхнем углу.

Создание правил

Для подключений, указанных в списке, вы можете создать разрешающие или блокирующие правила. Нажмите и удерживайте подключение в списке, после чего выберите соответствующую опцию:

- **Добавить разрешающее правило**, чтобы создать правило, разрешающее соединения выбранного приложения с соответствующими IP-адресом и портом.
- **Добавить запрещающее правило**, чтобы создать правило, блокирующее все соединения выбранного приложения с соответствующими IP-адресом и портом.

Плавающее окно

Чтобы иметь возможность всегда видеть активные интернет-соединения и контролировать количество входящего и исходящего трафика, можно включить плавающее окно, которое будет отображаться поверх всех приложений (см. Рисунок 19).

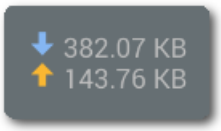

Рисунок 19. Плавающее окно

Чтобы включить плавающее окно:

1. Откройте вкладку **Ограничение** и установите флажок **Информация о текущем трафике** (см. Рисунок 20).
2. Разрешите приложению отображать плавающее окно поверх других окон.

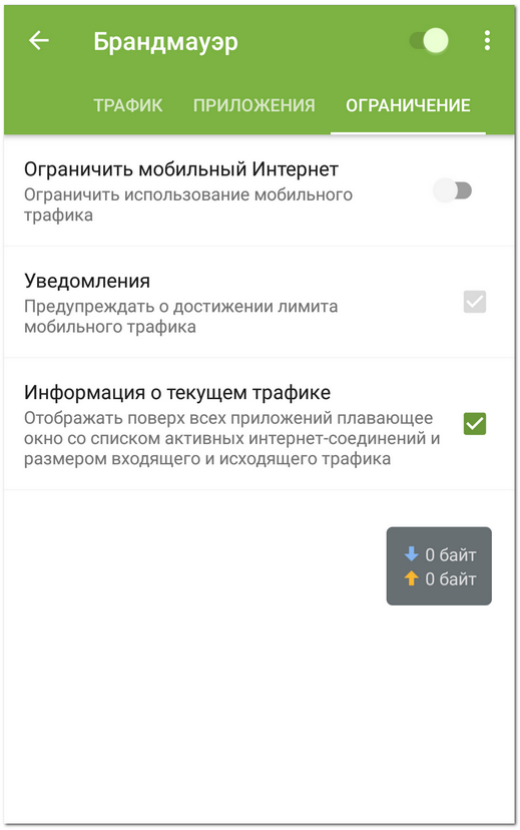

Рисунок 20. Вкладка Ограничение

Размер трафика учитывается с момента включения окна.

- Чтобы открыть список приложений, использующих интернет-соединение (см. Рисунок 21), нажмите на плавающее окно.
- Чтобы закрыть список приложений, нажмите X.
- Чтобы скрыть окно, снимите флажок **Информация о текущем трафике**.

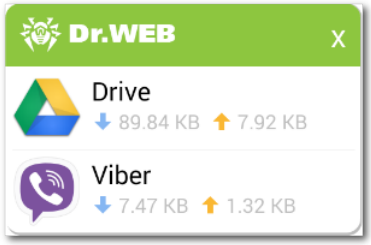

Рисунок 21. Список приложений, использующих интернет-соединение

8.6.2. Обработка трафика приложений

Брандмауэр Dr.Web позволяет настроить обработку интернет-трафика на уровне приложений и, таким образом, контролировать доступ программ и процессов к сетевым ресурсам. Ознакомиться с информацией об интернет-трафике, используемом

установленными на вашем устройстве приложениями, а также настроить для них правила доступа к сетевым ресурсам вы можете на вкладке **Приложения** (см. Рисунок 22).

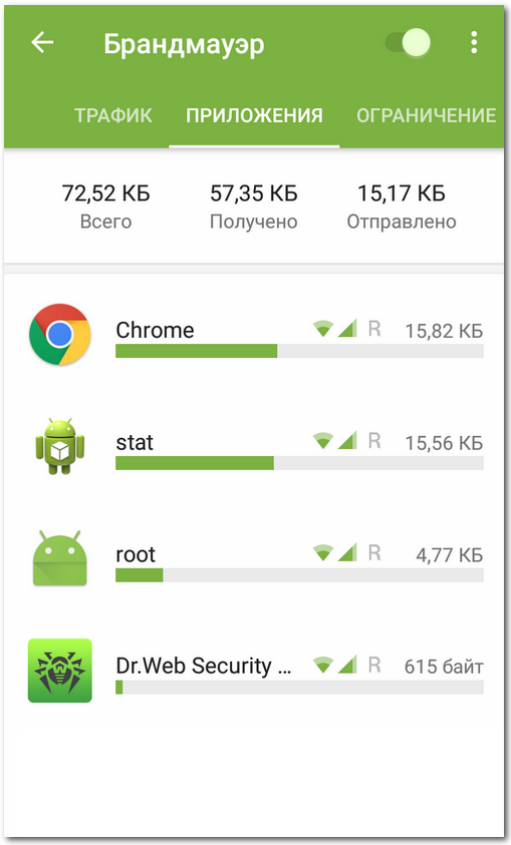

Рисунок 22. Вкладка Приложения

На вкладке **Приложения** показывается общее количество переданных по сети данных, а также размер полученного и отправленного трафика. Вы можете посмотреть список приложений (и групп приложений), для каждого из которых указан размер израсходованного интернет-трафика.

Чтобы просмотреть список всех установленных на устройстве приложений, включая приложения с нулевым значением израсходованного трафика, на вкладке **Приложения** нажмите **Меню** и установите флажок **Все приложения**.

Приложения с измененными настройками выделены значком .

Настройки приложений

Чтобы открыть настройки приложения (или группы приложений), нажмите на приложение в списке.

Не контролировать приложение

> Настройка доступна на устройствах с Android 5.0 или более поздними версиями.
>
> Настройка недоступна для некоторых системных приложений.

Брандмауэр Dr.Web реализован на базе VPN для Android. VPN препятствует работе приложений, которые используют технологию, несовместимую с VPN, например, Wi-Fi Direct. Это может привести к невозможности подключения устройства к другим устройствам. В этом случае не рекомендуется полностью отключать Брандмауэр Dr.Web. Вместо этого отключите контроль Брандмауэра Dr.Web для нужного приложения (группы приложений):

1. На вкладке **Приложения** (см. Рисунок 22) выберите приложение (группу приложений).
2. На экране **Настройки приложения** нажмите **Меню** ⋮.
3. Выберите **Не контролировать приложение** (см. Рисунок 23).

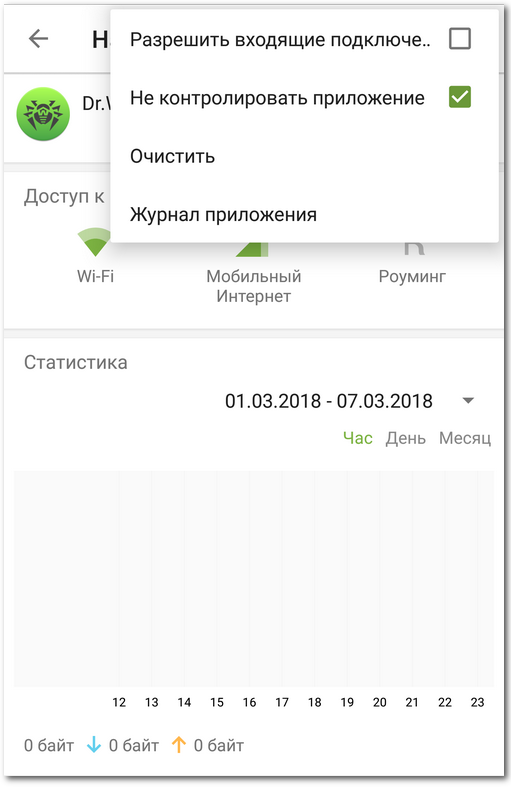

Рисунок 23. Настройка Не контролировать приложение

Рекомендуется отключать контроль Брандмауэра Dr.Web только для тех приложений, которым доверяете.

При включении этой опции, Брандмауэр Dr.Web не контролирует сетевые подключения этого приложения, даже если в настройках Брандмауэра Dr.Web установлены ограничения. Трафик приложения не учитывается.

Доступ к передаче данных

Для каждого приложения вы можете разрешить/запретить использование Wi-Fi, мобильного Интернета и Интернета в роуминге с помощью соответствующих опций в разделе **Доступ к передаче данных**.

Статистика

Статистика использования Интернета показана в разделе Статистика в виде диаграммы.

Правила для IP-адресов и портов

Настроить правила обработки подключений для выбранного приложения (группы приложений) можно в разделе Правила для IP-адресов и портов.

Журнал приложения

События, связанные с сетевой активностью приложений, установленных на устройстве, записываются в журналы приложений.

8.6.2.1. Статистика использования интернет-трафика

На экране **Настройки приложения** вы можете ознакомиться со статистикой использования интернет-трафика приложения в виде графической диаграммы (см. Рисунок 24).

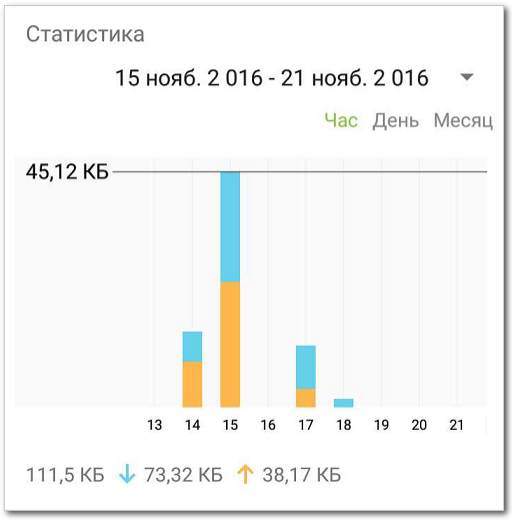

Рисунок 24. Статистика использования интернет-трафика приложения

На диаграмме оранжевым цветом отмечен исходящий трафик приложения, голубым – входящий. Под диаграммой приведены численные значения израсходованного трафика (общего, исходящего и входящего).

При просмотре статистики использования интернет-трафика вы можете выполнить следующие действия:

- Выбрать период времени для просмотра статистики в соответствующем списке над диаграммой. Вы можете просмотреть статистику за текущий день, последнюю неделю, текущий месяц, предыдущий месяц или самостоятельно задать период времени, указав даты его начала и окончания.
- В рамках выбранного периода настроить отображение статистики по часам, дням или месяцам.

Удаление статистики

- Удаление статистики для всех приложений:
  1. На экране **Брандмауэр** на любой вкладке нажмите **Меню** и выберите опцию **Очистить**.
  2. В открывшемся окне установите флажок **Очистить статистику**. Нажмите **ОК**.
- Удаление статистики для отдельного приложения:
  1. На экране **Брандмауэр** на вкладке **Приложения** выберите приложение, для которого вы хотите очистить статистику.
  2. На экране **Настройки приложения** нажмите **Меню** и выберите опцию **Очистить**.
  3. В открывшемся окне установите флажок **Очистить статистику для этого приложения**. Нажмите **ОК**.

8.6.2.2. Правила подключений

На экране **Настройки приложения** вы также можете задать правила подключений этого приложения к определенным IP-адресам и портам.

Создание правила

1. Чтобы создать правило, нажмите кнопку **Добавить правило** в разделе **Правила для IP-адресов и портов**. Вы можете добавить разрешающие и запрещающие правила в зависимости от значения соответствующей опции:
   - **Блокировать подключения из списка** – запрещающее правило.
   - **Разрешить только подключения из списка** – разрешающее правило.
2. В открывшемся окне в поле **Адрес сервера** укажите действительный IP-адрес (в формате a.b.c.d), диапазон IP-адресов (в формате a1.b1.c1.d1-a2.b2.c2.d2) или целую сеть (в формате a.b.c.0/n, где n – число от 1 до 32) или оставьте данное поле пустым (в таком случае необходимо обязательно определить порт подключения).

В поле **Порт** укажите номер действительного порта или оставьте его пустым (в таком случае требуется обязательно задать IP-адрес подключения). В случае если одно из полей оставлено пустым, правило будет действовать для любых IP-адресов или портов. Нажмите кнопку **ОК**, чтобы сохранить созданное правило.

Если вы выбрали опцию **Разрешить только подключения из списка** и не добавили ни одного адреса в список, блокироваться будут все подключения.

3. Чтобы отредактировать существующее правило, нажмите и удерживайте его в списке, далее нажмите кнопку **Редактировать**.

Кроме того, вы можете добавлять разрешающие и запрещающие правила при просмотре журналов приложений или списка текущих подключений.

Удаление правил

- Чтобы удалить правило, нажмите и удерживайте его в списке, далее нажмите кнопку **Удалить**.
- Чтобы удалить все правила для определенного приложения:
  1. На экране **Брандмауэр** на вкладке **Приложения** выберите это приложение (см. Рисунок 22).
  2. На экране **Настройки приложения** нажмите **Меню** и выберите опцию **Очистить**.
  3. В открывшемся окне установите флажок **Удалить правила для этого приложения**. Нажмите **ОК**.
- Чтобы удалить все правила для всех приложений:
  1. На экране **Брандмауэр** нажмите **Меню** и выберите опцию **Очистить**.
  2. В открывшемся окне установите флажок **Удалить правила для приложений**. Нажмите **ОК**.

Разрешение входящих подключений

Чтобы разрешить все входящие подключения для приложения:

1. На вкладке **Приложения** (см. Рисунок 22) выберите приложение, для которого нужно разрешить входящие подключения.
2. На экране **Настройки приложения** нажмите **Меню**.
3. Установите флажок **Разрешить входящие подключения**.

Информация о соединениях, инициированных с любых удаленных адресов с портом, открытым данным приложением, фиксируется в журнале приложения и статистике работы брандмауэра лишь частично. Кроме того, любые соединения с этими адресами могут быть исключены из проверки брандмауэром и для остальных приложений. Такой режим работы не является безопасным и в общем случае использовать его не рекомендуется.

Разрешение входящих подключений оправдано в том случае, когда иными способами невозможно избежать отключения брандмауэра, например, если на устройстве настроен сервер, принимающий соединения из внешних сетей.

8.6.3. Ограничение использования мобильного Интернета

С помощью Брандмауэра Dr.Web вы можете установить лимит на использование мобильного Интернета.

