Dr.WEB®
Security Space
для BlackBerry

Защити созданное

Руководство пользователя

Dr.Web Security Space для BlackBerry
Версия 10.01
Руководство пользователя
19.11.2015

«Доктор Веб», Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: www.drweb.com
Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Глава 1. Введение

Благодарим вас за выбор **Dr.Web Security Space для BlackBerry** (далее - **Dr.Web**). Данный антивирусный продукт надежно защищает мобильные устройства, работающие под управлением операционной системы BlackBerry™ от различных вирусных угроз, созданных специально для этих устройств.

В приложении применены наиболее передовые разработки и технологии **«Доктор Веб»** по обнаружению и обезвреживанию вредоносных объектов, которые могут представлять угрозу функционированию устройства и его информационной безопасности.

Настоящее руководство призвано помочь пользователям устройств под управлением ОС BlackBerry установить и настроить **Dr.Web**, а также ознакомиться с его основными функциями.

Используемые обозначения

В руководстве используются следующие обозначения:

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов **«Доктор Веб»** или их компонентов.
Зеленое и подчеркнутое начертание	Ссылки на страницы руководства и веб-сайты.
Курсив	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Основные возможности приложения

Dr.Web представляет собой надежное антивирусное решение для пользователей устройств, работающих под управлением операционной системы BlackBerry. Приложение выполняет следующие функции:

- непрерывная защита файловой системы устройства в режиме реального времени (проверка сохраняемых файлов, устанавливаемых программ и т.д.);
- проверка всех файлов системы или отдельных файлов и папок по запросу пользователя;
- проверка архивов;
- проверка SD-карты (или другого внешнего накопителя);
- обнаружение угроз в файлах *.lnk (определяемых **Dr.Web** как Exploit.Cpllnk);
- удаление обнаруженных угроз безопасности или перемещение их в карантин;
- обновление вирусных баз **Dr.Web** через интернет-соединение;
- ведение статистики обнаруженных угроз и действий приложения, а также журнала регистрации событий;
- помощь в выявлении и устранении проблем безопасности и уязвимостей устройства.

Удобный графический интерфейс позволяет полностью настроить параметры работы приложения

с учетом нужд пользователя и установить оптимальный уровень защиты устройства.

Системные требования

Для установки и работы **Dr.Web** требуется, чтобы мобильное устройство работало под управлением операционной системы BlackBerry версии 10.3.2 и выше.

Для загрузки обновлений вирусных баз требуется соединение с сетью Интернет.

Глава 2. Лицензирование

Для работы **Dr.Web** требуется лицензия. Лицензия позволяет полноценно использовать возможности продукта на протяжении всего срока действия и регулирует права пользователя, установленные в соответствии с пользовательским договором.

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, вы можете активировать демонстрационный период. Он обеспечивает полную функциональность основных компонентов, но срок действия существенно ограничен.

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

Активировать лицензию или демонстрационный период, а также перейти к покупке лицензии можно на соответствующем экране (см. Рисунок 1), который открывается при первом запуске приложения, а также при отсутствии действующей лицензии.

Чтобы открыть экран для получения лицензии:

1. Выберите пункт **О программе** в меню приложения.
2. Нажмите кнопку **Обновить лицензию**.

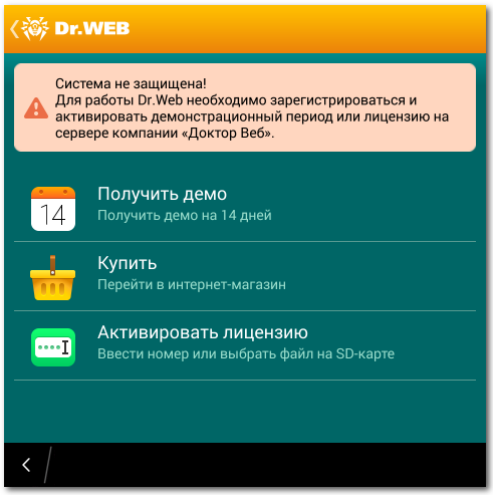


Рисунок 1. Лицензирование

Лицензионный ключевой файл

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

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

- период, в течение которого разрешено использование продукта;
- перечень компонентов, разрешенных к использованию;
- другие ограничения.

Лицензионный ключевой файл является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- лицензия распространяется на все используемые приложением модули;
- целостность лицензии 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 следует открывать его в текстовых редакторах во избежание его случайной порчи.

Активация демонстрационного периода

Если вы установили приложение в ознакомительных целях, вы можете активировать демонстрационный период на 14 дней.

Чтобы активировать демонстрационный период:

1. Нажмите **Получить демо** на экране для получения лицензии (см. Рисунок 1).
2. Откроется окно для ввода адреса электронной почты, для которого будет активирован демонстрационный период. Введите действительный адрес электронной почты.
3. Нажмите кнопку **Получить демо**. Демонстрационный период будет активирован.

