Dr.WEB

Mobile Security Suite (Android)

Руководство пользователя

Dr.Web Mobile Security Suite (Android)
Версия 12.9
Руководство пользователя
23.05.2025

ООО «Доктор Веб», Центральный офис в России

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

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

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

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение

Dr.Web Mobile Security Suite (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.

На устройствах под управлением Android TV режим централизованной защиты недоступен. Чтобы проверить, поддерживают ли работу в режиме централизованной защиты ваше устройство и версия приложения Dr.Web, см. раздел Режим централизованной защиты.

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`	Наименования файлов и каталогов, фрагменты программного кода.

Обозначение	Комментарий
`storage/Android/`	
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.
- Отслеживает изменения в системной области.
- Удаляет обнаруженные угрозы безопасности или перемещает их в карантин.
- Разблокирует устройство, если его заблокировала программа-вымогатель.
- Фильтрует входящие звонки и СМС-сообщения (фильтрация СМС-сообщений недоступна в версиях приложения, установленных из Google Play).
- 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 сайтам, а также категориям сайтов в стандартном браузере Android, Google Chrome, Яндекс.Браузер, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Спутник, Boat Browser и Atom.
- Находит и помогает устранить проблемы безопасности и уязвимости.
- Контролирует интернет-соединения, 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:

Параметр	Требования
Операционная система	Android версии 4.4–15 Android TV (на телевизорах, медиаплеерах и игровых консолях)
Процессор	x86/x86-64/ARMv7/ARMv8/ARMv9
Свободная оперативная память	Не менее 512 МБ
Свободная основная память	Не менее 45 МБ (для хранения данных)
Разрешение экрана	Не менее 800×480
Прочее	Интернет-соединение (для обновления вирусных баз). На устройствах под управлением Android TV режим централизованной защиты недоступен

- 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, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Спутник, Boat Browser и Atom.
- 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 кастомизированными 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 приложение устанавливается во внутреннюю память устройства. Для корректной работы Dr.Web не следует переносить установленное приложение на съемные носители.

Для корректной работы Dr.Web необходимо открыть следующие порты:

Назначение	Направление	Номера портов
Для активации и продления лицензии	исходящий	443
Для обновления	исходящий	80
Для соединения с сервером централизованной защиты	исходящий, входящий	2193 (в том числе для UDP)
Для соединения с облачным сервисом Dr.Web Cloud (обеспечивает работу URL-фильтра)	исходящие	2075 (в том числе для UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)
Для соединения с Google Mobile Services (обеспечивает передачу пуш-уведомлений)	исходящие	443 (TCP), 5228 (TCP), 5229 (TCP), 5230 (TCP)

3. Установка Dr.Web Mobile Security Suite

Dr.Web можно установить:

- С лицензионного диска.
- С сайта компании «Доктор Веб».
- Из Google Play.
- Из HUAWEI AppGallery.
- Из Xiaomi GetApps.
- С помощью программы синхронизации с компьютером.

Установка с лицензионного диска

На некоторых устройствах при подключении к компьютеру с помощью USB-кабеля необходимо разрешить передачу файлов.

Чтобы установить Dr.Web, 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.

Копирование установочного файла с диска и запуск на устройстве

1. Вставьте диск в привод.
2. Скопируйте установочный файл с диска на компьютер.
3. Подключите мобильное устройство к компьютеру с помощью USB-кабеля.
4. Перетащите установочный файл в открывшееся окно.
5. Отключите мобильное устройство от компьютера и отсоедините кабель.
6. На мобильном устройстве при помощи файлового менеджера найдите и запустите установочный файл.
7. В открывшемся окне нажмите кнопку **Установить**.
8. 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 откройте экран **Установка неизвестных приложений** и запретите установку приложений из выбранного источника.

Установка с сайта компании «Доктор Веб»

Чтобы установить Dr.Web, 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.

Скачать 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 откройте экран **Установка неизвестных приложений** и запретите установку приложений из выбранного источника.

Установка из Google Play

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

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

Чтобы установить приложение

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

   

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

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

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

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

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

Установка из HUAWEI AppGallery

Чтобы установить Dr.Web из HUAWEI AppGallery, убедитесь, что:

- У вас есть аккаунт Huawei.
- Ваше устройство привязано к аккаунту Huawei.
- На устройстве есть доступ к интернету.
- Устройство удовлетворяет системным требованиям.

Чтобы установить приложение

1. Откройте HUAWEI AppGallery на устройстве, найдите в списке приложений Dr.Web и нажмите кнопку **Установить**.

   

   Если Dr.Web не отображается в HUAWEI AppGallery, значит, ваше устройство не удовлетворяет системным требованиям.

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

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

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

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

Установка из Xiaomi GetApps

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

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

Чтобы установить приложение

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

   

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

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

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 Mobile Security Suite

Обновление Dr.Web

На устройствах с Android 14 и более поздними версиями после обновления Dr.Web необходимо повторно предоставить разрешение на доступ к специальным возможностям.

Настройка автоматического обновления для версии с сайта «Доктор Веб»

Если ваша версия Dr.Web скачана с сайта компании «Доктор Веб», вы можете включить уведомления о доступности новой версии. Для этого:

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

Если установлен этот флажок, Dr.Web проверяет наличие новой версии приложения при каждом обновлении вирусных баз. При появлении новой версии приложения вы получите уведомление и сможете оперативно скачать ее и установить.

Обновление через Google Play вручную

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

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

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

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

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

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

Обновление через HUAWEI AppGallery

Вы можете настроить автоматическое обновление приложений, установленных из HUAWEI AppGallery, в том числе Dr.Web. Для этого в приложении HUAWEI AppGallery в пункте **Управление** используйте переключатель **Автообновление по Wi-Fi**.

Вы также можете запустить обновление вручную:

1. Откройте приложение **HUAWEI AppGallery** и нажмите **Управление**.
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 и исключите Dr.Web из администраторов устройства 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**.

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

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

Удаление Dr.Web через HUAWEI AppGallery

Если вы установили Dr.Web из HUAWEI AppGallery, вы можете удалить приложение, выполнив следующие шаги:

1. Откройте приложение HUAWEI AppGallery.
2. Нажмите **Управление**.
3. На открывшемся экране нажмите **Диспетчер установки**.
4. В списке установленных приложений выберите Dr.Web и нажмите **Удалить**.
5. Подтвердите действие.

5. Лицензирование

Лицензия позволяет использовать функции приложения на протяжении всего срока действия и регулирует права пользователя, установленные в соответствии с пользовательским договором.

Лицензия требуется для работы всех компонентов Dr.Web в следующих версиях приложения:

- Загруженных из вашего личного кабинета поставщика услуги «Антивирус Dr.Web».
- Полученных от администратора антивирусной сети вашей компании.
- Для устройств под управлением Android TV.

Лицензия требуется для работы всех компонентов, кроме SpIDer Guard, Сканера и Аудитора безопасности, в следующих версиях приложения:

- Загруженных с сайта компании «Доктор Веб» https://download.drweb.com/android/.
- В версии Dr.Web, установленной из Google Play.
- В версии, установленной из HUAWEI AppGallery.

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 ее активировать.

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

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**, откройте приложение и выполните одно из следующих действий:

- В версиях Dr.Web, требующих лицензии для работы всех компонентов:
  - Нажмите **Подробнее** в уведомлении об отсутствии лицензии в верхней части главного экрана Dr.Web.
  - На главном экране Dr.Web нажмите **Меню** и выберите пункт **Лицензия**.
- В версиях Dr.Web, требующих лицензии для работы некоторых компонентов:

- На главном экране Dr.Web выберите один из компонентов, требующих приобретения лицензии.
- На главном экране Dr.Web нажмите **Меню** и выберите пункт **Лицензия**.

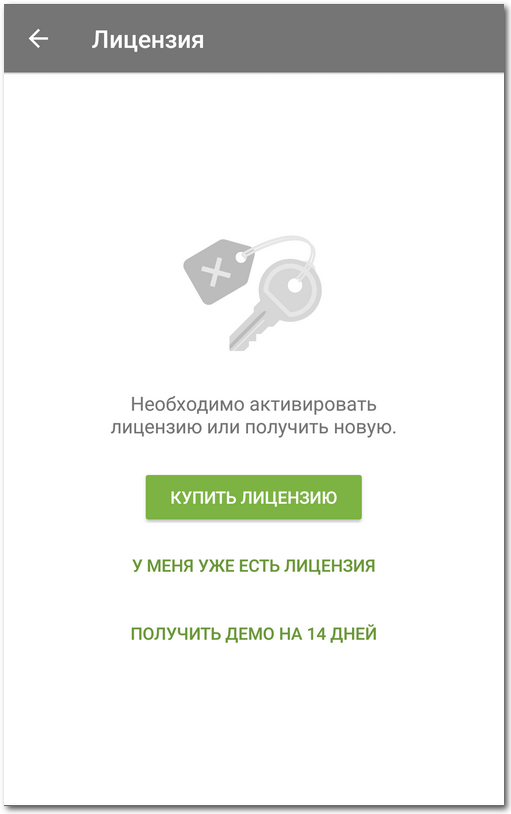

Рисунок 1: Экран Лицензия

5.2. Демонстрационная лицензия

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

Чтобы активировать демонстрационную лицензию

1. Откройте приложение.
2. Перейдите на экран Лицензия.
3. Выберите **Получить демо на 14 дней**.
4. Укажите ваши личные данные:
   - 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.

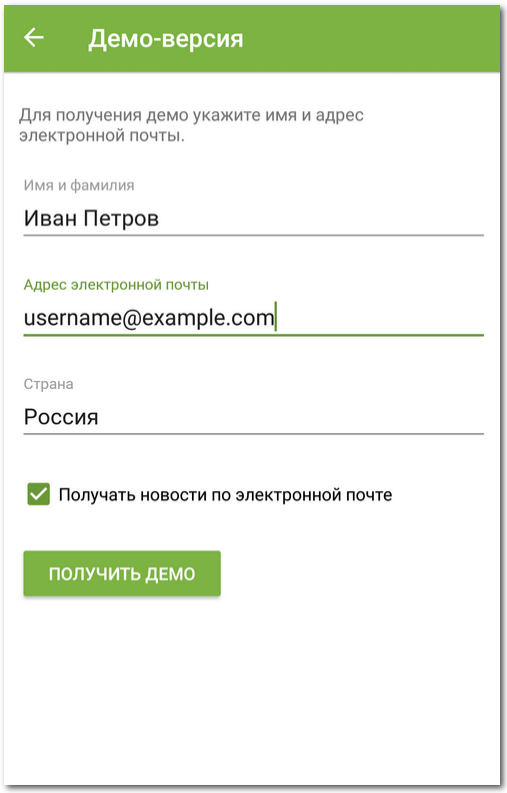

Рисунок 2: Получение демонстрационной лицензии

5.3. Покупка лицензии

Если приложение установлено из Google Play

1. Откройте 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. Если вы пользуетесь банковской картой любой страны, кроме Российской Федерации и Республики Беларусь, на экране **Покупка лицензии** (см. Рисунок 3) выберите один из следующих вариантов:

- **Подписка на месяц**. Подписка на месяц дает возможность использовать лицензию в течение месяца с момента оплаты подписки. После этого подписка автоматически продлевается и оплачивается раз в месяц.
- **Лицензия на 1 год**. Лицензия действует в течение одного года с момента покупки лицензии.
- **Лицензия на 2 года**. Лицензия действует в течение двух лет с момента покупки лицензии.

При выборе любого из вариантов откроется экран покупки лицензии. Через некоторое время после совершения оплаты лицензия активируется автоматически.

В качестве подтверждения покупки лицензии на 1 или 2 года на ваш адрес электронной почты будет отправлен лицензионный ключевой файл. Если из-за возможных технических сбоев лицензия не активируется, обратитесь в службу технической поддержки: https://support.drweb.com/.

Если к вашему профилю Google привязана банковская карта, выпущенная на территории Российской Федерации или Республики Беларусь, выберите вариант **Лицензия на 1-3 года**. Откроется страница интернет-магазина «Доктор Веб». Далее следуйте инструкции по покупке лицензии на сайте компании «Доктор Веб».

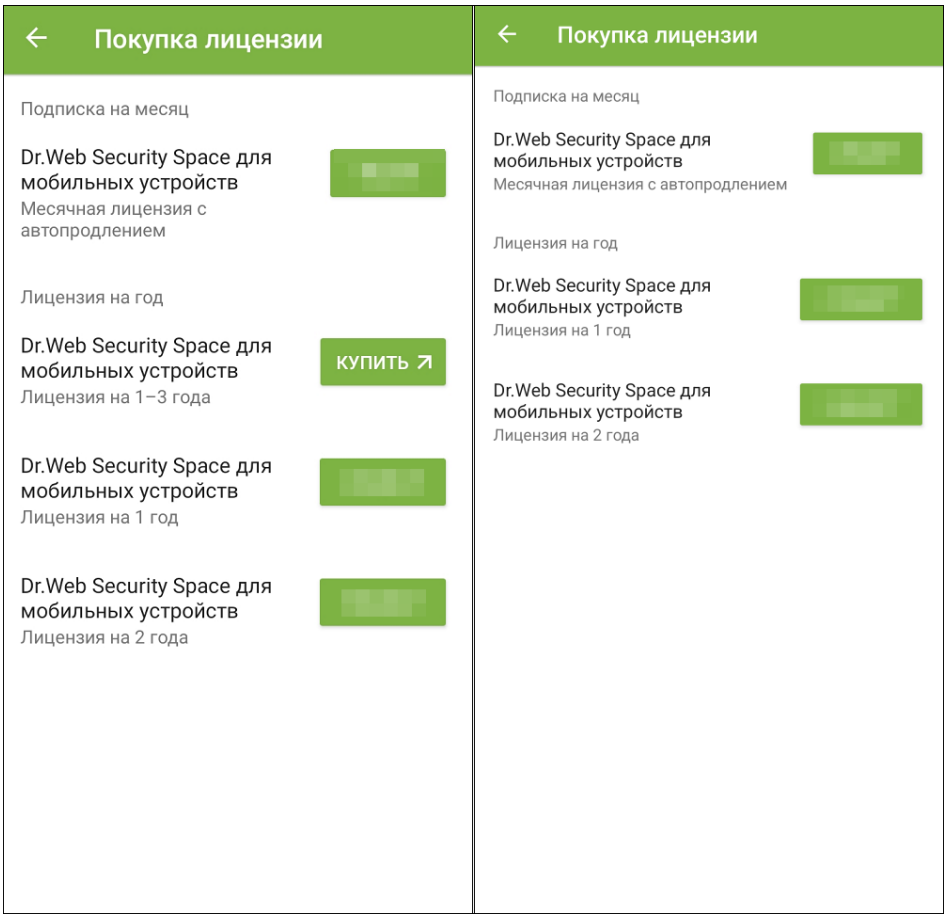

Рисунок 3: Покупка лицензии для РФ и РБ (слева) и для остальных стран (справа)

Если приложение установлено с сайта компании «Доктор Веб» или из Xiaomi GetApps

1. Откройте приложение.
2. Перейдите на экран Лицензия.
3. Выберите **Купить лицензию**. Откроется страница интернет-магазина «Доктор Веб».

   Вы также можете перейти на нее по ссылке https://products.drweb.ru/biz/v4/.
4. Укажите сферу деятельности компании, осуществляется ли переход по программе миграции и требуется ли сертифицированная версия.
5. В разделе **Защита мобильных устройств Dr.Web Mobile Security Suite** выберите **Android** и количество защищаемых устройств. Минимальное количество защищаемых устройств — 5. Чтобы развернуть раздел, нажмите «плюс».
6. Выберите срок действия лицензии.

   

   По умолчанию в корзину также добавлена лицензия для защиты 5 рабочих станций **Dr.Web Desktop Security Suite**. Если лицензия для защиты рабочих станций не требуется, удалите ее из корзины, нажав «минус» слева от указанного количества станций.
7. Нажмите **Оформить заказ**.
8. 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 СМС-сообщения на указанный номер телефона.
9. Зарегистрируйте полученный серийный номер.

Если приложение установлено из HUAWEI AppGallery

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

   Создайте аккаунт Huawei или войдите в существующий. После входа в аккаунт предоставьте приложению необходимые разрешения.

   На этом шаге приложение может запросить доступ к данным вашего аккаунта Huawei. Если вы разрешите доступ, поле с адресом электронной почты заполнится автоматически. Если вы его запретите, вам будет предложено выбрать адрес из списка во всплывающем окне.
4. На экране **Купить лицензию** 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 оплаты лицензия активируется автоматически. В качестве

подтверждения покупки на ваш адрес электронной почты будет отправлен лицензионный ключевой файл. Если из-за возможных технических сбоев лицензия не активируется, обратитесь в службу технической поддержки: https://support.drweb.com/.

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 Mobile Security Suite.

Начиная с 01.09.2024, Dr.Web Mobile Security Suite не входит в состав лицензий на программные продукты Dr.Web для ПК. Если вы приобрели такую лицензию позднее 31.08.2024, для работы с Dr.Web Mobile Security Suite вам потребуется приобрести отдельную лицензию.

Чтобы активировать лицензию

- Зарегистрируйте серийный номер:
  - В приложении, если на устройстве с установленным приложением есть активное интернет-соединение.
  - На сайте «Доктор Веб», если на устройстве с установленным приложением нет интернет-соединения.
- Используйте ключевой файл (только для приложения, установленного с сайта «Доктор Веб»).

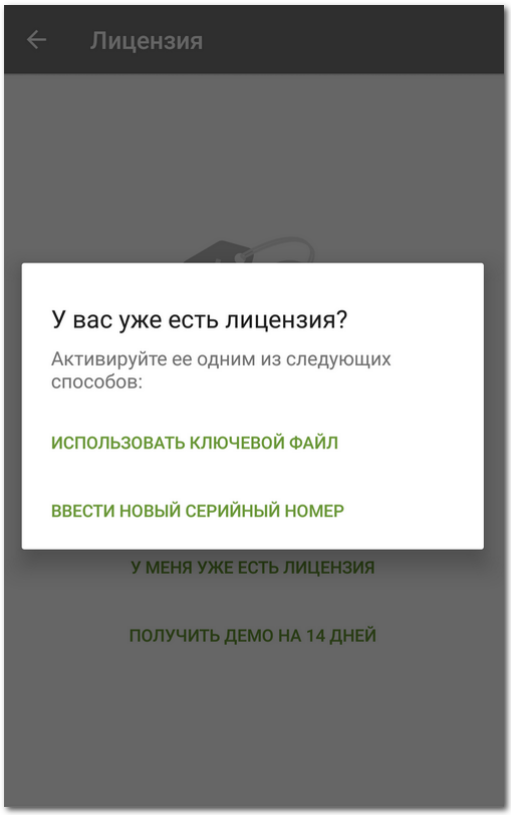

Рисунок 4: Активация лицензии

Регистрация серийного номера в приложении

Чтобы зарегистрировать серийный номер и активировать лицензию в приложении

1. Откройте 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**.

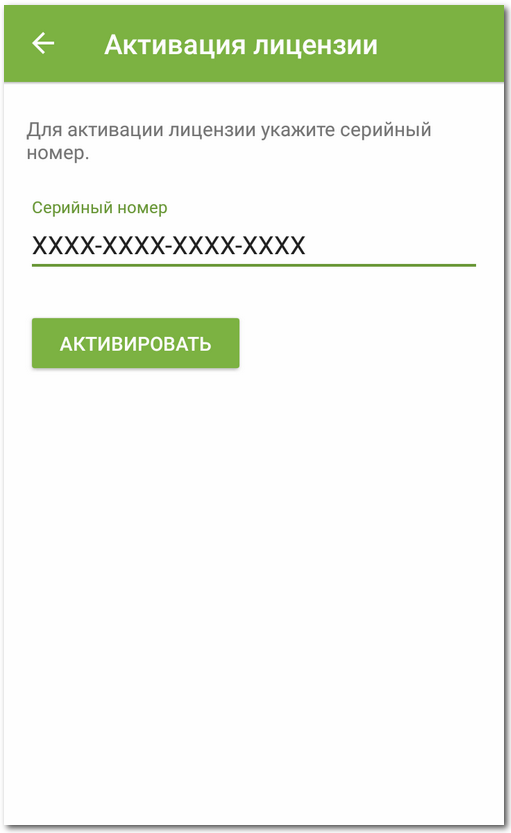

Рисунок 5: Регистрация серийного номера

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

Откроется главный экран Dr.Web. Внизу экрана появится сообщение, что лицензия активирована.

Регистрация серийного номера на сайте

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.

Чтобы зарегистрировать серийный номер на сайте

1. Зайдите на сайт https://products.drweb.com/register/.

2. Введите серийный номер, полученный при покупке Dr.Web.
3. Заполните форму со сведениями о покупателе.
4. Лицензионный ключевой файл будет выслан в ZIP-архиве по указанному вами адресу электронной почты.

Лицензионный ключевой файл

Лицензионный ключевой файл содержит права пользователя на использование продуктов Dr.Web.

Файл имеет расширение .key и содержит, в частности, следующую информацию:

- Период, в течение которого разрешено использование приложения.
- 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.

Использование ключевого файла

Вы можете использовать ключевой файл только с приложением, установленным с сайта «Доктор Веб».

Чтобы использовать ключевой файл

1. Скопируйте ключевой файл на ваше устройство в папку во внутренней памяти.

   Вы можете распаковать архив и скопировать только файл с расширением .key или перенести на устройство 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 Dr.Web. 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.

Редактирование ключевого файла делает его недействительным. Чтобы избежать порчи файла, не сохраняйте 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. Откройте 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» или из Xiaomi GetApps

Вы можете восстановить лицензию двумя способами:

- Зарегистрировать серийный номер.
- Использовать ключевой файл.

Если приложение установлено из HUAWEI AppGallery

1. Откройте приложение.

2. Перейдите на экран Лицензия.
3. На экране **Лицензия** выберите **У меня уже есть лицензия**.
4. Нажмите **Восстановить покупку в HUAWEI AppGallery**.
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.

Восстановление демонстрационной лицензии

1. Откройте 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. Приостановка и отмена подписки

Если вы пользуетесь лицензией по подписке, при необходимости вы можете приостановить подписку на заданный период времени или отменить подписку с помощью приложения Play Маркет.

Приостановка подписки

Подписка будет приостановлена по окончании текущего расчетного периода. Лицензия будет действительна до момента приостановки подписки.

Чтобы приостановить подписку

1. Откройте приложение **Play Маркет**.
2. Нажмите на значок вашего профиля Google в правом верхнем углу экрана.
3. Выберите **Платежи и подписки** > **Подписки**.
4. Выберите приложение Dr.Web в списке подписок.
5. На экране **Управление подпиской** выберите **Приостановить платежи**.
6. Задайте период, на который вы хотите приостановить платежи.
7. Подтвердите приостановку.

Вы можете возобновить приостановленную подписку в любой момент до окончания периода, на который были приостановлены платежи.

Чтобы возобновить подписку

1. Откройте приложение **Play Маркет**.
2. Нажмите на значок вашего профиля Google в правом верхнем углу экрана.
3. Выберите **Платежи и подписки** > **Подписки**.
4. Выберите приложение Dr.Web в списке подписок.
5. На экране **Управление подпиской** выберите **Возобновить**.
6. Подтвердите возобновление платежей.

Отмена подписки

Если вы удалите приложение Dr.Web, подписка отменена не будет.

После отмены подписки лицензия продолжит действовать до момента истечения текущего расчетного периода.

Чтобы отменить подписку

1. Откройте приложение **Play Маркет**.
2. Нажмите на значок вашего профиля Google в правом верхнем углу экрана.
3. Выберите **Платежи и подписки** > **Подписки**.
4. Выберите приложение Dr.Web в списке подписок.
5. На экране **Управление подпиской** выберите **Отменить подписку**.
6. На экране **Хотите приостановить подписку?** нажмите **Нет**.
7. На экране **Почему Вы хотите отменить подписку?** выберите любую из опций и нажмите **Далее**.
8. На экране **Отменить подписку?** нажмите **Отменить подписку**.

5.7. Продление лицензии

Чтобы просмотреть информацию об используемой лицензии:

- **На Android**. На главном экране Dr.Web (см. Рисунок 8) нажмите **Меню** и выберите пункт **Лицензия**.
- **На Android TV**. На главном экране Dr.Web 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 вы подписаны на услугу «Антивирус Dr.Web», в режиме централизованной защиты на экране **Лицензия** также показывается дата окончания подписки.

Продление лицензии

> Лицензия по подписке через Google Play не требует ручного продления. Подписка продлевается и оплачивается автоматически раз в месяц.

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» или в Xiaomi GetApps, 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 Dr.Web нажмите **Меню** и выберите пункт **Лицензия**.
  2. На экране **Лицензия** нажмите **Продлить лицензию из Google Play**.

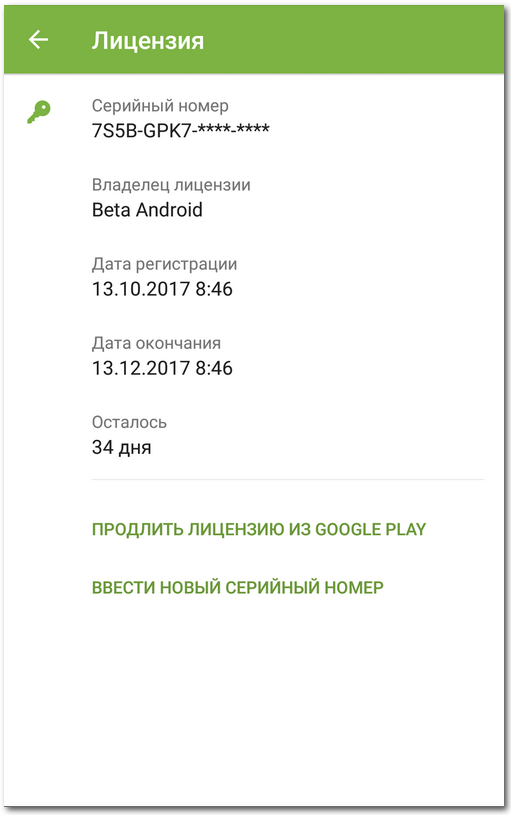

Рисунок 6: Продление лицензии

3. На экране **Продление лицензии** 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. В качестве подтверждения покупки на ваш адрес электронной почты будет отправлен лицензионный ключевой файл. Если из-за возможных технических сбоев лицензия не активируется, обратитесь в службу технической поддержки: https://support.drweb.com/.

- Если вы приобрели вашу текущую лицензию в HUAWEI AppGallery:
  1. На главном экране Dr.Web нажмите **Меню** и выберите пункт **Лицензия**.
  2. На экране **Лицензия** нажмите **Продлить лицензию из HUAWEI AppGallery**.
  3. На экране **Продление лицензии** 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. В качестве подтверждения покупки на ваш адрес электронной почты будет отправлен лицензионный ключевой файл. Если из-за возможных технических сбоев лицензия не активируется, обратитесь в службу технической поддержки: https://support.drweb.com/.

5.8. Настройка уведомлений об окончании срока действия лицензии

На мобильных устройствах вы можете включить уведомления о скором окончании срока действия лицензии (кроме случая использования лицензии по подписке из Google Play).

Чтобы включить уведомления

1. На главном экране Dr.Web нажмите **Меню** и выберите **Настройки** (см. Настройки).
2. Выберите пункт **Лицензия**.
3. Установите флажок **Уведомления**.

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.

На этом же экране вам предлагается принять положение об отправке статистики работы приложения и найденных угроз на серверы компании «Доктор Веб», а также на серверы Google и Яндекс.

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

Если ваша версия Dr.Web предоставлена 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.

После установки Dr.Web и принятия Лицензионного соглашения предоставьте приложению необходимые разрешения. Разрешения также могут потребоваться при первом нажатии на один из компонентов или их включении.

На устройствах с Android 14 и более поздними версиями после обновления Dr.Web необходимо повторно предоставить разрешение на доступ к специальным возможностям.

- Dr.Web запрашивает следующие разрешения при первом запуске приложения:
  - Доступ к фото, мультимедиа и файлам на устройстве.
  - Доступ ко всем файлам (на устройствах с Android 11 и более поздними версиями).

  Эти разрешения необходимы для работы приложения.
  - Разрешение на отправку уведомлений (на устройствах с Android 13 и более поздними версиями).

Разрешение требуется для того, чтобы Dr.Web мог использовать панель уведомлений для сообщений о состоянии защиты устройства и работе компонентов Dr.Web. Если разрешение не будет предоставлено, Dr.Web не сможет сообщить вам об обнаружении угроз и событиях компонентов, пока вы не откроете приложение.

- Фильтр звонков и СМС запрашивает следующие разрешения:
  - Осуществлять телефонные звонки и управлять ими.
  - Отправлять и просматривать СМС-сообщения.
  - Доступ к контактам.
  - Доступ к уведомлениям.
  - Доступ к списку вызовов (на устройствах с Android 9 и более поздними версиями).
  - Разрешение назначить Dr.Web приложением по умолчанию для автоматического определения номеров и защиты от спама (на устройствах с Android 10 и более поздними версиями).
- URL-фильтр запрашивает доступ к специальным возможностям Android для работы в поддерживаемых браузерах.
- Антивор Dr.Web запрашивает следующие разрешения:
  - Доступ к телефонным звонкам и управлению ими.
  - Возможность отправлять и просматривать СМС-сообщения.
  - Доступ к контактам.
  - Доступ к уведомлениям.
  - Доступ к данным о местоположении устройства.
  - Доступ к специальным возможностям Android.
  - Разрешение назначить Dr.Web администратором устройства.
- Брандмауэр Dr.Web запрашивает следующие разрешения:
  - Подключение к сети VPN для отслеживания трафика.
  - Наложение поверх других окон.
- Dr.Web на Android TV запрашивает следующие разрешения:
  - Доступ к контактам.
  - Доступ к фото, мультимедиа и файлам на устройстве.
  - Доступ ко всем файлам (на устройствах с Android 11 и более поздними версиями).

В режиме централизованной защиты запрашиваются следующие разрешения:

- Основные разрешения (доступ к фото, мультимедиа и файлам, контактам и др.) — для работы большинства функций приложения.
- Разрешение на отправку уведомлений (на устройствах с Android 13 и более поздними версиями) — для отображения сообщений о состоянии защиты и работе компонентов.
- Доступ ко всем файлам (на устройствах с Android 11 и более поздними версиями) — для осуществления проверки устройства.

- Фильтр звонков и СМС (в зависимости от версии Android, см. выше) — для фильтрации входящих звонков и СМС.
- Администрирование устройства — для защиты приложения от удаления и для полноценной работы Антивора.
- Доступ к специальным возможностям — для фильтрации приложений и полноценной работы URL-фильтра, Антивора и Родительского контроля.
- Наложение поверх других окон — для фильтрации приложений и работы Брандмауэра.

На устройствах с Android 13 и более поздними версиями может быть закрыт доступ к уведомлениям и доступ к специальным возможностям. Чтобы Dr.Web работало корректно, разрешите доступ. Для этого:

1. В настройках устройства выберите раздел **Приложения**.
2. Выберите Dr.Web.

   Откроется экран **О приложении**.
3. Перейдите к расширенным настройкам внизу экрана или в меню в правом верхнем углу.

   Если меню расширенных настроек не появляется, включите любой компонент Dr.Web, кроме Брандмауэра, и предоставьте запрашиваемое разрешение на доступ к уведомлениям или доступ к специальным возможностям. Появится уведомление о блокировке настроек. Затем повторите шаги этой инструкции, начиная с первого.
4. Нажмите **Разрешить доступ к настройкам**.