1. Чтобы включить/отключить функцию ограничения мобильного Интернета, используйте переключатель **Ограничить мобильный Интернет** на вкладке **Ограничение** (см. Рисунок 25).

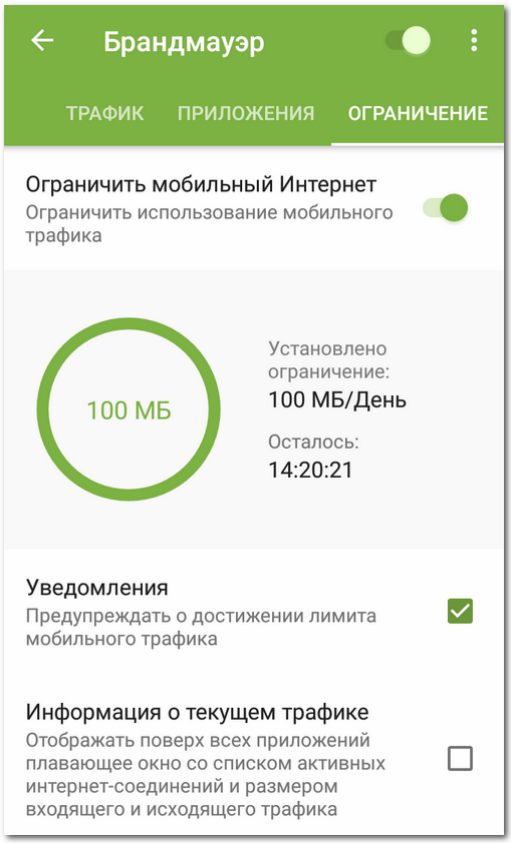

Рисунок 25. Ограничение мобильного Интернета

2. При включении ограничения задайте лимит мобильного трафика (в мегабайтах или гигабайтах). Вы можете выбрать период действия ограничения: день, неделя или месяц.
3. При необходимости, укажите количество израсходованного трафика с начала действия выбранного периода ограничения:
   - Если в качестве периода действия ограничения выбран день, отсчет времени начинается с 00:00 текущего дня.
   - Если в качестве периода действия ограничения выбрана неделя, отсчет времени начинается с 00:00 текущего дня.

- Если в качестве периода действия ограничения выбран месяц, отсчет времени начинается с 00:00 первого числа текущего календарного месяца.

При включении ограничения использования мобильного Интернета на вкладке **Ограничение** экрана настроек брандмауэра показывается диаграмма, отображающая размер оставшегося трафика. Рядом с диаграммой показывается установленный лимит и обратный отсчет времени до окончания периода действия ограничения (см. Рисунок 25).

При использовании ограничения мобильного трафика возможен его небольшой перерасход, не превышающий 4 КБ.

Уведомления

Вы можете настроить оповещения о достижении лимита мобильного трафика. Для этого установите флажок **Уведомления** на вкладке **Ограничение**.

Информация о текущем трафике

Чтобы иметь возможность всегда видеть активные интернет-соединения и контролировать количество входящего и исходящего трафика, установите флажок **Информация о текущем трафике**.

8.6.4. Журнал Брандмауэра Dr.Web

Чтобы просмотреть список всех событий, связанных с работой Брандмауэра Dr.Web, на экране **Брандмауэр** нажмите **Меню** в правом верхнем углу экрана и выберите опцию **Журнал**.

Просмотр журнала

Для упрощения поиска информации вы можете использовать функции сортировки записей и быстрого скроллинга (путем перемещения специального графического элемента в правой части экрана) при просмотре списка событий.

Чтобы отсортировать записи в журнале:

1. На экране **Журнал** нажмите **Меню**.
2. Выберите критерий сортировки.

Для каждого события в журнале показывается следующая информация:

- Дата и время соединения (для TCP) или время, за которое получены пакеты данных с соответствующими величинами трафика (для UDP). Например: 18/02/2014 2:07:11 - 18/02/2014 2:07:12.
- Локальный адрес и локальный порт. Например: src: 10.2.3.5:6881.

- Входящий и исходящий трафик (в байтах) или количество заблокированных пакетов. Например: in:103 out:112 или blocked packets:1.
- Идентификатор приложения на устройстве, ассоциированный с этим трафиком (User ID). Например: uid=10071.
- Количество ситуаций сетевых заторов (только для TCP). Например: traffic jam=0. Заторы трафика – это особая ситуация, когда клиентская программа не успевает разгружать TCP-буфер, что может быть причиной медленной передачи данных по сети.

Копирование адреса

При желании вы можете скопировать адрес в буфер обмена.

Нажмите и удерживайте строчку с адресом на странице журнала. Вы перейдете в режим копирования. Доступные для копирования адреса будут подсвечены серым. Нажмите на нужный адрес, а затем нажмите на значок в правом верхнем углу экрана. Адрес будет скопирован в буфер.

Чтобы выйти из режима копирования, нажмите на значок ← в левом верхнем углу.

Очистка журнала

1. На экране **Брандмауэр** нажмите **Меню** и выберите опцию **Очистить**.
2. В открывшемся окне установите флажок **Очистить журнал** и нажмите **ОК**.

Размер журнала

По умолчанию для файла журнала установлен максимальный размер, равный 5 МБ. Чтобы изменить максимально разрешенный размер файла журнала:

1. На экране **Брандмауэр** нажмите **Меню** и выберите опцию **Очистить**.
2. В открывшемся окне измените значение, указанное в поле **Максимальный размер журнала** и нажмите **ОК**.

> Максимальный размер журнала должен быть больше 0 МБ.

8.6.5. Журналы приложений

Чтобы просмотреть список событий, связанных с сетевыми подключениями того или иного приложения, установленного на вашем устройстве, на вкладке **Приложения** найдите нужное приложение в списке и нажмите на него. На экране **Настройки приложения** нажмите **Меню** и выберите пункт **Журнал приложения**.

Просмотр журнала приложения

Все события для данного приложения объединены по датам. Чтобы просмотреть список событий за какую-либо дату, нажмите на нее в списке. Для каждого события в списке показывается следующая информация:

- Время соединения (для TCP) или время, за которое получены пакеты данных с соответствующими величинами трафика (для UDP).
- Локальный адрес и локальный порт.
- Входящий и исходящий трафик или количество заблокированных пакетов.

Для соединений, указанных в журнале приложения, вы можете создать разрешающие или блокирующие правила. Нажмите и удерживайте соединение в списке, после чего выберите соответствующую опцию:

- **Добавить разрешающее правило**, чтобы создать правило, разрешающее соединения выбранного приложения с соответствующими IP-адресом и портом.
- **Добавить запрещающее правило**, чтобы создать правило, блокирующее все соединения выбранного приложения с соответствующими IP-адресом и портом.

Очистка журнала приложения

1. На экране **Настройки приложения** нажмите **Меню** ⋮ и выберите опцию **Очистить**.
2. Установите флажок **Очистить журнал для этого приложения**. Нажмите **ОК**.

Отключение регистрации событий для приложения

1. На экране **Настройки приложения** нажмите **Меню** ⋮ и выберите опцию **Очистить**.
2. Установите флажок **Не вести журнал для этого приложения**. Нажмите **ОК**.

8.7. Аудитор безопасности

Dr.Web проводит диагностику безопасности вашего устройства и дает рекомендации по устранению выявленных проблем и уязвимостей с помощью специального компонента – Аудитора безопасности. Компонент начинает работать автоматически после первого запуска приложения и регистрации лицензии.

Возможные проблемы и способы их устранения

Чтобы просмотреть список обнаруженных проблем безопасности (см. Рисунок 26), выберите раздел **Аудитор безопасности** на главном экране приложения.

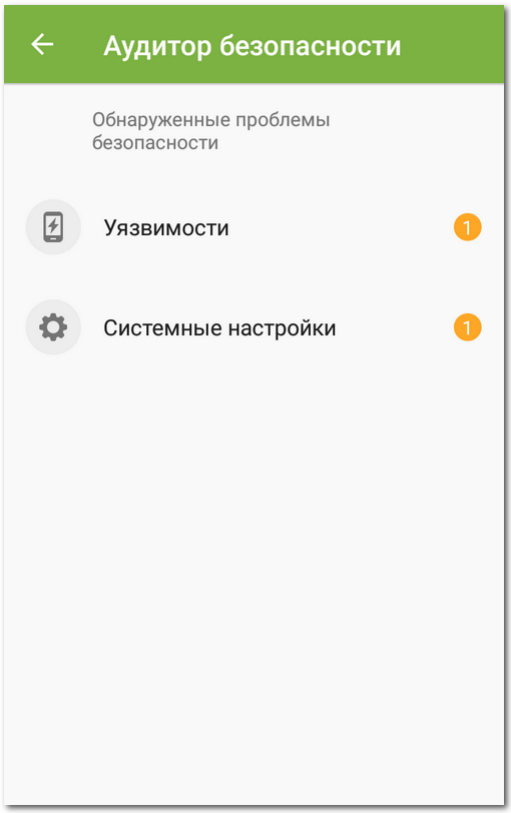

Рисунок 26. Обнаруженные проблемы безопасности

Dr.Web выявляет следующие типы проблем безопасности:

- Приложения с наивысшим приоритетом обработки SMS.
- Скрытые администраторы устройства.
- Уязвимости и системные настройки, влияющие на безопасность устройства.

Чтобы просмотреть подробную информацию о той или иной проблеме и способе ее устранения, раскройте список соответствующей категории и выберите проблему/уязвимость в списке.

Скрытые администраторы устройства

Приложения, активированные в качестве администраторов устройства, но при этом отсутствующие в списке администраторов в соответствующем разделе настроек, не могут быть удалены стандартными средствами операционной системы. С большой вероятностью, такие приложения небезопасны.

Если вы не знаете, почему приложение скрывает свое присутствие в списке администраторов устройства, рекомендуется удалить его. Для удаления приложения нажмите кнопку **Удалить** на экране с подробной информацией о проблеме, связанной с этим приложением.

Системные настройки

Аудитор безопасности обнаруживает следующие системные настройки, влияющие на безопасность устройства:

- **Отладка по USB**. Эта настройка предназначена для разработчиков и позволяет копировать данные с компьютера на устройство под управлением Android и наоборот, устанавливать на устройство приложения, просматривать данные журналов установленных приложений, а также удалять их в некоторых случаях. Если вы не являетесь разработчиком и не используете режим отладки, рекомендуется его отключить. Для перехода к соответствующему разделу системных настроек нажмите кнопку **Настройки** на экране с подробной информацией о данной проблеме.
- **Установка приложений из неизвестных источников**. Эта настройка является основной причиной распространения угроз на устройствах с Android 7.1 и более ранними версиями.

  Приложения, загруженные не из официального каталога приложений, с большой вероятностью могут оказаться небезопасными и причинить вред устройству. Для снижения риска установки небезопасных приложений рекомендуется запретить установку приложений из неизвестных источников. Для перехода к соответствующему разделу системных настроек нажмите кнопку **Настройки** на экране с подробной информацией о данной проблеме.

  Рекомендуется проверять все устанавливаемые приложения на наличие угроз. Перед проверкой необходимо убедиться, что вирусные базы Dr.Web обновлены.
- **Конфликты ПО**. Использование конфликтующего ПО, в частности, браузеров, не поддерживаемых URL-фильтром, снижает безопасность устройства. При работе в таких браузерах пользователь не будет защищен от нежелательных и вредоносных интернет-ресурсов. Поэтому рекомендуется использовать, в том числе, в качестве браузера по умолчанию, встроенный браузер Android, Google Chrome, Яндекс.Браузер, Microsoft Edge, Firefox, Opera, Adblock Browser, Dolphin Browser, Спутник и Boat Browser.
- **Уведомления Dr.Web заблокированы**. При заблокированных уведомлениях Dr.Web не может оперативно информировать об обнаруженных угрозах. Это снижает защиту устройства и может привести к его заражению. Поэтому рекомендуется перейти в настройки вашего устройства и включить уведомления Dr.Web.

Уязвимости

Под *уязвимостью* понимается недостаток в программном коде, который может быть использован злоумышленниками для нарушения работы системы.

Dr.Web обнаруживает в системе устройства такие уязвимости, как Janus, BlueBorne, Master Key (#8219321), Extra Field (#9695860), Name Length Field (#9950697), Fake ID (#13678484), ObjectInputStream Serialization (CVE-2014-7911), PendingIntent (CVE-2014-8609), Android Installer Hijacking, OpenSSLX509Certificate (CVE-2015-3825), Stagefright и Stagefright 2.0, SIM Toolkit (CVE-2015-3843). Воспользовавшись данными уязвимостями, злоумышленники

могут добавить программный код в ряд приложений, в результате чего данные приложения могут начать выполнять функции, представляющие угрозу безопасности устройства. Dr.Web также выявляет наличие в системе уязвимости Heartbleed – ошибки в криптографическом программном обеспечении OpenSSL, позволяющей злоумышленникам получить доступ к конфиденциальным данным пользователя.

В случае обнаружения одной или нескольких из перечисленных уязвимостей, проверьте доступность обновлений для операционной системы вашего устройства на сайте производителя, поскольку в новых версиях они могут быть устранены. В случае отсутствия обновлений рекомендуется устанавливать приложения только из проверенных источников.

Приложения, использующие уязвимость Fake ID

Если на устройстве обнаружены приложения, использующие уязвимость Fake ID, они отображаются в отдельной категории Аудитора безопасности. Эти приложения могут быть вредоносными, поэтому рекомендуется их удалить. Чтобы удалить приложение, нажмите кнопку **Удалить** на экране с подробной информацией о проблеме, связанной с данным приложением, или воспользуйтесь средствами операционной системы.

Пользовательские сертификаты

Если на устройстве были обнаружены пользовательские сертификаты, информация об этом будет отображена в Аудиторе безопасности. Из-за установленных пользовательских сертификатов третьи лица могут просматривать вашу сетевую активность. Если вы не знаете назначение обнаруженных сертификатов, рекомендуется удалить их с устройства.

Root-доступ

Кроме того, устройство может стать уязвимым к различным типам угроз, если на нем открыт root-доступ, т.е. выполнены изменения, связанные с получением прав суперпользователя (root). Это позволяет изменять и удалять системные файлы, что может привести к неработоспособности устройства. Если вы выполнили данные изменения самостоятельно, рекомендуется отменить их в целях безопасности. Если же наличие root-доступа является технической особенностью вашего устройства или необходимо вам для выполнения тех или иных задач, будьте особенно внимательны при установке приложений из неизвестных источников.