Покупка лицензии

Чтобы купить лицензию:

1. Нажмите **Купить** на экране для получения лицензии (см. Рисунок 1) или перейдите по ссылке http://estore.drweb.com/mobile. Будет открыта страница интернет-магазина **«Доктор Веб»**.
2. Выберите срок действия лицензии и количество защищаемых устройств.
3. Нажмите кнопку **Купить**.

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

Активация лицензии

Если вы уже являетесь владельцем действующей лицензии на программные продукты **Dr.Web Security Space** или **Антивирус Dr.Web** (поставка в коробке или в виде электронной лицензии), вам доступны приведенные ниже способы активации имеющейся лицензии.

Регистрация серийного номера

1. На экране для получения лицензии (см. Рисунок 1) выберите вариант **Активировать лицензию**.
2. Выберите пункт **Ввести серийный номер**.
3. Введите серийный номер.
4. Если вы регистрируете данный серийный номер впервые, откроется экран ввода личных

данных, необходимых для активации лицензии. Заполните все поля.

5. Нажмите кнопку **Получить лицензию**.

Копирование ключевого файла на устройство

1. Скопируйте ключевой файл в папку **downloads**, во внутренней памяти устройства.
2. На экране для получения лицензии (см. Рисунок 1) выберите пункт **Активировать лицензию**.
3. Выберите пункт **Загрузить**. В информационном окне **Копировать из файла** нажмите **ОК**.
4. Ключевой файл будет установлен и готов к использованию. Откроется окно с информацией о сроке действия лицензии. Нажмите **ОК**.

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

Чтобы проверить возможность использования ключевого файла:

1. Откройте ключевой файл в текстовом редакторе (например, в Блокноте).
2. Проверьте, присутствует ли компонент DrWebGUI в списке значений параметра Applications в группе [Key]: если данный компонент находится в списке, ключевой файл может быть использован для работы **Dr.Web**.

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

Получение ключевого файла при регистрации серийного номера на сайте компании «Доктор Веб»

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.
2. Введите регистрационный серийный номер, полученный при покупке **Dr.Web**.
3. Заполните форму со сведениями о покупателе.
4. Ключевой файл будет выслан по указанному вами адресу электронной почты в виде ZIP-архива, содержащего файл с расширением *.key.
5. Извлеките ключевой файл на компьютер, с которого вы можете скопировать его на устройство.

Продление лицензии

В некоторых случаях, например, при окончании срока действия лицензии, вам может потребоваться заменить уже существующий и зарегистрированный в системе лицензионный ключевой файл. **Dr.Web** поддерживает обновление ключевого файла «на лету», при котором его не требуется переустанавливать или прерывать его работу.

Информация о лицензии

Чтобы просмотреть информацию об используемой лицензии, на главном экране (см. Рисунок 2) вызовите меню приложения и выберите пункт **О программе**.

На открывшемся экране вы можете просмотреть следующую информацию о лицензии:

- имя владельца лицензии;
- даты регистрации и окончания срока действия лицензии.

Настройка уведомлений

Вы можете включить/отключить использование уведомлений о скором окончании срока действия лицензии с помощью опции **Уведомления** в разделе **Лицензия** в настройках **Dr.Web** (см.

Рисунок 3).

Обновление лицензии

Для обновления лицензии необходимо приобрести и активировать новую лицензию.

Вы также можете приобрести новую лицензию или продлить текущую лицензию на вашей персональной странице на официальном сайте компании **«Доктор Веб»**. Чтобы перейти на эту страницу, выберите пункт **О программе** в меню приложения и перейдите по ссылке **Мой Dr.Web**.

Глава 3. Установка и удаление

Dr.Web можно приобрести и установить непосредственно из BlackBerry World, или же скопировать и запустить на устройстве установочный файл приложения.

Удаление приложения возможно через BlackBerry World или средствами операционной системы устройства.

Установка приложения

Установить **Dr.Web** можно из BlackBerry World, а также путем запуска установочного файла на устройстве.

Установка приложения через BlackBerry World

1. Откройте BlackBerry World на устройстве, найдите в списке приложений **Dr.Web** и нажмите кнопку **Загрузить**.

   Если **Dr.Web** не отображается в BlackBerry World, значит ваше устройство не удовлетворяет минимальным системным требованиям.

2. Далее откроется экран с информацией о функциях устройства, к которым требуется доступ для работы приложения:
   - если вы устанавливаете **Dr.Web** для использования в течение бесплатного демонстрационного периода (14 дней), для покупки лицензии по его истечении требуется доступ к функции осуществления покупок внутри приложения;
   - для работы **SpIDer Guard** и **Сканера Dr.Web** требуется доступ к данным приложений и SD-карте (или другому внешнему накопителю), а также возможность чтения и записи данных;
   - для обновления вирусных баз требуется доступ к сети Интернет и сетевым настройкам устройства.