Если необходимые разрешения не предоставлены, откроется экран **Требуются разрешения** (см. Рисунок 7). Вы можете предоставить все разрешения или только обязательные. Обязательные для работы компонентов разрешения отмечены желтым значком. Необязательные разрешения отмечены серым значком. После предоставления разрешений значок меняется на зеленый.

Если вы предоставите все запрашиваемые компонентом разрешения, работа с приложением продолжится автоматически. Если вы предоставите только обязательные разрешения, вы сможете продолжить работу с приложением, нажав кнопку **Продолжить**. Необязательные разрешения можно будет предоставить при следующем переходе к этому компоненту с главного экрана Dr.Web или на экране настроек.

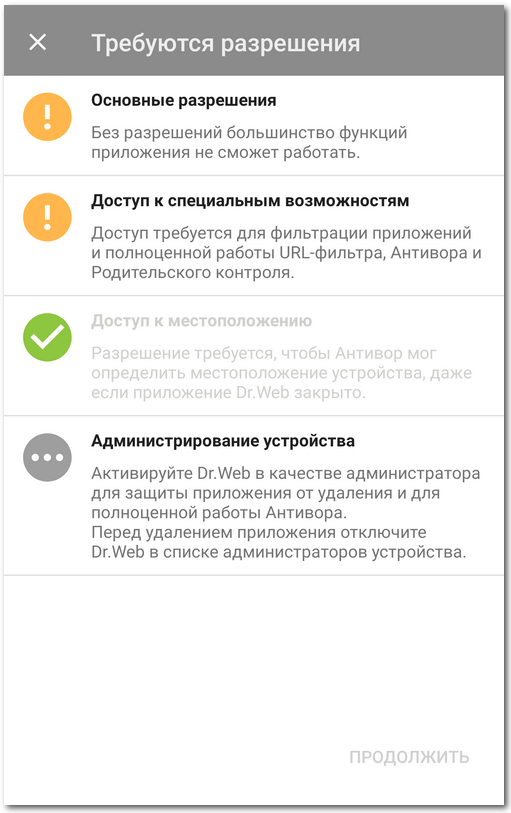

Рисунок 7: Требуются разрешения

Если вы отклоните один или несколько запросов на предоставление обязательных разрешений, вам будет предложено перейти на экран настроек:

- На устройствах с Android 9 или более ранними версиями:
  1. Нажмите **Перейти в Настройки** и выберите раздел **Разрешения**.
  2. Выберите пункт **Память** или **Хранилище** и предоставьте разрешение, используя переключатель.
- На устройствах с Android 10:
  1. Нажмите **Перейти в Настройки** и выберите раздел **Разрешения**.
  2. Выберите пункт **Память** или **Хранилище** в категории **Запрещено** и выберите опцию **Разрешить**.
- На устройствах с Android 11 или более поздними версиями:
  1. Нажмите **Перейти в Настройки** и выберите раздел **Разрешения**.
  2. Выберите пункт **Файлы и медиаконтент** или **Хранилище** в категории **Запрещено** и выберите опцию **Разрешить управление всеми файлами**. С помощью этой опции вы предоставляете доступ к фото и мультимедиа, а также доступ ко всем файлам.

Чтобы открыть список всех разрешений для Dr.Web

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 располагается список основных компонентов Dr.Web.

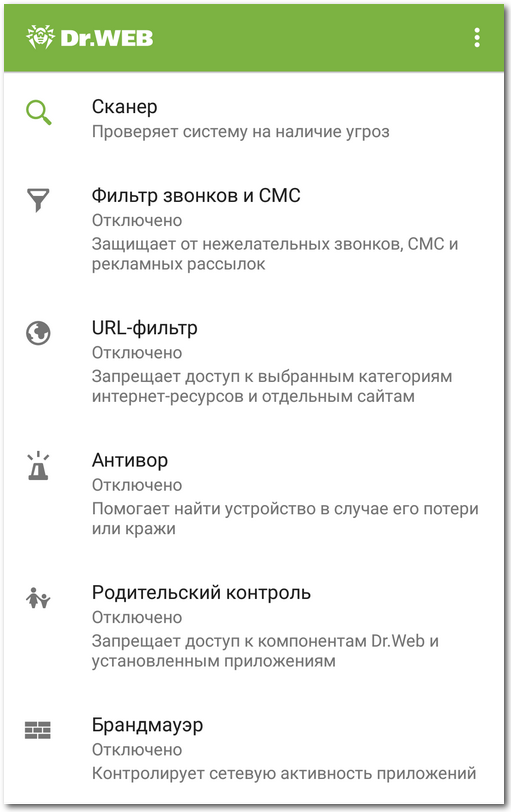

Рисунок 8: Главный экран Dr.Web

Меню в правом верхнем углу главного экрана позволяет:

- Открыть экран с информацией о лицензии.
- Открыть статистику.
- Открыть 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.

Панель состояния

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

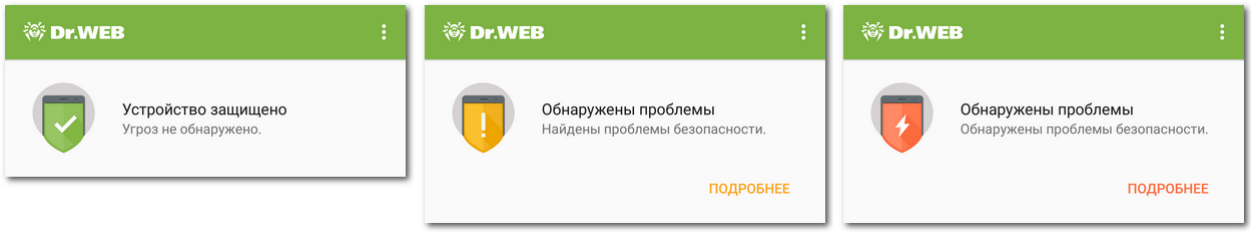

Рисунок 9: Панель состояния

- Зеленый индикатор означает, что устройство защищено. Дополнительных действий не требуется.
- Желтый индикатор означает, что Dr.Web обнаружил проблемы безопасности, например, отсутствие лицензии или уязвимость. Чтобы узнать больше о найденных проблемах и устранить их, нажмите **Подробнее**.
- Красный индикатор означает, что Dr.Web обнаружил подозрительные изменения в системной области или угрозы. Чтобы открыть результаты проверки и обезвредить угрозы, нажмите **Подробнее**.

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

6.4. Уведомления

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

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

Категории уведомлений

Категория	Уведомления
Обнаружение угрозы	• Уведомления об угрозах, обнаруженных компонентом SplDer Guard. • Уведомления об угрозах, обнаруженных Сканером Dr.Web.
Безопасные приложения	Уведомления об отсутствии угроз в только что установленных приложениях или обновлениях. На устройствах с Android 7.1 или более

Категория	Уведомления
	ранними версиями уведомления этой категории можно включить или отключить в общих настройках Dr.Web.
Статус антивирусной защиты	Если панель уведомлений отключена, эта категория содержит следующие уведомления: • **Система защищена**. Показывается, если компонент SpIDer Guard включен и не запущена проверка Сканера Dr.Web. • Уведомление о типе проверки Сканера Dr.Web. Показывается, если запущена одна из проверок: быстрая, полная или выборочная. • Уведомление о проверке внешнего накопителя. Показывается при проверке SD-карты и съемных носителей компонентом SpIDer Guard. Если панель уведомлений включена, на ней отображается сообщение о том, что идет проверка, если запущена одна из проверок Сканера Dr.Web.
Статус дополнительных компонентов	• **Дополнительные компоненты включены**. Показывается, если включены Фильтр звонков и СМС, URL-фильтр, Антивор Dr.Web или Брандмауэр Dr.Web. • **Агент включен**. Показывается в режиме централизованной защиты, если отключены Фильтр звонков и СМС (разрешены все входящие звонки и СМС), URL-фильтр, Антивор Dr.Web и Брандмауэр Dr.Web. • **Агент и дополнительные компоненты включены**. Показывается в режиме централизованной защиты, если включены Фильтр звонков и СМС, URL-фильтр, Антивор Dr.Web или Брандмауэр Dr.Web.
Уведомления от друзей	Уведомления, полученные от друзей.
Настройка компонентов защиты	**Настройка компонентов...** Показывается при определении местоположения устройства по запросу от друга, если включен Антивор Dr.Web в версии, скачанной из Google Play.
Другое	• **Требуются разрешения**. Показывается при открытии приложения, если ранее был отклонен запрос на доступ к фото, мультимедиа и файлам. В версии приложения, полученной от администратора антивирусной сети вашей компании или от поставщика услуги «Антивирус Dr.Web», уведомление показывается при открытии приложения, если ранее было отклонено любое из запрашиваемых разрешений. • Уведомления о лицензии: ▫ **Ошибка при проверке лицензии**. Показывается, если при проверке лицензии произошла ошибка. Возможно, лицензия отсутствует или не подтверждена сервером. ▫ **Осталось дней: <число дней>**. Показывается, если истекает срок действия лицензии и в настройках приложения установлен флажок Уведомления. ▫ **Закончился срок действия лицензии**. Показывается, если вы пользуетесь услугой «Антивирус Dr.Web» и срок действия лицензии истек.

Категория	Уведомления
	▫ **Обратитесь к администратору антивирусной сети**. Показывается, если вы пользуетесь услугой «Антивирус Dr.Web» и ваша лицензия была заблокирована. • **Доступна новая версия Dr.Web**. Показывается в версии, скачанной с сайта «Доктор Веб», если появилась новая версия и в настройках приложения установлен флажок Новая версия. • Уведомления Антивора Dr.Web: ▫ **SIM-карта не найдена**. ▫ **Обнаружена новая SIM-карта**. • Уведомление Фильтра звонков и СМС: **Запрещены все входящие звонки и СМС**. Показывается при включении профиля **Блокировать все**. • Уведомления Брандмауэра Dr.Web: ▫ **Брандмауэр Dr.Web отключен**. Показывается, если VPN-подключение приложения Dr.Web разорвано. ▫ **Превышена квота мобильного трафика**. Показывается, если превышено установленное ограничение мобильного трафика и в настройках Брандмауэра установлен флажок Уведомления. • **Новое сообщение**. Показывается, если получено сообщение от администратора антивирусной сети.
Группировать уведомления	Эта категория не содержит конкретных уведомлений, но она позволяет сгруппировать все уведомления Dr.Web в одно разворачивающееся уведомление.

Панель уведомлений

Панель уведомлений Dr.Web (см. Рисунок 10) используется для быстрого доступа к основным функциям приложения. Кроме того, она оперативно отображает предупреждения о подозрительных изменениях в системной области и угрозах.

Если Dr.Web обнаружит подозрительные изменения в системной области или угрозы, на устройствах с Android 11 и более ранними версиями значок приложения на панели уведомлений поменяется на . На устройствах с Android 12 и более поздними версиями значок приложения поменяется на , а индикатор состояния защиты сменит цвет на красный .

Рисунок 10: Панель уведомлений на Android 11 (слева) и Android 12 (справа)

На Android TV панель уведомлений недоступна.

Чтобы включить панель уведомлений Dr.Web

1. На главном экране Dr.Web выберите **Меню** > **Настройки**.
2. Выберите **Общие настройки**.
3. Включите опцию **Панель уведомлений**.

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

Если ваше устройство не поддерживает использование SIM-карт, вместо опции **Фильтр** на панели уведомлений отображается опция **Загрузки**, которая позволяет запустить проверку объектов, загруженных на устройство.

Если Dr.Web работает в режиме централизованной защиты и у вас нет прав на изменение настроек Фильтра звонков и СМС или URL-фильтра, соответствующие опции **Фильтр** и **URL-фильтр** будут недоступны на панели уведомлений.

С помощью панели уведомлений можно выполнить следующие действия:

- На устройствах с Android 11 и более ранними версиями:
  - Открыть приложение. Для этого нажмите значок .
  - Запустить быструю, полную или выборочную проверку. Нажмите **Сканер**.
  - Выбрать фильтр для входящих звонков и сообщений. Нажмите **Фильтр**.
  - Выбрать категории сайтов, к которым вы хотите ограничить доступ. Нажмите **URL-фильтр**.
- На устройствах с Android 12 и более поздними версиями:
  - Открыть приложение (при зеленом индикаторе защиты). Для этого нажмите .
  - Предоставить необходимые для работы приложения разрешения (при желтом индикаторе). Нажмите .
  - Открыть результаты проверки (при красном индикаторе). Нажмите .
  - Запустить быструю, полную или выборочную проверку. Нажмите .
  - Выбрать фильтр для входящих звонков и сообщений. Нажмите .
  - Выбрать категории сайтов, к которым вы хотите ограничить доступ. Нажмите .

- Просмотреть состояние защиты, текущие и рекомендуемые действия. Нажмите ⌄.

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 Android TV виджет недоступен.

Чтобы добавить виджет Dr.Web

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

Виджет без индикатора сообщает об активной защите устройства компонентом SpIDer Guard. Виджет с желтым индикатором сообщает, что компонент SpIDer Guard выключен. Нажмите на виджет, чтобы возобновить работу SpIDer Guard.

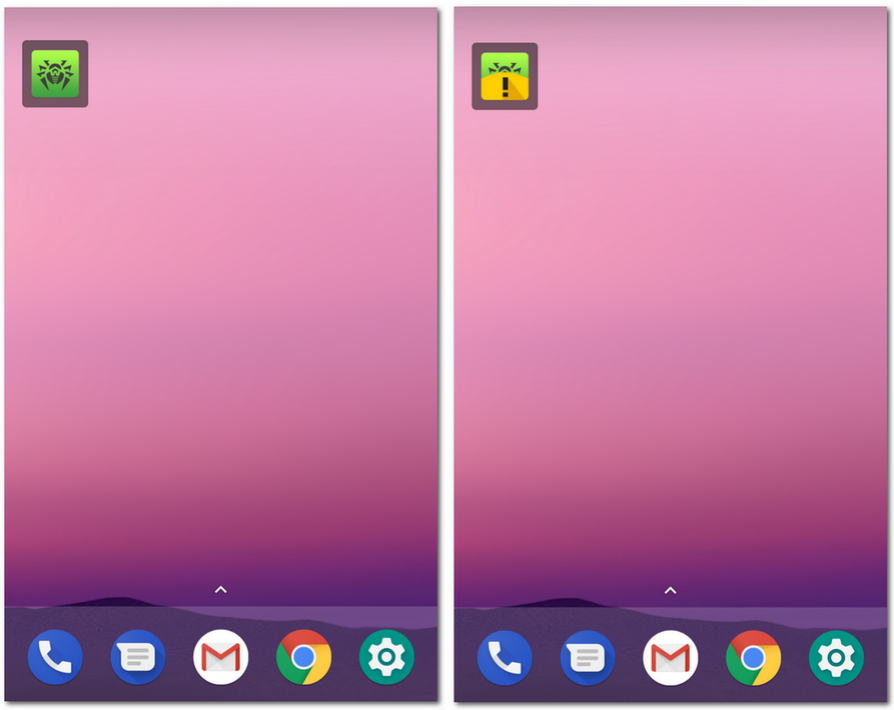

Рисунок 11: Виджет Dr.Web

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 Dr.Web нажмите **Меню** и выберите пункт **О программе**.
2. Нажмите **Мой Dr.Web**.

7. Учетная запись Dr.Web

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

По умолчанию пароль от учетной записи или отпечаток пальца 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 более поздних версиях).
  - **Настройки** > **Специальные возможности**.
  - **Настройки** > **Безопасность** > **Местоположение** (на Android 6.0 и более поздних версиях).
  - **Настройки** > **Безопасность** > **Администраторы устройства** > **Dr.Web Security Space**.
  - **Настройки** > **Дополнительные настройки** > **Сброс настроек** (название и расположение настройки отличаются на разных устройствах).

  На устройствах Xiaomi также защищен доступ к настройке **Контроль активности**.

Если на устройстве включен Родительский контроль, получить доступ к перечисленным выше разделам и настройкам с помощью отпечатка пальца можно в случае, если в настройках Родительского контроля включена опция **Разблокировка с помощью отпечатка пальца**.

Вы также можете защитить паролем или отпечатком пальца доступ к Фильтру звонков и СМС, URL-фильтру и настройкам приложения (см. раздел Блокировка доступа к приложениям и компонентам).

Создание учетной записи

1. На главном экране Dr.Web нажмите **Меню** в правом верхнем углу.

2. Выберите пункт **Учетная запись**.
3. На экране **Учетная запись** нажмите кнопку **Создать**.
4. Укажите адрес электронной почты.

   Адрес может понадобиться позже, если вы забудете пароль. Поэтому укажите адрес, к которому у вас есть доступ.

   Обратите внимание, что после регистрации учетной записи адрес электронной почты нельзя изменить. Чтобы использовать другой адрес, вам понадобится удалить учетную запись и создать ее заново с новым адресом.

   Для регистрации адреса электронной почты требуется активное интернет-соединение.

5. Нажмите кнопку **Далее**.
6. Придумайте пароль. Пароль должен содержать не менее 4 символов.
7. Повторите пароль и нажмите **Далее**.

   На следующем экране вы увидите подтверждение того, что учетная запись успешно создана.

8. Нажмите **Готово**.

Управление учетной записью

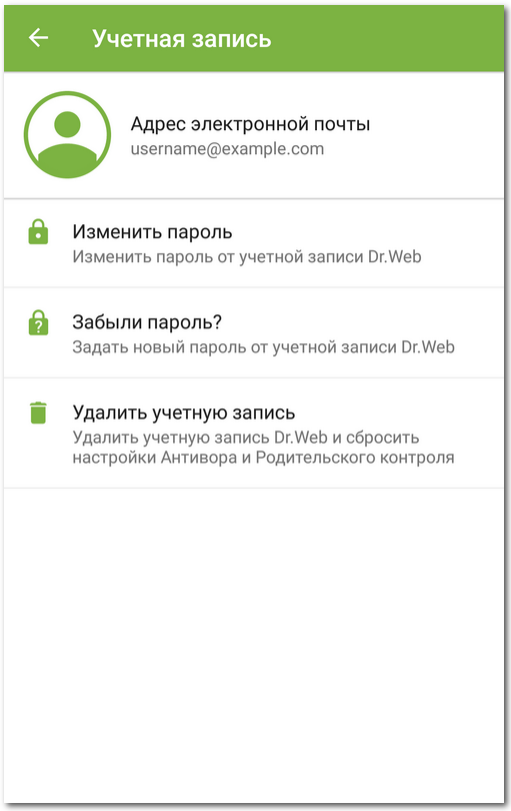

Рисунок 12: Учетная запись

На экране **Учетная запись** (см. Рисунок 12) вы можете выполнить следующие действия:

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

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

Чтобы изменить пароль или удалить учетную запись, введите текущий пароль от учетной записи или отсканируйте отпечаток пальца.

Вы также можете удалить учетную запись через сайт. Для этого:

1. Откройте страницу Dr.Web в Google Play и выберите раздел **Безопасность данных**.
2. На экране **Безопасность данных** прокрутите страницу вниз до подраздела **Удаление данных** и нажмите **Открыть сайт разработчика**. Вы также можете перейти на сайт по ссылке: https://arss.drweb.com.
3. Введите адрес электронной почты, который вы использовали при создании учетной записи, и нажмите **Продолжить**.
4. Появится экран подтверждения адреса электронной почты. Если адрес верен, нажмите **Продолжить**. Если адрес неверен, вернитесь на предыдущую страницу и введите его заново.
5. Введите код подтверждения из письма, отправленного на указанный адрес электронной почты, и нажмите **Продолжить**. Если вы не получили код, нажмите **Отправить снова**. Первый присланный код становится недействительным сразу после повторного запроса кода.

   > Код действителен 1 час. Если в течение этого времени кодом не воспользовались, необходимо запросить его заново.

   Появится экран подтверждения удаления.
6. Чтобы удалить учетную запись, нажмите **Удалить**. Чтобы отменить удаление, нажмите **Отмена**.

8. Компоненты Dr.Web

На главном экране Dr.Web 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 СМС блокирует нежелательные звонки и СМС-сообщения.
- URL-фильтр ограничивает доступ пользователя к интернет-ресурсам.
- 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 СМС** и **Антивор Dr.Web** недоступны.

8.1. Антивирусная защита

- SplDer Guard проверяет файловую систему в режиме реального времени.
- Сканер Dr.Web позволяет запустить проверку на наличие угроз вручную.
- На экране Результаты проверки вы можете выбрать действия, чтобы обезвредить обнаруженные угрозы безопасности.

8.1.1. SplDer Guard: постоянная антивирусная защита

SplDer Guard включается автоматически после принятия Лицензионного соглашения. Компонент работает независимо от того, запущено приложение или нет. Если SplDer Guard включен, в строке состояния Android отображается значок Dr.Web  .

На некоторых устройствах значок Dr.Web может не показываться, когда приложение работает в фоновом режиме. Это происходит, потому что прошивка устройства оптимизирует фоновые процессы, чтобы сэкономить энергию или улучшить производительность. Чтобы закрепить значок Dr.Web в строке состояния Android, снимите ограничения с приложения в фоновом режиме: проверьте настройки устройства и встроенного диспетчера приложений. Настройки зависят от модели устройства. Зачастую достаточно в недавних приложениях нажать значок с замком у приложения Dr.Web.

SplDer Guard защищает систему, даже если значок Dr.Web не отображается в строке состояния. Если будет установлено вредоносное приложение, компонент среагирует и

покажет уведомление об угрозе. Вы можете проверить работу SpIDer Guard с помощью тестового файла EICAR.

Если SpIDer Guard обнаружит подозрительное изменение в системной области или угрозу, на экране появятся:

- Значок в строке состояния Android в левом верхнем углу экрана:
  - — на Android 4.4,
  - — на Android 5.0–11,
  - — на Android 12 и более поздних версий.
- Всплывающее уведомление об обнаружении угрозы (см. Рисунок 13).
- Значок (на Android 11 и более ранних версий) или (на Android 12 и более поздних версий) на панели уведомлений.
- Сообщение с красным индикатором на панели состояния.

Чтобы открыть результаты проверки, нажмите значок ( ) или на сообщение на панели состояния.

> 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.

Чтобы отключить или снова включить SpIDer Guard

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

Настройки SpIDer Guard

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

Чтобы открыть настройки SpIDer Guard

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

Файлы в архивах

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

Встроенная SD-карта и съемные носители

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. При этом показывается соответствующее уведомление.

Системная область

Чтобы отслеживать изменения в системной области, установите флажок **Системная область**. Если эта настройка включена, SpIDer Guard отслеживает изменения (добавление, изменение и удаление файлов) и уведомляет об удалении любых файлов, а также добавлении и изменении исполняемых файлов: `.jar`, `.odex`, `.so`, файлов формата APK, ELF, и др.

Повторная проверка системной области

Чтобы запустить повторную проверку системной области, нажмите **Повторная проверка системной области**. SpIDer Guard заново проверит все изменения в системной области, которые были проигнорированы ранее.

Уведомления о системной области

Чтобы включить уведомления об изменении любых файлов в системной области (не только исполняемых), установите флажок **Уведомления о системной области**.

Дополнительные опции

Чтобы включить/отключить проверку системы на наличие файлов, которые могут представлять угрозу, выберите **Дополнительные опции** и установите/снимите соответствующие флажки:

- Подозрительные объекты,
- Рекламные программы,
- Программы дозвона,
- Программы-шутки,
- Потенциально опасные программы,

- Программы взлома,
- Уязвимые программы.

Статистика

Приложение регистрирует события, связанные с работой SpIDer Guard: включение/отключение, обнаружение угроз безопасности и результаты проверки памяти устройства и устанавливаемых приложений. Статистика SpIDer Guard отображается в разделе **События** 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, появится всплывающее уведомление от SpIDer Guard.

Рисунок 13: Обнаружение тестового файла EICAR на Android 10 (слева) и Android 12 (справа)

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 вашей компании или списком оплаченных услуг. Проверка может запускаться по расписанию, заданному на сервере централизованной защиты.

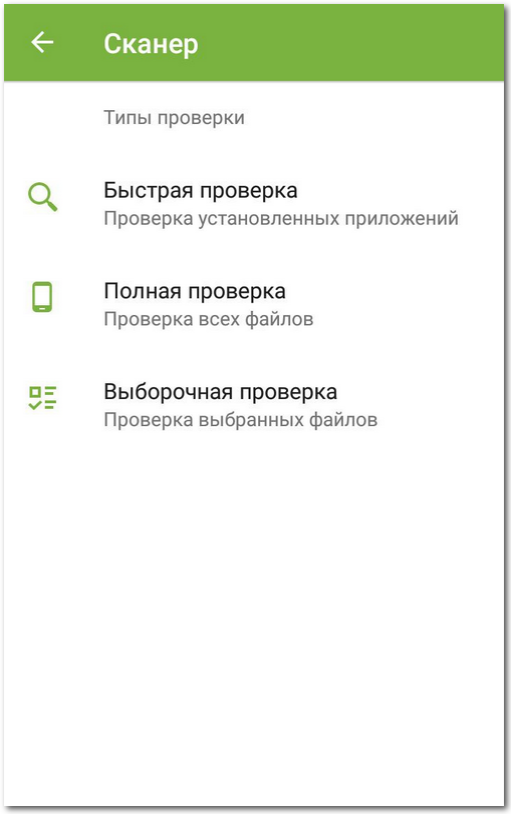

Рисунок 14: Сканер Dr.Web

Проверка

Чтобы проверить систему, на главном экране Dr.Web выберите пункт **Сканер**, затем на экране **Сканер** (см. Рисунок 14) 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 15). 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.

На устройствах с Android 11 и 12 для проверки папок `/Android/data` и `/Android/obb` необходимо предоставить разрешение на доступ Dr.Web к этим папкам.

Чтобы разрешить доступ к папке /Android/data или /Android/obb

1. Выберите пункт **Выборочная проверка**.
2. Выберите папку `/Android/data` или `/Android/obb` в списке объектов файловой системы.
3. В диалоговом окне нажмите **Разрешить**.
4. Нажмите **Использовать эту папку**.

На устройствах с Android 13 и более поздними версиями папки `/Android/data` и `/Android/obb` защищены системой и недоступны для проверки.

Если в ходе любой проверки Сканер Dr.Web обнаружит угрозы, внизу экрана сканирования появится значок . Нажмите значок, чтобы открыть результаты проверки (см. Рисунок 16) и обезвредить угрозы. Если вы закрыли экран сканирования или закрыли приложение, вы можете открыть результаты проверки, нажав значок на панели уведомлений.

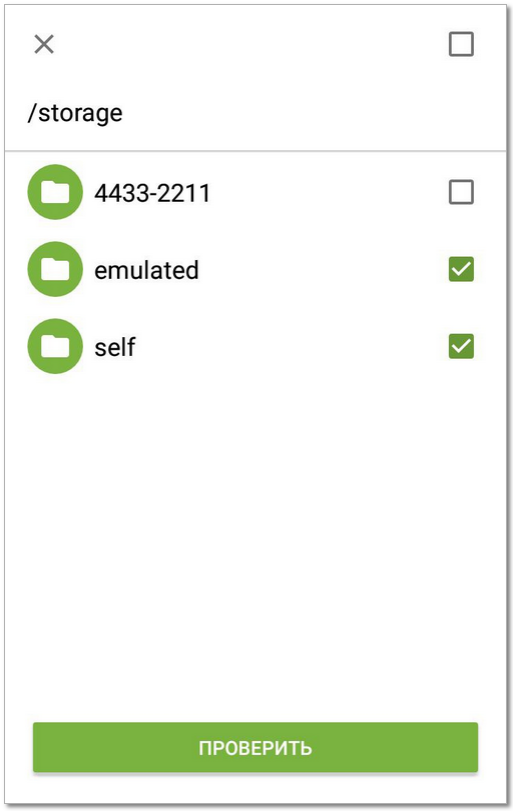

Рисунок 15: Выборочная проверка

Отправка подозрительных файлов в антивирусную лабораторию «Доктор Веб»

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

Чтобы отправить файл в лабораторию

1. Нажмите и удерживайте файл в списке объектов файловой системы (см. Рисунок 15), затем нажмите кнопку **Отправить в лабораторию**.
2. На следующем экране введите адрес вашей электронной почты, если вы хотите получить результаты анализа отправленного файла.
3. Выберите одну из категорий для вашего запроса:
   - **Подозрение на вирус**, если вы считаете, что файл представляет угрозу.
   - **Ложное срабатывание**, если вы считаете, что файл ошибочно отнесен к угрозам.
4. Нажмите кнопку **Отправить**.

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

Настройки Сканера Dr.Web

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

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

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

- Чтобы включить/отключить проверку системы на наличие файлов, которые могут представлять угрозу, в настройках Сканера выберите **Дополнительные опции** и установите/снимите соответствующие флажки:
  - Подозрительные объекты,
  - Рекламные программы,
  - Программы дозвона,
  - Программы-шутки,

- Потенциально опасные программы,
- Программы взлома,
- Уязвимые программы.

Статистика

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

8.1.3. Результаты проверки

Как открыть результаты проверки

- Если Сканер Dr.Web обнаружит угрозы, на экране сканирования появится значок  .

  Чтобы открыть результаты проверки, нажмите на этот значок.
- Если SplDer Guard обнаружит подозрительное изменение в системной области или угрозу, на экране появятся:
  - Значок в строке состояния Android в левом верхнем углу экрана:
    -  — на Android 4.4,
    -  — на Android 5.0–11,
    -  — на Android 12 и более поздних версий.
  - Всплывающее уведомление об обнаружении угрозы (см. Рисунок 13).
  - Значок  (на Android 11 и более ранних версий) или  (на Android 12 и более поздних версий) на панели уведомлений.
  - Сообщение с красным индикатором на панели состояния.

  Чтобы открыть результаты проверки, нажмите значок  () или на сообщение на панели состояния.

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

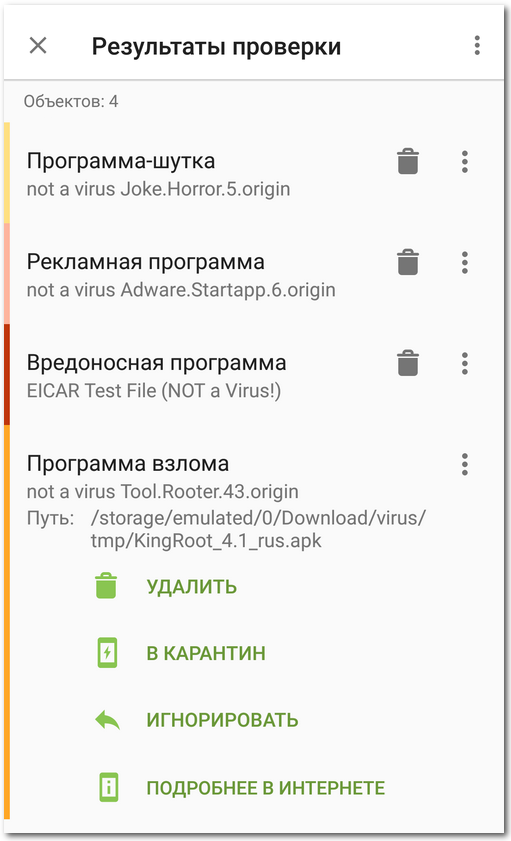

Рисунок 16: Результаты проверки

Обезвреживание угроз

На экране **Результаты проверки** вы можете ознакомиться со списком угроз и подозрительных изменений в системной области. Для каждого объекта указаны его тип и название, а также значок опции, которую рекомендуется выбрать для этого объекта.