8.8. Статистика

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

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

Просмотр статистики

На вкладке **Статистика** находятся два информационных раздела (см. Рисунок 27):

- **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.

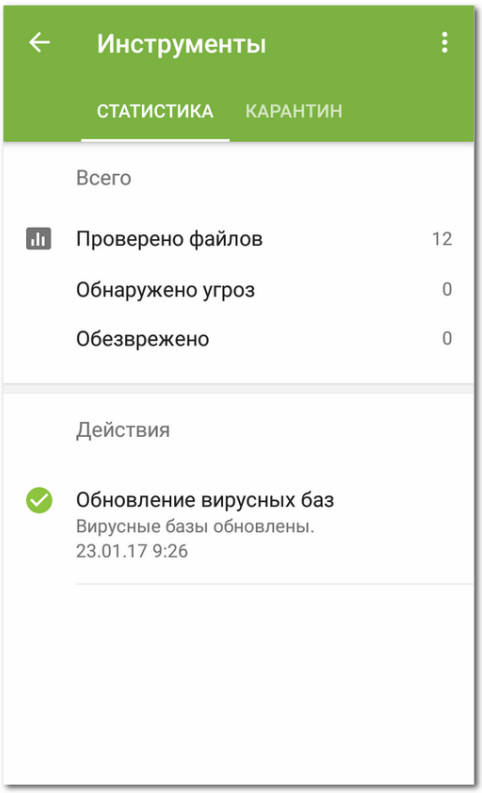

Рисунок 27. Статистика

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 дальнейшей отправки в службу технической поддержки «Доктор Веб» 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.

8.9. Карантин

Для обнаруженных угроз в Dr.Web реализована функция перемещения в карантин – особую папку, предназначенную для их изоляции и безопасного хранения (см. Рисунок 28).

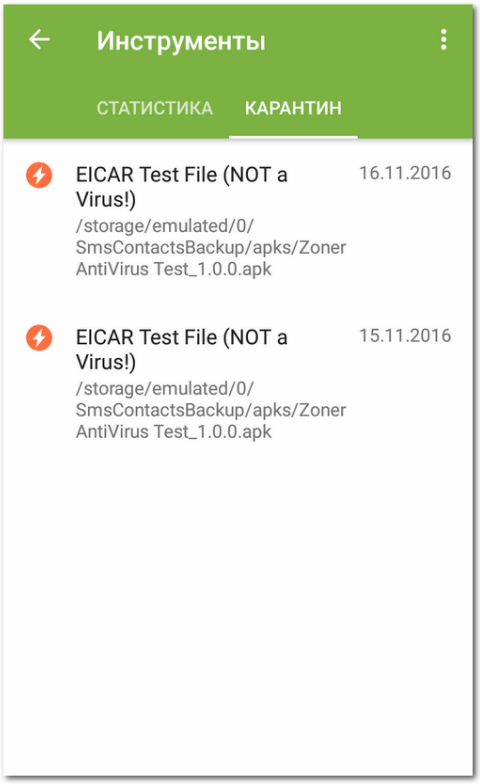

Рисунок 28. Карантин

Просмотр списка объектов в карантине

Чтобы просмотреть список угроз, перемещенных в карантин:

1. На главном экране нажмите **Меню** .

> На Android TV на главном экране выберите пункт **Разное**.

2. Выберите пункт **Карантин**.

Откроется список всех угроз, находящихся в карантине.

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**.

8.10. Сервис сокращения URL

В некоторых случаях, например, при наличии ограничений на количество символов в SMS и сообщениях в социальных сетях, вам может понадобиться использовать сокращенные URL. Dr.Web позволяет сокращать ссылки и проверять их содержание с

помощью специального сервиса сокращения ссылок, тем самым защищая пользователей от вирусных угроз.

Проверка и сокращение URL

1. Выделите URL, который вы хотите проверить и сократить, и воспользуйтесь функцией вашего браузера, позволяющей поделиться ссылкой.
2. В открывшемся меню выберите пункт **Сократить URL**. Страница, расположенная по указанному URL, будет проверена на наличие угроз, и если она безопасна, URL будет сокращен и добавлен в буфер обмена. Если на странице содержатся угрозы безопасности, сервис выдаст соответствующее предупреждение.

9. Настройки

Чтобы перейти к настройкам приложения (см. Рисунок 29), на главном экране нажмите **Меню** и выберите пункт **Настройки**.

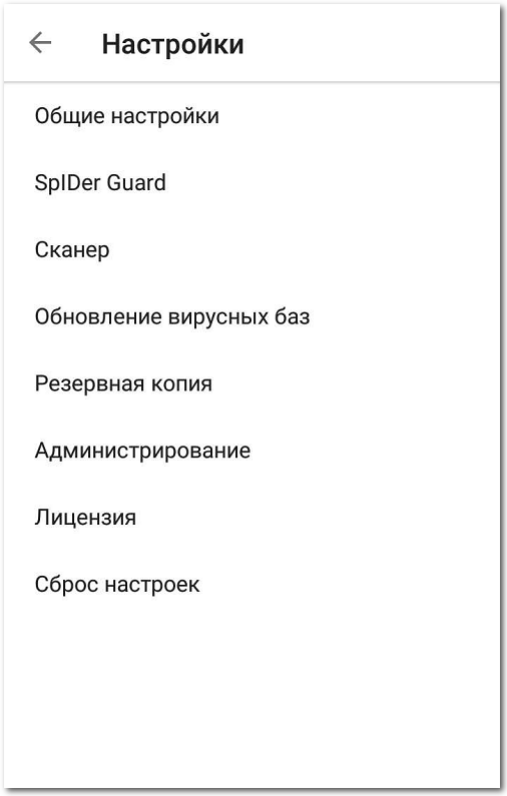

Рисунок 29. Настройки

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 и изменить параметры отправки статистики (см. раздел Общие настройки).
- **SpIDer Guard**. Позволяет задать настройки для компонента SpIDer Guard, который осуществляет постоянную проверку на наличие угроз безопасности (см. раздел Настройки SpIDer 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).
- **Резервная копия**. Позволяет выполнить импорт и экспорт настроек приложения (см. раздел Резервная копия).

- **Администрирование**. Позволяет переключиться в режим централизованной защиты (опция доступна для версии приложения, установленной с сайта «Доктор Веб»).
- **Лицензия**. Позволяет включить или отключить использование уведомлений о скором окончании срока действия лицензии (кроме версии приложения с бессрочной лицензией Dr.Web Security Space Life) (см. раздел Настройка уведомлений об окончании срока действия лицензии).
- **Сброс настроек**. Позволяет сбросить пользовательские настройки и вернуться к настройкам по умолчанию (см. раздел Сброс настроек).

> Если на устройстве включен компонент Антивор Dr.Web, при изменении некоторых настроек приложения (**Сброс настроек**, **Резервная копия** и **Администрирование**) вам понадобится ввести пароль от учетной записи Dr.Web.

9.1. Общие настройки

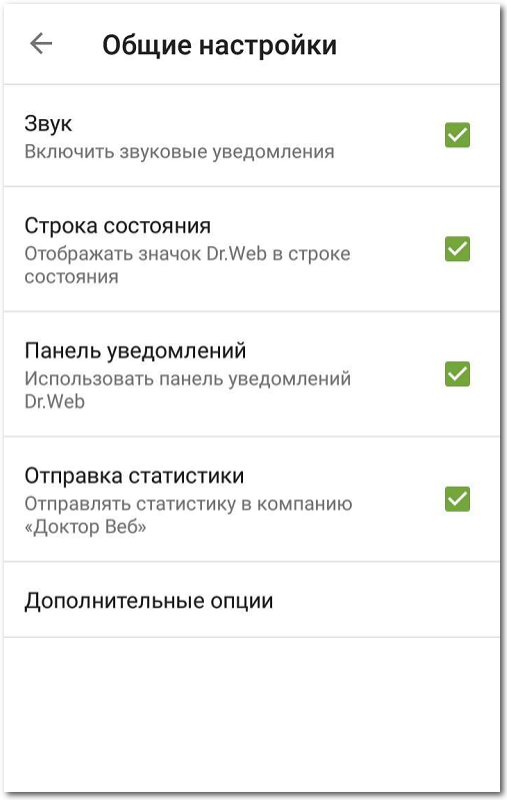

Рисунок 30. Общие настройки

На экране **Общие настройки** (см. Рисунок 30) 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 (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.

  На устройствах с Android 6.0 или более поздними версиями, если опция **Панель уведомлений** отключена, компонент SplDer Guard не показывает уведомление: Проверка <*название приложения*> завершена. Угроз не обнаружено.

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

- **Отправка статистики**. Позволяет включить и отключить отправку статистики в компанию «Доктор Веб».
- **Дополнительные опции**. Содержит дополнительные настройки:
  - **Системные приложения**. Позволяет включить или отключить информирование об обнаружении угроз в системных приложениях. По умолчанию эта опция отключена.

9.2. Обновление вирусных баз

Для обнаружения угроз безопасности Dr.Web 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.

В режиме централизованной защиты блокируется возможность ручного запуска обновлений, обновления загружаются автоматически с сервера централизованной защиты. Если на сервере централизованной защиты разрешен запуск приложения в мобильном режиме, при разрыве соединения с сервером централизованной защиты обновление вирусных баз может быть запущено вручную.

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 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 29).
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.

При работе в режиме централизованной защиты настройки обновлений могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг.

9.3. Резервная копия

Вы можете сохранить текущие настройки приложения в файл во внутренней памяти устройства. При необходимости (например, в случае переустановки Dr.Web или его использования на другом устройстве), вы сможете загрузить их из этого файла.

Чтобы сохранить текущую конфигурацию:

1. На экране настроек (см. Рисунок 29) выберите раздел **Резервная копия**.
2. Введите пароль от учетной записи.

   Пароль требуется в том случае, если компонент Антивор Dr.Web включен и настроен.
3. В открывшемся окне выберите **Экспорт данных**.
4. Установите пароль, который будет использоваться для защиты файла настроек, и нажмите кнопку **OK**.

Все настройки и данные приложения сохраняются в файле `Internal storage/Android/data/com.drweb/files/DrWebPro.bkp`.

Чтобы загрузить настройки из файла:

1. На экране настроек (см. Рисунок 29) выберите раздел **Резервная копия**.
2. Введите пароль от учетной записи.

   Пароль требуется в том случае, если компонент Антивор Dr.Web включен и настроен.
3. Выберите **Импорт настроек**.
4. Подтвердите загрузку параметров из файла.
5. В дереве файлов найдите файл с настройками и нажмите на него.
6. Введите пароль, установленный для файла настроек, и нажмите **OK**.

   Все текущие настройки будут удалены и заменены загруженными из файла.

9.4. Сброс настроек

Вы можете в любой момент сбросить пользовательские настройки приложения, в том числе настройки фильтрации звонков и сообщений, Антивора Dr.Web, Брандмауэра Dr.Web и URL-фильтра, и восстановить настройки по умолчанию.

1. На экране настроек (см. Рисунок 29) в разделе **Сброс настроек** выберите пункт **Сброс настроек**.
2. Введите пароль от учетной записи Dr.Web.
3. Подтвердите возврат к настройкам по умолчанию.

10. Режим централизованной защиты

Если вы установили Dr.Web с сайта компании «Доктор Веб», вы можете использовать его для работы в сети, контролируемой Центром Управления Dr.Web, или для подключения к антивирусной услуге Dr.Web AV-Desk, предоставленной вашим IT-провайдером. Для антивирусной защиты в таком централизованном режиме вам не потребуется устанавливать дополнительные программные модули или удалять установленный ранее Dr.Web.

Режим централизованной защиты недоступен:

- Для версии Dr.Web, установленной из Google Play.
- Для устройств под управлением Android TV.

Компоненты, контролируемые с сервера централизованной защиты

Настройки компонентов Dr.Web могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг.

С сервера централизованной защиты могут контролироваться следующие компоненты Dr.Web:

- Сканер Dr.Web. Сканирование устройства по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций с сервера централизованной защиты.
- SpIDer Guard.
- Фильтр звонков и SMS.
- Антивор Dr.Web.
- URL-фильтр.
- Фильтр приложений.

Лицензирование в режиме централизованной защиты

Лицензионный ключевой файл будет получен автоматически с сервера централизованной защиты, и ваша персональная лицензия не будет использоваться. В случае окончания срока действия лицензии или ее блокировки и появления соответствующего предупреждения, обратитесь к администратору антивирусной сети компании за новой лицензией или продлите подписку на услугу Dr.Web AV-Desk.

Обновление в режиме централизованной защиты

В режиме централизованной защиты блокируется возможность ручного запуска обновлений, обновления загружаются автоматически с сервера централизованной

защиты. Настройки обновлений могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг. Если на сервере централизованной защиты разрешен запуск приложения в мобильном режиме, при разрыве соединения с сервером централизованной защиты обновление вирусных баз может быть запущено вручную.

10.1. Переход в режим централизованной защиты

Чтобы начать работать в режиме централизованной защиты, подключитесь к серверу централизованной защиты.

Автоматическое подключение

Если Dr.Web установлен при помощи мастера установки, предоставленного администратором антивирусной сети, подключение к серверу централизованной защиты осуществляется автоматически. Для этого необходимо, чтобы ваше устройство находилось в одной сети Wi-Fi с сервером централизованной защиты.

Подключение с вводом параметров

Для подключения к серверу централизованной защиты понадобятся параметры подключения, которые предоставляются администратором антивирусной сети компании или IT-провайдером.

1. Убедитесь в наличии подключения к сети.
2. На экране **Настройки** (см. Рисунок 29) выберите **Администрирование**.

   Если на устройстве включен Антивор Dr.Web, введите пароль от учетной записи Dr.Web.
3. Установите флажок **Агент Dr.Web**.

   

   В приложении, установленном при помощи мастера установки, предоставленного администратором антивирусной сети, флажок **Агент Dr.Web** установлен по умолчанию.
4. При включении режима централизованной защиты восстанавливаются последние параметры подключения. Если вы подключаетесь к серверу впервые или параметры подключения изменились, необходимо указать следующие параметры:
   - IP-адрес сервера централизованной антивирусной защиты, предоставленный администратором антивирусной сети.
   - Дополнительные параметры для авторизации рабочей станции: идентификатор (присвоенный вашему устройству для регистрации на сервере) и пароль. Указанные значения параметров сохраняются, и при повторном подключении к серверу вводить их заново не требуется. Чтобы подключиться в качестве новой станции («Новичка»), нажмите **Меню** и выберите опцию **Подключиться как новичок**.

5. Нажмите кнопку **Подключиться**.
6. Dr.Web может запросить следующие разрешения:
   - Получить доступ к контактам.
   - Осуществлять телефонные звонки и управлять ими.
   - Отправлять и просматривать SMS-сообщения.
   - Получить доступ к данным о местоположении устройства.

   Нажмите **Разрешить** на всех сообщениях. Если вы отклоните один из запросов, вы не сможете подключиться к серверу.

Подключение с конфигурационным файлом

Настройки подключения к серверу централизованной защиты содержатся в файле `install.cfg`, который предоставляется администратором антивирусной сети компании или IT-провайдером.

1. Убедитесь в наличии подключения к сети.
2. Поместите файл `install.cfg` в корневую папку или любую из папок первого уровня вложенности внутренней памяти устройства.
3. На экране настроек (см. Рисунок 29) выберите **Администрирование**.

   Если на устройстве включен Антивор Dr.Web, при переходе в раздел **Администрирование** вам понадобится ввести пароль от учетной записи Dr.Web.
4. Установите флажок **Агент Dr.Web**.

   Если файл загружен на устройство, поля для ввода параметров подключения к серверу будут заполнены автоматически.

   > В приложении, установленном при помощи мастера установки, предоставленного администратором антивирусной сети, флажок **Агент Dr.Web** установлен по умолчанию. Приложение начинает искать конфигурационный файл и пытаться подключиться к серверу сразу после установки. Если файл не был найден или он содержит неверные параметры подключения, необходимо снять и установить заново флажок **Агент Dr.Web** и ввести параметры вручную или использовать конфигурационный файл с корректными настройками.

5. Нажмите кнопку **Подключиться**.

Сброс параметров подключения

1. Нажмите **Меню** на экране ввода параметров подключения.
2. Выберите опцию **Сбросить параметры подключения**.

После сброса параметров файл `install.cfg`, содержащий используемые параметры подключения, будет удален. Если на устройстве есть другой файл `install.cfg`, будут использоваться параметры подключения из этого файла. Таким образом, параметры

подключения будут сброшены только после того, как будут удалены все файлы `install.cfg`.

Ошибки при подключении

Неподдерживаемая опция. Ошибка возникает, если на сервере включены опции шифрования и/или сжатия трафика, не поддерживаемые Dr.Web. Обратитесь к администратору антивирусной сети или IT-провайдеру для решения проблемы.

Срок действия лицензии (подписки) истек. Для подключения к серверу централизованной защиты обратитесь к администратору антивирусной сети для получения лицензии или продлите подписку на услугу Dr.Web AV-Desk.

Подписка заблокирована. Для подключения к серверу централизованной защиты обратитесь к IT-провайдеру, предоставляющему услугу Dr.Web AV-Desk, для разблокировки подписки.

Подключение не установлено. На сервере централизованной защиты запрещен запуск Dr.Web для Android. Ошибка возникает, если ваш тарифный план не предусматривает использование Dr.Web для Android или запуск Dr.Web для Android запрещен администратором антивирусной сети.

10.2. Фильтр приложений

Если на сервере централизованной защиты включена возможность настройки фильтра приложений, вы можете настроить список приложений, которые могут быть запущены на вашем устройстве. Для этого выполните следующие действия:

1. На главном экране приложения откройте раздел **Администрирование**.
2. Выберите приложения, которые будут доступны на устройстве.
3. Нажмите кнопку **Разрешить выбранные**. Заданные настройки будут переданы на сервер и сохранены как персональные настройки для вашего устройства.

Если вы являетесь администратором антивирусной сети, на сервере централизованной защиты вы можете настроить списки доступных приложений для всех устройств в сети на основе ваших персональных настроек, сохраненных на сервере.

Функция доступна на устройствах с Android 4.4.

10.3. Переход в автономный режим

Чтобы перевести Dr.Web в автономный режим, откройте экран настроек (см. Рисунок 29) и выберите пункт **Администрирование**. После этого снимите флажок **Агент Dr.Web**.

При включении режима автономной работы восстанавливаются все настройки антивируса, установленные до перехода в централизованный режим, или настройки по умолчанию. Также возобновляется доступ ко всем функциональным возможностям Dr.Web.

Для работы в автономном режиме требуется действующая персональная лицензия. Лицензия, полученная автоматически с сервера централизованной защиты, в данном режиме использоваться не может. При необходимости вы можете купить или продлить персональную лицензию.

11. Dr.Web на Android TV

На главном экране приложения (см. Рисунок 31) доступны следующие опции:

- События
- Сканер
- Брандмауэр
- Аудитор безопасности
- Разное

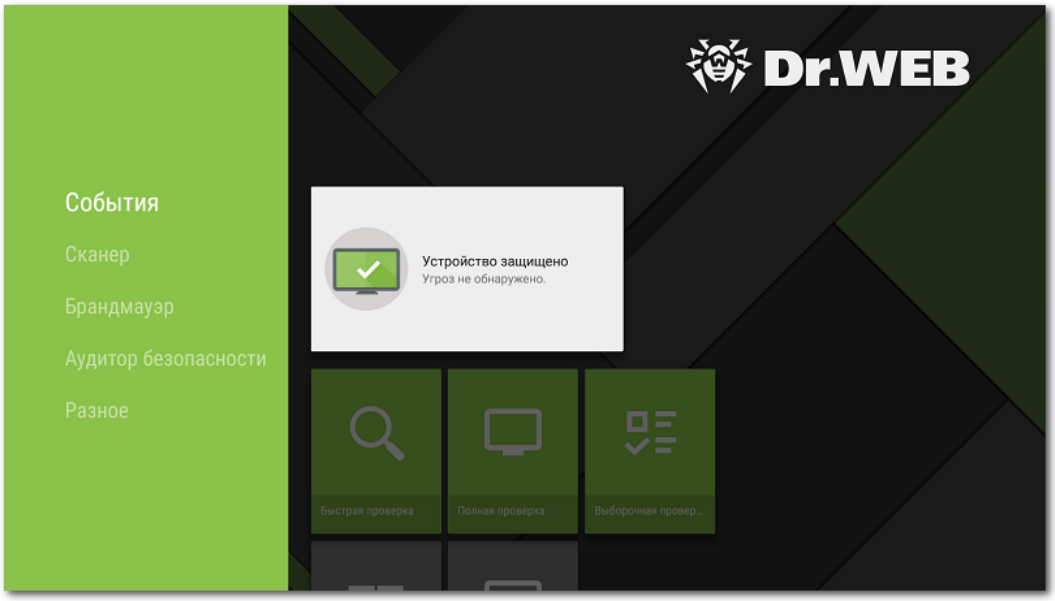

Рисунок 31. Dr.Web для Android TV

Особенности работы Dr.Web на Android TV

На устройствах под управлением Android TV режим централизованной защиты недоступен.

Разрешения

При первом запуске приложение попросит вас предоставить следующие разрешения:

- Доступ к фото, мультимедиа и файлам на устройстве.
- Доступ к контактам.

Разрешите приложению доступ к необходимым функциям и данным.

Интерфейс

- Нет возможности создания виджета для рабочего стола.
- Недоступна панель уведомлений.

11.1. События на Android TV

Панель **События** отображает текущее состояние защиты устройства.

- Индикатор зеленого цвета указывает на то, что устройство защищено. Дополнительных действий не требуется.
- Индикатор желтого цвета указывает на то, что приложение обнаружило проблемы, отсутствует лицензия и т.д. Чтобы узнать больше о найденных угрозах и устранить их, нажмите на панель состояния.
- Индикатор красного цвета означает, что приложение обнаружило угрозы безопасности. Чтобы обезвредить угрозы, нажмите на панель состояния.

Если приложение обнаружило несколько событий, требующих внимания пользователя, нажмите на панель состояния. Откроется окно **События**, в котором будут отображены все важные сообщения.

11.2. Антивирусная защита на Android TV

Основной функцией, реализованной в Dr.Web, является постоянная проверка файловой системы в режиме реального времени. Кроме того, Dr.Web осуществляет сканирование системы по запросу пользователя. При обнаружении угроз безопасности к ним применяются действия, выбранные пользователем.

11.2.1. Постоянная защита SpIDer Guard на Android TV

Включение постоянной защиты

При первом запуске Dr.Web постоянная защита автоматически включается после принятия Лицензионного соглашения. SpIDer Guard работает независимо от того, запущено приложение или нет. При обнаружении угроз безопасности в нижней части экрана появляется предупреждающий значок и сообщение о найденных угрозах.

Настройка

Чтобы включить, настроить или отключить постоянную защиту, на главном экране приложения выберите **Разное** - > **Настройки** - > **SpIDer Guard** (см. раздел Настройки Dr.Web на Android TV).

Статистика

Приложение регистрирует события, связанные с работой SpIDer Guard: включение/отключение, обнаружение угроз безопасности и результаты проверки памяти устройства и устанавливаемых приложений. Статистика SpIDer Guard отображается в разделе **Действия** на вкладке **Статистика** и отсортирована по дате (см. раздел Статистика).

11.2.2. Сканер Dr.Web на Android TV

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

Рекомендуется периодически пользоваться функцией сканирования файловой системы, если компонент SpIDer Guard какое-то время был неактивен. Обычно при этом достаточно проводить быструю проверку системы.

Проверка

Чтобы проверить систему, на главном экране выберите опцию **Сканер** (см. Рисунок 32) и выполните одно из следующих действий:

- Чтобы запустить сканирование только установленных приложений, выберите пункт **Быстрая проверка**.
- Чтобы запустить сканирование всех файлов системы, выберите пункт **Полная проверка**.
- Чтобы проверить отдельные файлы и папки, выберите пункт **Выборочная проверка**, затем выберите объект для проверки в появившемся окне.

  Вы можете проверить всю папку целиком. Для этого выберите опцию **Проверить папку**. Чтобы перейти на один уровень выше, выберите опцию **Наверх**.

Если на вашем устройстве открыт root-доступ, вы можете выбрать для проверки папки `/sbin` и `/data`, расположенные в корневой папке.

По окончании сканирования на экран выводится следующая информация:

- Количество проверенных объектов.
- Количество обнаруженных угроз.
- Время запуска сканирования.
- Длительность сканирования.

Чтобы открыть список обнаруженных угроз, нажмите **OK**.

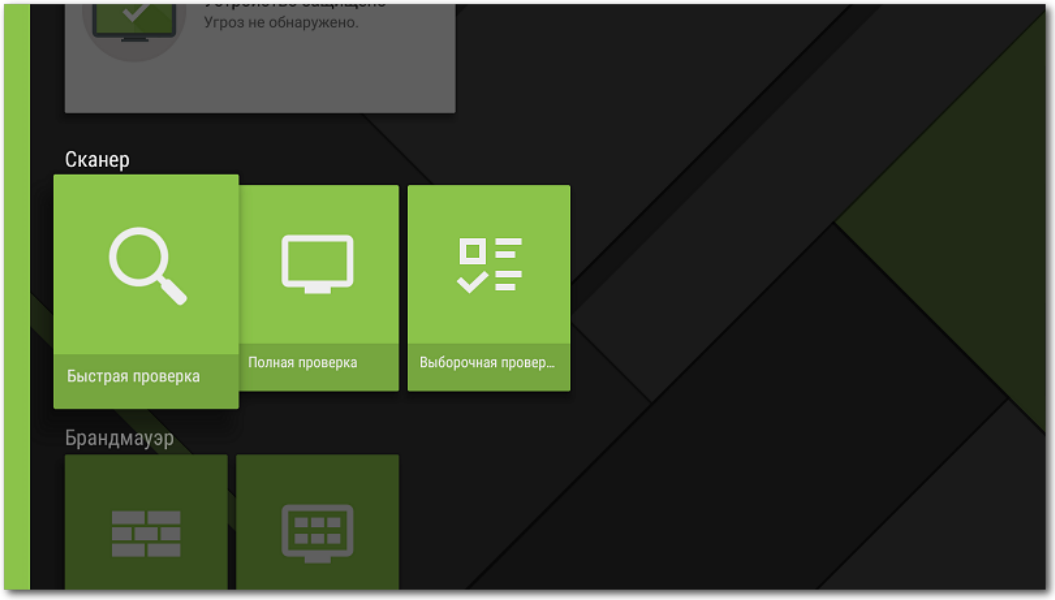

Рисунок 32. Сканер Dr.Web

Настройки Сканера Dr.Web

Для доступа к настройкам Сканера Dr.Web на главном экране приложения выберите **Разное** - > **Настройки** - > **Сканер** (см. раздел Настройки Dr.Web на Android TV).

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).

11.2.3. Обезвреживание угроз на Android TV

Просмотр списка угроз

Если компонент SplDer Guard обнаружит угрозу, внизу экрана появится предупреждающее сообщение с названием обнаруженной угрозы. Чтобы открыть список угроз, на главном экране выберите опцию **События**.

Чтобы открыть список угроз, обнаруженных Сканером Dr.Web, после окончания сканирования нажмите **OK**. Список угроз может быть закрыт только после применения действия к каждой из угроз.

Для каждой угрозы в списке показывается следующая информация:

- 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.

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.

11.2.4. Обнаружение угроз в системных приложениях на Android TV

Приложения, установленные в системной области, в некоторых случаях могут выполнять функции, характерные для вредоносных программ, поэтому при проверке системы Dr.Web 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 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**.

Данную операцию 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 **Разное** - > **Настройки** - > **Общие настройки** - > **Дополнительные опции**.

11.3. Брандмауэр Dr.Web на Android TV

Брандмауэр Dr.Web защищает ваше устройство от несанкционированного доступа извне и предотвращения утечки важных данных по сети. Этот компонент позволяет контролировать подключения и передачу данных по сети Интернет и блокировать подозрительные соединения.