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

1. Вредоносная программа.
2. Потенциально опасная программа.
3. Программа взлома.
4. Рекламная программа.
5. Изменения в системной области:
   - Новые файлы в системной области.
   - Изменение системных файлов.
   - Удаление системных файлов.
6. Программа-шутка.

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

Обезвреживание всех угроз

Чтобы удалить сразу все угрозы

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

Чтобы переместить в карантин сразу все угрозы

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

Обезвреживание угроз по одной

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

Вылечить, чтобы вылечить инфицированное приложение.

Опция доступна для некоторых угроз в системных приложениях, если на устройстве разрешен root-доступ.

Удалить, чтобы полностью удалить угрозу из памяти устройства.

В некоторых случаях Dr.Web не может удалить приложения, которые используют специальные возможности Android. Если Dr.Web не удалит приложение после выбора опции **Удалить**, перейдите в безопасный режим и удалите приложение вручную. Если Dr.Web предоставлен доступ к специальным возможностям, удаление приложения произойдет автоматически после выбора опции **Удалить**.

Опция недоступна для угроз в системных приложениях в следующих случаях:

- Если на устройстве не разрешен root-доступ.
- Если удаление приложения может привести к потере работоспособности устройства.
- Если обнаружена модификация угрозы. Чтобы определить, действительно ли приложение представляет угрозу, сообщите о ложном срабатывании.

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

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

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

Заблокировать, чтобы отключить приложению доступ к интернет-соединениям.

Опция доступна для угроз в системных приложениях.

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

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

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

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

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

8.1.3.1. Угрозы в системных приложениях

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

Для системных приложений доступна опция **Заблокировать**. Выберите ее, чтобы Брандмауэр Dr.Web заблокировал все интернет-соединения для системного приложения, определенного как угроза.

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

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

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

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

  Это действие потребуется повторять при каждой перезагрузке устройства.

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

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

На Android TV установите флажок **Системные приложения** в разделе **Разное** > **Настройки** > **Общие настройки** > **Дополнительные опции**.

8.1.3.2. Изменения в системной области

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

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

Компонент SpIDer Guard может отслеживать изменения в системной области. Вы можете включить проверку системной области в настройках SpIDer Guard. Если компонент обнаружит подозрительные изменения, он уведомит об этом.

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

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

Для обнаруженных изменений доступны следующие опции:

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

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

8.1.3.3. Угрозы, использующие уязвимость Stagefright

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

Угрозы, использующие уязвимость Stagefright, обнаруживаются и обезвреживаются Брандмауэром Dr.Web. Включите его, чтобы обеспечить защиту от Stagefright-эксплойтов.

Брандмауэр Dr.Web анализирует содержимое мультимедийных 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. Приложения-блокировщики устройства

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

От действий программ-вымогателей могут пострадать ваши фотографии, видео и документы. Кроме того, они похищают и передают на серверы злоумышленников различную информацию об инфицированном устройстве (в том числе идентификатор IMEI), данные из адресной книги (имена контактов, номера телефонов и адреса электронной почты), отслеживают входящие и исходящие вызовы и могут их

блокировать. Вся собранная информация, в том числе о телефонных звонках, также передается на управляющий сервер.

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

Если мобильное устройство заблокировано программой-вымогателем и на нем включен SpIDer Guard, вы можете разблокировать устройство.

Чтобы разблокировать устройство

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

   

   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 СМС

Фильтр звонков и СМС блокирует нежелательные звонки и СМС-сообщения, в том числе рекламные СМС-рассылки, звонки и сообщения с неизвестных и скрытых номеров.

Вы можете включить запрещающий или разрешающий фильтр.

- Запрещающий фильтр блокирует добавленные контакты, ключевые слова или маски.
- Разрешающий фильтр разрешает звонки и СМС только от добавленных контактов или масок.

При включении одного фильтра другой отключается.

Для фильтрации вы можете выбрать один из стандартных списков или создать свой собственный.

СМС-фильтр не работает в версиях приложения из Google Play.

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

СМС-фильтр может работать некорректно из-за технических ограничений Android. Заблокированные сообщения могут отображаться в журнале СМС.

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

Разрешения

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

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

Нажмите **Разрешить** в каждом окне.

На устройствах с Android 9 и более поздними версиями Фильтр звонков и СМС также запрашивает доступ к списку вызовов.

На устройствах с Android 10 и более поздними версиями Фильтр звонков и СМС также запрашивает разрешение на использование Dr.Web в качестве приложения по умолчанию для автоматического определения номеров и защиты от спама.

Без необходимых разрешений компонент не будет работать.

Если вы пользуетесь телефоном Xiaomi с установленным приложением **Безопасность**, в этом приложении предоставьте Dr.Web разрешение для управления СМС.

8.2.1. Запрещающий фильтр

Запрещающий фильтр блокирует звонки и СМС от добавленных контактов.

Как использовать запрещающий фильтр

- Включить опцию **Блокировать все**, чтобы заблокировать все входящие звонки и СМС-сообщения.
- Добавить контакты в **Черный список**.
- Создать свои собственные списки.

Чтобы создать список

1. Откройте запрещающий фильтр.
2. Нажмите значок .
3. Укажите название списка.
4. Добавьте контакты или ключевые слова. Пустой список не получится сохранить.

Чтобы добавить контакты в список

1. На экране нужного списка нажмите значок . Выберите одну из опций:

   Контакты — добавить контакт из ваших контактов на устройстве.

   Журнал звонков — добавить контакт из недавних звонков. Доступно только в версии, скачанной с сайта.

   Журнал СМС — добавить контакт из недавних СМС-сообщений. Доступно только в версии, скачанной с сайта.

   Ключевое слово — добавить ключевое слово для блокировки СМС-сообщений. Доступно только в версии, скачанной с сайта.

   Dr.Web будет искать в сообщениях 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.

   Скрытый номер — заблокировать звонки с любых скрытых номеров. Доступно только в версии с Google Play. В версии с сайта и в версии с HUAWEI AppGallery вы можете добавить скрытый номер из журнала звонков или СМС.

   Новый контакт — создать новый контакт или маску.

   Импорт контактов — импортировать список контактов, сохраненный ранее.
2. При необходимости для каждого контакта отредактируйте имя и телефон, выберите, что нужно заблокировать: **Звонки** или **СМС**. Скрытые номера и номера, добавленные из ваших контактов, нельзя редактировать.

Чтобы сохранить контакты из списка на устройство

1. Выберите нужный список.
2. В правом верхнем углу нажмите значок .

8.2.2. Разрешающий фильтр

Разрешающий фильтр разрешает звонки и СМС только от добавленных контактов.

Как использовать разрешающий фильтр

- Включить опцию **Контакты**, чтобы принимать входящие звонки и СМС-сообщения только с номеров из ваших контактов.
- Создать свои собственные списки.

Чтобы создать список

1. Откройте разрешающий фильтр.
2. Нажмите значок  .
3. Укажите название списка.
4. Добавьте контакты. Пустой список не получится сохранить.

Чтобы добавить контакты в список

1. На экране нужного списка нажмите значок  . Выберите одну из опций:

   Контакты — добавить контакт из ваших контактов на устройстве.

   Журнал звонков — добавить контакт из недавних звонков. Доступно только в версии, скачанной с сайта.

   Журнал СМС — добавить контакт из недавних СМС-сообщений. Доступно только в версии, скачанной с сайта.

   Новый контакт — создать новый контакт или маску.

   Импорт контактов — импортировать список контактов, сохраненный ранее.
2. При необходимости для каждого контакта отредактируйте имя и телефон. Номер, добавленный из ваших контактов на устройстве, нельзя редактировать.

Чтобы сохранить контакты из списка на устройство

1. Выберите нужный список.
2. В правом верхнем углу нажмите значок  .

8.2.3. Маски

Маски позволяют добавлять похожие номера в списки запрещающего и разрешающего фильтров:

- Номера, начинающиеся с определенной последовательности цифр (или других символов).
- Номера, заканчивающиеся на определенную последовательность цифр (или других символов).
- Номера, содержащие определенную последовательность цифр (или других символов).

Чтобы добавить маску

1. На экране нужного списка нажмите значок  и выберите  **Новый контакт**.
2. При необходимости отредактируйте имя.
3. При вводе номера используйте звездочку `*` в начале, конце или с обеих сторон.

   Звездочка заменяет любую последовательность символов. Не используйте звездочку в середине номера или две звездочки подряд: такая маска не сработает.
4. Если вы добавляете маску в список запрещающего фильтра, выберите, что нужно заблокировать: **Звонки** или **СМС**.

Примеры масок

Пример	Комментарий
`+7*`	Все номера, начинающиеся с `+7`
`*0*`	Все номера, содержащие `0` в начале, середине или конце номера
`*0`	Все номера, заканчивающиеся на `0`

`*`
`+7*0`
`*0*0`
`**0`
`+7**`
	Примеры неправильных масок

8.2.4. Редактирование списков

Чтобы отредактировать список

1. Нажмите на список, который нужно отредактировать.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Чтобы удалить список

- Смахните название списка влево.

Если вы случайно удалите не тот список, нажмите **Отменить**. Стандартные списки нельзя удалить.

Чтобы удалить несколько списков

1. Нажмите и удерживайте сначала один список.
2. После вибросигнала выберите другие списки, которые нужно удалить.

3. Нажмите значок в правом верхнем углу.

Чтобы удалить контакт из списка

- Смахните его влево.

Чтобы удалить несколько контактов из списка

1. Нажмите и удерживайте сначала один контакт.
2. После вибросигнала выберите другие контакты, которые хотите удалить.
3. Нажмите значок в правом верхнем углу.

   Чтобы отменить случайное удаление контакта, нажмите **Отменить**.

> При удалении контакта из списка он не удаляется из ваших контактов на устройстве.

8.2.5. Заблокированные звонки и СМС

Чтобы открыть список заблокированных звонков и СМС-сообщений

1. На главном экране Dr.Web выберите **Фильтр звонков и СМС**.
2. Нажмите **Меню** и выберите **Заблокированные звонки** или **Заблокированные СМС**.

Если есть заблокированные звонки или СМС-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 СМС-сообщения доступна следующая информация:

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

Действия с заблокированными звонками и СМС

Чтобы позвонить

1. Нажмите на номер в списке заблокированных звонков или сообщений.
2. Нажмите **Позвонить**.

Чтобы отправить СМС-сообщение

1. Нажмите на номер в списке заблокированных звонков или сообщений.

2. Нажмите **Отправить СМС**.

Чтобы удалить звонок или СМС-сообщение

- Смахните его влево.

Чтобы удалить все звонки или СМС-сообщения

1. Нажмите **Меню** в правом верхнем углу экрана.
2. Нажмите **Очистить список**.

8.3. URL-фильтр

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

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

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

URL-фильтр использует облачный сервис Dr.Web Cloud. Для корректной работы компонента необходимые для связи с сервисом порты должны быть открыты.

Включение URL-фильтра

На главном экране Dr.Web выберите опцию **URL-фильтр**.

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.

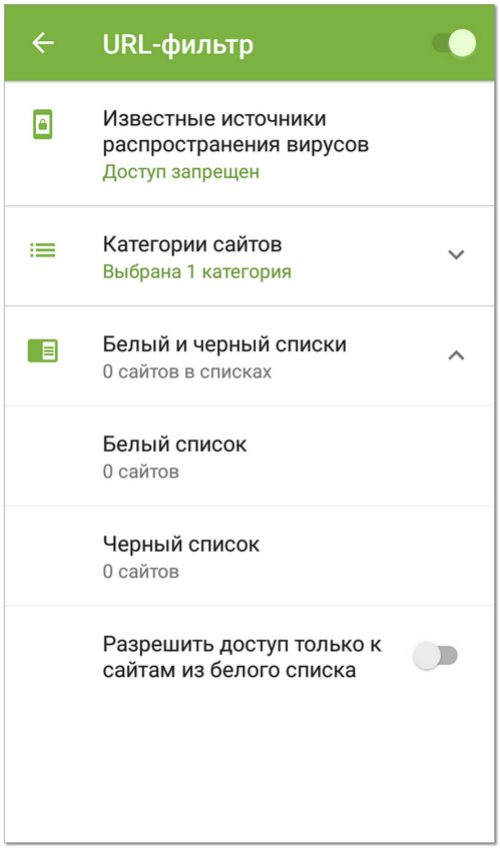

Рисунок 17: URL-фильтр

Категории сайтов

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

- 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;
- Пулы для добычи криптовалют.

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

Белый и черный списки

Вы можете составить списки 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 значок  в правом нижнем углу окна.
4. Укажите адрес сайта в одном из перечисленных форматов:
   - example.com
   - http://example.com
   - https://www.example.com
   - www.example.com

Вы можете добавить только конкретные адреса сайтов, добавление масок или ключевых слов не поддерживается.

5. Нажмите **Добавить URL**.

Если вы попытаетесь добавить адрес, 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 вашей компании или списком оплаченных услуг.

8.4. Антивор Dr.Web

Антивор Dr.Web позволяет управлять устройством при его потере или краже. Например, вы можете дистанционно удалить личные данные, определить местоположение устройства или заблокировать его. Чтобы разблокировать устройство, нужно ввести пароль:

- от учетной записи Dr.Web, если она настроена;
- от Антивора, если учетная запись не настроена.

Как управлять устройством с помощью Антивора

- Заранее настройте Антивор, например включите блокировку устройства при замене SIM-карты.
- Отправьте Антивору команду, чтобы, например, определить местоположение устройства.

8.4.1. Включение Антивора Dr.Web

1. На главном экране Dr.Web выберите **Антивор**.
2. На экране **Антивор** нажмите кнопку **Включить**.
3. Если вы включаете Антивор впервые, разрешите приложению доступ к специальным возможностям Android, а также к функциям и данным вашего устройства.

   > Если вы используете версию приложения с сайта «Доктор Веб» на телефоне Xiaomi с установленным приложением **Безопасность**, в этом приложении предоставьте Dr.Web разрешение для управления СМС.

   Антивор работает, только если предоставлены все разрешения.
4. Если на вашем устройстве не создана учетная запись Dr.Web, создайте ее.

   Если учетная запись уже создана, введите пароль от учетной записи. Если вы введете неправильный пароль 10 раз подряд, поле для ввода пароля будет временно заблокировано. Вы увидите сколько времени остается до следующей попытки.
5. Если Dr.Web не является администратором устройства, активируйте приложение в качестве администратора:
   - Чтобы предотвратить нежелательное удаление приложения.
   - Чтобы разрешить Антивору Dr.Web сбросить настройки устройства до заводских. Это защитит ваши данные при потере или краже устройства.
6. Чтобы добавить друзей, нажмите значок . Друзья помогут удаленно управлять вашим устройством в случае потери или кражи, а также если вы забудете пароль от учетной записи Dr.Web. Нажмите **Далее**.

7. Отредактируйте текст, который будет отображаться на экране вашего устройства в случае блокировки. Здесь можно указать, как с вами можно связаться и вернуть потерянное устройство. Нажмите **Далее**.
8. Отредактируйте текст уведомления, которое вы можете отправить друзьям, если Антивор заблокирует ваше устройство и вы забудете пароль. Нажмите **Далее**.
9. Включите необходимые настройки и нажмите **Готово**.

8.4.2. Настройка Антивора Dr.Web

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

Чтобы открыть Антивор

1. На главном экране Dr.Web выберите **Антивор**.
2. Если рядом с полем ввода пароля есть значок , нажмите значок и прикоснитесь к сканеру отпечатков пальцев.

   Если аутентификация по отпечатку пальца недоступна, 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 осталось до следующей попытки.

При обновлении с предыдущих версий на версию 12 ваш пароль от Антивора Dr.Web автоматически становится паролем от учетной записи Dr.Web.

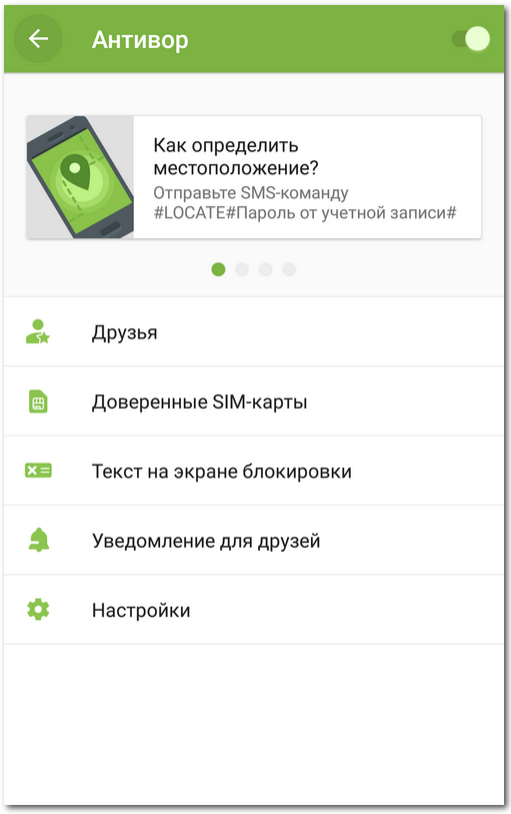

Рисунок 18: Антивор Dr.Web

Карточки с СМС-командами

Доступно только в версии приложения с сайта «Доктор Веб».

Карточки с СМС-командами расположены в верхней части экрана **Антивор** (см. Рисунок 18).

- Чтобы просмотреть все СМС-команды, листайте карточки вправо.
- Чтобы открыть полное описание СМС-команды или отправить СМС-команду, нажмите на карточку с этой командой.

Друзья

Друзья — это контакты, которым вы доверяете управлять вашим устройством с помощью команд, или которые доверяют вам. В приложении друзья разделены на две вкладки: Я доверяю и Мне доверяют.

Я доверяю

На этой вкладке расположен список друзей, которым вы доверяете управлять вашим устройством с помощью команд. Вы добавили эти контакты в друзья, указав их телефонные номера или адреса электронной почты.

Значок	Версия приложения	Комментарий
	Только версия с сайта «Доктор Веб»	Вы добавили телефонный номер. Друг может отправлять СМС-команды без пароля на ваше устройство.
	Любая	Вы добавили адрес электронной почты. Друг еще не подтвердил ваш запрос в друзья и не может отправлять пуш-команды Антивору. Чтобы подтвердить запрос, у добавленного друга на устройстве должно быть установлено приложение Dr.Web Security Space или бесплатная версия Dr.Web Light. Возможно, ваш запрос был пропущен. При необходимости отправьте повторный запрос.
	Любая	Вы добавили адрес электронной почты. Друг подтвердил ваш запрос в друзья и может отправлять пуш-команды Антивору. • Если на устройстве друга установлено приложение Dr.Web Security Space, друг может отправлять любые команды. • Если на устройстве друга установлено приложение Dr.Web Light, друг может помочь разблокировать ваше устройство, если оно заблокировано Антивором и вы не помните пароль.
	Любая	Вы добавили адрес электронной почты, но друг отклонил ваш запрос в друзья. Друг не может отправлять пуш-команды Антивору. В этом случае вы можете удалить контакт из списка друзей.

Чтобы добавить друга

- На вкладке **Я доверяю** нажмите значок  .
  - **Для версии приложения с сайта «Доктор Веб»**. Добавьте телефонный номер. С этого номера можно будет отправлять на ваше устройство СМС-команды без пароля. Для этого выберите одну из опций:
    -  **Контакты** — выбрать телефон из ваших контактов на устройстве.
    -  **Журнал звонков** — выбрать телефон из недавних звонков.
    -  **Журнал СМС** — выбрать телефон из недавних СМС-сообщений.
    -  **Новый контакт** — ввести новый телефонный номер.
  - **Для любой версии приложения**. Добавьте адрес электронной почты. На указанный адрес будет отправлено письмо с вашим запросом в друзья. Запрос можно подтвердить в приложении Dr.Web Security Space или в бесплатной версии Dr.Web Light. После подтверждения запроса друг сможет отправлять команды Антивору с

помощью уведомлений. Из Dr.Web Light можно будет отправить команду для разблокировки устройства и сброса пароля, если ваше устройство будет заблокировано. Из Dr.Web Security Space можно будет отправить любые команды.

Всего можно добавить до пяти адресов электронной почты (и до пяти телефонных номеров — в версии приложения с сайта «Доктор Веб»).

Чтобы отредактировать контакт друга

1. На вкладке **Я доверяю** выберите нужный контакт.
2. Нажмите значок .
3. Внесите изменения.
4. Нажмите значок , чтобы сохранить изменения.

> Вы не можете отредактировать запись, если этот контакт отклонил ваш запрос в друзья.

Чтобы удалить друга

- Смахните соответствующий контакт влево.

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

Мне доверяют

На вкладке **Мне доверяют** находится список друзей, которые доверяют вам управлять их устройством. Они добавили вас в друзья в Антиворе Dr.Web, указав ваш адрес электронной почты. Чтобы вы могли удаленно управлять устройством друга, требуется подтвердить запрос в друзья.

Статусы запросов в друзья

Значок	Комментарий
	Вы еще не подтвердили запрос в друзья. Чтобы вы могли отправлять пуш-команды на устройство друга, подтвердите запрос в друзья.
	Вы подтвердили запрос в друзья и можете удаленно управлять устройством друга с помощью пуш-команд.
	Вас удалили из списка друзей. Чтобы вы могли отправлять пуш-команды, друг должен отправить вам повторный запрос.

Чтобы подтвердить запрос в друзья

Выполните одно из следующих действий:

- Нажмите на уведомление с запросом, которое вы получили после добавления вас в друзья, и нажмите **Подтвердить**.
- Выберите нужный контакт на вкладке **Мне доверяют** и нажмите **Подтвердить**.

Чтобы отклонить запрос в друзья

Выполните одно из следующих действий:

- Нажмите на уведомление с запросом, которое вы получите после добавления вас в друзья, и нажмите **Отклонить**.
- Выберите нужный контакт на вкладке **Мне доверяют** и нажмите **Отклонить**.
- Удалите контакт из списка друзей.

Чтобы отредактировать контакт друга

1. На вкладке **Мне доверяют** выберите нужный контакт.
2. Нажмите значок .
3. Внесите изменения в запись.
4. Нажмите значок , чтобы сохранить изменения.

> Вы не можете отредактировать запись, если этот контакт удалил вас из друзей.

Чтобы удалить друга

- Смахните соответствующий контакт влево.

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

Чтобы разблокировать устройство друга

1. Нажмите на уведомление, полученное от друга.
2. Самостоятельно свяжитесь с другом, чтобы узнать код подтверждения. Не доверяйте полученным сообщениям, которые содержат код подтверждения, они могут быть отправлены мошенниками.
3. Введите код подтверждения.
4. Нажмите **Разблокировать**.

Доверенные SIM-карты

Доверенные SIM-карты — это список SIM-карт, которые вы используете на устройстве. По умолчанию Антивор блокирует устройство, если обнаруживает на нем SIM-карту не из списка доверенных. В этом случае, если ваше устройство украдут и заменят SIM-карту, им нельзя будет воспользоваться. При замене одной доверенной SIM-карты на другую из этого списка Антивор не блокирует 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. На устройстве с Android 5.0 или более ранними версиями сделать доверенной можно только одну SIM-карту (одновременно добавить обе SIM-карты нельзя).

У каждой SIM-карты в списке указаны имя, а также ее идентификатор (на устройствах с Android 5.0 или более ранними версиями) или оператор мобильной связи (на устройствах с Android 5.1 или более поздними версиями).

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

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

- Чтобы увидеть более подробную информацию о SIM-карте, нажмите на нее в списке. В зависимости от версии ОС могут быть доступны следующие поля: имя, оператор, идентификатор.
- Чтобы переименовать SIM-карту, нажмите на нее в списке. В открывшемся экране укажите новое имя в поле **Имя** и нажмите **Сохранить**.
- Чтобы удалить SIM-карту из списка доверенных, смахните ее влево.

SIM-карта, которая используется в данный момент, не может быть удалена из списка доверенных.

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.

Чтобы изменить текст на экране блокировки

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

Уведомление для друзей

Уведомление для друзей — это уведомление, которое вы можете отправить друзьям, если Антивор заблокирует ваше устройство и вы забудете пароль. После получения уведомления друзья должны узнать у вас код подтверждения, чтобы сбросить ваш пароль и вы могли задать новый.

Чтобы изменить текст уведомления

- Нажмите **Уведомление для друзей**, наберите новый текст и нажмите **Сохранить**.

Настройки

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 СМС друзьям о замене SIM-карты

Доступно только в версии приложения с сайта «Доктор Веб».

По умолчанию опция отключена.

Если эта опция включена, Антивор Dr.Web отправит СМС-сообщения всем контактам 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 СМС-сообщения контактам из списка друзей. Антивор может отправить максимум пять таких СМС-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, СМС-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 (кроме СМС, так как Dr.Web не является приложением для приема и отправки СМС по умолчанию). Dr.Web не будет удален и продолжит блокировать устройство.

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 СМС-команд будет недоступна, однако вы сможете использовать остальные функции Антивора Dr.Web.

8.4.3. Команды Антивора Dr.Web

Используйте команды Антивора Dr.Web, чтобы дистанционно управлять устройством.

- Пуш-команды отправляются через пуш-уведомления и не отображаются на устройстве получателя.
- СМС-команды отправляются через СМС-сообщения и отображаются на устройстве получателя.

Требования для использования команд Антивора

Устройство	Пуш-команды	СМС-команды
Отправитель	Устройство с любой версией приложения. Антивор включен, в Антиворе подтвержден запрос в друзья получателя.	Установка приложения Dr.Web не требуется. • Любое устройство, если пароль указан в СМС-команде. • Устройство с телефонным номером, добавленным в список друзей получателя, если пароль не указан в СМС-команде.
Получатель	Устройство с любой версией приложения. Антивор включен.	Устройство с версией приложения с сайта или из HUAWEI AppGallery. Антивор включен.

Присутствующая на некоторых устройствах системная настройка **Экран блокировки** может препятствовать вводу пароля от учетной записи Dr.Web на устройстве, заблокированном командой. По умолчанию настройка отключена. Если вы включали ее, в настройках устройства откройте **Приложения** > **Dr.Web** > **Другие разрешения** и отключите настройку **Экран блокировки**.

8.4.3.1. Пуш-команды

Что такое пуш-команды

Пуш-команды — это команды для управления Антивором Dr.Web, для отправки которых используются пуш-уведомления Android. Пуш-уведомления, которые содержат пуш-команды, не отображаются на устройстве получателя, но обрабатываются приложением.

Не гарантируется корректная работа пуш-уведомлений в версии из HUAWEI AppGallery, установленной не на устройствах Huawei, так как для отправки могут использоваться мобильные службы, не обновленные до актуальной версии.

Что требуется для использования пуш-команды

1. Для отправки и получения пуш-команд устройства должны быть подключены к интернету.
2. На устройстве получателя должно быть установлено приложение Dr.Web Security Space. На устройстве отправителя — Dr.Web Security Space или Dr.Web Light.
3. На устройстве получателя должен быть включен Антивор.
4. Пуш-команда может быть отправлена только с устройства, на котором ранее был подтвержден запрос в друзья получателя.

- Из приложения Dr.Web Security Space друг может отправлять любые пуш-команды.
- Из приложения Dr.Web Light друг может разблокировать устройство получателя, используя компонент Помощь другу.

Чтобы отправить пуш-команду

1. На экране **Антивор** нажмите **Друзья**.
2. Выберите вкладку **Мне доверяют**.
3. Выберите друга, на чье устройство нужно отправить команду.
4. Выберите команду.

Доставка пуш-команд может занимать до 15 минут.

Команды

Присутствующая на некоторых устройствах системная настройка **Экран блокировки** может препятствовать разблокировке устройства, заблокированного командой. Заранее убедитесь, что настройка отключена.

Команда	Действие
Определить местоположение	Получить координаты мобильного устройства. В ответ на команду вы получите ссылку с координатами 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.
Заблокировать устройство	Заблокировать устройство. Чтобы разблокировать устройство, нужно ввести пароль от учетной записи Dr.Web.
Заблокировать устройство и включить звуковой сигнал	Заблокировать устройство и включить на нем звуковой сигнал, который будет звучать даже после перезагрузки устройства. Чтобы разблокировать устройство, нужно ввести пароль от учетной записи Dr.Web.

Команда	Действие
Удалить данные	Удалить все данные с устройства. Если Dr.Web активирован в качестве администратора на устройстве друга, эта команда сбросит настройки устройства до заводских. Эта команда также будет выполнена, если устройство заблокировано и в настройках Антивора Dr.Web включена опция **Удалить данные**.
Сбросить пароль	Разблокировать устройство и сбросить пароль от учетной записи Dr.Web. Для отправки команды требуется код подтверждения. Код отображается на устройстве друга.

8.4.3.2. СМС-команды

Вы можете отправлять СМС-команды только на устройства, на которых установлена версия приложения с сайта «Доктор Веб».

Чтобы СМС-команды работали на телефоне Xiaomi с установленным приложением **Безопасность**, в этом приложении Dr.Web должно быть предоставлено разрешение для управления СМС.

СМС-команды — это команды для дистанционного управления Антивором Dr.Web, отправленные через СМС-сообщения. С помощью СМС-команд вы можете узнать, где находится ваше мобильное устройство, а также заблокировать его функции и удалить персональную информацию.

Вы можете отправить СМС-команду следующим образом:

- С указанием пароля — с любого устройства.
- Без указания пароля — с устройства друга.

Не рекомендуется отправлять СМС-команды с паролем на потерянное или украденное устройство: злоумышленники могут увидеть полученное СМС с паролем и разблокировать устройство. Чтобы можно было отправить СМС-команду без пароля, заранее добавьте номера телефонов в список друзей.

СМС-команды

Присутствующая на некоторых устройствах системная настройка **Экран блокировки** может препятствовать разблокировке устройства, заблокированного командой. Заранее убедитесь, что настройка отключена.

Команда	Действие
#LOCK#*Пароль***#**	Заблокировать устройство.

Команда	Действие
	В ответ на команду вы получите СМС-сообщение: «Антивор Dr.Web - Устройство <*название устройства*> заблокировано».
#SIGNAL#*Пароль***#**	Заблокировать устройство и включить на нем звуковой сигнал, который будет звучать даже после перезагрузки устройства. В ответ на команду вы получите СМС-сообщение: «Антивор Dr.Web - Устройство <*название устройства*> заблокировано».
#LOCATE#*Пароль***#**	Получить координаты мобильного устройства в СМС-сообщении. В ответ на команду вы получите ссылку с координатами 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 СМС-сообщение: «Антивор Dr.Web - Удаление данных на устройстве <*название устройства*>».
#RESETPASSWORD#	Разблокировать устройство и задать новый пароль. Эта команда может быть выполнена, только если она отправлена с номера телефона, указанного в списке друзей.

СМС-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 СМС-команды #LOCATE#, были наиболее точными, разрешите использование беспроводных сетей для определения местоположения в настройках мобильного устройства.

Отправка СМС-команд через Антивор Dr.Web

Через Антивор Dr.Web вы можете отправлять СМС-команды устройствам, на которых тоже включен Антивор Dr.Web.

Чтобы отправить СМС-команду

1. На экране **Антивор** (см. Рисунок 18) нажмите на любую карточку с СМС-командой.
2. Нажмите **Отправить СМС-команду**.
3. На экране **Отправка СМС-команды**:
   1. В списке **Команда** выберите необходимую команду:
      - **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#.
   2. В поле **Кому** укажите телефонный номер получателя.
   3. В поле **Пароль получателя** укажите пароль от учетной записи получателя.

      Если ваш номер добавлен в список друзей получателя, можете оставить поле пустым.
   4. В списке **От кого** выберите SIM-карту, с которой будет отправлена команда.

      Эта опция доступна на устройствах с двумя SIM-картами с Android 5.1 или более поздними версиями.
   5. Нажмите кнопку **Отправить**.

8.4.4. Отключение Антивора Dr.Web

Чтобы отключить Антивор Dr.Web

1. На главном экране Dr.Web выберите **Антивор**.
2. Введите пароль от учетной записи Dr.Web или Антивора.
3. На экране **Антивор** (см. Рисунок 18) отключите Антивор, используя переключатель в правом верхнем углу экрана.
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 запретить доступ к любому установленному приложению или группе приложений, а также к настройкам компонентов Dr.Web.

Как работает Родительский контроль

На устройстве, пользователю которого вы хотите заблокировать доступ к приложениям и настройкам компонентов Dr.Web, должно быть установлено приложение Dr.Web. Вы активируете компонент Родительский контроль на устройстве пользователя и указываете параметры вашей учетной записи Dr.Web. После активации компонента вы задаете ограничения на доступ пользователя устройства к приложениям, группам приложений или настройкам компонентов Dr.Web. При попытке запустить заблокированное приложение или открыть настройки компонента пользователь устройства видит экран блокировки или экран ввода пароля. Доступ к заблокированному приложению или компоненту возможен только после ввода пароля от вашей учетной записи Dr.Web или распознавания вашего отпечатка пальца.

Основные функции Родительского контроля

Родительский контроль позволяет:

- полностью запретить доступ к приложению или группе приложений;
- полностью запретить доступ к настройкам компонентов Dr.Web;
- создавать ограничения на доступ к приложению или группе приложений в заданном временном интервале;
- создавать пользовательские группы блокируемых приложений;
- отслеживать события, связанные с блокируемыми приложениями и компонентами.

Включение Родительского контроля

Чтобы включить Родительский контроль

1. На главном экране Dr.Web выберите **Родительский контроль**.
2. Если на устройстве не создана учетная запись Dr.Web, создайте ее.

Если учетная запись создана, введите пароль от учетной записи. Если вы введете неправильный пароль 10 раз подряд, поле для ввода пароля будет временно заблокировано. Вы увидите, сколько времени остается до следующей попытки.

3. На экране **Родительский контроль** нажмите кнопку **Включить**.
4. Если Dr.Web не является администратором устройства, активируйте приложение в качестве администратора. Это поможет предотвратить нежелательное удаление приложения. Кроме того, при потере или краже устройства вы сможете защитить свои данные, сбросив настройки устройства до заводских с помощью Антивора Dr.Web.

Отключение Родительского контроля

Чтобы отключить Родительский контроль

1. На главном экране Dr.Web выберите **Родительский контроль**.
2. Введите пароль от учетной записи Dr.Web.
3. Отключите Родительский контроль, используя переключатель в правом верхнем углу экрана, и нажмите **ОК**.

Режим обучения

В верхней части главного экрана компонента Родительский контроль (см. Рисунок 19) доступны мини-слайды, позволяющие перейти в режим обучения. Режим обучения помогает быстро освоить основные функции Родительского контроля.

Режим обучения состоит из четырех разделов:

- Приложения: запрет доступа к приложениям и группам приложений.
- Доступ по времени: ограничение доступа к приложениям и группам приложений по времени.
- Компоненты: запрет доступа к настройкам компонентов Dr.Web.
- Настройки: настройки и журнал Родительского контроля.

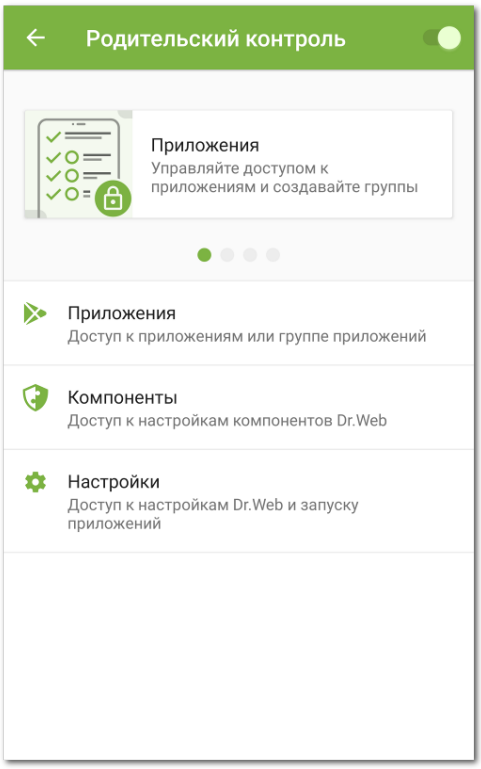

Рисунок 19: Родительский контроль

Мини-слайды позволяют открыть один из разделов режима обучения. Смахните мини-слайд влево или вправо, чтобы перейти к следующему или предыдущему мини-слайду. Нажмите на мини-слайд, чтобы открыть соответствующий раздел режима обучения.

В режиме обучения доступны полноэкранные слайды, рассказывающие о том, как пользоваться основными функциями Родительского контроля. Смахните текущий слайд влево, чтобы перейти к следующему.

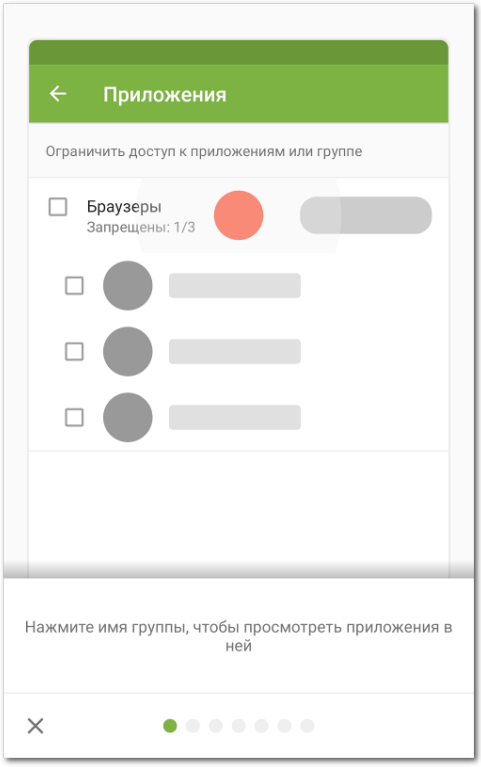

Рисунок 20: Слайд режима обучения

Чтобы выйти из режима обучения, нажмите ✕ в левом нижнем углу экрана.

8.5.1. Блокировка доступа к приложениям и компонентам

Приложения

Раздел **Приложения** содержит список всех приложений, установленных на устройстве.

Запрет доступа к приложениям и группам приложений

Компонент Родительский контроль позволяет блокировать доступ к отдельным приложениям или целым группам приложений. При попытке открыть приложение, к которому запрещен или ограничен доступ, появляется экран блокировки приложения, закрывающий доступ к самому приложению. Получить доступ к приложению возможно с помощью пароля от учетной записи Dr.Web или заданного отпечатка пальца.

Чтобы запретить доступ к приложению или всем приложениям группы, уставите флажок напротив имени приложения или группы. Чтобы снова разрешить доступ, снимите флажок.

Группы приложений

По умолчанию приложения разделены на системные группы по категориям. Чтобы просмотреть приложения в группе, нажмите на имя группы.

> На устройствах с Android 8.0 и более ранними версиями все приложения входят в системную группу **Другие**.

Вы также можете создавать пользовательские группы приложений.

Чтобы создать пользовательскую группу

1. Нажмите значок в правом нижнем углу экрана.
2. В открывшемся меню выберите **Новая группа**.
3. Введите имя новой группы.
4. Нажмите напротив приложений, которые вы хотите добавить в новую группу.
5. Нажмите , чтобы сохранить новую группу.

Пользовательские группы отображаются в верху списка групп приложений.

Чтобы редактировать пользовательскую группу

1. Смахните имя группы влево.
2. Нажмите значок .
3. Внесите необходимые изменения.
4. Нажмите значок в правом верхнем углу экрана.

Чтобы удалить пользовательскую группу

1. Смахните имя группы влево.
2. Нажмите значок .

Чтобы удалить несколько пользовательских групп

1. Нажмите и удерживайте имя одной из групп, подлежащих удалению.
2. Выберите остальные группы, подлежащие удалению.
3. Удалите группы, нажав значок в правом верхнем углу экрана.

> Системные группы редактировать или удалять нельзя.

Если в настройках Родительского контроля включена опция **Запретить браузеры без URL-фильтра** или **Запретить запуск новых приложений**, в списке приложений появляется системная группа **Браузеры без URL-фильтра** или **Новые приложения** соответственно. Чтобы разрешить доступ к приложениям из этих групп, отключите соответствующие опции в настройках Родительского контроля.

Поиск в списке приложений

Для удобства навигации по списку приложений вы можете воспользоваться поиском.

Чтобы выполнить поиск по имени приложения или группы

1. Нажмите значок  в правом нижнем углу экрана.
2. В открывшемся меню выберите **Поиск**.
3. Введите запрос в поле поиска в нижней части экрана.

Ограничение доступа по времени

Вы можете блокировать доступ к группам приложений на постоянной основе и в заданные периоды времени.

Тип блокировки отображается справа от имени группы. Возможны два типа блокировки:

- **Всегда** — доступ к группе заблокирован постоянно.
- **Интервал** — доступ к группе заблокирован в определенный период времени.

По умолчанию при блокировке группы приложений доступ блокируется всегда.

Чтобы задать период блокировки

1. Нажмите на тип блокировки справа от группы приложений.
2. Нажмите  в правом нижнем углу экрана.
3. Выберите дни недели, в которые ограничение будет действовать.
4. Нажмите **Начало** и задайте время начала действия ограничения.
5. Нажмите **ОК**, чтобы подтвердить выбранное время начала.
6. Нажмите **Окончание** и задайте время окончания действия ограничения.
7. Нажмите **ОК**, чтобы подтвердить выбранное время окончания.
8. Нажмите  в правом верхнем углу экрана, чтобы сохранить ограничение.

Для одного ограничения можно задать только один временной интервал. Чтобы блокировать группу приложений в другие дни недели и часы, создайте дополнительные ограничения.

Ограничения можно редактировать и удалять.

Чтобы редактировать ограничение

1. Нажмите на тип блокировки справа от группы приложений.
2. Смахните влево нужное ограничение.
3. Нажмите значок .
4. Внесите необходимые изменения.
5. Сохраните изменения, нажав значок в правом верхнем углу экрана.

Чтобы удалить ограничение

1. Нажмите на тип блокировки справа от группы приложений.
2. Смахните влево нужное ограничение.
3. Нажмите значок .

Компоненты

Помимо доступа к приложениям или группам приложений вы также можете запретить доступ к настройкам компонентов Dr.Web: Фильтра звонков и СМС, URL-фильтра, Брандмауэра, а также настройкам приложения Dr.Web.

Чтобы запретить доступ к настройкам компонентов

1. На главном экране Родительского контроля выберите раздел **Компоненты**.
2. Установите флажки напротив компонентов Dr.Web, доступ к которым вы хотите запретить:

- Фильтр звонков и СМС. Позволяет владельцу учетной записи создавать списки номеров, с которых пользователь устройства может получать звонки и сообщения. Например, можно разрешить входящие звонки и СМС-сообщения только с определенных номеров или номеров из списка контактов. Пользователь устройства не сможет изменить список разрешенных или запрещенных номеров.
- URL-фильтр. Позволяет владельцу учетной записи ограничить доступ пользователя устройства к конкретным сайтам, веб-страницам, а также к категориям сайтов (например, «Наркотики», «Оружие», «Терроризм», «Сайты для взрослых» и др.). Пользователь устройства не сможет изменить список сайтов и категорий сайтов, к которым он имеет доступ.
- Брандмауэр. Позволяет владельцу учетной записи ограничить использование мобильного трафика, контролировать передачу данных и управлять интернет-соединениями приложений на устройстве пользователя. Пользователь не сможет изменить установленные правила и ограничения.

- Настройки Dr.Web. Позволяет владельцу учетной записи запретить пользователю устройства заходить в настройки Dr.Web и изменять их. Например, пользователь не сможет сбросить настройки.

> ⚠ Для компонентов Dr.Web невозможно задать ограничение доступа по времени. Доступ будет запрещен всегда.

Для доступа к заблокированному компоненту требуется ввести пароль от учетной записи Dr.Web или отсканировать отпечаток пальца (при соответствующей настройке).

Экран блокировки

При попытке запуска заблокированного приложения появляется экран блокировки (см. Рисунок 21). Для доступа к приложению необходимо ввести пароль от учетной записи и нажать кнопку **Разблокировать**. Получить доступ к приложению также можно с помощью отпечатка пальца, если в настройках Родительского контроля включена опция **Разблокировка с помощью отпечатка пальца**.

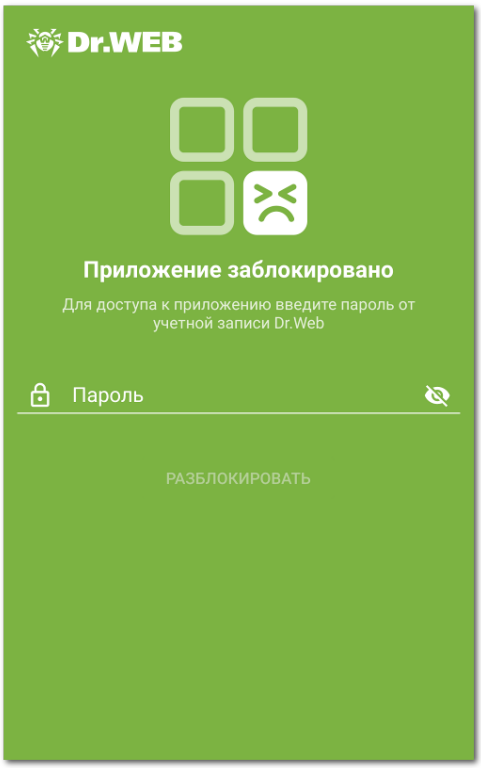

Рисунок 21: Экран блокировки приложения

Новые приложения

Если в настройках Родительского контроля включена опция **Запретить запуск новых приложений**, все приложения, установленные после включения опции, попадают в

блокируемую системную группу **Новые приложения**. При запуске приложения из группы **Новые приложения** на экране блокировки доступна опция, позволяющая разрешить доступ к приложению на постоянной основе.

Чтобы разрешить доступ к новому приложению

1. Запустите нужное приложение.
2. На экране блокировки приложения введите пароль от учетной записи Dr.Web.
3. Установите флажок напротив опции **Исключить из группы «Новые приложения»**.
4. Нажмите кнопку **Разблокировать**.

8.5.2. Настройки Родительского контроля

В раздел **Настройки** можно перейти с главного экрана компонента. Раздел позволяет управлять настройками Родительского контроля, а также перейти к журналу Родительского контроля.

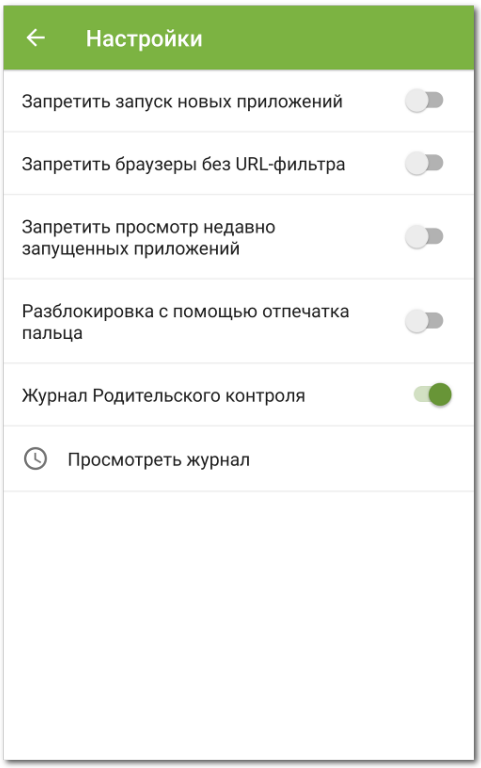

Рисунок 22: Настройки Родительского контроля

В разделе **Настройки** доступны следующие опции:

- **Запретить запуск новых приложений**. Позволяет запретить доступ к приложениям, устанавливаемым на устройство после включения опции. Новые приложения включаются в системную группу **Новые приложения**. Доступ к приложениям группы запрещен всегда.

Доступ к конкретному приложению можно разрешить с помощью опции **Исключить из группы «Новые приложения»** на экране блокировки этого приложения.

- **Запретить браузеры без URL-фильтра**. Позволяет запретить доступ к браузерам, не поддерживающимся URL-фильтром. Браузеры включаются в системную группу **Браузеры без URL-фильтра**. Доступ к приложениям этой группы запрещен всегда.

Для включения опции необходимо, чтобы на устройстве был включен URL-фильтр.

- **Запретить просмотр недавно запущенных приложений**. Позволяет запретить вызов экрана недавно запущенных приложений на устройстве. При попытке вызвать экран недавно запущенных приложений появится экран блокировки.

При использовании сторонних системных оболочек опция может работать некорректно.

- **Разблокировка с помощью отпечатка пальца**. Позволяет использовать отпечаток пальца вместо пароля от учетной записи Dr.Web для разблокировки приложений и компонентов.

Перед включением опции убедитесь, что на устройстве зарегистрирован только отпечаток владельца учетной записи Dr.Web.

Сканер отпечатков пальцев будет отключен после многократных ошибок распознавания отпечатка. Для повторного включения сканера необходимо разблокировать устройство иным заданным способом (графическим ключом, ПИН-кодом или паролем).

- **Журнал Родительского контроля**. Включает ведение журнала Родительского контроля. После включения опции доступна опция **Просмотреть журнал**.

8.5.3. Журнал Родительского контроля

В журнале Родительского контроля регистрируются события, связанные с приложениями и компонентами, доступ к которым запрещен или ограничен.

По умолчанию события журнала Родительского контроля представлены в виде списка событий, сгруппированных по дате. В журнале регистрируются следующие события:

- События приложений:
  - попытка запуска,
  - разблокировка.
- События компонентов и Родительского контроля:
  - включение,
  - выключение.

Для каждого события указано время.

Отображение событий в журнале

Для удобства просмотра вы можете управлять отображением событий в журнале Родительского контроля: сортировать, фильтровать или группировать события. Также доступен поиск по событиям.

Фильтр событий

Чтобы сортировать или фильтровать события по заданному параметру, нажмите значок  в правом нижнем углу экрана и выберите **Фильтр**.

Доступны следующие варианты сортировки:

- сначала старые,
- сначала новые,
- по алфавиту от А до Я,
- по алфавиту от Я до А.

Вы также можете задать фильтр по типу события: разблокировка, попытка запуска приложений; включение, выключение компонентов.

Чтобы сортировать или фильтровать список событий, выберите нужные значения и вернитесь к списку событий.

Вы можете восстановить отображение событий по умолчанию, нажав ↺ в правом верхнем углу экрана **Фильтр событий**.

Поиск

Чтобы искать в журнале событий Родительского контроля

1. Нажмите значок  в правом нижнем углу экрана.
2. В открывшемся меню выберите **Поиск**.
3. Введите запрос в поле поиска в нижней части экрана.

Группировка

Вы можете группировать события по приложению или компоненту. При таком виде группировки журнал Родительского контроля представляет собой список приложений и компонентов, события которых были зарегистрированы в журнале (см. Рисунок 23).

Чтобы сгруппировать события журнала Родительского контроля, на экране журнала нажмите **Меню** в правом верхнем углу и установите флажок **Группировать**. Нажмите на имя приложения или компонента, чтобы раскрыть список относящихся к нему событий.

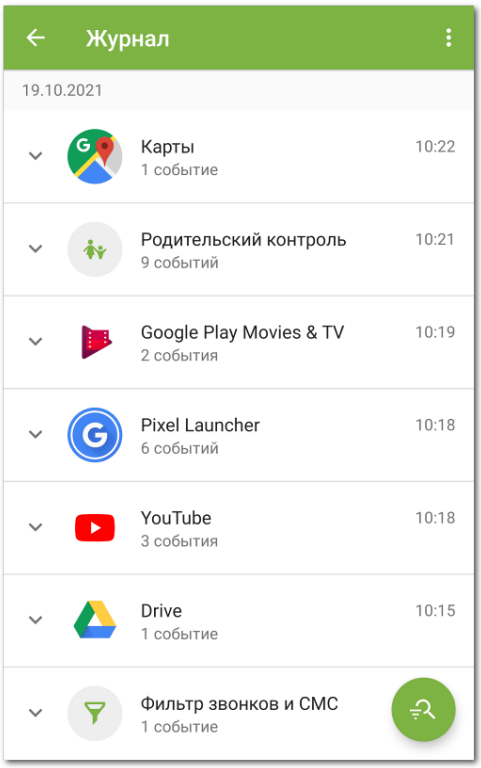

Рисунок 23: Группировка событий

Фильтр групп

При желании вы можете сортировать группы событий по заданному параметру.

Чтобы сортировать сгруппированные события

1. Нажмите значок в правом нижнем углу экрана.
2. Выберите опцию **Фильтр**.
3. На экране **Фильтр групп** выберите тип сортировки.
4. Вернитесь к списку событий.

Вы можете восстановить отображение событий по умолчанию, нажав в правом верхнем углу экрана **Фильтр групп**.

Сохранение журнала

Чтобы сохранить журнал событий в файл, на экране журнала нажмите **Меню** в правом верхнем углу и выберите **Сохранить журнал**.

Журнал сохраняется в файл `DrWeb_Parental_Log.txt`, расположенный в папке `Android/data/com.drweb/files` во внутренней памяти устройства.

> На устройствах с Android 11 или более поздними версиями журнал сохраняется в папке `Download/DrWeb`.

Очистка журнала

Чтобы удалить все события из журнала Родительского контроля, на экране журнала нажмите **Меню** и выберите пункт **Очистить журнал**.

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 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-туннель не создается и интернет-трафик не шифруется.

Чтобы включить Брандмауэр Dr.Web

1. На главном экране Dr.Web выберите опцию **Брандмауэр**.
2. Нажмите кнопку **Включить** или используйте переключатель в правом верхнем углу экрана.

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

Чтобы включить Брандмауэр 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. Откройте настройки сети **Dr.Web**.
3. На экране **Dr.Web** 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 права на использование VPN переходят к другому приложению, Брандмауэр Dr.Web будет отключен, о чем будет выведено соответствующее уведомление. Чтобы снова включить Брандмауэр Dr.Web, достаточно нажать на это уведомление.

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

Начальный экран

На начальном экране Брандмауэра расположены карточки с информацией из его разделов:

- Ограничение трафика (при наличии активного ограничения): отображает информацию о текущем ограничении трафика.
- Активные приложения: отображает диаграмму объема входящего и исходящего трафика, использованного активными сетевыми соединениями приложений.

- Все приложения: отображает суммарный объем входящего и исходящего трафика, использованного установленными на устройстве приложениями.

Нажмите **Подробнее** на карточках трафика приложений и ограничения трафика, чтобы перейти к соответствующему разделу.

Меню в правом верхнем углу начального экрана позволяет:

- перейти к настройке ограничения мобильного трафика;
- открыть журнал Брандмауэра.

8.6.1. Управление сетевой активностью приложений

Брандмауэр Dr.Web позволяет контролировать использование трафика на устройстве и задавать общие настройки интернет-доступа приложений. Возможности общего управления включают в себя:

- отслеживание активного трафика приложений в режиме реального времени;
- просмотр списка приложений, использовавших интернет-трафик, и объема израсходованного ими трафика;
- управление доступом к передаче данных приложений по Wi-Fi, мобильному интернету и в роуминге;
- ограничение суммарного расхода трафика в течение заданного периода времени.

8.6.1.1. Активные приложения

В разделе **Активные приложения** в режиме реального времени показывается список активных соединений, инициированных установленными на устройстве приложениями. Раздел предоставляет вам быстрый доступ к управлению текущим интернет-трафиком приложений.

На карточке раздела на начальном экране Брандмауэра отображаются приложения с наибольшим активным трафиком. Нажмите **Подробнее**, чтобы открыть полный список приложений с активными соединениями.

Для каждого приложения на экране **Активные приложения** (см. Рисунок 24) отображается следующая информация:

- Суммарный объем входящего и исходящего по установленным соединениям трафика.
- Доступ к передаче данных по Wi-Fi, мобильному интернету и в роуминге.
- Наличие пользовательских настроек. Приложения с измененным доступом к передаче данных отмечены значком .
- Наличие системных угроз с заблокированным интернет-соединением. Системные приложения с заблокированным доступом к передаче данных отмечены значком .

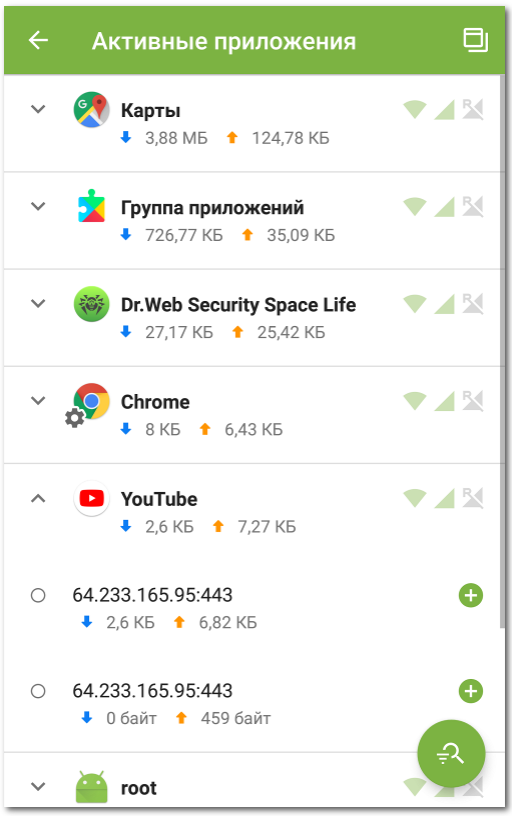

Рисунок 24: Активные приложения

Соединения приложений

Нажмите значок ⌄ слева от имени приложения на экране **Активные приложения**, чтобы увидеть подробную информацию о соединениях, установленных приложением:

- список установленных соединений;
- объем входящего и исходящего по каждому из установленных соединений трафика;
- наличие правила для соединения:
  - ● разрешающее,
  - ● запрещающее,
  - ● перенаправляющее,
  - ○ правило не задано.

Чтобы скопировать адрес соединения, нажмите и удерживайте строчку с адресом соединения. Адрес будет скопирован в буфер.

Нажмите на строку соединения, чтобы перейти на экран Соединение.

Правила соединений

Вы можете управлять соединениями, устанавливаемыми приложениями, с помощью разрешающих, запрещающих и перенаправляющих правил (см. раздел Правила

соединений). Для создания или редактирования правила нажмите значок или справа от соединения.

Сортировка приложений

Чтобы сортировать список приложений, нажмите значок в правом нижнем углу экрана, затем нажмите **Фильтр** и выберите нужные параметры сортировки:

- по убыванию трафика — приложения с наибольшим трафиком вверху списка;
- по возрастанию трафика — приложения с наименьшим трафиком вверху списка;
- по алфавиту от А до Я;
- по алфавиту от Я до А.

По умолчанию приложения отсортированы по убыванию трафика (приложения с наибольшим трафиком расположены вверху списка). Чтобы восстановить сортировку по умолчанию, нажмите значок на экране **Фильтр**.

Поиск

Чтобы быстро перейти к нужному вам приложению, воспользуйтесь поиском по имени приложения. Для этого нажмите значок в правом нижнем углу экрана, затем нажмите **Поиск** и введите запрос в поле поиска в нижней части экрана.

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.

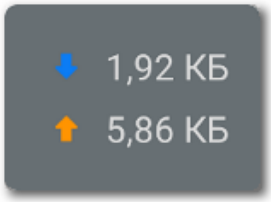

Рисунок 25:
Плавающее окно

Чтобы включить плавающее окно

1. Откройте экран **Активные приложения** и нажмите значок в правом верхнем углу экрана (см. Рисунок 24).
2. Разрешите приложению отображать плавающее окно поверх других окон.

Если разрешение на отображение плавающего окна поверх других окон отозвано, плавающее окно перестает отображаться. Чтобы включить его снова, нажмите на значок в правом верхнем углу экрана и предоставьте запрашиваемое разрешение.

> Общий размер использованного трафика учитывается с момента включения окна.

- Чтобы открыть список приложений, использующих интернет-соединение, нажмите на плавающее окно.
- Чтобы закрыть список приложений, нажмите .

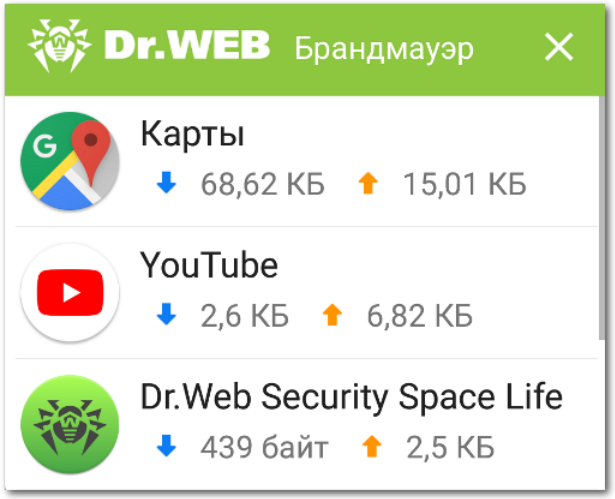

Рисунок 26: Список приложений, использующих интернет-соединение

Чтобы отключить плавающее окно

- Откройте экран **Активные приложения** и нажмите значок в правом верхнем углу экрана.

8.6.1.2. Все приложения

В разделе **Все приложения** доступен список всех соединений, инициированных установленными на устройстве приложениями с момента включения Брандмауэра Dr.Web (в том числе удаленными с устройства приложениями при соответствующей настройке). Раздел позволяет управлять доступом любого приложения к интернет-трафику.

На карточке раздела на начальном экране Брандмауэра отображается суммарный входящий и исходящий трафик приложений с момента включения Брандмауэра. Нажмите **Подробнее**, чтобы открыть полный список приложений.

Для каждого приложения на экране **Все приложения** отображается следующая информация:

- суммарный объем входящего и исходящего по установленным соединениям трафика;
- доступ к передаче данных по Wi-Fi, мобильному интернету и в роуминге.

Нажмите на имя приложения, чтобы перейти на экран Приложение и просмотреть статистику, настройки и правила для приложения.

Доступ к передаче данных

На экране **Все приложения** вы можете настроить доступ к передаче данных по Wi-Fi, мобильному интернету или в роуминге для всех или нескольких приложений в списке с помощью панели **Доступ к передаче данных** (подробнее см. раздел Доступ к передаче данных).

Фильтрация и сортировка приложений

Чтобы фильтровать или сортировать список приложений, нажмите значок в правом нижнем углу экрана, затем нажмите **Фильтр** и выберите нужные параметры фильтрации или сортировки:

- Отображать приложения:
  - с нулевым трафиком.
- Сортировать:
  - по убыванию трафика — приложения с наибольшим трафиком вверху списка;
  - по возрастанию трафика — приложения с наименьшим трафиком вверху списка;
  - по алфавиту от А до Я;
  - по алфавиту от Я до А.