Особенности использования

Брандмауэр Dr.Web реализован на базе технологии VPN для Android, что позволяет ему работать, не требуя получения прав суперпользователя (root) на устройстве. Реализация технологии VPN на Android связана с определенными ограничениями:

- В первую очередь, в каждый момент времени только одно приложение на устройстве может использовать VPN. В результате, когда приложение включает VPN на устройстве, открывается окно с запросом разрешения использования VPN для этого приложения. Если пользователь предоставит такое разрешение, приложение начинает использовать VPN, при этом другое приложение, использовавшее VPN до этого момента, теряет эту возможность. Такой запрос появляется при первом включении Брандмауэра Dr.Web и далее при каждой перезагрузке устройства. Кроме того, он может появляться и тогда, когда другие приложения запрашивают VPN. VPN

приходится делить между приложениями во времени, и брандмауэр может работать, только когда он полностью владеет правами на использование VPN.

- Включение Брандмауэра Dr.Web может привести к невозможности подключения устройства, на котором он запущен, к другим устройствам напрямую через Wi-Fi или локальную сеть. Это зависит от модели устройства и используемых для подключения приложений.
- При включенном Брандмауэре Dr.Web устройство не может использоваться в качестве точки доступа Wi-Fi.

> ⚠ Технология VPN для Android используется только для реализации функций брандмауэра, при этом VPN-туннеля не создаётся и интернет-трафик не шифруется.

Включение Брандмауэра Dr.Web

1. На главном экране приложения (см. Рисунок 33) выберите опцию **Брандмауэр**.
2. Чтобы включить Брандмауэр Dr.Web, нажмите кнопку **Включить** или используйте переключатель в правом верхнем углу экрана. По умолчанию брандмауэр отключен. При включении брандмауэра появится запрос на разрешение использования VPN Dr.Web. Для работы брандмауэра необходимо предоставить данное разрешение.

> ⚠ Если в ходе работы права на использование VPN переходят к другому приложению, Брандмауэр Dr.Web будет отключен, о чем будет выведено соответствующее предупреждение.
>
> ---
>
> Если вы работаете с устройством в режиме ограниченного доступа (гостевого профиля), вам недоступны настройки Брандмауэра Dr.Web.

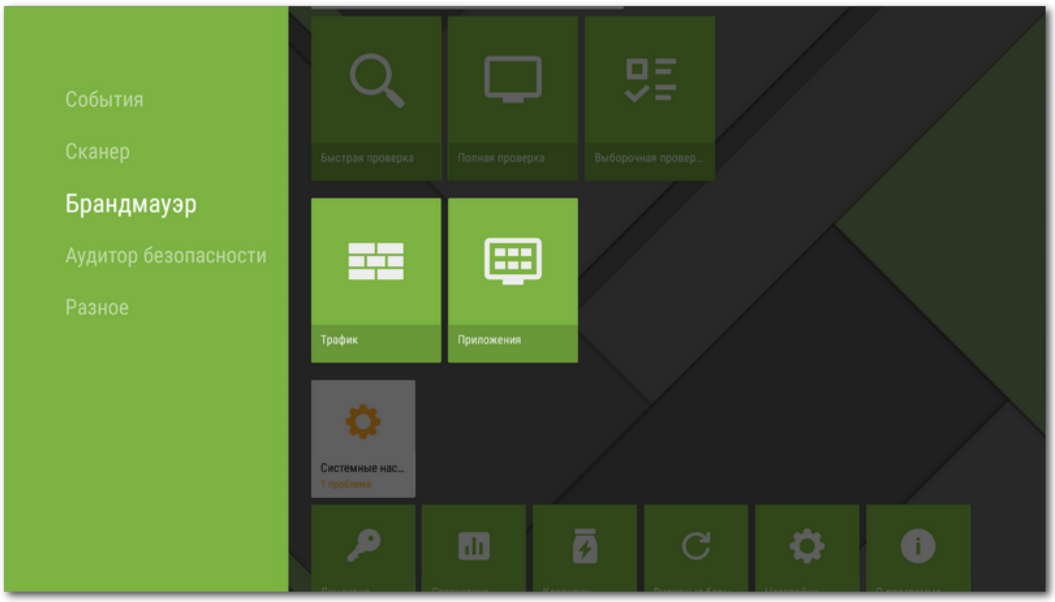

Рисунок 33. Брандмауэр Dr.Web на Android TV

11.3.1. Текущая активность сетевых подключений на Android TV

Информацию о текущей активности сетевых подключений можно получить на вкладке **Трафик** (см. Рисунок 34).

Вкладка Трафик

На вкладке в режиме реального времени показывается список подключений, инициированных установленными на устройстве приложениями. Для просмотра подробной информации о подключениях какого-либо приложения (IP-адресов и портов подключений, а также размере исходящего/входящего трафика), нажмите на него в списке.

Для подключений, указанных в списке, вы можете создать разрешающие или блокирующие правила. Нажмите и удерживайте подключение в списке, после чего выберите соответствующую опцию:

- **Добавить разрешающее правило**, чтобы создать правило, разрешающее соединения выбранного приложения с соответствующими IP-адресом и портом.
- **Добавить запрещающее правило**, чтобы создать правило, блокирующее все соединения выбранного приложения с соответствующими IP-адресом и портом.

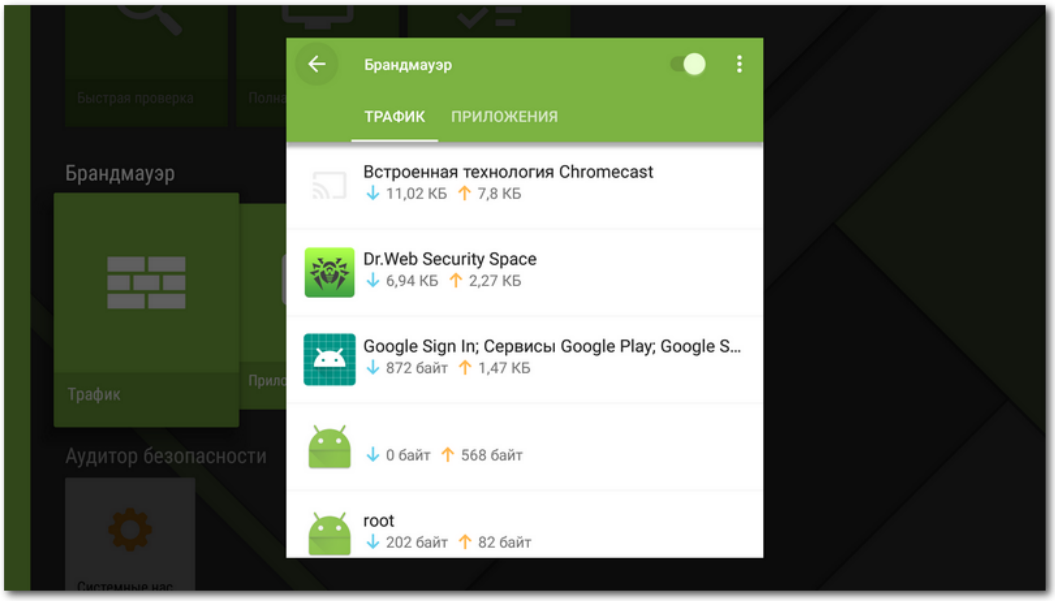

Рисунок 34. Вкладка Трафик

11.3.2. Обработка трафика приложений на Android TV

Брандмауэр Dr.Web позволяет настроить обработку интернет-трафика на уровне приложений и, таким образом, контролировать доступ программ и процессов к сетевым ресурсам. Ознакомиться с информацией об интернет-трафике, используемом установленными на вашем устройстве приложениями, а также настроить для них

правила доступа к сетевым ресурсам вы можете на вкладке **Приложения** (см. Рисунок 35).

На вкладке **Приложения** показывается общее количество переданных по сети данных, а также размер полученного и отправленного трафика. Вы можете посмотреть список приложений (и групп приложений), для каждого из которых указан размер израсходованного интернет-трафика.

Чтобы просмотреть список всех установленных на устройстве приложений, включая приложения с нулевым значением израсходованного трафика, на вкладке **Приложения** нажмите **Меню** и установите флажок **Все приложения**.

Приложения с измененными настройками выделены значком .

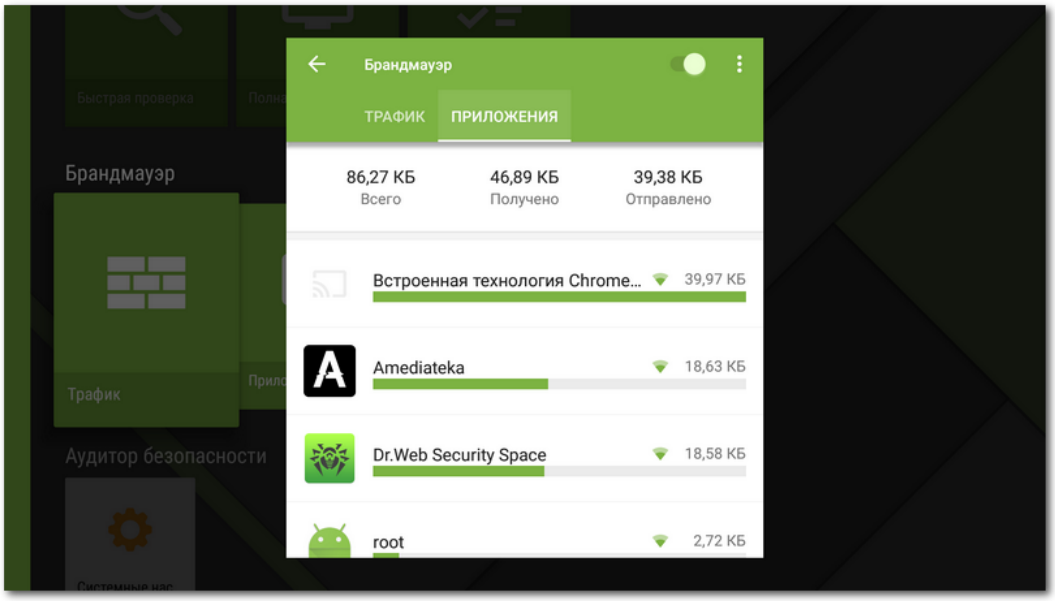

Рисунок 35. Вкладка Приложения

Настройки приложений

Чтобы открыть настройки приложения (или группы приложений), нажмите на приложение в списке.

Не контролировать приложение

Настройка недоступна для некоторых системных приложений.

Брандмауэр Dr.Web реализован на базе VPN для Android. VPN препятствует работе приложений, которые используют технологию, несовместимую с VPN, например, Wi-Fi Direct. Это может привести к невозможности подключения устройства к другим устройствам. В этом случае не рекомендуется полностью отключать Брандмауэр Dr.Web. Вместо этого отключите контроль Брандмауэра Dr.Web для нужного приложения (группы приложений):

1. На вкладке **Приложения** (см. Рисунок 35) выберите приложение (группу приложений).
2. На экране **Настройки приложения** нажмите **Меню** ⋮.
3. Выберите **Не контролировать приложение**.

Рекомендуется отключать контроль Брандмауэра Dr.Web только для тех приложений, которым доверяете.

При включении этой опции, Брандмауэр Dr.Web не контролирует сетевые подключения этого приложения, даже если в настройках Брандмауэра Dr.Web установлены ограничения. Трафик приложения не учитывается.

Доступ к передаче данных

Для каждого приложения вы можете разрешить/запретить использование Wi-Fi с помощью соответствующей опций в разделе **Доступ к передаче данных**.

Статистика

Статистика использования Интернета показана в разделе Статистика в виде диаграммы.

Правила для IP-адресов и портов

Настроить правила обработки подключений для выбранного приложения (группы приложений) можно в разделе Правила подключения.

Журнал приложения

События, связанные с сетевой активностью приложений, установленных на устройстве, записываются в журналы приложений.

11.3.2.1. Статистика использования интернет-трафика на Android TV

На экране с подробной информацией о трафике приложения (группы приложений) вы можете ознакомиться со статистикой использования Интернета данным приложением в виде графической диаграммы (см. Рисунок 36).

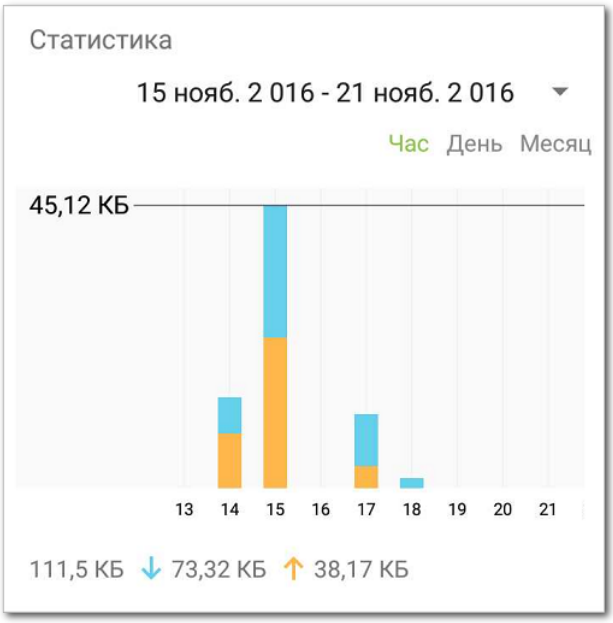

Рисунок 36. Статистика использования интернет-трафика

На диаграмме оранжевым цветом отмечен исходящий трафик приложения, голубым – входящий. Под диаграммой приведены численные значения израсходованного трафика (общего, исходящего и входящего).

При просмотре статистики использования интернет-трафика вы можете выполнить следующие действия:

- Выбрать период времени для просмотра статистики в соответствующем списке над диаграммой. Вы можете просмотреть статистику за текущий день, последнюю неделю, текущий месяц, предыдущий месяц или самостоятельно задать период времени, указав даты его начала и окончания.
- В рамках выбранного периода настроить отображение статистики по часам, дням или месяцам.

Удаление статистики

- Удаление статистики для всех приложений:
  1. На экране **Брандмауэр** на любой вкладке нажмите **Меню** и выберите опцию **Очистить**.
  2. В открывшемся окне установите флажок **Очистить статистику**. Нажмите **ОК**.
- Удаление статистики для отдельного приложения:
  1. На вкладке **Приложения** выберите приложение, для которого вы хотите очистить статистику.
  2. На экране **Настройки приложения** нажмите **Меню** и выберите опцию **Очистить**.
  3. В открывшемся окне установите флажок **Очистить статистику для этого приложения**. Нажмите **ОК**.

11.3.2.2. Правила подключений на Android TV

На экране с подробной информацией о трафике приложения (группы приложений) вы также можете задать правила подключений этого приложения к определенным IP-адресам и портам.