По умолчанию приложения отсортированы по убыванию трафика (приложения с наибольшим трафиком расположены вверху списка), приложения с нулевым трафиком отображаются. Чтобы восстановить вид списка приложений по умолчанию, нажмите значок на экране **Фильтр**.

Поиск

Чтобы быстро перейти к нужному вам приложению, воспользуйтесь поиском по списку приложений. Для этого нажмите значок в правом нижнем углу экрана **Все приложения**, затем нажмите **Поиск** и введите запрос в поле поиска в нижней части экрана.

Настройки всех приложений

Чтобы задать настройки для всех приложений, на экране **Все приложения** нажмите **Меню** и выберите опцию **Настройки**.

Доступны следующие настройки:

- **Использовать протокол IPv6**. Позволяет включить или отключить использование протокола IPv6 в параллели с IPv4.
- **Разрешить протокол DNS поверх TCP**. Позволяет включить или отключить использование протокола DNS поверх TCP для перенаправления DNS-запросов и сокрытия доменных имен.

  Использование протокола DNS поверх TCP может препятствовать отображению доменных имен на экранах Брандмауэра.

  Настройка работает на устройствах, которые поддерживают данный тип протокола. По умолчанию настройка отключена.

- **Запретить подключения для новых приложений**. Позволяет запретить доступ к сети для приложений, установленных после включения настройки. Вы можете запретить подключения по Wi-Fi и мобильному интернету, установив соответствующие флажки под настройкой.
- **Сохранять правила и статистику после удаления приложений**. Позволяет хранить данные удаленного с устройства приложения в течение выбранного периода времени: недели, месяца или года.

Все правила

Экран **Все правила** содержит список всех правил соединений всех приложений (групп приложений).

Чтобы открыть список всех правил, на экране **Все приложения** нажмите **Меню** и выберите опцию **Все правила**.

Правила сгруппированы по имени приложения или группы приложений, установившей соединение. Приложения отсортированы в алфавитном порядке. Чтобы раскрыть список правил для приложения, нажмите значок ⌄ слева от имени приложения или группы приложений. Правила для приложения представлены в порядке их применения.

Чтобы изменить порядок применения правил

- Нажмите и удерживайте значок ═ напротив правила, которое вы хотите переместить, и перетяните правило на желаемую позицию в списке.

Чтобы выполнить поиск по списку всех правил

- Нажмите значок  в правом нижнем углу экрана **Все правила** и введите запрос в поле поиска в нижней части экрана.

Правила приложений могут храниться на устройстве в течение указанного срока после удаления приложения при соответствующей настройке.

Очистка данных приложений

Чтобы удалить настройки, правила и статистику всех приложений

1. На экране **Все приложения** нажмите **Меню** и выберите опцию **Очистить**.
2. Установите флажки напротив тех данных, которые вы хотите удалить.
3. Нажмите **Очистить**.

8.6.1.3. Доступ к передаче данных

Вы можете управлять доступом к передаче данных как для всех приложений на устройстве, так и для индивидуальных приложений:

- по Wi-Fi ,
- по мобильному интернету ,
- в мобильному интернету в роуминге .

Разрешенные виды доступа отмечены зеленым цветом, запрещенные виды доступа — серым.

По умолчанию для всех приложений передача данных через Wi-Fi и по мобильному интернету разрешена, передача данных по мобильному интернету в роуминге запрещена.

Чтобы изменить доступ к передаче данных для всех приложений

- На экране **Все приложения** нажмите **Wi-Fi**, **Мобильный интернет** или **Роуминг** в верхней части экрана.

Чтобы изменить доступ к передаче данных для нескольких приложений

1. На экране **Все приложения** нажмите и удерживайте одно из приложений.
2. Выберите остальные приложения, для которых вы хотите изменить доступ к передаче данных.
3. Используйте значки в правом верхнем углу экрана, чтобы разрешить/запретить передачу данных соответствующим способом для всех выбранных приложений.

Чтобы выйти из режима изменения доступа, нажмите ✕ в левом верхнем углу экрана.

Чтобы изменить доступ к передаче данных для одного приложения

- На экране Приложение перейдите на вкладку **Настройки** и коснитесь значка , или .

Приложения с измененным доступом к передаче данных отмечены значком .

8.6.1.4. Ограничение использования мобильного трафика

С помощью Брандмауэра Dr.Web вы можете установить лимит на использование мобильного трафика в указанный период времени.

> Функция недоступна на устройствах, для которых не предусмотрено использование SIM-карт (отсутствует слот для SIM-карт).

Чтобы задать ограничение трафика

1. На начальном экране Брандмауэра Dr.Web нажмите **Меню** и выберите опцию **Ограничение трафика**.
2. Нажмите **Лимит**.
3. Задайте лимит трафика (в мегабайтах или гигабайтах).
4. При необходимости укажите количество израсходованного трафика с начала действия выбранного периода ограничения (отсчет времени начинается с 00:00 текущего дня).
5. Нажмите **Сохранить**.
6. Выберите период действия ограничения: день, неделя или месяц. При выборе периода **Неделя** или **Месяц** укажите день недели или число месяца, в которое ограничение будет обновлено в пределах текущего выбранного периода.
7. При желании установите флажок **Предупреждать о достижении лимита мобильного трафика**, чтобы получать предупреждения о достижении установленного лимита.
8. Нажмите значок в правом верхнем углу экрана.

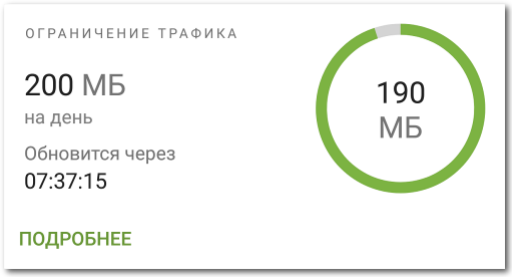

Рисунок 27: Ограничение трафика

При включении ограничения использования трафика на начальном экране Брандмауэра Dr.Web на карточке **Ограничение трафика** показывается диаграмма, отображающая объем оставшегося мобильного трафика. Рядом с диаграммой показывается установленный лимит и обратный отсчет времени до обновления периода действия ограничения (см. Рисунок 27).

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

Нажмите **Подробнее** на карточке ограничения, чтобы перейти к экрану **Ограничение трафика**.

Чтобы изменить текущее ограничение трафика

1. Откройте экран **Ограничение трафика**.
2. Внесите необходимые изменения.
3. Нажмите значок в правом верхнем углу экрана, чтобы сохранить изменения.

Чтобы отключить ограничение трафика

- На экране **Ограничение трафика** нажмите кнопку **Отключить** и подтвердите действие.

8.6.2. Трафик индивидуальных приложений

Брандмауэр Dr.Web позволяет настроить и отслеживать обработку интернет-трафика на уровне индивидуальных приложений и соединений, устанавливаемых ими. Таким образом вы можете контролировать доступ программ и процессов к сетевым ресурсам.

На экране **Приложение** для каждого приложения (в отдельных случаях — для группы приложений) возможно просмотреть статистику использования трафика, задать индивидуальные правила и настройки использования трафика и установки соединений, а также просмотреть все события Брандмауэра, связанные с приложением.

Чтобы открыть экран **Приложение**, выполните одно из следующих действий:

- На экране **Активные приложения** или **Все приложения** нажмите на имя приложения в списке.
- На экране Соединение нажмите значок ↗ справа от имени приложения.

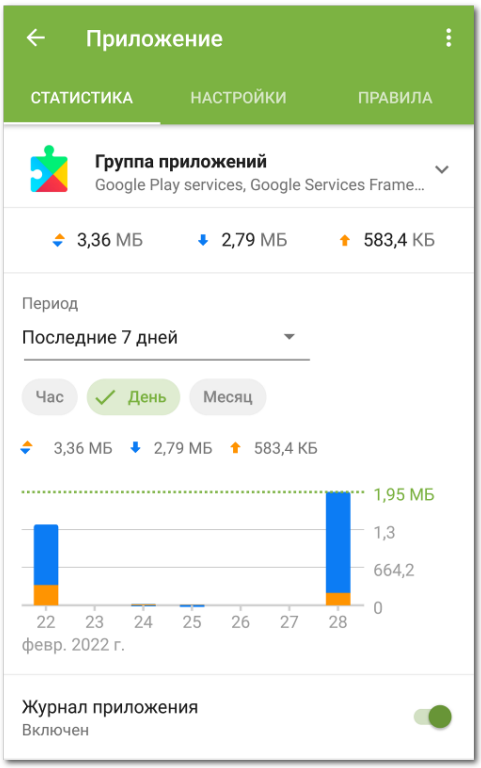

Рисунок 28: Экран Приложение

На экране **Приложение** доступны три вкладки: **Статистика**, **Настройки** и **Правила**.

8.6.2.1. Статистика использования интернет-трафика

Статистика использования интернет-трафика любым установленным приложением отображается в виде графической диаграммы.

Чтобы ознакомиться со статистикой использования трафика, на экране **Активные приложения** или **Все приложения** нажмите на имя приложения в списке.

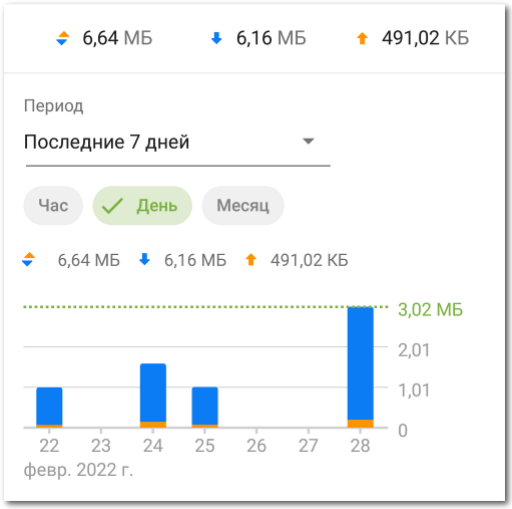

Рисунок 29: Статистика использования интернет-трафика приложения

На вкладке **Статистика** под именем приложения указан объем трафика, израсходованного приложением с момента включения Брандмауэра.

На диаграмме оранжевым цветом отмечен исходящий трафик приложения, синим — входящий. Над диаграммой приведены численные значения трафика (общего, исходящего и входящего), израсходованного за указанный период времени.

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

- Выбрать период времени для просмотра статистики. Вы можете просмотреть статистику за текущий день, последние 7 дней, текущий месяц, предыдущий месяц или самостоятельно задать период времени, указав даты его начала и окончания. Выберите нужный период времени в выпадающем списке **Период** над диаграммой.
- В рамках выбранного периода настроить отображение статистики по часам, дням или месяцам. Выберите соответствующий вариант отображения над диаграммой.

Диаграмму можно смахнуть влево или вправо до нужного значения, если график отображается не полностью.

Удаление статистики

- Удаление статистики для отдельного приложения:
  1. На экране **Активные приложения** или **Все приложения** нажмите на имя приложения, статистику которого вы хотите очистить.
  2. На экране **Приложение** нажмите **Меню** в правом верхнем углу и выберите опцию **Очистить**.
  3. В открывшемся окне установите флажок **Статистику приложения** и нажмите **Очистить**.

- Удаление статистики для всех приложений:
  1. На экране **Все приложения** нажмите **Меню** и выберите опцию **Очистить**.
  2. В открывшемся окне установите флажок **Статистику приложений** и нажмите **Очистить**.

После удаления приложения с устройства статистика приложения будет удалена автоматически в течение 5 минут.

Журнал приложения

События, связанные с сетевой активностью приложений, установленных на устройстве, записываются в журналы приложений. Используйте переключатель, чтобы начать или возобновить ведение журнала приложения. Чтобы перейти в журнал, нажмите **Просмотреть журнал**.

8.6.2.2. Настройки приложения

Доступ к передаче данных

Вы можете разрешить или запретить приложению передавать данные по Wi-Fi, мобильному интернету и по мобильному интернету в роуминге, коснувшись соответствующего значка (см. раздел Доступ к передаче данных).

Блокировать все соединения, кроме разрешенных правилами

Чтобы запретить по умолчанию все соединения для приложения, установите флажок **Блокировать все соединения, кроме разрешенных правилами**. Если разрешающие правила для приложения не будут заданы, приложение не сможет устанавливать никакие соединения.

При включении настройки **Блокировать все соединения, кроме разрешенных правилами** для приложения будет автоматически добавлено разрешающее правило для порта 53. Наличие правила (для протоколов DNS, UDP или ALL) обязательно для работы разрешающих правил с доменными именами.

Для корректной работы настройки при наличии разрешающих правил с доменными именами необходимо также отключить использование персонального DNS-сервера в настройках устройства.

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 вы можете отключить контроль Брандмауэра Dr.Web для нужного приложения (группы приложений), установив флажок **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.

8.6.2.3. Правила соединений

Управление трафиком приложений происходит на уровне соединений, которые устанавливают приложения. Вы можете задать разрешающие, запрещающие и перенаправляющие правила соединений с определенными IP-адресами и портами для каждого приложения, установленного на устройстве.

Правила соединений доступны на вкладке Правила экрана **Приложение**, а также на экране Все правила.

Соединения

Общая информация о каждом соединении представлена на экране **Соединение** (см. Рисунок 30). Чтобы перейти к этому экрану, выполните одно из следующих действий:

- На экране Активные приложения нажмите значок ⌄ слева от имени приложения, а затем нажмите на строку соединения.
- В журнале Брандмауэра:
  - В режиме группировки по дате: нажмите на строку соединения.
  - В режиме группировки по имени приложения: раскройте список соединений приложения с помощью значка ⌄ слева от имени приложения, а затем нажмите на строку соединения.
- В журнале приложения раскройте список соединений с помощью значка ⌄ справа от даты события, а затем нажмите на строку соединения.

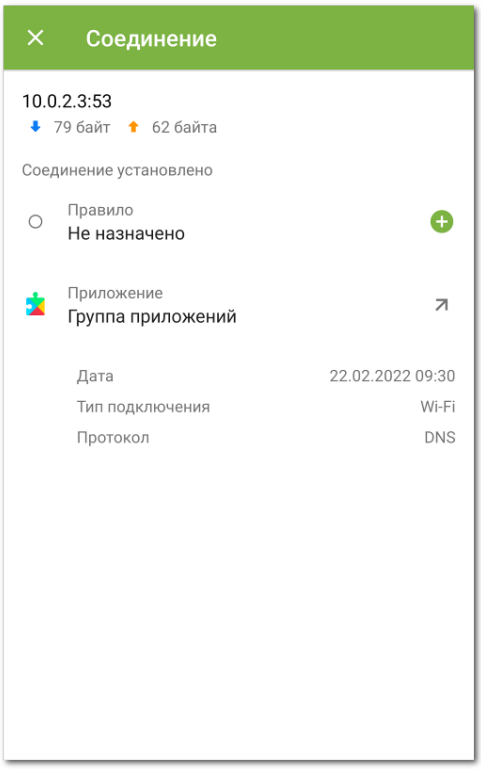

Рисунок 30: Экран Соединение

На экране **Соединение** доступна следующая информация:

- адрес и порт соединения;
- имя хоста (при его наличии);
- объем входящего и исходящего трафика, полученного или переданного соединением;
- статус соединения;
- правило соединения;
- приложение, установившее соединение;
- дата и время;
- тип подключения;
- протокол.

Чтобы скопировать адрес соединения

1. Нажмите и удерживайте строчку с адресом. Вы перейдете в режим копирования. Адрес будет выделен серым.
2. Нажмите значок в правом верхнем углу экрана. Адрес будет скопирован в буфер.

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

Правила соединений

Создание правил

Чтобы создать новое правило для соединения

1. Для соединения без правил:
   - На экране **Соединение** нажмите значок справа от пункта **Правило**.
   - На экране **Активные приложения** раскройте список установленных соединений и нажмите значок справа от адреса соединения.

   Для любого соединения:

   - На экране **Приложение** на вкладке **Правила** нажмите значок в правой нижней части экрана.
2. В открывшемся окне выберите тип правила:
   - разрешающее,
   - запрещающее,
   - перенаправляющее.
3. Проверьте правильность IP-адреса/имени хоста. Если адрес не указан, укажите действительный IP-адрес (в формате a.b.c.d для IPv4-адресов или [a:b:c:d:e:f:g:h] для IPv6-адресов), диапазон IP-адресов (в формате a1.b1.c1.d1-a2.b2.c2.d2 или [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2]) или целую сеть (в формате a.b.c.0/n, где n — число от 1 до 32). В случае создания перенаправляющего правила укажите адрес перенаправления в поле ниже. Вместо адреса вы можете указать имя хоста.
4. Нажмите **Дополнительно**, чтобы установить дополнительную настройку **Протокол** — сетевой протокол для соединения.
5. Нажмите значок , чтобы сохранить изменения.

Приложения с заданными правилами соединений отмечены значком .

Просмотр правил

Чтобы увидеть правила соединений

- Для индивидуального приложения:
  - Откройте экран **Приложение** и перейдите на вкладку **Правила**.

  Вкладка содержит список всех правил, заданных для данного приложения, в порядке их применения.
- Для всех приложений:

1. На начальном экране Брандмауэра на карточке раздела **Все приложения** нажмите **Подробнее**.
2. На экране **Все приложения** нажмите **Меню** и выберите опцию **Все правила**.

Экран **Все правила** содержит список всех правил соединений, сгруппированных по имени приложения или группы приложений, установившей соединение. Приложения отсортированы в алфавитном порядке. Чтобы раскрыть список правил для приложения, нажмите значок слева от имени приложения или группы приложений. Правила для приложения представлены в порядке их применения.

Чтобы изменить порядок применения правил

- Нажмите и удерживайте значок напротив правила, которое вы хотите переместить, и перетяните правило на желаемую позицию в списке.

Чтобы выполнить поиск по списку всех правил

- Нажмите значок в правом нижнем углу экрана **Все правила** и введите запрос в поле поиска в нижней части экрана.

Правила приложений могут храниться на устройстве в течение указанного срока после удаления приложения при соответствующей настройке.

Редактирование правил

Чтобы отредактировать существующее правило

1. Выполните одно из следующих действий:
   - На экране **Соединение** нажмите значок справа от правила.
   - На экране **Активные приложения** нажмите значок слева от имени приложения, а затем нажмите значок напротив соединения, правило которого будет изменено.
   - На экране **Приложение** на вкладке **Правила** нажмите на строку правила.
   - На экране **Все правила** нажмите значок слева от имени приложения, а затем нажмите на строку правила.
2. Внесите необходимые изменения.
3. Нажмите значок , чтобы сохранить изменения.

Удаление правил

Чтобы удалить правило

- На экране редактирования правила:
  1. Нажмите **Удалить правило**.

2. В открывшемся окне нажмите **Удалить**.

- На вкладке **Правила** или экране **Все правила**:
  1. Смахните правило влево и нажмите значок .
  2. В открывшемся окне нажмите **Удалить**.

Чтобы удалить все правила для определенного приложения

1. На экране **Приложение** нажмите **Меню** в правом верхнем углу и выберите опцию **Очистить**.
2. В открывшемся окне установите флажок **Правила для приложения**. Нажмите **Очистить**.

Чтобы удалить все правила для всех приложений

1. На экране **Все правила** нажмите **Меню** и выберите опцию **Очистить**.
2. Нажмите **Очистить**.

Импорт и экспорт правил

Созданные списки правил можно экспортировать в файл во внутренней памяти устройства. При необходимости (например, в случае переустановки Dr.Web или его использования на другом устройстве) вы сможете импортировать правила из этого файла.

Чтобы экспортировать правила в файл

- Правила индивидуального приложения:
  1. На экране **Приложение** на вкладке **Правила** нажмите **Меню** в правом верхнем углу и выберите опцию **Экспорт правил**.
  2. Нажмите **ОК**.
- Правила всех приложений:
  1. На экране **Все правила** нажмите **Меню** в правом верхнем углу и выберите опцию **Экспорт правил**.
  2. Нажмите **ОК**.

Правила экспортируются в файл `DrWeb_Firewall_Rules_<имя_приложения>.hsts`, если это правила для приложения, или в файл `DrWeb_Firewall_Rules_ALL.hsts`, если это правила для всех приложений. Файл с правилами сохраняется в папке `Internal storage/Android/data/com.drweb/files/`.

На устройствах с Android 11 или более поздними версиями файл с правилами сохраняется в папке `Download/DrWeb`.

Чтобы импортировать правила из файла

- Правила индивидуального приложения:
  1. На экране **Приложение** на вкладке **Правила** нажмите **Меню** в правом верхнем углу и выберите опцию **Импорт правил**.
  2. В дереве файлов найдите файл с правилами и нажмите на него.
- Правила всех приложений:
  1. На экране **Все правила** нажмите **Меню** в правом верхнем углу и выберите опцию **Импорт правил**.
  2. В дереве файлов найдите файл с правилами и нажмите на него.

Блокировать все соединения, кроме разрешенных правилами

Вы можете запретить все соединения приложения, кроме разрешенных правилами, установив соответствующий флажок на экране настроек приложения.

8.6.2.4. Журнал приложения

События сетевых соединений регистрируются в журналах приложений.

Чтобы включить ведение журнала приложения

- На экране **Приложение** на вкладке **Статистика** используйте переключатель **Журнал приложения**.

Чтобы открыть журнал приложения

- На экране **Приложение** на вкладке **Статистика** выберите пункт **Просмотреть журнал**.

Все соединения данного приложения объединены по датам. Чтобы открыть список соединений за какую-либо дату, нажмите на значок справа от даты. Для каждого соединения в журнале доступна следующая информация:

- адрес и порт соединения;
- израсходованный трафик;
- время установки соединения;
- наличие правила для соединения:
  - разрешающее,
  - запрещающее,
  - перенаправляющее,
  - правило не задано.

Нажмите на строку соединения, чтобы перейти на экран Соединение и настроить для него правила.

Чтобы скопировать адрес соединения

- Нажмите и удерживайте строчку с адресом соединения. Адрес будет скопирован в буфер.

Чтобы очистить журнал приложения

1. На экране журнала приложения нажмите значок  в правом верхнем углу экрана.
2. В открывшемся окне нажмите кнопку **Очистить**.

Чтобы отключить ведение журнала приложения

- На экране **Приложение** на вкладке **Статистика** используйте переключатель **Журнал приложения**.

8.6.3. Журнал Брандмауэра Dr.Web

События, связанные с работой Брандмауэра, регистрируются в журнале Брандмауэра Dr.Web.

Чтобы открыть список всех событий, связанных с работой Брандмауэра Dr.Web, на начальном экране компонента Брандмауэр нажмите **Меню**  и выберите опцию **Журнал**.

В журнале Брандмауэра отображается следующая информация о событии:

- имя приложения;
- адрес и порт соединения (а также адрес перенаправления, если задано соответствующее правило);
- израсходованный трафик;
- дата и время события;
- наличие правила для соединения.

При нажатии на событие открывается экран Соединение.

Чтобы фильтровать или сортировать события в журнале Брандмауэра

1. Нажмите значок  в правом нижнем углу экрана **Журнал**, затем нажмите **Фильтр**.
2. Выберите нужные параметры фильтрации или сортировки:
   - Сортировать:
     - сначала новые — последние события вверху журнала;

  - сначала старые — последние события внизу журнала;
  - по алфавиту от А до Я;
  - по алфавиту от Я до А.
- Отображать соединения:
  - установленные,
  - сброшенные,
  - перенаправленные,
  - с ошибкой.

По умолчанию события отсортированы по дате (последние события расположены вверху журнала), отображаются все виды соединений. Чтобы восстановить вид журнала по умолчанию, нажмите значок  на экране **Фильтр**.

Для удобства просмотра журнала вы также можете группировать события по приложению.

Чтобы группировать события по приложению

- На экране **Журнал** нажмите **Меню**  в правом верхнем углу и установите флажок **Группировать**.

Чтобы выполнить поиск по журналу Брандмауэра

1. Нажмите значок  в правом нижнем углу экрана **Журнал**, затем нажмите **Поиск**.
2. Введите запрос в поле поиска в нижней части экрана.

Чтобы скопировать адрес соединения

- Нажмите и удерживайте строчку с адресом соединения. Адрес будет скопирован в буфер.

Чтобы очистить журнал Брандмауэра

1. Нажмите **Меню**  и выберите опцию **Очистить**.
2. Подтвердите действие, нажав кнопку **Очистить**.

Размер журнала

По умолчанию для файла журнала установлен размер, равный 5 МБ.

Чтобы изменить максимально разрешенный размер файла журнала

1. На экране журнала Брандмауэра нажмите **Меню** и выберите опцию **Размер журнала**.
2. В открывшемся окне измените значение и нажмите **ОК**.

> Максимальный размер журнала должен быть больше 0 МБ и меньше либо равен 99 МБ.

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

Dr.Web обнаруживает следующие проблемы безопасности:

- Уязвимости.
- Системные настройки, которые влияют на безопасность устройства.
- Конфликтующее ПО.
- Приложения, использующие уязвимость Fake ID.
- Настройки оптимизации.

Чтобы открыть список обнаруженных проблем безопасности, на главном экране Dr.Web выберите **Аудитор безопасности**.

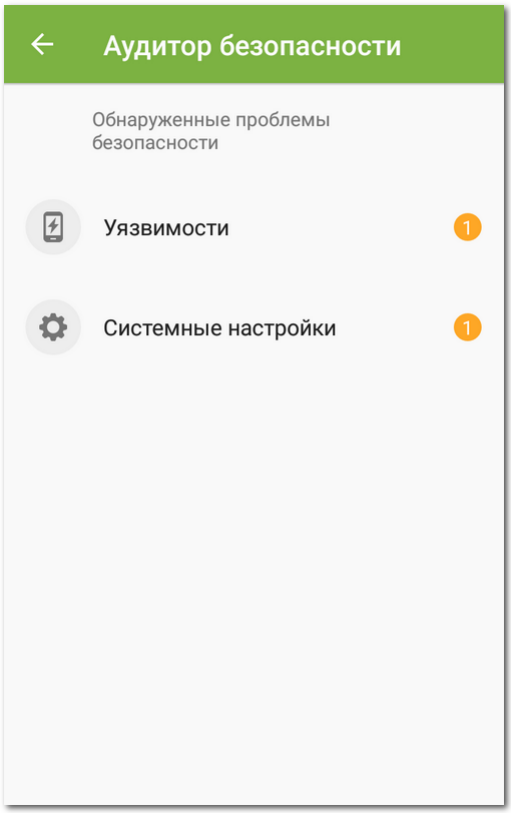

Рисунок 31: Аудитор безопасности

8.7.1. Уязвимости

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

Аудитор безопасности обнаруживает в системе устройства следующие уязвимости: BlueBorne, EvilParcel, Extra Field, Fake ID, Janus, ObjectInputStream Serialization, OpenSSLX509Certificate, PendingIntent, SIM Toolkit, Stagefright и Stagefright 2.0.

Воспользовавшись уязвимостями, злоумышленники могут добавить программный код в приложения, в результате чего эти приложения могут начать выполнять функции, представляющие угрозу безопасности устройства.

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.

Root-доступ

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.

8.7.2. Системные настройки

Аудитор безопасности обнаруживает следующие системные настройки, которые влияют на безопасность устройства:

- **Отладка разрешена**. 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 об этой проблеме.
- **Установка из неизвестных источников разрешена**. Установка приложений из неизвестных источников 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 об этой проблеме.

  Рекомендуется проверять все устанавливаемые приложения на наличие угроз. Перед проверкой необходимо убедиться, что вирусные базы Dr.Web обновлены.
- **Уведомления Dr.Web заблокированы**. В этом случае 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.
- **Установлен пользовательский сертификат**. 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.

8.7.3. Конфликтующее 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, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Спутник, Boat Browser и Atom.

8.7.4. 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 этим приложением, или воспользуйтесь средствами ОС.

8.7.5. Настройки оптимизации

Операционная система устройства может завершать процессы приложений, которые в настоящий момент вы активно не используете. Такая оптимизация фоновых процессов помогает сэкономить энергию или улучшить производительность, но может отразиться на работе приложений.

Приложение Dr.Web должно непрерывно работать, чтобы обеспечить постоянную антивирусную защиту и эффективность дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

Чтобы приложение работало корректно, снимите ограничения с приложения в фоновом режиме. Для этого проверьте настройки устройства и встроенного диспетчера приложений.

Набор настроек зависит от модели устройства:

- Asus
- Huawei
- Meizu
- Nokia
- OnePlus
- Oppo
- Samsung
- Sony
- Realme
- Xiaomi

Инструкции, представленные в указанных разделах, могут частично не соответствовать отдельным устройствам, поскольку настройки могут отличаться на разных моделях устройства и версиях операционной системы. В случае несоответствия уточните порядок действий в руководстве пользователя вашей модели устройства. Если это не поможет решить проблему, обратитесь в службу технической поддержки.

Отзыв разрешений

Предупреждение отображается, если приложению Dr.Web не предоставлен доступ к специальным возможностям.

Начиная с версии 6.0 ОС Android отзывает предоставленные пользователем разрешения, если приложение не использовалось в течение нескольких месяцев. ОС Android 12 и более поздних версий также запрещает показ уведомлений и очищает кеш приложения. Таким образом система экономит ресурсы памяти устройства и защищает данные пользователей. Однако Dr.Web не сможет обеспечивать постоянную защиту устройства, если разрешения, необходимые для его основных функций и работы компонентов, будут отозваны. Для обеспечения стабильной работы приложения рекомендуется отключить автоматический отзыв разрешений в настройках устройства. Для перехода к соответствующему разделу системных настроек нажмите кнопку **Настройки** на экране с подробной информацией об этой проблеме.

Доступ к настройкам

На устройствах с Android 13 и более поздними версиями система по умолчанию закрывает приложениям доступ к определенным настройкам. Это делается, чтобы защитить конфиденциальные данные от их неправомерного использования вредоносными приложениями. Однако компонентам Dr.Web требуется доступ к таким настройкам, как специальные возможности устройства и чтение уведомлений, чтобы защищать ваши данные и блокировать нежелательный контент. Чтобы перейти к системной настройке, разрешающей доступ к необходимым для работы Dr.Web настройкам, следуйте инструкциям на экране с подробной информацией об этой проблеме.

Параметр **Быстрый запуск** в меню специальных возможностей активирует кнопку, которая позволяет одним нажатием включать/отключать доступ Dr.Web к специальным возможностям из любого места на устройстве. Рекомендуется отключить **Быстрый запуск** во избежание случайного нажатия.

8.7.5.1. Asus

Чтобы на устройствах Asus приложение Dr.Web работало в фоне корректно, выполните следующие действия:

- Разрешите автозапуск

  Автозапуск позволяет запустить процессы приложения сразу после включения устройства. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Разрешите работу в фоне

  Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы разрешить автозапуск

1. В настройках устройства откройте **Менеджер автозапуска**.
2. Разрешите автозапуск для приложения Dr.Web.

Чтобы разрешить работу в фоне

1. В приложении **Мобильный диспетчер** откройте **Настройки**.
2. Отключите настройки **Очистка в режиме ожидания.**

8.7.5.2. Huawei

Устройства, поддерживающие управление вручную

На устройствах Huawei, поддерживающих автоматическое и ручное управление запуском приложений, разрешите ручное управление запуском для приложения Dr.Web.

Управление вручную позволяет приложению оставаться запущенным, даже если оно не активно, и запускать процессы сразу после включения устройства. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

Чтобы включить ручное управление

- На устройствах под управлением Android:
  1. В настройках устройства откройте **Батарея** > **Запуск приложения**.
  2. Выберите **Управление вручную**.

- На устройствах под управлением Harmony OS:
  1. В настройках устройства откройте раздел настроек запуска приложений.
  2. Найдите в списке Dr.Web и используйте переключатель справа, чтобы включить управление вручную.
  3. В открывшемся окне включите все дополнительные настройки управления и нажмите **OK**.

Другие устройства Huawei

Чтобы на других устройствах Huawei приложение Dr.Web работало в фоне корректно, измените следующие настройки:

- Разрешите работу в фоне

  Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.
- Отключите оптимизацию батареи

  

  Если Dr.Web является администратором устройства, данная настройка оптимизации недоступна.

  Чтобы оптимизировать использование батареи, операционная система может завершить приложение Dr.Web. Это прервет постоянную антивирусную защиту устройства и работу включенных дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.
- Разрешите работу при выключенном экране

  Работа при выключенном экране необходима для постоянной антивирусной защиты устройства и для работы дополнительных компонентов: Фильтра звонков и СМС, Антивора и Брандмауэра.
- Разрешите всплывающие окна, если включен Антивор или Родительский контроль

  В фоновом режиме Антивор и Родительский контроль используют всплывающие окна, чтобы ограничить доступ к отдельному приложению или устройству целиком.

  

  Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы разрешить работу в фоне

1. Откройте недавние приложения.
2. У приложения Dr.Web нажмите значок с замком.

Чтобы отключить оптимизацию батареи

1. В настройках устройства откройте **Расширенные настройки** > **Менеджер батареи** > **Защищенные приложения**.
2. Для приложения Dr.Web выберите **Защищено**.

Чтобы разрешить работу при выключенном экране

1. В настройках устройства выберите **Приложения** > **Dr.Web** > **Батарея**.
2. Включите опцию **Работа при выключенном экране**.

Чтобы разрешить всплывающие окна

1. В настройках устройства выберите **Приложения**.
2. В списке приложений выберите Dr.Web.
3. В списке разрешений включите отображение всплывающих окон в фоне.

8.7.5.3. Meizu

Чтобы на устройствах Meizu приложение Dr.Web работало в фоне корректно, измените следующие настройки:

- Отключите оптимизацию батареи

  

  Если Dr.Web является администратором устройства, данная настройка оптимизации недоступна.

  Чтобы оптимизировать использование батареи, операционная система может завершить приложение Dr.Web. Это прервет постоянную антивирусную защиту устройства и работу включенных дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Закрепите Dr.Web в фоновом режиме

  Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Разрешите работу при выключенном экране

  Работа при выключенном экране необходима для постоянной антивирусной защиты устройства и для работы дополнительных компонентов: Фильтра звонков и СМС, Антивора и Брандмауэра.

Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы отключить оптимизацию батареи

1. В настройках устройства откройте **Расширенные настройки** > **Менеджер батареи** > **Защищенные приложения**.
2. Для приложения Dr.Web выберите **Защищено**.

Чтобы закрепить Dr.Web в фоновом режиме

1. Откройте недавние приложения.
2. У приложения Dr.Web нажмите значок с замком.

Чтобы разрешить работу при выключенном экране

1. В настройках устройства выберите **Приложения** > **Dr.Web** > **Батарея**.
2. Включите опцию **Работа при выключенном экране**.

8.7.5.4. Nokia

Чтобы приложение Dr.Web работало исправно в фоне на устройствах Nokia, остановите работу приложения Power saver.

Если Dr.Web является администратором устройства, данная настройка оптимизации недоступна.

Приложение Power saver оптимизирует использование батареи, что может привести к завершению приложения Dr.Web. Это прервет постоянную антивирусную защиту устройства и работу включенных дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы остановить Power saver

1. В настройках устройства откройте **Приложения** > **Все приложения**.
2. Нажмите меню в правом верхнем углу экрана и выберите **Показать системные**.
3. Выберите **Power saver** и нажмите **Остановить**.

Приложение будет остановлено до следующего перезапуска устройства.

8.7.5.5. OnePlus

Чтобы на устройствах OnePlus приложение Dr.Web работало в фоне корректно, измените следующие настройки:

- Отключите оптимизацию батареи

  Если Dr.Web является администратором устройства, данная настройка оптимизации недоступна.

  Чтобы оптимизировать использование батареи, операционная система может завершить приложение Dr.Web. Это прервет постоянную антивирусную защиту устройства и работу включенных дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Закрепите Dr.Web в фоновом режиме

  Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

Кроме того, на некоторых устройствах требуется отключить глубокую оптимизацию и автозапуск.

После установки обновлений операционной системы настройки оптимизации могут быть сброшены. В этом случае вам потребуется изменить их еще раз.

Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы отключить оптимизацию батареи

1. В настройках устройства откройте **Батарея** > **Оптимизация батареи**.
2. Выберите приложение Dr.Web.
3. Выберите опцию **Не оптимизировать** и нажмите **Готово**.

Чтобы закрепить Dr.Web в фоновом режиме

1. Откройте недавние приложения.
2. У приложения Dr.Web нажмите значок с замком.

Чтобы отключить глубокую оптимизацию

1. В настройках устройства откройте **Батарея** > **Оптимизация батареи**.
2. Нажмите значок настроек в правом верхнем углу.
3. Отключите глубокую оптимизацию.

Чтобы отключить автозапуск

1. В настройках устройства откройте **Приложения**.
2. Нажмите значок настроек в правом верхнем углу.
3. Выберите **Автозапуск**.
4. Отключите автозапуск для приложения Dr.Web.

8.7.5.6. Oppo

Чтобы на устройствах Oppo приложение Dr.Web работало в фоне корректно, измените следующие настройки:

- Разрешите автозапуск

  Автозапуск позволяет запустить процессы приложения сразу после включения устройства. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.
- Закрепите Dr.Web в фоновом режиме

  Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.
- Разрешите работу в фоне, если на вашем устройстве есть приложение Центр безопасности

Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы разрешить автозапуск

1. В настройках устройства откройте **Менеджер приложений**.
2. Выберите приложение Dr.Web.
3. Разрешите автозапуск.

Чтобы закрепить Dr.Web в фоновом режиме

1. Откройте недавние приложения.
2. Выставьте значок с замком для приложения Dr.Web.

Чтобы разрешить работу в фоне

1. Откройте **Центр безопасности**.
2. Выберите **Разрешения на конфиденциальность** > **Менеджер запуска**.
3. Предоставьте Dr.Web разрешение работать в фоновом режиме.

8.7.5.7. Samsung

Чтобы на устройствах Samsung приложение Dr.Web работало в фоне корректно, измените следующие настройки:

- Закрепите Dr.Web в фоновом режиме

Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы закрепить Dr.Web в фоновом режиме

1. Откройте недавние приложения.
2. Нажмите значок Dr.Web. В выпадающем меню выберите **Не закрывать** или **Закрепить это приложение**.

   У закрепленного приложения появится значок с замком.

8.7.5.8. Sony

Чтобы на устройствах Sony приложение Dr.Web работало в фоне корректно, отключите оптимизацию заряда батареи для Dr.Web.

Если Dr.Web является администратором устройства, данная настройка оптимизации недоступна.

Чтобы оптимизировать использование батареи, операционная система может остановить приложение Dr.Web. Это прервет постоянную антивирусную защиту устройства и работу включенных дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

> Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы отключить оптимизацию батареи

1. На начальном экране устройства нажмите .
2. Выберите **Настройки** > **Аккумулятор**.
3. Нажмите и выберите **Экономия заряда батареи**.
4. Нажмите **Приложения**. Отобразится список приложений, которые экономят заряд батареи.
5. Установите флажок у Dr.Web. Приложение отобразится на вкладке **Не экономят**.

> В режиме Ultra STAMINA исключить приложения из оптимизации невозможно.

8.7.5.9. Realme

Чтобы на устройствах Realme приложение Dr.Web работало в фоне корректно, измените следующие настройки:

- Разрешите работу в фоне

Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Разрешите автозапуск
- Разрешите отображение поверх других приложений

  Dr.Web использует всплывающие окна, отображающиеся поверх других приложений, чтобы ограничить доступ к отдельному приложению или устройству целиком.

> Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы разрешить работу в фоне

1. В настройках устройства откройте **Управление приложениями** > **Dr.Web** > **Использование батареи**.
2. Выберите опцию **Разрешить работу в фоновом режиме**.

Чтобы разрешить автозапуск

1. В настройках устройства откройте **Управление приложениями** > **Dr.Web** > **Использование батареи**.
2. Выберите опцию **Разрешить автоматический запуск**.

Чтобы разрешить отображение поверх других приложений

1. В настройках устройства откройте **Управление приложениями** > **Dr.Web**.
2. Включите переключатель **Поверх других приложений**.

8.7.5.10. Xiaomi

Чтобы на устройствах Xiaomi приложение Dr.Web работало в фоне корректно, измените следующие настройки:

- Разрешите автозапуск

  Автозапуск позволяет запустить процессы приложения сразу после включения устройства. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Разрешите работу в фоне

  Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Закрепите Dr.Web в фоновом режиме

  Работа в фоне позволяет приложению оставаться запущенным, даже если оно не активно. Это необходимо для постоянной антивирусной защиты устройства и для исправной работы дополнительных компонентов: Фильтра звонков и СМС, URL-фильтра, Антивора, Родительского контроля и Брандмауэра.

- Разрешите всплывающие окна, если включен Антивор или Родительский контроль

  В фоновом режиме Антивор и Родительский контроль используют всплывающие окна, чтобы ограничить доступ к отдельному приложению или устройству целиком.

Настройки и их расположение могут отличаться на разных моделях устройства и версиях операционной системы. Если эта инструкция не решает проблему, обратитесь в службу технической поддержки.

Чтобы разрешить автозапуск

1. В настройках устройства выберите **Приложения**.
2. В списке приложений выберите Dr.Web.
3. Разрешите автозапуск.

Чтобы разрешить работу в фоне

1. В настройках устройства выберите **Приложения**.
2. В списке приложений выберите Dr.Web.
3. Выберите настройку **Контроль активности**.
4. Выберите опцию **Нет ограничений**.

Чтобы закрепить Dr.Web в фоновом режиме

1. Откройте недавние приложения.
2. У приложения Dr.Web нажмите значок с замком.

Некоторые версии ОС также позволяют закреплять приложения в фоновом режиме через встроенное приложение **Безопасность**:

1. В приложении **Безопасность** откройте раздел **Ускорение**.
2. Нажмите значок настроек в правом верхнем углу экрана.
3. Выберите пункт **Закрепленные приложения**.
4. В списке приложений найдите Dr.Web.
5. Используйте переключатель справа от Dr.Web, чтобы закрепить приложение в фоновом режиме.

Чтобы разрешить всплывающие окна

1. В настройках устройства выберите **Приложения**.
2. В списке приложений выберите Dr.Web.
3. Выберите **Другие разрешения**.
4. В списке разрешений включите отображение всплывающих окон в фоне.

8.8. Статистика

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

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

Просмотр статистики

На вкладке **Статистика** находятся два информационных раздела (см. Рисунок 32):

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

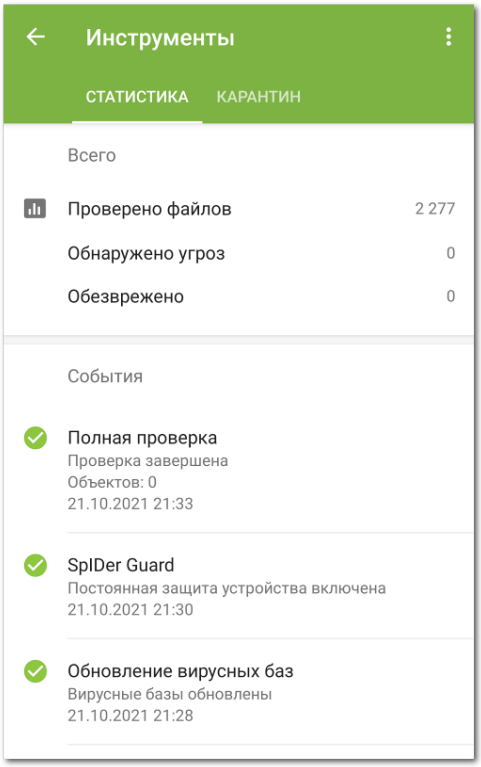

Рисунок 32: Статистика

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.

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

8.9. Карантин

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

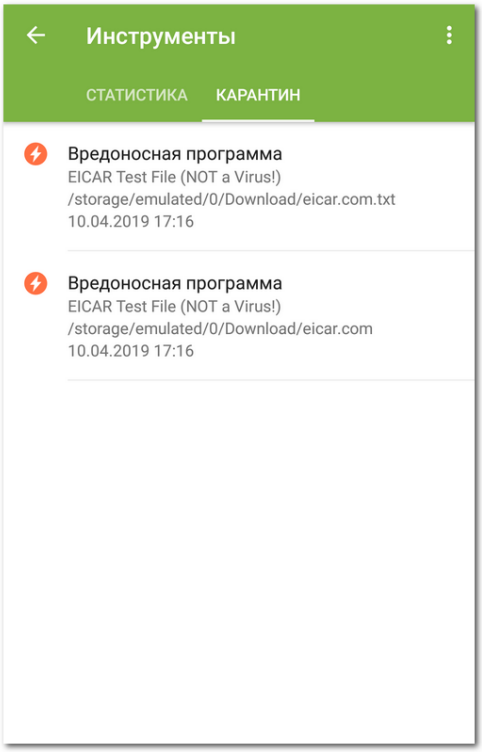

Рисунок 33: Карантин

Просмотр списка объектов в карантине

Чтобы просмотреть список угроз, перемещенных в карантин:

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

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

2. Выберите пункт **Карантин**.

Откроется список всех угроз, находящихся в карантине.

Просмотр информации об угрозах

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

Для каждой угрозы вы можете просмотреть следующую информацию:

- имя файла;
- путь к файлу;
- дата и время перемещения в карантин.

Доступные опции

Для каждой угрозы доступны следующие опции:

- **Подробнее в Интернете** — для просмотра описания угрозы на сайте «Доктор Веб».
- **Восстановить** — для возвращения файла в ту папку, в которой файл находился до перемещения (пользуйтесь данной функцией, только если вы уверены, что файл безопасен).
- **Удалить** — для удаления файла из карантина и из системы.
- **Ложное срабатывание** — для отправки файла в антивирусную лабораторию «Доктор Веб» на анализ. Анализ покажет, действительно ли файл представляет угрозу или это ложное срабатывание. Если произошло ложное срабатывание, оно будет исправлено. Чтобы получить результаты анализа, укажите свой адрес электронной почты.

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

Удаление всех объектов из карантина

Чтобы удалить все объекты, перемещенные в карантин:

1. Откройте раздел **Карантин**.
2. На экране **Карантин** нажмите **Меню** и выберите пункт **Удалить все**.
3. Нажмите **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 **OK**, чтобы вернуться в раздел **Карантин**.

9. Настройки

Чтобы перейти к настройкам приложения, на главном экране Dr.Web нажмите **Меню** и выберите пункт **Настройки**.

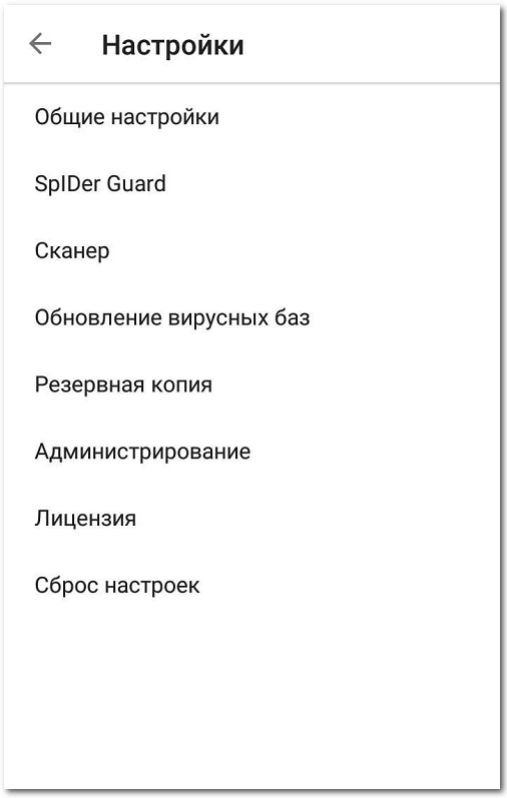

Рисунок 34: Настройки

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 постоянно проверяет файловую систему на наличие угроз и отслеживает изменения в системной области (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 (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

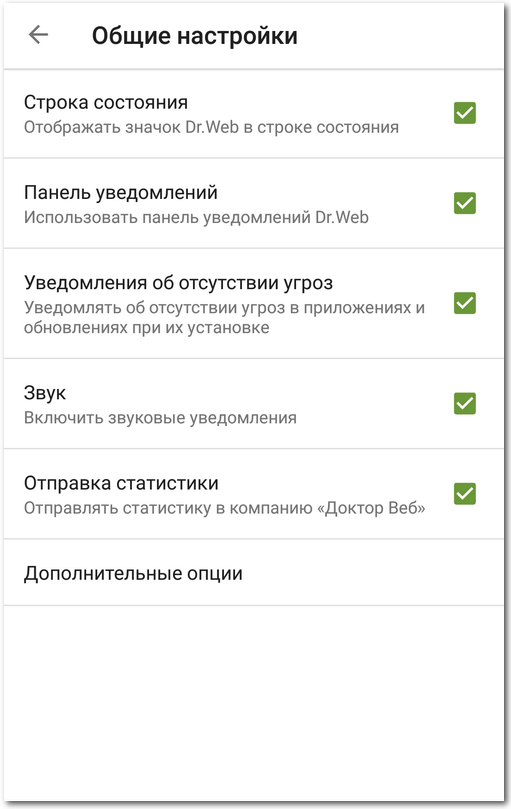

Рисунок 35: Общие настройки

На экране **Общие настройки** доступны следующие опции:

- **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.
- **Уведомления об отсутствии угроз**. Позволяет включить и отключить уведомления о том, что в только что установленных приложениях или обновлениях угроз не обнаружено.

Настройка недоступна на устройствах с Android 8.0 или более поздними версиями. В этом случае уведомления категории **Безопасные приложения** можно включить или отключить в настройках устройства.

- **Звук**. Позволяет настроить звуковые оповещения об обнаружении угроз, их удалении или перемещении в карантин. По умолчанию звуковые уведомления включены.
- **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 угрозах в системных приложениях, которые не могут быть удалены без потери работоспособности устройства. 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 обновить вирусные базы вручную. 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 не обновлялись более 24 часов (например, при отсутствии подключения к интернету), вам нужно запустить обновление вручную.

Чтобы узнать, требуется ли вам выполнить обновление вирусных баз вручную

1. На главном экране Dr.Web нажмите **Меню** и выберите **Вирусные базы**.

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

Чтобы запустить обновление

1. На главном экране Dr.Web нажмите **Меню** и выберите **Вирусные базы**.
2. В открывшемся 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 мобильной сети при загрузке обновлений

1. На главном экране Dr.Web нажмите **Меню** и выберите **Настройки** (см. Рисунок 34).
2. Выберите раздел **Обновление вирусных баз**.
3. Чтобы не использовать мобильную сеть при загрузке обновлений, установите флажок **Обновление по Wi-Fi**.

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

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

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

9.3. Резервная копия

Вы можете экспортировать 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 импортировать настройки из этого файла.

В режиме централизованной защиты импорт и экспорт настроек не доступны.

Чтобы экспортировать текущие настройки в файл

1. На экране настроек (см. Рисунок 34) 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 настроек**.
4. Установите пароль, который будет использоваться для защиты файла настроек, и нажмите кнопку **ОК**.

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

На устройствах с Android 11 или более поздними версиями файл с настройками сохраняется в папке `Download/DrWeb`.

Чтобы импортировать настройки из файла

1. На экране настроек (см. Рисунок 34) 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 **ОК**.

   Все текущие настройки будут удалены и заменены импортированными 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.

В режиме централизованной защиты сброс настроек недоступен.

Чтобы сбросить настройки

1. На экране настроек (см. Рисунок 34) 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

Компьютеры и другие устройства, на которых установлены взаимодействующие компоненты Dr.Web, образуют *антивирусную сеть*. Антивирусная сеть имеет архитектуру клиент-сервер. Сервер управляет клиентом с помощью Агента Dr.Web. Режим централизованной защиты — это режим работы приложения под управлением Агента Dr.Web.

Версия Dr.Web Mobile Security Suite, описываемая в данном руководстве, совместима с Dr.Web AV-Desk 10 и 13 версии и Dr.Web Enterprise Security Suite 10, 11, 12 и 13 версии.

Режим централизованной защиты доступен для следующих версий Dr.Web:

- Загруженных с сайта компании «Доктор Веб» https://download.drweb.com/android/.
- Загруженных из вашего личного кабинета поставщика услуги «Антивирус Dr.Web».
- Полученных от администратора антивирусной сети вашей компании.

Режим централизованной защиты недоступен:

- Для версий Dr.Web, установленных из Google Play.
- Для версии, установленной из HUAWEI AppGallery.
- 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 вашей компании или списком оплаченных услуг.

С сервера централизованной защиты могут контролироваться следующие компоненты:

- 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 СМС.
- Антивор Dr.Web.
- URL-фильтр.
- Фильтр приложений.

Лицензирование в режиме централизованной защиты

В режиме централизованной защиты лицензионный ключевой файл скачивается автоматически с сервера централизованной защиты, ваша персональная лицензия не

используется. В случае окончания срока действия лицензии или ее блокировки и появления соответствующего предупреждения обратитесь к администратору антивирусной сети вашей компании за новой лицензией или продлите подписку на услугу «Антивирус Dr.Web».

Обновление вирусных баз в режиме централизованной защиты

В режиме централизованной защиты блокируется возможность обновить вирусные базы вручную, обновления загружаются автоматически с сервера централизованной защиты. Настройки обновлений могут быть изменены или заблокированы в соответствии с политикой безопасности вашей 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.

Обновление приложения в режиме централизованной защиты

Некоторые версии сервера централизованной защиты поддерживают обновление Dr.Web Mobile Security Suite. Если в настройках приложения установлен флажок **Новая версия**, вы будете получать уведомления о доступности новой версии приложения и сможете оперативно установить ее. Обратитесь к администратору антивирусной сети вашей компании за подробностями.

Для версий приложения, загруженных с сайта компании «Доктор Веб», обновление с сервера централизованной защиты недоступно. Для таких версий в режиме централизованной защиты возможно только обновление вирусных баз.

10.1. Переход в режим централизованной защиты

Чтобы перевести приложение в режим централизованной защиты, подключитесь к серверу централизованной защиты.

Для подключения к серверу централизованной защиты 11.0.0 или более поздней версии, требуется Dr.Web 11.0.0 или более поздняя версия.

После подключения к серверу могут быть запрошены следующие разрешения:

- Основные разрешения (доступ к фото, мультимедиа и файлам, контактам и др.) — для работы большинства функций приложения.
- Фильтр звонков и СМС (использование Dr.Web в качестве приложения для звонков по умолчанию) — для фильтрации входящих звонков и СМС.
- Администрирование устройства — для защиты приложения от удаления и для полноценной работы Антивора.

- Доступ к специальным возможностям — для фильтрации приложений и полноценной работы URL-фильтра, Антивора и Родительского контроля.
- Наложение поверх других окон — для фильтрации приложений и работы Брандмауэра.

Подключение к серверу централизованной защиты

Автоматическое подключение

Версии Dr.Web, полученные от администратора антивирусной сети вашей компании или от поставщика услуги «Антивирус Dr.Web», подключаются к серверу централизованной защиты автоматически. Для этого инсталляционный пакет должен быть запущен с внутренней памяти устройства.

Подключение с вводом параметров

Для подключения к серверу централизованной защиты понадобятся параметры подключения, которые предоставляются администратором антивирусной сети вашей компании или поставщиком услуги «Антивирус Dr.Web».

1. Убедитесь в наличии подключения к сети.
2. На экране **Настройки** (см. Рисунок 34) выберите **Администрирование**.

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

   Флажок **Агент Dr.Web** установлен по умолчанию в версиях Dr.Web, полученных от администратора антивирусной сети вашей компании или от поставщика услуги «Антивирус Dr.Web».
4. При включении режима централизованной защиты восстанавливаются последние параметры подключения.

   Однако если на вашем устройстве сохранен конфигурационный файл, используются параметры подключения из этого файла. Чтобы использовать другие параметры подключения, например, из инсталляционного пакета, сбросьте параметры подключения.

   Если вы подключаетесь к серверу впервые или параметры подключения изменились, укажите следующие параметры:
   - IP-адрес сервера централизованной защиты.
   - 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**.

Подключение с конфигурационным файлом

Параметры подключения к серверу централизованной защиты содержатся в файле `install.cfg`, который предоставляется администратором антивирусной сети компании или поставщиком услуги «Антивирус Dr.Web».

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 34) 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.

   > Флажок **Агент Dr.Web** установлен по умолчанию в версиях Dr.Web, полученных от администратора антивирусной сети компании или от поставщика услуги «Антивирус Dr.Web». 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 поставщику услуги «Антивирус Dr.Web» для решения проблемы.

Срок действия лицензии (подписки) истек. Обратитесь к администратору антивирусной сети для получения лицензии или продлите подписку на услугу «Антивирус Dr.Web».

Подписка заблокирована. Обратитесь к поставщику услуги «Антивирус Dr.Web» для разблокировки подписки.

Запуск Dr.Web для Android запрещен на сервере. 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. Администрирование

Если на сервере централизованной защиты включена возможность изменения конфигурации Фильтра приложений, вы можете выбрать приложения, которые разрешено запускать на вашем устройстве.

Вы можете разрешить/запретить запуск как системных, так и пользовательских приложений. Системные приложения находятся в верху списка и по умолчанию уже отмечены как разрешенные. Ниже по списку расположены пользовательские приложения.

Чтобы настроить Фильтр приложений

1. На главном экране Dr.Web 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.

> Настройки запуска приложений, заданные на пользовательском устройстве, будут применены, только если на сервере централизованной защиты для этого устройства включен Фильтр приложений.

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.

10.3. Переход в автономный режим

Чтобы перевести Dr.Web в автономный режим, откройте экран настроек (см. Рисунок 34) и выберите пункт **Администрирование**. После этого снимите флажок **Агент Dr.Web**.

При включении автономного режима 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 Dr.Web (см. Рисунок 36) доступны следующие опции:

- События
- Сканер
- Брандмауэр
- Аудитор безопасности
- Разное

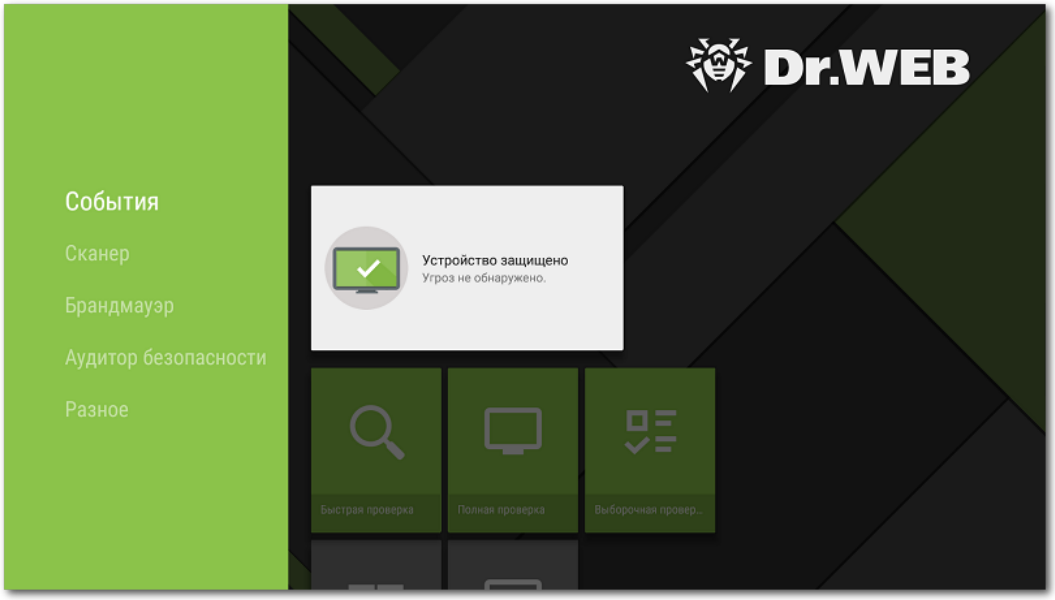

Рисунок 36: Dr.Web на Android TV

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.

На устройствах с Android 11 или более поздними версиями приложение также запрашивает разрешение на доступ ко всем файлам.

Чтобы предоставить доступ ко всем файлам

1. В окне запроса на разрешение нажмите кнопку **Перейти в Настройки**.
2. На экране системных настроек Dr.Web выберите пункт **Разрешения**.
3. Выберите пункт **Файлы и медиафайлы**.
4. Выберите опцию **Разрешить в любом режиме**.
5. В диалоговом окне нажмите кнопку **Разрешить**.

Интерфейс

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

11.1. События на Android TV

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

- Зеленый индикатор означает, что устройство защищено. Дополнительных действий не требуется.
- Желтый индикатор означает, что Dr.Web обнаружил проблемы безопасности, например, отсутствие лицензии или уязвимость. Чтобы узнать больше о найденных проблемах и устранить их, выберите панель состояния.
- Красный индикатор означает, что Dr.Web обнаружил подозрительные изменения в системной области или угрозы. Чтобы открыть результаты проверки и обезвредить угрозы, выберите панель состояния.

Если Dr.Web обнаружил несколько событий, требующих внимания, выберите панель состояния. Откроется окно **События**, в котором будут отображены все важные сообщения.

11.2. Антивирусная защита на Android TV

- SpIDer Guard проверяет файловую систему в режиме реального времени.
- Сканер Dr.Web позволяет запустить проверку на наличие угроз вручную.
- На экране Результаты проверки вы можете выбрать действия, чтобы обезвредить обнаруженные угрозы безопасности.

11.2.1. Постоянная защита SpIDer Guard на Android TV

Включение постоянной защиты

После активации лицензии постоянная защита включается автоматически. SpIDer Guard работает независимо от того, запущено приложение или нет. Если SpIDer Guard обнаружит подозрительное изменение в системной области или угрозу, в нижней части экрана появится предупреждающее сообщение.

Настройка

Чтобы включить, настроить или отключить постоянную защиту, на главном экране Dr.Web 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 **События** 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 Dr.Web выберите опцию **Сканер** (см. Рисунок 37) 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 результаты проверки, выберите **OK**.