Создание правила

1. Чтобы создать правило, нажмите кнопку **Добавить правило** в разделе **Правила для IP-адресов и портов**. Вы можете добавить разрешающие и запрещающие правила в зависимости от значения соответствующей опции:
   - **Блокировать подключения из списка** – запрещающее правило.
   - **Разрешить только подключения из списка** – разрешающее правило.
2. В открывшемся окне в поле **Адрес сервера** укажите действительный IP-адрес (в формате a.b.c.d), диапазон IP-адресов (в формате a1.b1.c1.d1-a2.b2.c2.d2) или целую сеть (в формате a.b.c.0/n, где n – число от 1 до 32) или оставьте данное поле пустым (в таком случае необходимо обязательно определить порт подключения). В поле **Порт** укажите номер действительного порта или оставьте его пустым (в таком случае требуется обязательно задать IP-адрес подключения). В случае если одно из полей оставлено пустым, правило будет действовать для любых IP-адресов или портов. Нажмите кнопку **ОК**, чтобы сохранить созданное правило.

   Если вы выбрали опцию **Разрешить только подключения из списка** и не добавили ни одного адреса в список, блокироваться будут все подключения.
3. Чтобы отредактировать существующее правило, нажмите и удерживайте его в списке, далее нажмите кнопку **Редактировать**.

Кроме того, вы можете добавлять разрешающие и запрещающие правила при просмотре журналов приложений или списка текущих подключений.

Удаление правил подключения

- Чтобы удалить правило, нажмите и удерживайте его в списке, далее нажмите кнопку **Удалить**.
- Чтобы удалить все правила для определенного приложения:
  1. На экране **Брандмауэр** на вкладке **Приложения** выберите это приложение (см. Рисунок 35).
  2. На экране **Настройки приложения** нажмите **Меню** и выберите опцию **Очистить**.
  3. В открывшемся окне установите флажок **Удалить правила для этого приложения**. Нажмите **ОК**.
- Чтобы удалить все правила для всех приложений:
  1. На экране **Брандмауэр** нажмите **Меню** и выберите опцию **Очистить**.

2. В открывшемся окне установите флажок **Удалить правила для приложений**. Нажмите **ОК**.

Разрешение входящих подключений

Чтобы разрешить все входящие подключения для приложения:

1. На вкладке **Приложения** (см. Рисунок 35) выберите приложение, для которого нужно разрешить входящие подключения.
2. На экране **Настройки приложения** нажмите **Меню** ⋮.
3. Установите флажок **Разрешить входящие подключения**.

Информация о соединениях, инициированных с любых удаленных адресов с портом, открытым данным приложением, фиксируется в журнале приложения и статистике работы брандмауэра лишь частично. Кроме того, любые соединения с этими адресами могут быть исключены из проверки брандмауэром и для остальных приложений. Такой режим работы не является безопасным и в общем случае использовать его не рекомендуется.

Разрешение входящих подключений оправдано в том случае, когда иными способами невозможно избежать отключения брандмауэра, например, если на устройстве настроен сервер, принимающий соединения из внешних сетей.

11.3.3. Журнал Брандмауэра Dr.Web на Android TV

Чтобы просмотреть список всех событий, связанных с работой Брандмауэра Dr.Web, на экране **Брандмауэр** нажмите **Меню** ⋮ в правом верхнем углу экрана и выберите опцию **Журнал**.

Просмотр журнала событий

Для упрощения поиска информации вы можете использовать функции сортировки записей и быстрого скроллинга (путем перемещения специального графического элемента в правой части экрана) при просмотре списка событий. Для сортировки записей в журнале, выберите критерий сортировки в меню на экране журнала.

Для каждого события в журнале показывается следующая информация:

- Дата и время соединения (для TCP) или время, за которое получены пакеты данных с соответствующими величинами трафика (для UDP). Например: 18/02/2014 2:07:11 - 18/02/2014 2:07:12.
- Локальный адрес и локальный порт. Например: src: 10.2.3.5:6881.
- Входящий и исходящий трафик (в байтах) или количество заблокированных пакетов. Например: in:103 out:112 или blocked packets:1.

- Идентификатор приложения на устройстве, ассоциированный с этим трафиком (User ID). Например: uid=10071.
- Количество ситуаций сетевых заторов (только для TCP). Например: traffic jam=0. Заторы трафика – это особая ситуация, когда клиентская программа не успевает разгружать TCP-буфер, в результате образуется затор, что может быть причиной медленной передачи данных по сети.

Очистка журнала

1. На экране **Брандмауэр** нажмите **Меню** и выберите опцию **Очистить**.
2. В открывшемся окне установите флажок **Очистить журнал** и нажмите **ОК**.

Размер журнала

По умолчанию для файла журнала установлен максимальный размер, равный 5 МБ. Чтобы изменить максимально разрешенный размер файла журнала:

1. На экране **Брандмауэр** нажмите **Меню** и выберите опцию **Очистить**.
2. В открывшемся окне измените значение, указанное в поле **Максимальный размер журнала**. Нажмите кнопку **ОК**.

11.3.4. Журналы приложений на Android TV

Чтобы просмотреть список событий, связанных с сетевыми подключениями того или иного приложения, установленного на вашем устройстве, на вкладке **Приложения** найдите нужное приложение в списке и нажмите на него. На экране **Настройки приложения** нажмите **Меню** и выберите пункт **Журнал приложения**.

Просмотр журнала приложения

Все события для данного приложения объединены по датам. Чтобы просмотреть список событий за какую-либо дату, нажмите на нее в списке. Для каждого события в списке показывается следующая информация:

- Время соединения (для TCP) или время, за которое получены пакеты данных с соответствующими величинами трафика (для UDP).
- Локальный адрес и локальный порт.
- Входящий и исходящий трафик или количество заблокированных пакетов.

Для соединений, указанных в журнале приложения, вы можете создать разрешающие или блокирующие правила. Нажмите и удерживайте соединение в списке, после чего выберите соответствующую опцию:

- **Добавить разрешающее правило**, чтобы создать правило, разрешающее соединения выбранного приложения с соответствующими IP-адресом и портом.

- **Добавить запрещающее правило**, чтобы создать правило, блокирующее все соединения выбранного приложения с соответствующими IP-адресом и портом.

Очистка журнала приложения

1. На экране **Настройки приложения** нажмите **Меню** ⋮ и выберите опцию **Очистить**.
2. В открывшемся окне установите флажок **Очистить журнал для этого приложения**. Нажмите **ОК**.

Отключение регистрации событий для приложения

1. На экране **Настройки приложения** нажмите **Меню** ⋮ и выберите опцию **Очистить**.
2. В открывшемся окне установите флажок **Не вести журнал для этого приложения**. Нажмите **ОК**.

11.4. Аудитор безопасности на Android TV

Dr.Web проводит диагностику и анализ безопасности вашего устройства и устраняет выявленные проблемы и уязвимости с помощью специального компонента – **Аудитора безопасности**. Данный компонент начинает работать автоматически после первого запуска приложения и регистрации лицензии.

Возможные проблемы и способы их устранения

Чтобы просмотреть список обнаруженных проблем безопасности (см. Рисунок 37), выберите **Аудитор безопасности** на главном экране приложения.

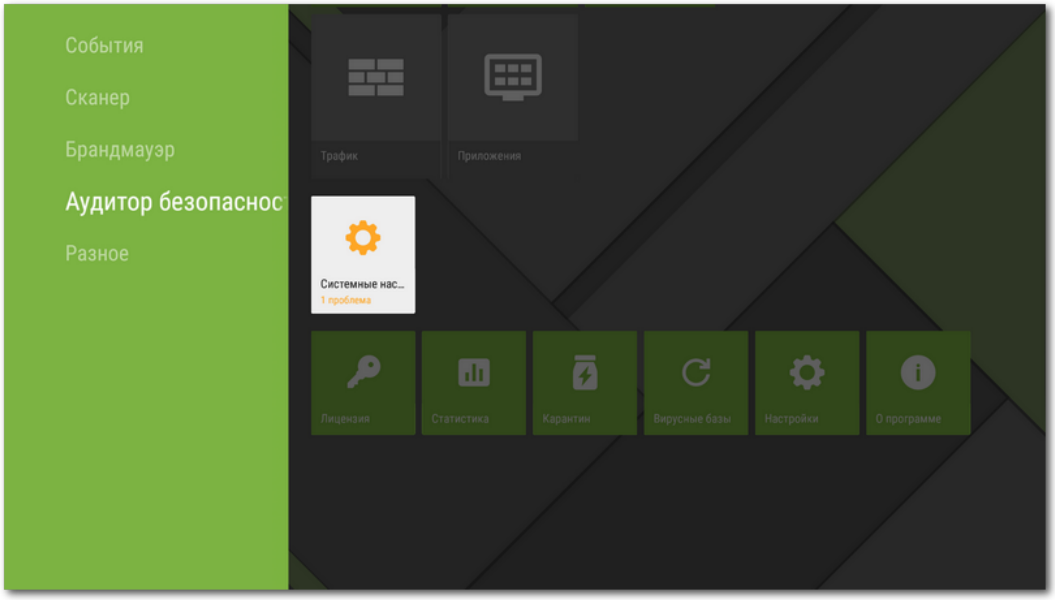

Рисунок 37. Список проблем безопасности, обнаруженных на устройстве

Dr.Web выявляет следующие типы проблем безопасности: наличие приложений с наивысшим приоритетом обработки SMS, скрытых администраторов устройства, уязвимостей и системных настроек, влияющих на безопасность устройства. Чтобы просмотреть подробную информацию о той или иной проблеме и способе ее устранения, раскройте список соответствующей категории и выберите проблему/уязвимость в списке.

Системные настройки

К системным настройкам, влияющим на безопасность устройства, относятся режим отладки и разрешение установки приложений из неизвестных источников. Кроме того, небезопасным является использование конфликтующего ПО:

- **Отладка по USB** предназначена для разработчиков и позволяет копировать данные с компьютера на устройство под управлением Android и наоборот, устанавливать на устройство приложения, просматривать данные журналов установленных приложений, а также удалять их в некоторых случаях. Если вы не являетесь разработчиком и не используете режим отладки, рекомендуется его отключить. Для перехода к соответствующему разделу системных настроек нажмите кнопку **Настройки** на экране с подробной информацией о данной проблеме.
- **Установка приложений из неизвестных источников** является основной причиной распространения угроз для устройств под управлением Android. Приложения, загруженные не из официального каталога приложений (Google Play) с большой вероятностью могут оказаться небезопасными и причинить вред устройству. Для снижения риска установки небезопасных приложений рекомендуем запретить установку приложений из неизвестных источников. Для перехода к соответствующему разделу системных настроек нажмите кнопку **Настройки** на экране с подробной информацией о данной проблеме. Кроме того, рекомендуется проверять все устанавливаемые приложения на наличие угроз. Перед проверкой необходимо убедиться, что вирусные базы Dr.Web обновлены.
- **Конфликты ПО**. Использование конфликтующего ПО.
- **Уведомления Dr.Web заблокированы**. При заблокированных уведомлениях Dr.Web не может оперативно информировать об обнаруженных угрозах. Это снижает защиту устройства и может привести к его заражению. Поэтому рекомендуется перейти в настройки вашего устройства и включить уведомления Dr.Web.

Уязвимости

Под *уязвимостью* понимается недостаток в программном коде, который может быть использован злоумышленниками для нарушения работы системы.

Dr.Web позволяет обнаружить в системе устройства такие уязвимости, как Janus, BlueBorne, Master Key (#8219321), Extra Field (#9695860), Name Length Field (#9950697), Fake ID (#13678484), ObjectInputStream Serialization (CVE-2014-7911), PendingIntent (CVE-2014-8609), Android Installer Hijacking, OpenSSLX509Certificate (CVE-2015-3825), Stagefright и

Stagefright 2.0, SIM Toolkit (CVE-2015-3843). Воспользовавшись данными уязвимостями, злоумышленники могут добавить программный код в ряд приложений, в результате чего данные приложения могут начать выполнять функции, представляющие угрозу безопасности устройства. Dr.Web также выявляет наличие в системе уязвимости Heartbleed – ошибки в криптографическом программном обеспечении OpenSSL, позволяющей злоумышленникам получить доступ к конфиденциальным данным пользователя.

В случае обнаружения одной или нескольких из перечисленных уязвимостей, проверьте доступность обновлений для операционной системы вашего устройства на сайте производителя, поскольку в новых версиях они могут быть устранены. В случае отсутствия обновлений рекомендуем устанавливать приложения только из проверенных источников.

Пользовательские сертификаты

Если на устройстве были обнаружены пользовательские сертификаты, информация об этом будет отображена в Аудиторе безопасности. Из-за установленных пользовательских сертификатов третьи лица могут просматривать вашу сетевую активность. Если вы не знаете назначение обнаруженных сертификатов, рекомендуется удалить их с устройства.

Приложения, использующие уязвимость Fake ID

Если на устройстве были обнаружены приложения, использующие уязвимость Fake ID, они будут отображаться в отдельной категории Аудитора безопасности. Эти приложения могут быть вредоносными, поэтому рекомендуется их удалить. Чтобы удалить приложение, нажмите кнопку **Удалить** на экране с подробной информацией о проблеме, связанной с данным приложением, или воспользуйтесь средствами операционной системы.

Root-доступ

Кроме того, устройство может стать уязвимым к различным типам угроз, если на нем открыт root-доступ, т.е. выполнены изменения, связанные с получением прав суперпользователя (root). Это позволяет изменять и удалять системные файлы, что может привести к неработоспособности устройства. Если вы выполнили данные изменения самостоятельно, рекомендуем отменить их в целях безопасности. Если же наличие root-доступа является технической особенностью вашего устройства или необходимо вам для выполнения тех или иных задач, будьте особо внимательны при установке приложений из неизвестных источников.

11.5. Разное

Раздел **Разное** (см. Рисунок 38) позволяет перейти к настройкам приложения, получить доступ к карантину и статистике. Вы можете ознакомиться с информацией о версии приложения, о лицензии и датах ее активации и окончании срока действия. Также вы можете посмотреть дату последнего обновления вирусных баз и выполнить обновление вручную.