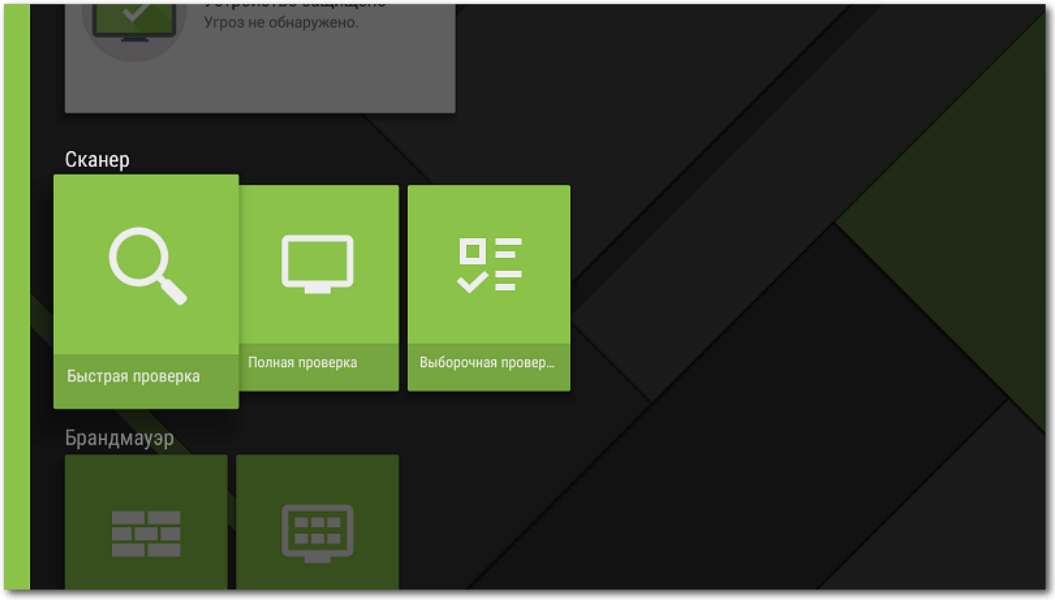

Рисунок 37: Сканер Dr.Web

Настройки Сканера Dr.Web

Для доступа к настройкам Сканера Dr.Web на главном экране Dr.Web 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 **События** на вкладке **Статистика**, отсортированные по дате (см. раздел Статистика).

11.2.3. Результаты проверки на Android TV

Как открыть результаты проверки

Если компонент SplDer Guard обнаружит подозрительное изменение в системной области или угрозу, внизу экрана появится предупреждающее сообщение. Чтобы открыть результаты проверки, на главном экране Dr.Web выберите опцию **События**.

Чтобы открыть результаты проверки Сканера Dr.Web, после окончания проверки выберите **ОК**.

Обезвреживание угроз

На экране **Результаты проверки** вы можете ознакомиться со списком угроз и подозрительных изменений в системной области. Для каждого объекта указаны его тип и название, а также значок опции, которую рекомендуется выбрать для этого объекта.

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

1. Вредоносная программа.
2. Потенциально опасная программа.
3. Программа взлома.
4. Рекламная программа.
5. Изменения в системной области:
   - Новые файлы в системной области.
   - Изменение системных файлов.
   - Удаление системных файлов.
6. Программа-шутка.

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

Обезвреживание всех угроз

Чтобы удалить сразу все угрозы

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

Чтобы переместить в карантин сразу все угрозы

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

карантин.

Обезвреживание угроз по одной

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

 **Вылечить**, чтобы вылечить инфицированное приложение.

Опция доступна для некоторых угроз в системных приложениях, если на устройстве разрешен root-доступ.

 **Удалить**, чтобы полностью удалить угрозу из памяти устройства.

В некоторых случаях Dr.Web не может удалить приложения, которые используют специальные возможности Android. Если Dr.Web не удалит приложение после выбора опции **Удалить**, перейдите в безопасный режим и удалите приложение вручную. Если Dr.Web предоставлен доступ к специальным возможностям, удаление приложения произойдет автоматически после выбора опции **Удалить**.

Опция недоступна для угроз в системных приложениях в следующих случаях:

- Если на устройстве не разрешен root-доступ.
- Если удаление приложения может привести к потере работоспособности устройства.
- Если обнаружена модификация угрозы. Чтобы определить, действительно ли приложение представляет угрозу, сообщите о ложном срабатывании.

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

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

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

 **Заблокировать**, чтобы отключить приложению доступ к интернет-соединениям.

Опция доступна для угроз в системных приложениях.

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

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

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

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

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

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.

Чтобы включить Брандмауэр Dr.Web

1. На главном экране Dr.Web выберите опцию **Брандмауэр** (см. Рисунок 38).
2. Выполните одно из следующих действий:
   - Используйте переключатель справа от пункта **Журнал**.
   - Выберите пункт **Трафик** или **Журнал** и нажмите **Включить**.

По умолчанию Брандмауэр отключен. Dr.Web запрашивает разрешение на подключение к VPN. Для работы Брандмауэра необходимо предоставить это 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.

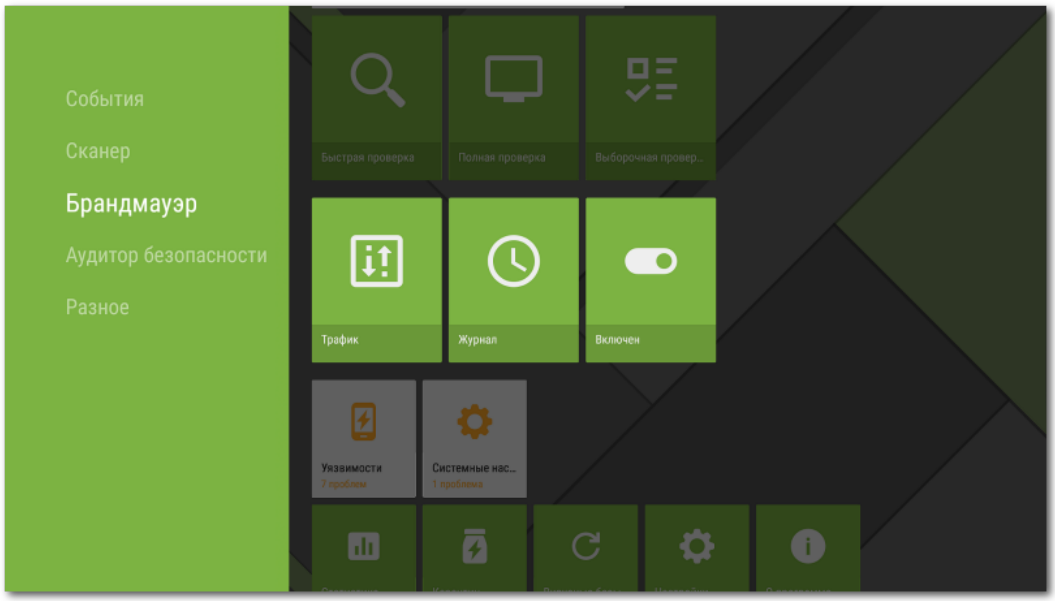

Рисунок 38: Брандмауэр Dr.Web на Android TV

11.3.1. Активность сетевых подключений на Android TV

Информацию об активности сетевых подключений можно получить на экране **Трафик**. На экране доступны две вкладки: **Активные приложения** и **Все приложения** (см. Рисунок 39).

Вкладка Активные приложения

На вкладке в режиме реального времени показывается список соединений, инициированных установленными на устройстве приложениями.

Для каждого приложения на вкладке **Активные приложения** отображается следующая информация:

- Суммарный объем входящего и исходящего по установленным соединениям трафика.
- Доступ к передаче данных по Wi-Fi.

- Наличие пользовательских настроек. Приложения с измененным доступом к передаче данных отмечены значком ⚙.

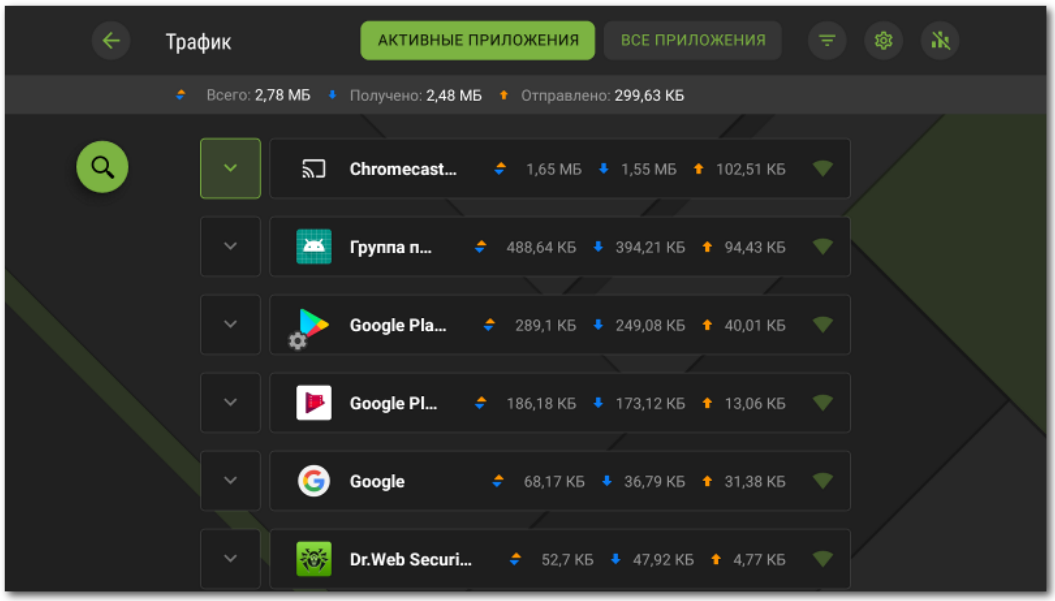

Рисунок 39: Вкладка Активные приложения

Соединения приложений

Нажмите значок ⌄ слева от имени приложения, чтобы увидеть подробную информацию о соединениях, установленных приложением:

- список установленных соединений;
- объем входящего и исходящего по каждому из установленных соединений трафика;
- наличие правила для соединения:
  - 🟢 разрешающее,
  - 🔴 запрещающее,
  - 🟠 перенаправляющее,
  - ○ правило не задано.

Нажмите на строку соединения, чтобы перейти на экран Соединение.

Вкладка Все приложения

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 **Все приложения**.

На вкладке **Все 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.

Для каждого приложения на вкладке **Все приложения** отображается следующая информация:

- Суммарный объем входящего и исходящего по установленным соединениям трафика.
- Доступ к передаче данных по Wi-Fi.
- Наличие пользовательских настроек. Приложения с измененным доступом к передаче данных отмечены значком  .

Фильтрация и сортировка приложений

Чтобы фильтровать или сортировать список приложений, нажмите значок  в правом верхнем углу экрана и выберите нужные параметры фильтрации или сортировки:

- Отображать приложения с нулевым трафиком.
- Сортировать:
  - по убыванию трафика — приложения с наибольшим трафиком вверху списка;
  - по возрастанию трафика — приложения с наименьшим трафиком вверху списка;
  - по алфавиту от А до Я;
  - по алфавиту от Я до А.

По умолчанию приложения отсортированы по убыванию трафика (приложения с наибольшим трафиком расположены вверху списка), приложения с нулевым трафиком отображаются. Чтобы восстановить вид списка приложений по умолчанию, нажмите **Сбросить** на экране **Фильтр**.

Поиск

Чтобы быстро перейти к нужному вам приложению, воспользуйтесь поиском по имени приложения. Для этого нажмите значок  в левой части экрана и введите запрос в поле поиска.

Настройки

Чтобы задать настройки для всех приложений, на экране **Трафик** нажмите  в правом верхнем углу экрана.

Доступны следующие настройки:

- **Использовать протокол IPv6**. Позволяет включить или отключить использование протокола IPv6 в параллели с IPv4.
- **Разрешить протокол DNS поверх TCP**. Позволяет включить или отключить использование протокола DNS поверх TCP для перенаправления DNS-запросов и сокрытия доменных имен.

  Использование протокола DNS поверх TCP может препятствовать отображению доменных имен на экранах Брандмауэра.

  Настройка работает на устройствах, которые поддерживают данный тип протокола. По умолчанию настройка отключена.

- **Запретить подключения для новых приложений**. Позволяет запретить доступ к сети для приложений, установленных после включения настройки. Настройка активна по умолчанию.
- **Запретить подключения для всех приложений**. Позволяет запретить доступ к сети для всех приложений, установленных на устройстве. Если доступ к сети будет предоставлен одному из приложений, настройка будет отключена.
- **Сохранять правила и статистику после удаления приложений**. Позволяет хранить данные удаленного с устройства приложения в течение выбранного периода времени: недели, месяца или года.

Удаление статистики, настроек и правил для приложений

Чтобы удалить статистику, настройки и правила для всех приложений

1. На экране **Трафик** нажмите в правом верхнем углу экрана.
2. Установите флажок напротив нужной опции и нажмите **Очистить**.

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 установленным на вашем устройстве приложением, а также настроить для него правила доступа к сетевым ресурсам вы можете на экране приложения (см. Рисунок 40).

На экране доступны две вкладки:

- На вкладке Статистика вы можете просмотреть статистику использования интернет-трафика, а также изменить индивидуальные настройки приложения.
- На вкладке Правила вы можете управлять правилами соединений, инициируемых приложением.

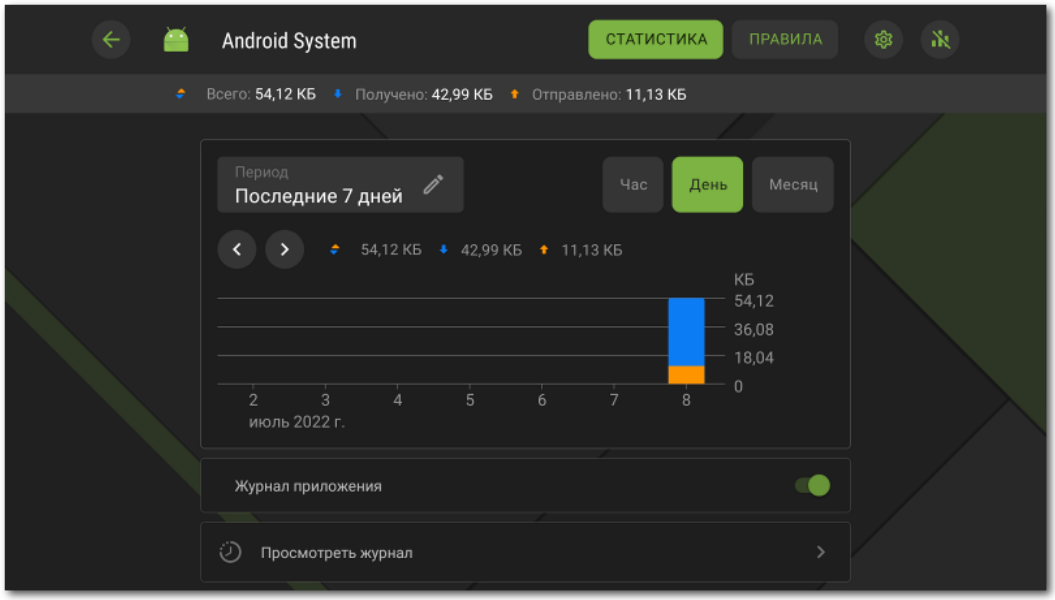

Рисунок 40: Экран приложения

Группа приложений

Некоторые служебные приложения могут быть объединены в группу приложений. Чтобы просмотреть список приложений, входящих в группу, на экране приложения нажмите на счетчик справа от заголовка **Группа приложений**.

11.3.2.1. Статистика и настройки приложения на Android TV

На вкладке **Статистика** экрана с подробной информацией о трафике приложения (группы приложений) вы можете ознакомиться со статистикой использования интернета данным приложением в виде графической диаграммы, а также изменить настройки Брандмауэра для этого приложения.

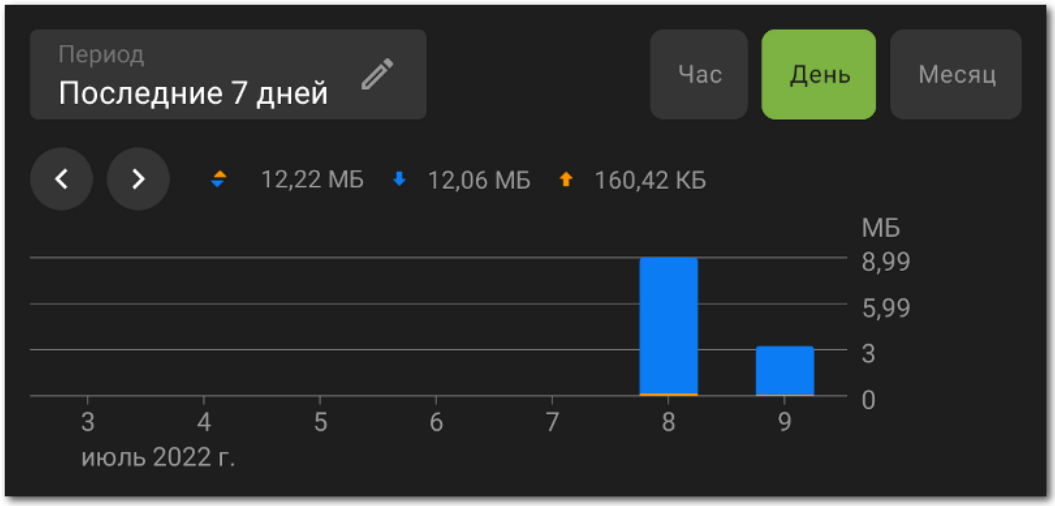

Рисунок 41: Статистика использования интернет-трафика

Статистика использования интернет-трафика

На диаграмме оранжевым цветом отмечен исходящий трафик приложения, синим — входящий. Над 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 поле над диаграммой. Вы можете просмотреть статистику за текущий день, последние 7 дней, 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 с помощью опций над диаграммой.

Удаление статистики

- Удаление статистики для всех приложений:
  1. На экране **Брандмауэр** выберите **Трафик**.
  2. На экране **Трафик** нажмите  в правом верхнем углу.
  3. Установите флажок **Статистику приложений** и нажмите **Очистить**.
- Удаление статистики для отдельного приложения:
  1. На экране **Трафик** выберите приложение, для которого вы хотите очистить статистику.
  2. На экране приложения нажмите  в правом верхнем углу.
  3. Установите флажок **Статистику приложения** и нажмите **Очистить**.

После удаления приложения с устройства статистика приложения будет удалена автоматически в течение 5 минут.

Журнал приложения

События, связанные с сетевой активностью приложений, установленных на устройстве, записываются в журналы приложений. Используйте переключатель, чтобы начать или возобновить ведение журнала приложения. Чтобы перейти в журнал, нажмите **Просмотреть журнал**.

Настройки приложения

Чтобы перейти к настройкам приложения (группы приложений), на вкладке **Статистика** нажмите ⚙ в правом верхнем углу экрана (см. Рисунок 40).

Доступ к передаче данных по Wi-Fi

Используйте переключатель, чтобы запретить или разрешить передачу данных по Wi-Fi для этого приложения. По умолчанию доступ разрешен. Индикатор доступа отображается справа в строке приложения на экране **Трафик** (зеленый индикатор — доступ разрешен, серый — запрещен).

Блокировать все соединения, кроме разрешенных правилами

Чтобы запретить по умолчанию все соединения для приложения, используйте переключатель **Блокировать все соединения, кроме разрешенных правилами**. Если разрешающие правила для приложения не будут заданы, приложение не сможет устанавливать никакие соединения.

При включении настройки **Блокировать все соединения, кроме разрешенных правилами** для приложения будет автоматически добавлено разрешающее правило для порта 53. Наличие правила (для протоколов DNS, UDP или ALL) обязательно для работы разрешающих правил с доменными именами.

⚠ Для корректной работы настройки при наличии разрешающих правил с доменными именами необходимо также отключить использование персонального DNS-сервера в настройках устройства.

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). Для этого используйте переключатель **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.

11.3.2.2. Правила соединений на Android TV

Управление трафиком приложений происходит на уровне соединений, которые устанавливают приложения. Вы можете задать разрешающие, запрещающие и перенаправляющие правила соединений с определенными IP-адресами и портами для каждого приложения, установленного на устройстве.

Соединения

Общая информация о каждом соединении представлена на экране **Соединение** (см. Рисунок 42). Чтобы перейти к этому экрану, выполните одно из следующих действий:

- На вкладке Активные приложения экрана **Трафик** нажмите значок ⌄ слева от имени приложения, а затем нажмите на строку соединения.
- В журнале Брандмауэра:
  - В режиме группировки по дате: нажмите на строку соединения.
  - В режиме группировки по имени приложения: раскройте список соединений приложения с помощью значка ⌄ слева от имени приложения, а затем нажмите на строку соединения.
- В журнале приложения раскройте список соединений с помощью значка ⌄ справа от даты события, а затем нажмите на строку соединения.

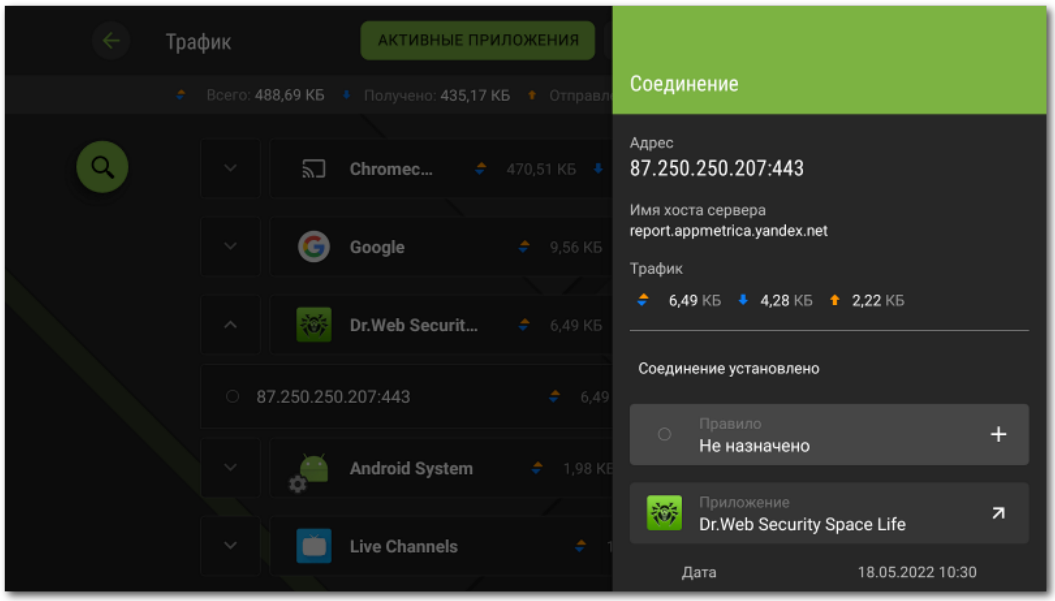

Рисунок 42: Экран Соединение

На экране **Соединение** доступна следующая информация:

- адрес и порт соединения;
- имя хоста (при его наличии);
- объем входящего и исходящего трафика, полученного или переданного соединением;
- статус соединения;
- правило соединения;
- приложение, установившее соединение;
- дата и время;
- тип подключения;
- протокол.

Правила соединений доступны на вкладке Правила экрана приложения.

Правила соединений

Создание правил

Чтобы создать новое правило для соединения

1. Для соединения без правил:
   - На экране **Соединение** нажмите значок + справа от пункта **Правило**.

   Для любого соединения:
   - На экране приложения на вкладке **Правила** нажмите значок  в левой части экрана.
2. В открывшемся окне выберите тип правила:
   - 🟢 разрешающее,
   - 🔴 запрещающее,
   - 🟠 перенаправляющее.
3. Проверьте правильность IP-адреса/имени хоста. Если адрес не указан, укажите действительный IP-адрес (в формате a.b.c.d для IPv4-адресов или [a:b:c:d:e:f:g:h] для IPv6-адресов), диапазон IP-адресов (в формате a1.b1.c1.d1-a2.b2.c2.d2 или [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2]) или целую сеть (в формате a.b.c.0/n, где n — число от 1 до 32). В случае создания перенаправляющего правила укажите адрес перенаправления в поле ниже. Вместо адреса вы можете указать имя хоста.
4. Нажмите **Дополнительно**, чтобы установить дополнительную настройку **Протокол** — сетевой протокол для соединения.
5. Нажмите **Сохранить**.

Приложения с заданными правилами соединений отмечены значком .

Просмотр правил

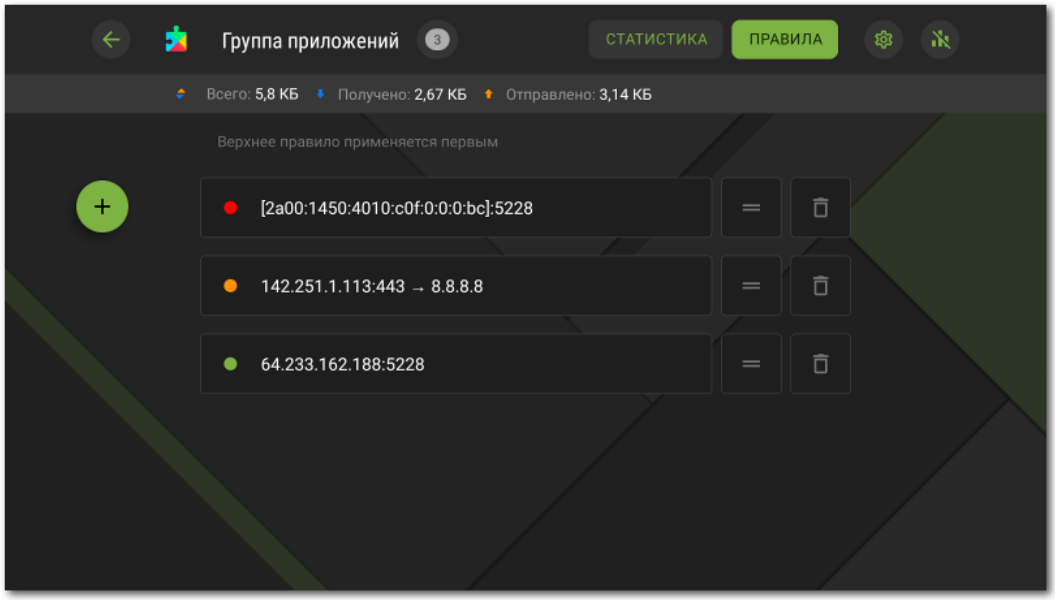

Рисунок 43: Вкладка Правила

Чтобы увидеть правила соединений приложения

- Откройте экран приложения и перейдите на вкладку **Правила**.

Вкладка содержит список всех правил, заданных для данного приложения, в порядке их применения.

Чтобы изменить порядок применения правил

- Нажмите и удерживайте значок напротив правила, которое вы хотите переместить, и перетяните правило на желаемую позицию в списке.

Редактирование правил

Чтобы отредактировать существующее правило

1. Выполните одно из следующих действий:
   - На экране **Соединение** нажмите значок справа от правила.
   - На экране приложения на вкладке **Правила** нажмите на строку правила.
2. Внесите необходимые изменения.
3. Нажмите **Сохранить**.

Удаление правил

Чтобы удалить правило

- На экране редактирования правила:
  1. Нажмите **Удалить правило**.
  2. В открывшемся окне нажмите **Удалить**.
- На вкладке **Правила** экрана приложения:
  1. Нажмите значок справа от правила.
  2. В открывшемся окне нажмите **Удалить**.

Чтобы удалить все правила для определенного приложения

1. На экране приложения на вкладке **Правила** нажмите значок в правом верхнем углу экрана.
2. В открывшемся окне установите флажок **Правила для приложения** и нажмите **Очистить**.

Чтобы удалить все правила для всех приложений

1. На экране **Брандмауэр** выберите **Трафик**.
2. На экране **Трафик** нажмите значок в правом верхнем углу экрана.
3. В открывшемся окне установите флажок **Настройки и правила для приложений** и нажмите **Очистить**.

Блокировать все соединения, кроме разрешенных правилами

Вы можете запретить все соединения приложения, кроме разрешенных правилами, с помощью соответствующего переключателя на экране настроек приложения.

11.3.2.3. Журнал приложения на Android TV

Журналы приложений содержат список событий, связанных с сетевыми подключениями того или иного приложения, установленного на вашем устройстве.

Чтобы включить ведение журнала приложения

1. На экране **Трафик** выберите нужное приложение.
2. На экране приложения используйте переключатель **Журнал приложения**.

Чтобы открыть журнал приложения

1. На вкладке **Трафик** выберите нужное приложение в списке.
2. На экране приложения нажмите **Просмотреть журнал**.

Просмотр журнала приложения

Все события приложения объединены по датам. Чтобы просмотреть список событий за какую-либо дату, выберите дату в списке.

Для каждого события показывается следующая информация:

- адрес и порт соединения;
- израсходованный трафик;
- наличие правила для соединения:
  - 🟢 разрешающее,
  - 🔴 запрещающее,
  - 🟠 перенаправляющее,
  - ○ правило не задано.

Нажмите на строку соединения, чтобы перейти на экран Соединение и настроить для него правила.

Чтобы очистить журнал приложения

1. На экране **Журнал приложения** нажмите значок в правом верхнем углу экрана.
2. Нажмите **Очистить**.

Чтобы отключить ведение журнала приложения

1. На экране **Трафик** выберите нужное приложение.
2. На экране приложения используйте переключатель **Журнал приложения**.

11.3.3. Журнал Брандмауэра Dr.Web на Android TV

Чтобы просмотреть список всех событий, связанных с работой Брандмауэра Dr.Web, на экране **Брандмауэр** выберите **Журнал**.

В журнале Брандмауэра (см. Рисунок 44) отображается следующая информация о событии:

- имя приложения;
- адрес и порт соединения (а также адрес перенаправления, если задано соответствующее правило);

- израсходованный трафик;
- дата и время события;
- наличие правила для соединения.

При нажатии на событие открывается экран Соединение.

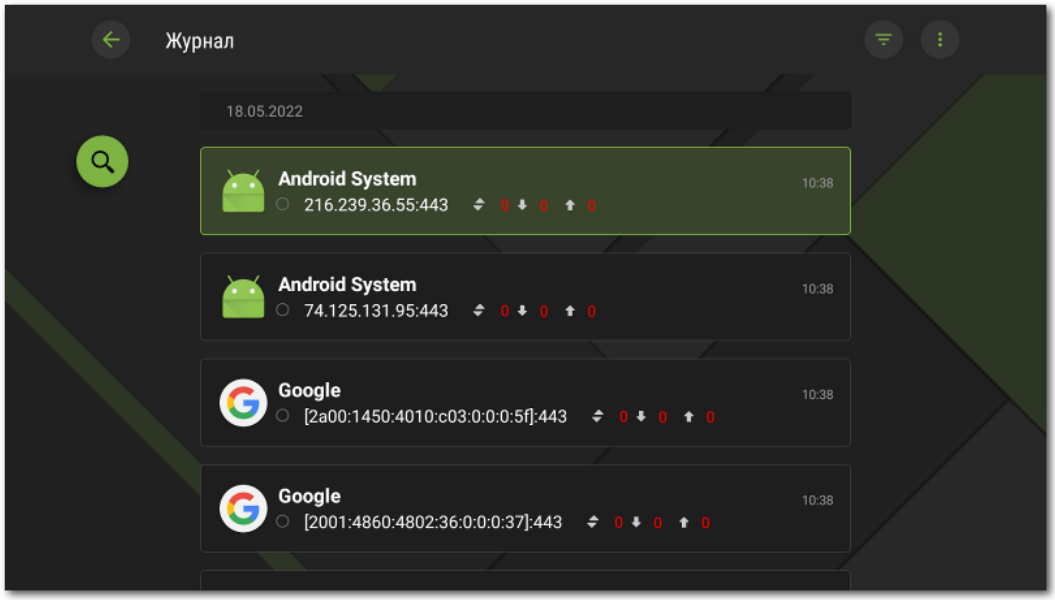

Рисунок 44: Журнал Брандмауэра Dr.Web

Чтобы фильтровать или сортировать события в журнале Брандмауэра

1. Нажмите значок в правом верхнем углу экрана **Журнал**.
2. Выберите нужные параметры фильтрации или сортировки:
   - Сортировать:
     - сначала новые — последние события вверху журнала;
     - сначала старые — последние события внизу журнала;
     - по алфавиту от А до Я;
     - по алфавиту от Я до А.
   - Отображать соединения:
     - установленные,
     - сброшенные,
     - перенаправленные,
     - с ошибкой.