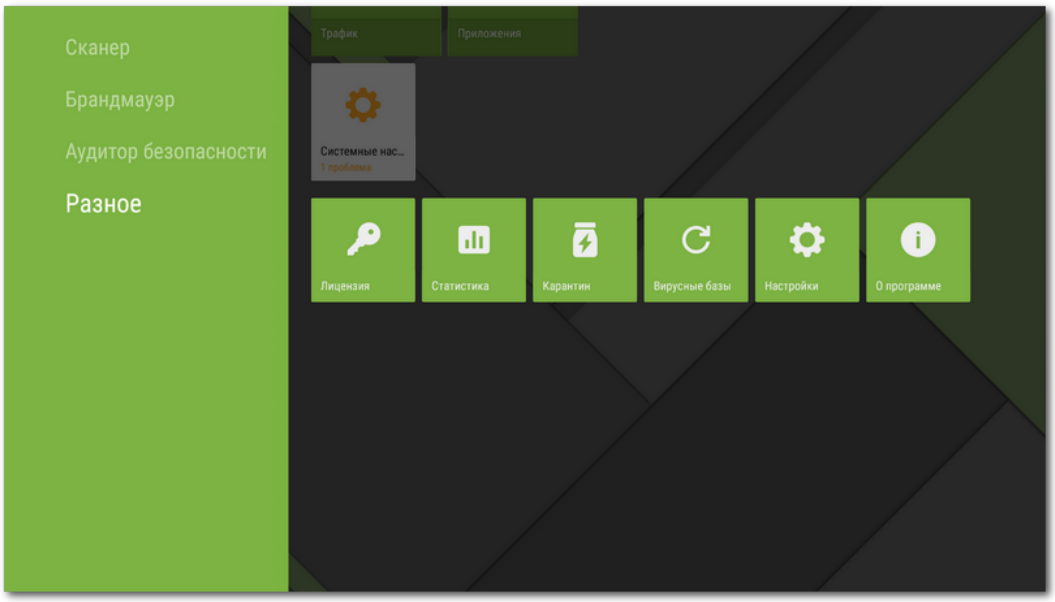

Рисунок 38. Разное

Лицензия

Вы можете просмотреть даты регистрации и окончания срока действия лицензии.

Из этого окна вы также можете приобрести и активировать новую лицензию.

Статистика

Раздел **Статистика** позволяет просмотреть информацию о результатах проверки Сканером Dr.Web, включении/отключении компонента SpIDer Guard, обнаруженных угрозах и действиях по их обезвреживанию (см. раздел Статистика).

Карантин

Карантин – это специальная папка, предназначенная для изоляции и безопасного хранения обнаруженных угроз (см. раздел Карантин).

Вирусные базы

Для обнаружения угроз безопасности Dr.Web 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

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

1. Откройте раздел **Вирусные базы**.
2. В открывшемся окне вы увидите статус вирусных баз и дату последнего обновления.

   Если вирусные базы устарели, вам нужно выполнить обновление вручную. Для этого нажмите **Обновить** на панели справа.

> Сразу после установки приложения рекомендуется выполнить обновление вирусных баз, чтобы Dr.Web 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

Раздел **Настройки** позволяет настроить компоненты антивирусной защиты, задать общие настройки приложения, включить и отключить функцию отправки статистики и сбросить настройки приложения до настроек по умолчанию (см. раздел Настройки Dr.Web на Android TV).

О программе

На экране **О программе** вы можете посмотреть версию приложения. Кроме того, на данном экране расположены ссылки на официальный сайт компании «Доктор Веб».

11.5.1. Настройки Dr.Web на Android TV

Общие настройки

- **Звук** позволяет настроить звуковые оповещения об обнаружении угроз, их удалении или перемещении в карантин. По умолчанию звуковые уведомления включены.

- **Отправка статистики** позволяет включить или отключить отправку статистики в компанию «Доктор Веб».
- **Дополнительные опции** содержит следующие дополнительные настройки:
  - **Системные приложения** позволяет включить или отключить информирование об обнаружении угроз в системных приложениях. По умолчанию эта опция отключена.

SpIDer Guard

- **Файлы в архивах** позволяет включить проверку файлов в архивах.

По умолчанию проверка архивов отключена. Включение проверки архивов может сказаться на быстродействии системы. 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**.

- **Встроенная SD-карта и съемные носители** позволяет включить проверку встроенной SD-карты и съемных носителей при каждом подключении. Если эта настройка включена, проверка запускается при каждом включении компонента SpIDer Guard.
- **Дополнительные опции** позволяет включить и отключить проверку системы на наличие рекламных программ и потенциально опасных программ (в том числе, программ взлома и программ-шуток).

Сканер

- **Файлы в архивах** позволяет включить проверку файлов в архивах.

По умолчанию проверка архивов отключена. Включение проверки архивов может сказаться на быстродействии системы. 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**.

- **Дополнительные опции** позволяет включить и отключить проверку системы на наличие рекламных программ и потенциально опасных программ (в том числе, программ взлома и программ-шуток).

Еще

- **Сброс настроек** позволяет в любой момент сбросить пользовательские настройки приложения и восстановить настройки по умолчанию.
- **Новая версия** (опция доступна для версии, установленной с сайта компании «Доктор Веб») позволяет настроить проверку доступности новой версии при каждом обновлении вирусных баз приложения. При появлении новой версии приложения вы получите стандартное уведомление и сможете ее оперативно загрузить и установить.

12. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.

13. Приложение А. Забыли пароль?

Если вы забыли пароль от учетной записи Dr.Web, вы можете задать новый:

- С помощью электронной почты, которую вы указали при регистрации учетной записи или настройке Антивора Dr.Web.
- С помощью SMS с номера друга.
- С помощью запроса в службу технической поддержки.

> Если Dr.Web работает в режиме централизованной защиты и Антивор Dr.Web был настроен на сервере, вы не сможете задать новый пароль указанными способами. В этом случае обратитесь к администратору антивирусной сети или IT-провайдеру.

Задать новый пароль с помощью электронной почты

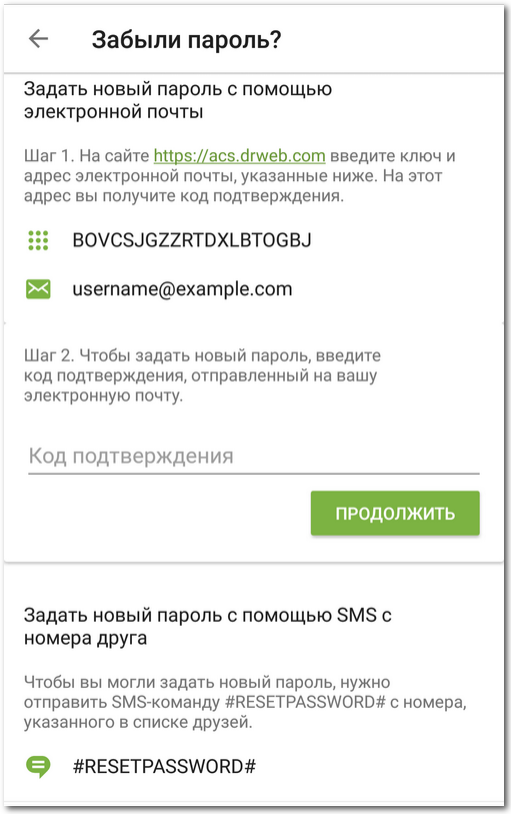

Рисунок 39. Задать новый пароль с помощью электронной почты

На экране **Забыли пароль?** (см. Рисунок 39) указаны:

Ключ. Это уникальная последовательность символов, которая была сгенерирована для вашей учетной записи.

Адрес электронной почты. Этот адрес вы использовали при регистрации учетной записи Dr.Web или настройке Антивора Dr.Web.

Чтобы задать новый пароль, выполните следующие действия:

1. На любом устройстве с доступом в Интернет откройте веб-страницу учетной записи Dr.Web: https://acs.drweb.com/ (см. Рисунок 40).

> Если у вас установлена версия Dr.Web 11.1.3 и ниже, для сброса настроек перейдите на страницу Антивора Dr.Web https://antitheft.drweb.com/ или обновите приложение до версии 12.

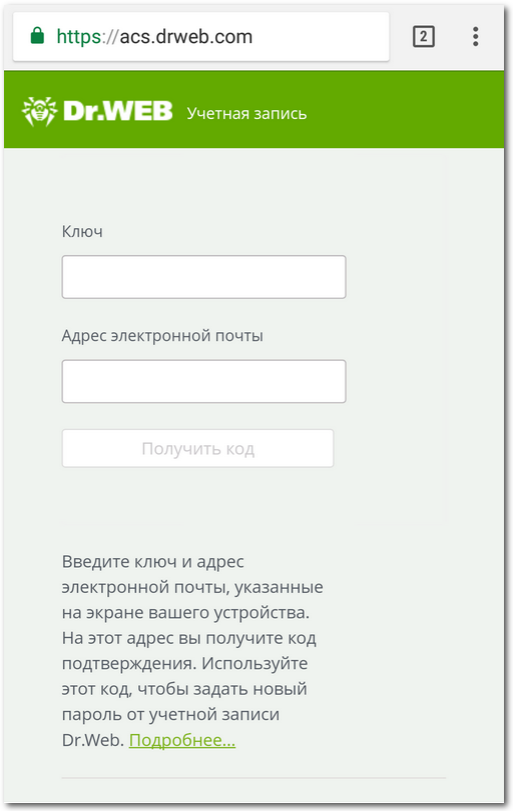

Рисунок 40. Учетная запись Dr.Web

2. На этой странице введите ключ и адрес электронной почты, указанные на экране **Забыли пароль?** (см. Рисунок 41).

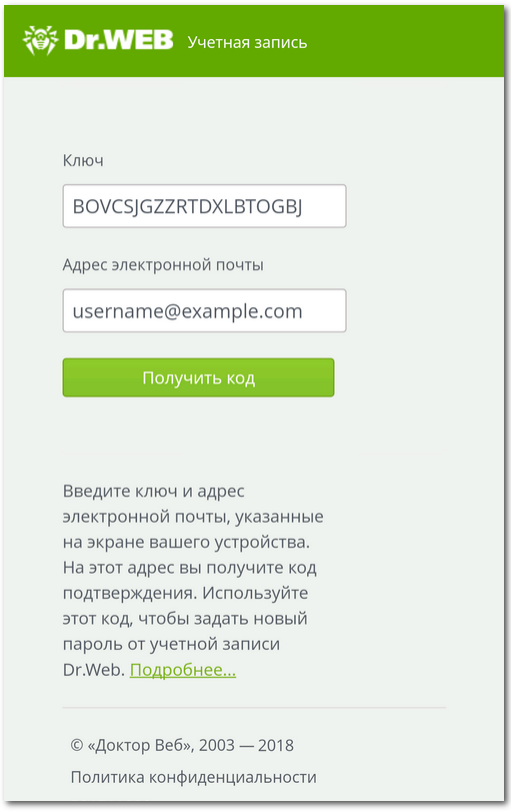

Рисунок 41. Ввод ключа и адреса электронной почты

3. Нажмите кнопку **Получить код**.

   Если данные введены правильно, вы увидите сообщение о том, что на ваш адрес электронной почты отправлено письмо с кодом подтверждения (см. Рисунок 42).

   Если в течение 10 минут вы не получите письмо:

   1. Проверьте папку Спам.
   2. Попробуйте ввести данные снова. Возможно, вы ввели неправильный ключ или не тот адрес электронной почты, который указан на экране **Забыли пароль?**.
   3. Если после этого вы не получили письмо, обратитесь в службу технической поддержки «Доктор Веб». Для этого нажмите **Не получили письмо?** (см. Рисунок 42).

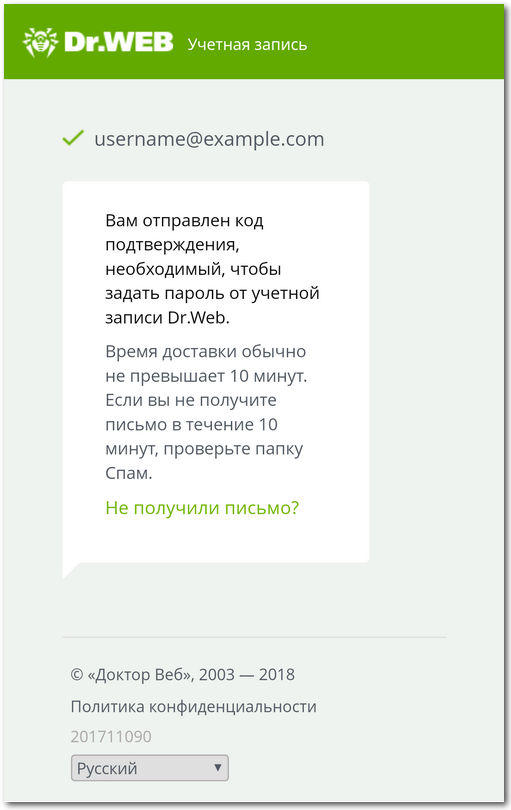

Рисунок 42. Уведомление

4. Откройте письмо от сервиса «Учетная запись Dr.Web». В письме указан код подтверждения.

5. На экране **Забыли пароль?** введите код подтверждения в поле **Код подтверждения** (см. Рисунок 43).

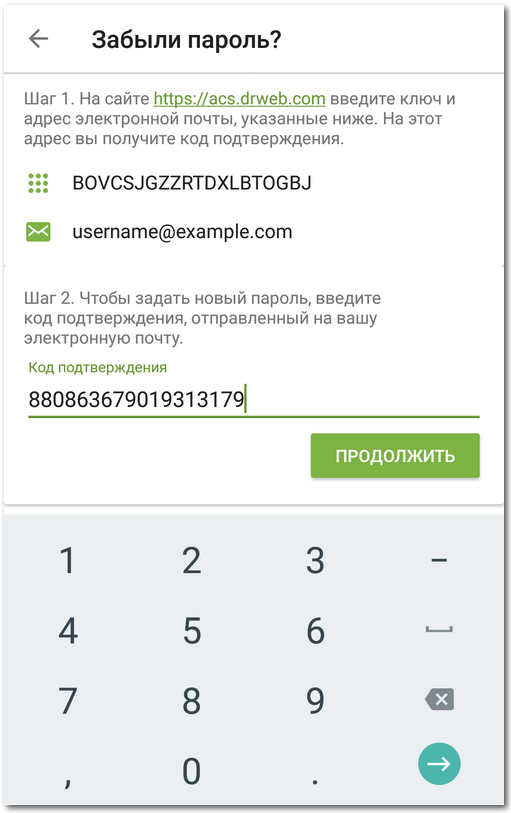

Рисунок 43. Ввод кода подтверждения, полученного по почте

6. Нажмите **Продолжить**.
7. На экране **Изменить пароль** введите новый пароль. Пароль должен содержать не менее 4 символов.