По умолчанию события отсортированы по дате (последние события расположены вверху журнала), отображаются все виды соединений. Чтобы восстановить вид журнала по умолчанию, нажмите **Сбросить** на экране **Фильтр**.

Для удобства просмотра журнала вы также можете группировать события по приложению.

Чтобы группировать события по приложению

- На экране **Журнал** нажмите ⋮ в правом верхнем углу и используйте переключатель **Группировать по имени приложения**.

Чтобы выполнить поиск по журналу Брандмауэра

- Нажмите значок  в левой части экрана и введите запрос в поле поиска.

Чтобы очистить журнал Брандмауэра

1. На экране **Журнал** нажмите ⋮ в правом верхнем углу и выберите опцию **Очистить журнал**.
2. Подтвердите действие, нажав кнопку **Очистить**.

Размер журнала

По умолчанию для файла журнала установлен размер, равный 5 МБ.

Чтобы изменить максимально разрешенный размер файла журнала

1. На экране **Журнал** нажмите ⋮ в правом верхнем углу и выберите опцию **Размер журнала**.
2. В открывшемся окне измените значение и нажмите **Сохранить**.

Максимальный размер журнала должен быть больше 0 МБ и меньше либо равен 99 МБ.

11.4. Аудитор безопасности на Android TV

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

Dr.Web обнаруживает следующие проблемы безопасности:

- Уязвимости.

- Системные настройки, которые влияют на безопасность устройства.
- Приложения, использующие уязвимость Fake ID.

Чтобы открыть список обнаруженных проблем безопасности, на главном экране Dr.Web выберите **Аудитор безопасности**.

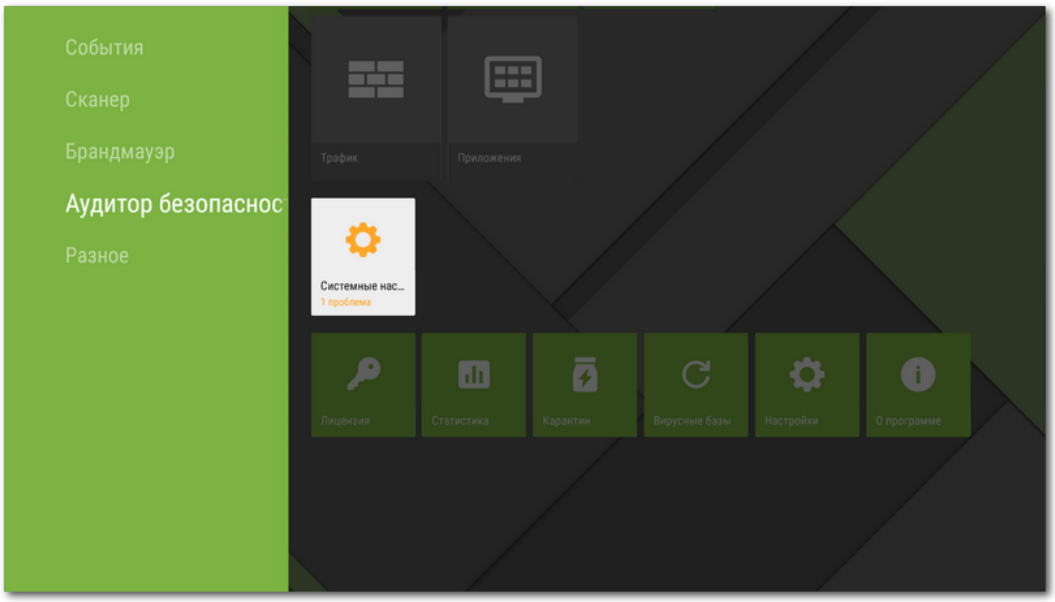

Рисунок 45: Аудитор безопасности

Уязвимости

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

Аудитор безопасности обнаруживает в системе устройства следующие уязвимости: BlueBorne, EvilParcel, Extra Field, Fake ID, Janus, ObjectInputStream Serialization, OpenSSLX509Certificate, PendingIntent, SIM Toolkit, Stagefright и Stagefright 2.0.

Воспользовавшись уязвимостями, злоумышленники могут добавить программный код в приложения, в результате чего эти приложения могут начать выполнять функции, представляющие угрозу безопасности устройства.

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.

Root-доступ

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.

Системные настройки

Аудитор безопасности обнаруживает следующие системные настройки, которые влияют на безопасность устройства:

- **Отладка разрешена**. 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 выберите **Настройки** на экране с подробной информацией об этой проблеме.
- **Установка из неизвестных источников разрешена**. Установка приложений из неизвестных источников является основной причиной распространения угроз для устройств под управлением Android. Приложения, загруженные не из официального каталога приложений 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 выберите **Настройки** на экране с подробной информацией об этой проблеме. Кроме того, рекомендуется проверять все устанавливаемые приложения на наличие угроз. Перед проверкой необходимо убедиться, что вирусные базы Dr.Web обновлены.
- **Уведомления Dr.Web заблокированы**. В этом случае 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.
- **Установлен пользовательский сертификат**. 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, выберите **Удалить** на экране с подробной информацией о проблеме, связанной с этим приложением, или воспользуйтесь средствами ОС.

11.5. Разное

Раздел **Разное** (см. Рисунок 46) 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.

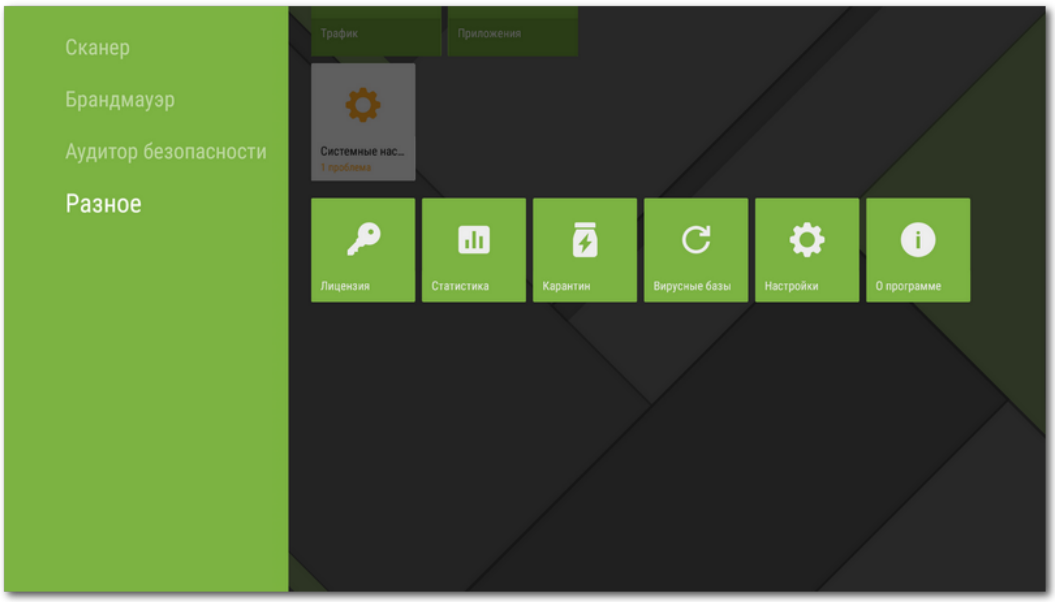

Рисунок 46: Разное

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 выберите **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 угрозах в системных приложениях, которые не могут быть удалены без потери работоспособности устройства. 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 APK-файлы 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.
- **Системная область** позволяет отслеживать изменения в системной области. Если эта настройка включена, SpIDer Guard отслеживает изменения (добавление, изменение и удаление файлов) и уведомляет об удалении любых файлов, а также добавлении и изменении исполняемых файлов: `.jar`, `.odex`, `.so`, файлов формата APK, ELF, и др.
- **Повторная проверка системной области** позволяет запустить повторную проверку системной области. SpIDer Guard заново проверит все угрозы в системной области, которые были проигнорированы ранее.
- **Уведомления о системной области** позволяет включить уведомления об изменении любых файлов в системной области (не только исполняемых).
- **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:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. 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»:

1. Заполните веб-форму в соответствующей секции раздела https://support.drweb.com/.
2. 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. Забыли пароль?

Если вы забыли пароль от учетной записи Dr.Web, сбросьте его и задайте новый:

- С помощью электронной почты. Эту почту вы указали при создании учетной записи или настройке Антивора Dr.Web.
- С помощью СМС. Эта опция доступна только в версии приложения с сайта, если в список друзей в Антиворе добавлен хотя бы один телефонный номер.
- С помощью уведомления. Эта опция доступна, если хотя бы один друг подтвердил ваш запрос в друзья в приложении Dr.Web Mobile Security Suite.
- С помощью запроса в службу технической поддержки. Служба технической поддержки сможет вам помочь, только если удостоверится, что вы являетесь владельцем устройства.

> ⚠ Если Dr.Web работает в режиме централизованной защиты и Антивор Dr.Web настроен на сервере, вы не сможете задать новый пароль указанными способами. В этом случае обратитесь к администратору антивирусной сети вашей компании или поставщику услуги «Антивирус Dr.Web» и воспользуйтесь символьным или QR-кодом восстановления.

Сбросить пароль с помощью электронной почты

На панели для сброса пароля с помощью электронной почты (см. Рисунок 47) указаны:

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

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

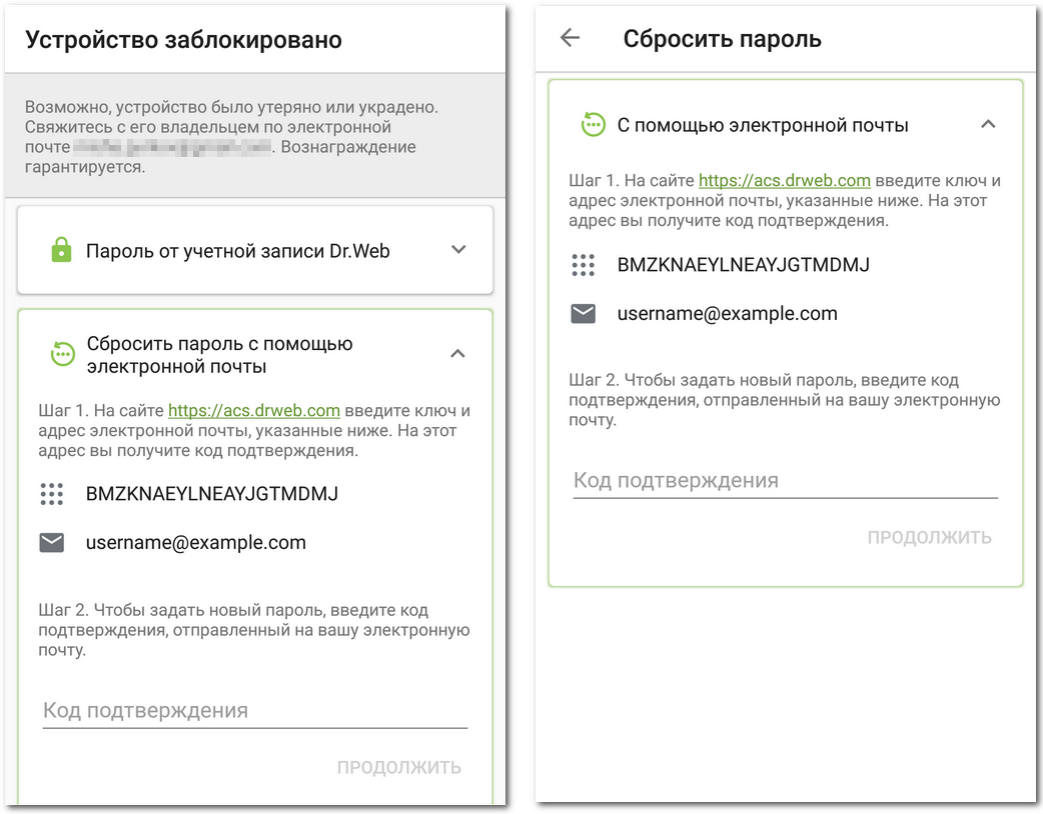

Рисунок 47: Сбросить пароль с помощью электронной почты Заблокированное (слева) и незаблокированное (справа) устройство

Чтобы сбросить пароль

1. На компьютере или любом другом устройстве откройте веб-страницу учетной записи Dr.Web: https://acs.drweb.com (см. Рисунок 48).

> Если у вас установлен Dr.Web 11.1.3 или более ранняя версия, для сброса пароля перейдите на страницу Антивора Dr.Web https://antitheft.drweb.com/ или обновите приложение до версии 12.

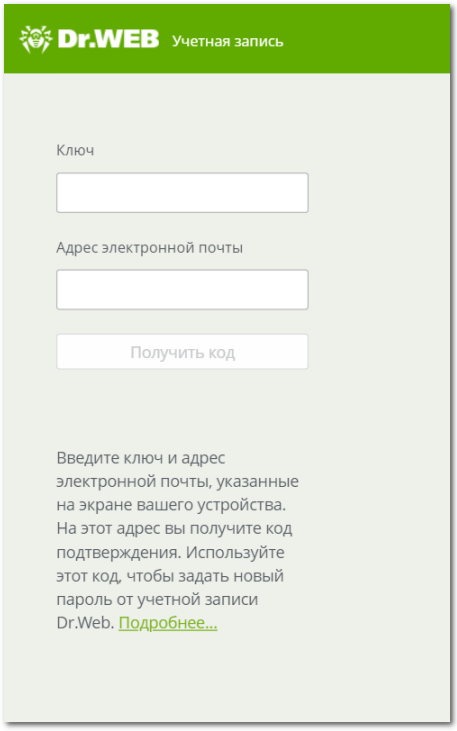

Рисунок 48: Учетная запись Dr.Web

2. На этой странице введите ключ и адрес электронной почты (см. Рисунок 49), указанные в приложении Dr.Web.

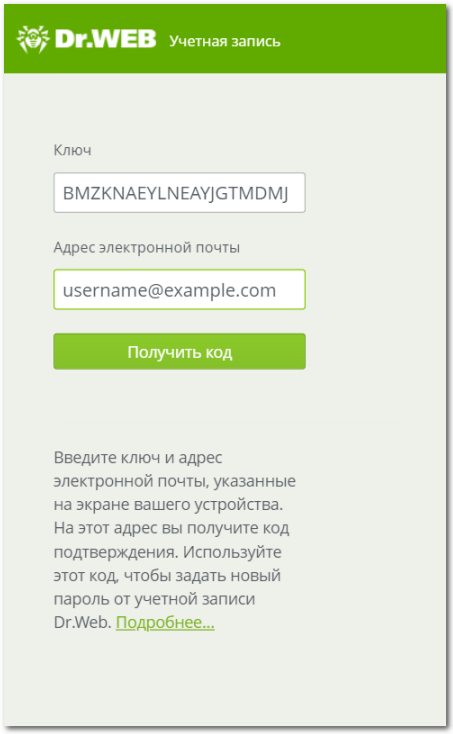

Рисунок 49: Ввод ключа и адреса электронной почты

3. Нажмите кнопку **Получить код**.

Если данные введены правильно, появится сообщение, что на ваш адрес электронной почты отправлено письмо с кодом подтверждения (см. Рисунок 50).

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 в приложении Dr.Web.
3. Если после этого вы не получили письмо, обратитесь в службу технической поддержки «Доктор Веб». Для этого нажмите **Не получили письмо?** (см. Рисунок 50).

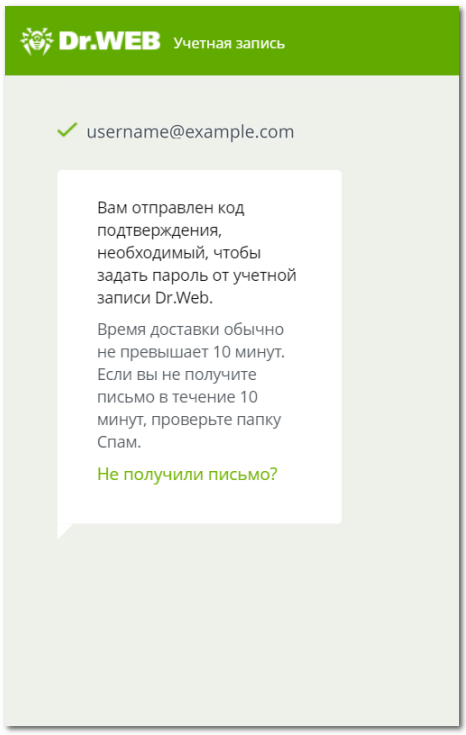

Рисунок 50: Уведомление об отправке кода подтверждения

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

5. В приложении Dr.Web введите код подтверждения в поле **Код подтверждения** (см. Рисунок 51).

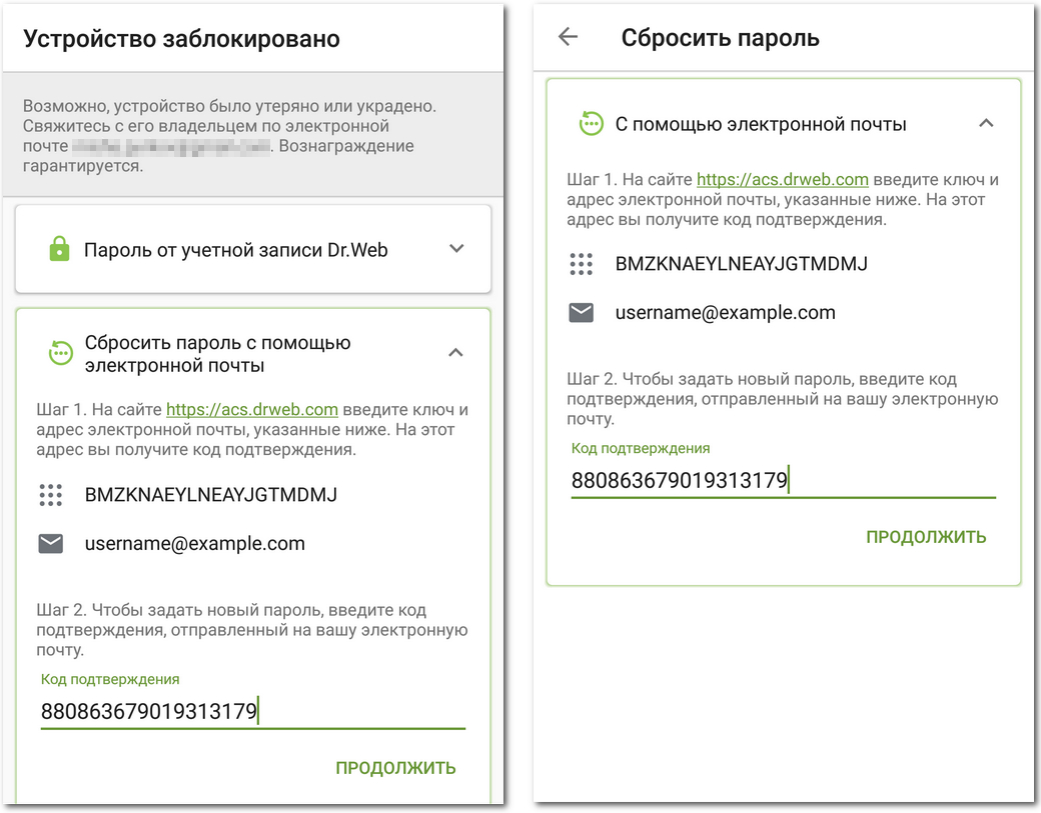

Рисунок 51: Ввод кода подтверждения, полученного по почте
Заблокированное (слева) и незаблокированное (справа) устройство

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

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

Сбросить пароль с помощью СМС с номера друга

Вы можете сбросить пароль этим способом, если выполняются следующие условия:

1. На вашем устройстве установлена версия приложения с сайта «Доктор Веб».
2. Ваше устройство включено и находится в зоне действия сети.
3. На вашем устройстве включен Антивор Dr.Web.
4. В список Я доверяю в Антиворе добавлен хотя бы один телефонный номер.
5. Номер, с которого будет отправлена СМС-команда, добавлен в список Я доверяю.
6. Вы знаете телефонный номер SIM-карты, которая используется на вашем устройстве. СМС-команда может быть отправлена только на этот номер.

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

Если вы используете сразу две SIM-карты на вашем устройстве, отправьте СМС-команду на любой из этих номеров.

Чтобы сбросить пароль

1. Отправьте СМС с текстом **#RESETPASSWORD#** на ваше устройство с номера друга.

   Список номеров, с которых можно отправить СМС-команду, расположен на экране **Устройство заблокировано** или **Сбросить пароль** (см. Рисунок 52). СМС-команда не зависит от регистра.

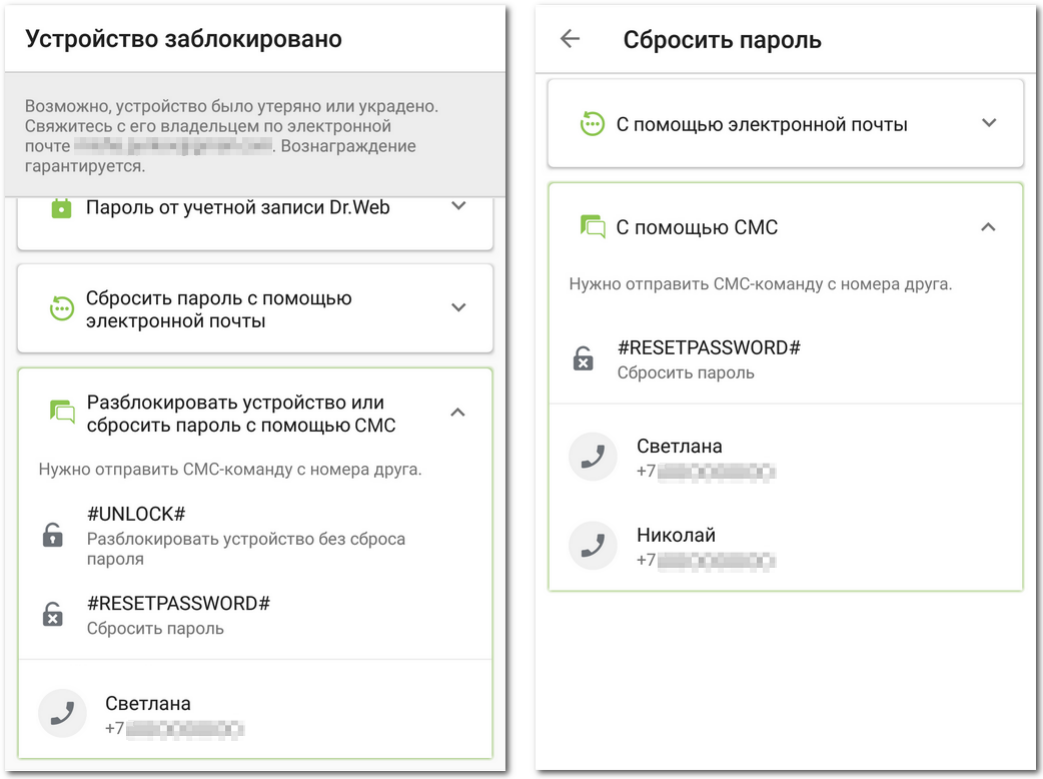

Рисунок 52: Сбросить пароль с помощью СМС с номера друга Заблокированное (слева) и незаблокированное (справа) устройство

2. При получении СМС на вашем устройстве автоматически появляется экран **Изменить пароль**. Введите новый пароль. Если устройство было заблокировано, оно разблокируется.

Если устройство заблокировано, вы можете разблокировать его без сброса пароля. Для этого отправьте на устройство СМС-команду **#UNLOCK#**.

Сбросить пароль с помощью уведомления

Вы можете сбросить пароль с помощью уведомления, если выполняются следующие условия:

- **Для вашего устройства**
  1. Устройство включено и подключено к интернету.
  2. Включен Антивор Dr.Web.
  3. В список Я доверяю в Антиворе добавлен хотя бы один адрес электронной почты.
- **Для устройства друга**
  - Если ваше устройство заблокировано:
    1. Устройство друга включено и подключено к интернету.
    2. На устройстве друга установлено приложение Dr.Web Light или Dr.Web Security Space.
    3. Друг подтвердил ваш запрос в друзья в компоненте Помощь другу или в Антиворе Dr.Web. Чтобы получить ваше уведомление, компоненты должны быть включены.
  - Если ваше устройство не заблокировано:
    1. Устройство друга включено и подключено к интернету.
    2. На устройстве друга установлено приложение Dr.Web Security Space.
    3. Друг подтвердил ваш запрос в друзья в Антиворе Dr.Web. Чтобы получить ваше уведомление, компонент должен быть включен.

Чтобы сбросить пароль

1. Отправьте другу уведомление. Для этого нажмите значок ➤ (см. Рисунок 53).
2. Сообщите другу код подтверждения, указанный на этой же панели.

   Друг должен ввести код подтверждения на своем устройстве и отправить команду Антивору для сброса пароля.
3. При получении команды на вашем устройстве автоматически появляется экран **Изменить пароль**. Введите новый пароль. Если устройство было заблокировано, оно разблокируется.

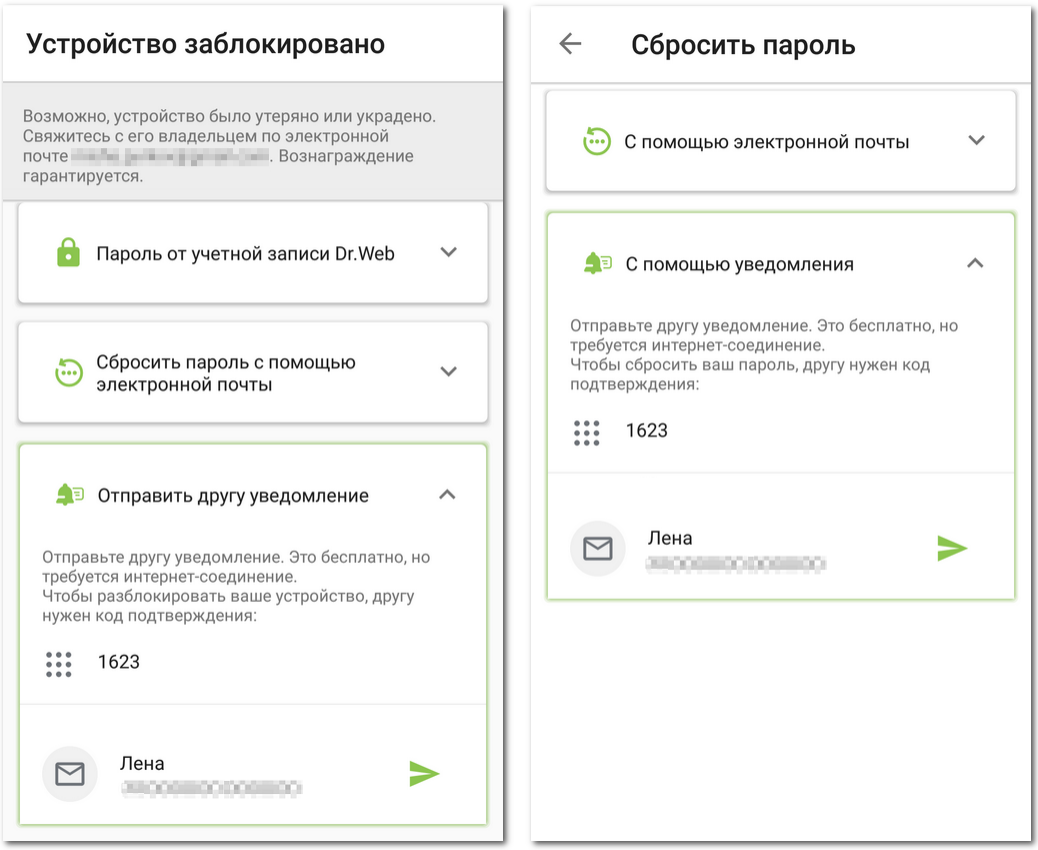

Рисунок 53: Сбросить пароль с помощью уведомления
Заблокированное (слева) и незаблокированное (справа) устройство

Сбросить пароль с помощью запроса в службу технической поддержки

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

1. Откройте страницу службы технической поддержки: https://support.drweb.com/.
2. В разделе **Техническая поддержка** выберите пункт **Работа программы Dr.Web**.
3. На открывшейся странице укажите данные вашей лицензии или номер заказа.
4. На вкладке **Для дома** выберите пункт **Android**.
5. На открывшейся странице заполните все поля.
6. Присоедините к запросу следующие файлы:
   - Фотография экрана **Устройство заблокировано** или **Сбросить пароль**, на которой различимы ключ и адрес электронной почты (см. Рисунок 47).
   - 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 вашего профиля 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.

7. 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.

8. На экране **Устройство заблокировано** или **Сбросить пароль** введите код подтверждения в поле **Код подтверждения** (см. Рисунок 51) и нажмите **Продолжить**.

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

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

10. Повторите пароль и нажмите **Сохранить**.

Разблокировать устройство с помощью запроса администратору

Если Dr.Web работает в режиме централизованной защиты и Антивор Dr.Web настроен на сервере, для разблокировки устройства вам необходимо связаться с администратором антивирусной сети вашей компании или поставщиком услуги «Антивирус Dr.Web». Вы можете воспользоваться двумя способами разблокировки:

- С помощью QR-кода:
  1. Свяжитесь с администратором антивирусной сети вашей компании или поставщиком услуги «Антивирус Dr.Web» любым доступным вам способом.
  2. Передайте администратору QR-код с экрана **Устройство заблокировано**. Нажмите и удерживайте QR-код, чтобы сохранить его на устройстве. Вы также можете передать фотографию экрана, на которой четко различим QR-код.

     Администратор отправит вам QR-код подтверждения разблокировки устройства.
  3. Убедитесь, что вы получили QR-код разблокировки, и нажмите **Продолжить**.
  4. В открывшемся окне нажмите кнопку **Сканировать QR-код** и наведите камеру устройства на QR-код разблокировки, полученный от администратора.

     В случае успешного распознавания QR-кода устройство будет разблокировано.
- С помощью символьного кода:
  1. На экране **Устройство заблокировано** нажмите **Другой способ**.

2. Свяжитесь с администратором антивирусной сети вашей компании или поставщиком услуги «Антивирус Dr.Web» любым доступным вам способом.
3. Сообщите администратору идентификатор и код восстановления, отображаемые на экране **Устройство заблокировано**.

   Администратор отправит вам код разблокировки устройства.
4. Убедитесь, что вы получили код разблокировки, и нажмите **Продолжить**.
5. В открывшемся окне в поле **Код разблокировки** введите код, полученный от администратора, и нажмите **Разблокировать**.

   Если код разблокировки был введен корректно, устройство будет разблокировано.

Если по каким-то причинам вы не можете завершить процедуру разблокировки устройства выбранным вами способом, переключиться на альтернативный способ можно, нажав **Другой способ** на экране **Устройство заблокировано**.

Для сброса пароля после разблокировки устройства свяжитесь с администратором антивирусной сети вашей компании или поставщиком услуги «Антивирус Dr.Web».