   Нажмите на значок справа от поля ввода, чтобы показать вводимые символы. Чтобы скрыть символы, нажмите на значок .
8. Повторите пароль и нажмите **Сохранить**.

Задать новый пароль с помощью SMS с номера друга

Вы можете задать новый пароль этим способом, если выполняются все условия:

1. Ваше устройство включено и находится в зоне действия сети.
2. На вашем устройстве включен Антивор Dr.Web.
3. В список друзей в Антиворе добавлен хотя бы один номер.
4. Номер, с которого будет отправлена SMS-команда, добавлен в список друзей.
5. Вы знаете телефонный номер SIM-карты, которая используется на вашем устройстве. SMS-команда может быть отправлена только на этот номер.

   Если вы не знаете этот номер, вы можете вставить SIM-карту с известным номером.

Если вы используете сразу 2 SIM-карты на вашем устройстве, SMS-команду можно отправить на любой из этих номеров.

Чтобы задать новый пароль, отправьте SMS с текстом **#RESETPASSWORD#** на ваше устройство. SMS-команда не зависит от регистра.

На экране **Забыли пароль?** в разделе **Список друзей** (см. Рисунок 44) вы можете проверить список номеров, с которых можно отправить SMS-команду.

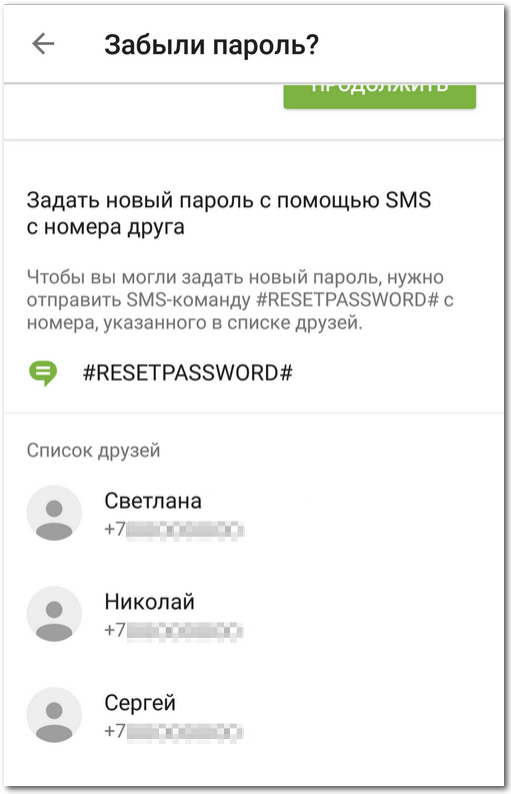

Рисунок 44. Задать новый пароль с помощью SMS с номера друга

При получении SMS на вашем устройстве автоматически появится экран **Изменить пароль**, где вы сможете задать новый пароль. Если устройство было заблокировано, оно разблокируется.

Задать новый пароль с помощью запроса в службу технической поддержки

Если вы не можете разблокировать устройство или задать новый пароль самостоятельно, вы можете отправить запрос в службу технической поддержки Dr.Web:

1. Откройте страницу службы технической поддержки: https://support.drweb.com/.
2. В разделе **Задать вопрос** ответьте на вопросы мастера поддержки, пока не откроется страница **Резюме запроса** (см. Рисунок 45).

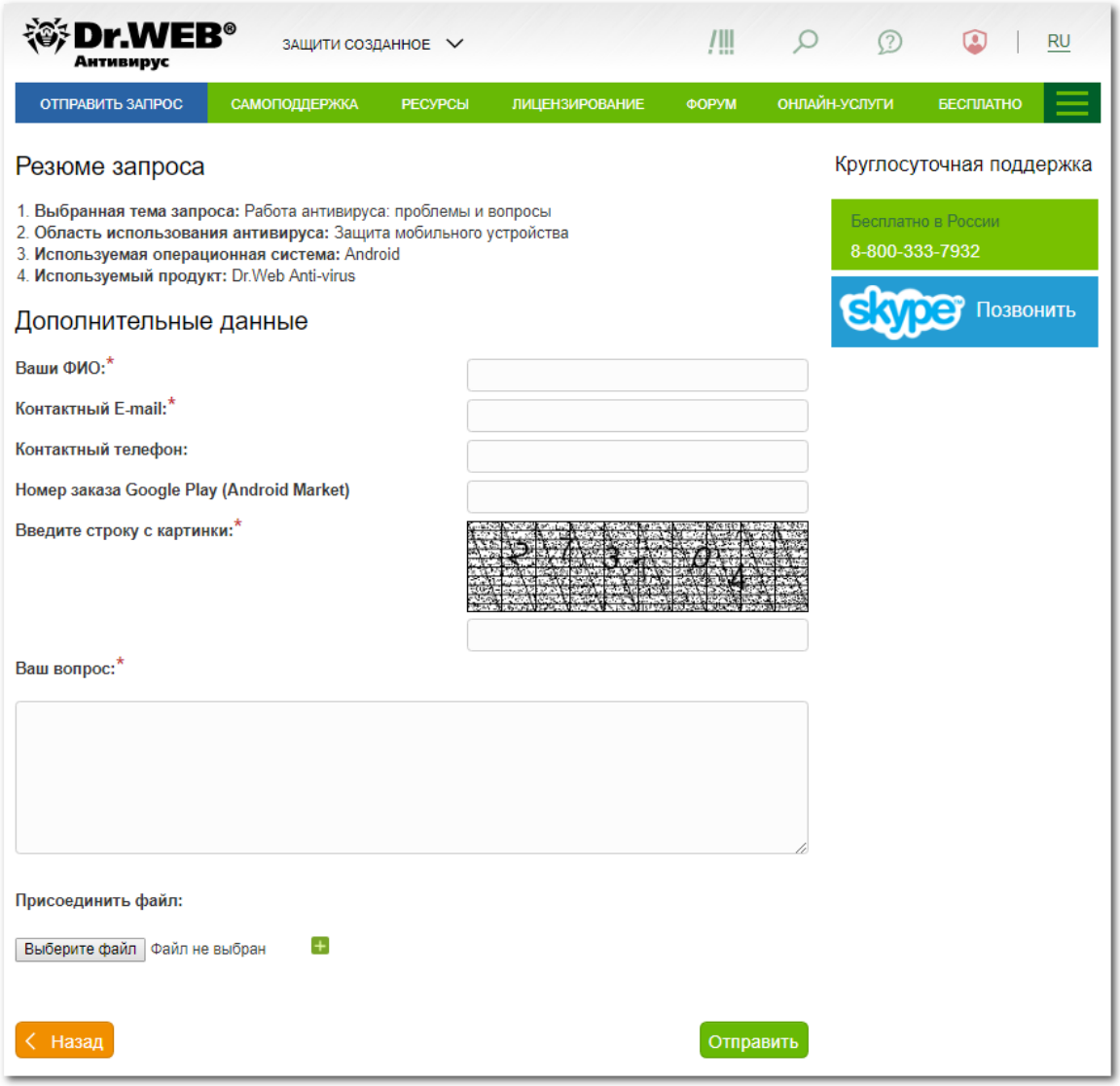

Рисунок 45. Резюме запроса

3. На странице **Резюме запроса** в разделе **Дополнительные данные** укажите запрашиваемые данные.
4. В поле **Ваш вопрос** кратко опишите вашу проблему.
5. Присоедините к запросу следующие файлы:
   - Фотография экрана **Забыли пароль?**, на которой должны быть ключ и адрес электронной почты (см. Рисунок 39).
   - Если у вас сохранилась оригинальная упаковка устройства, обязательно приложите к запросу фотографию упаковки с номером IMEI (уникальным 15-значным идентификатором вашего устройства).
   - Фотография или скан-копия чека на покупку устройства.
   - Фотография или скан-копия заполненного гарантийного талона.
   - Документы, подтверждающие оплату вами лицензии Dr.Web (письмо от интернет-магазина, платежный документ и др.). Если вы выиграли лицензию в аукционе

Dr.Web, укажите логин от вашей учетной записи к аккаунту на сайте «Доктор Веб». Если вы используете демо-версию, пропустите этот пункт.

Текст на изображениях должен быть четко различимым: специалисты службы технической поддержки обязаны убедиться, что вы владелец устройства и лицензии Dr.Web.

6. Нажмите кнопку **Отправить**.

   На адрес электронной почты, который вы указали в вашем запросе, вы получите письмо со ссылкой на ваш запрос. На странице вашего запроса будет указан код подтверждения.

7. На экране **Забыли пароль?** введите код подтверждения в поле **Код подтверждения** (см. Рисунок 43) и нажмите **Продолжить**.

8. На экране **Изменить пароль** введите новый пароль. Пароль должен содержать не менее 4 символов.

   Нажмите на значок справа от поля ввода, чтобы показать вводимые символы. Чтобы скрыть символы, нажмите на значок .

9. Повторите пароль и нажмите **Сохранить**.

14. Приложение Б. Дополнительная информация

Условия эксплуатации

Эксплуатация Dr.Web должна проводиться в нормальных климатических условиях:

1. Температура окружающего воздуха — от плюс 15 °C до плюс 35 °C;
2. Относительная влажность воздуха при температуре от плюс 25 °C до плюс 45 °C до 80 %;
3. Атмосферное давление — от 86 до 106 кПа (от 645 до 795 мм рт. ст.).

Правила транспортировки и хранения

При транспортировании и хранении ламинированных карт с информацией об изделии должны быть исключены резкие изменения температуры и относительной влажности окружающего воздуха, воздействие прямых солнечных лучей, механические воздействия способные повредить ламинированные карты или их упаковку. Транспортировка и хранение должны осуществляться в следующих климатических условиях:

1. Температура окружающего воздуха, °C: от минус 5 до плюс 55;
2. Относительная влажность воздуха, %: от 10 до 80 (при температуре 25 °C);
3. Атмосферное давление, кПа (мм рт. ст.): от 84,0 до 107,0 (от 630 до 800).

Правила реализации

Правила реализации Dr.Web Security Space для Android соответствуют требованиям законодательства Республики Беларусь, в частности:

- постановлению Совета Министров Республики Беларусь № 375 от 15 мая 2013 г. (Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY))
- приказу Оперативно-Аналитического Центра при Президенте Республики Беларусь № 94 от 17 декабря 2013 г. (О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY).

Программное средство Dr.Web Security Space для Android поставляется в виде дистрибутивов, размещенных на серверах ООО «Доктор Веб».

Дистрибутивы являются копией дистрибутивов, прошедших испытания в аккредитованной лаборатории для регистрации декларации, и хранятся в неизменном виде на серверах ООО «Доктор Веб».

Пользователь, приобретая Dr.Web Security Space для Android, получает ламинированную карту (носитель информации), оформленную в соответствии с корпоративными правилами компании ООО «Доктор Веб» и в соответствии с требованиями законодательства Республики Беларусь.

На носителе информации размещены:

- наименование и параметры программного продукта;
- серийный номер (лицензия) на Dr.Web Security Space для Android под стираемой защитной полосой;
- ссылка на дистрибутивы и эксплуатационную документацию Dr.Web Security Space для Android;
- товарный знак;
- страна изготовителя.

Эксплуатационные документы Dr.Web Security Space для Android содержат следующую информацию на русском языке:

- наименование и параметры средства защиты;
- товарный знак;
- страна изготовителя;
- назначение средства защиты;
- основные потребительские свойства;
- правила и условия безопасной эксплуатации (использования);
- правила и условия хранения, перевозки, реализации;
- меры, которые следует предпринять при обнаружении неисправности;
- местонахождение и контактные данные изготовителя;
- наименование и местонахождение уполномоченного представителя изготовителя, импортера, контактные данные;
- дата изготовления средств защиты информации;
- обязательства изготовителя (уполномоченного представителя изготовителя) по установке, сопровождению и поддержке средства защиты информации.

Для осуществления контроля реализации декларируемой партии изделий Dr.Web в соответствии с положениями постановлением Совета Министров Республики Беларусь № 375 от 15 мая 2013 г., изготавливаемые ламинированные карточки с серийными номерами вышеуказанного программного средства выпускаются в количестве, не превышающем декларируемый объём, и имеют уникальный идентификационный порядковый номер, наносимый в процессе их производства. Таким образом контролируется реализация всей декларируемой партии программного изделия Dr.Web Security Space для Android. Не допускается изменение/исправление идентификационного номера.

Монтаж (установка) и утилизация (удаление)

Установка и удаление Dr.Web производятся согласно разделам Установка Dr.Web и Обновление и удаление Dr.Web.

Гарантийные обязательства

1. Соблюдение Пользователем правил эксплуатации, транспортировки и хранения, указанных в эксплуатационной документации на Dr.Web, является обязательным.
2. Период применения Dr.Web, а также приобретения новых версий компонентов Dr.Web, определяется Пользователем, исходя из требуемого уровня защиты от вредоносных программ на объекте Пользователя.
3. Гарантийный срок эксплуатации программного обеспечения ограничен сроком действия, указанным на носителе информации.
4. Изготовитель в течение гарантийного срока гарантирует, что выполняемые Dr.Web функции соответствуют указанным в разработанной на него документации.
5. Изготовитель в течение гарантийного срока безвозмездно устраняет дефекты в функционировании Dr.Web, если эти дефекты получились по вине изготовителя.
6. Если в течение гарантийного срока Пользователь внес изменения в Dr.Web или в какую-либо его составляющую без согласования с Изготовителем изделия и/или нарушил правила эксплуатации, транспортировки и хранения, указанные в эксплуатационной документации на Dr.Web, то действие гарантии прекращается с момента внесения изменений и/или нарушения правил эксплуатации, транспортировки и хранения.
7. Администратор Dr.Web обязан подписаться на рассылку сообщений ленты новостей ООО «Доктор Веб» или периодически проверять в новостной ленте наличие сообщений об обновлении продукта или о компенсирующих мерах, направленных на нейтрализацию выявленной уязвимости.

Предметный указатель

Предметный указатель

Предметный указатель

Предметный указатель

P

C

Предметный указатель

Т

У

Ф

Ч