   Нажмите кнопку **Принять**.

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

Запуск установочного файла на устройстве

Загрузить установочный файл **Dr.Web** можно на сайте компании **«Доктор Веб»**.

1. Скопируйте установочный файл на устройство.
2. При помощи файлового менеджера найдите и запустите установочный файл.
3. В открывшемся окне нажмите кнопку **Установить**.
4. Далее откроется экран с информацией о функциях устройства, к которым требуется доступ для работы приложения. Нажмите кнопку **Принять**.

Dr.Web установлен и готов к использованию.

Удаление и обновление приложения

Вы можете обновить версию приложения или удалить ее с устройства через BlackBerry World. Кроме того, удаление приложения возможно средствами операционной системы без подключения к сети Интернет.

Удаление приложения через BlackBerry World

1. Откройте BlackBerry World, перейдите в раздел **My World** и выберите **Мои приложения и игры** -> **Установлено**.
2. В списке установленных на устройстве приложений нажмите и удерживайте значок приложения **Dr.Web**.
3. Нажмите  в правой нижней части экрана.
4. В открывшемся окне нажмите кнопку **Удалить**, чтобы удалить приложение с устройства безвозвратно, или **Деинсталлировать**, чтобы иметь возможность установить приложение повторно.

Удаление приложения без подключения к сети Интернет

1. На главном экране устройства нажмите и удерживайте значок приложения, пока значки на экране не начнут мигать.
2. Нажмите  на значке приложения.

Обновление приложения через BlackBerry World

1. Откройте BlackBerry World, перейдите в раздел **My World** и выберите **Мои приложения и игры** -> **Обновление**. Если обновления для **Dr.Web** доступны, приложение будет отображаться в данном списке.
2. Нажмите  рядом с приложением. Обновления будут загружены и установлены на устройство. При необходимости нажмите кнопку **Принять**, чтобы разрешить доступ к необходимым для приложения функциям устройства. Для начала работы с приложением нажмите кнопку **Открыть**.

Глава 4. Приступая к работе

Данный раздел описывает процедуру запуска и выхода из **Dr.Web**, а также пользовательский интерфейс приложения.

Запуск и завершение работы приложения

Запуск приложения

Чтобы запустить **Dr.Web**, откройте экран со списком приложений и нажмите значок **Dr.Web**  .

При первом запуске приложения откроется Лицензионное соглашение, которое необходимо принять для дальнейшей работы. Кроме того, в том же окне вы можете ознакомиться с информацией о программе повышения качества ПО, а также согласиться принять в ней участие, разрешив автоматическую отправку обезличенных сведений об обнаруженных угрозах и посещаемых веб-сайтах на серверы компаний **«Доктор Веб»** и Google. Вы можете в любой момент отказаться от отправки данной статистики в настройках приложения, сняв флажок **Отправка статистики** в разделе **Общие настройки**.

Выход из приложения

1. Коснитесь нижнего края экрана и проведите пальцем вверх, чтобы свернуть приложение на главном экране.
2. Чтобы закрыть свернутое приложение, нажмите  в правом нижнем углу рамки приложения.

Интерфейс

Главный экран **Dr.Web** (см. Рисунок 2) содержит информацию о текущем состоянии защиты системы, а также осуществляет доступ к следующим функциям приложения:

- **SpIDer Guard** – позволяет включить/выключить постоянную антивирусную защиту;
- **Сканер** – выполняет проверку системы по запросу пользователя (возможны три типа проверки: быстрая, полная, выборочная);
- **Обновление** – содержит информацию о дате последнего обновления приложения и позволяет запустить обновление приложения в случае необходимости;
- **Статистика** – позволяет просмотреть статистику обнаруженных угроз и действий приложения над ними;
- **Карантин** – позволяет просмотреть и обработать угрозы, перемещенные в карантин;
- **Аудитор безопасности** – позволяет выполнить анализ системы и устранить обнаруженные проблемы безопасности и уязвимости.

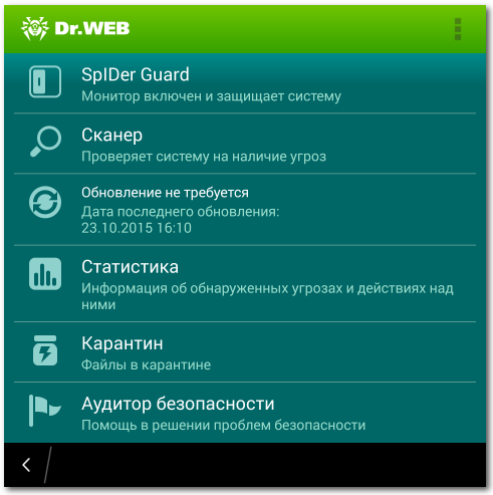


Рисунок 2. Главный экран приложения

Доступ к меню приложения и навигация по экранам

На экранах приложения, для которых доступны дополнительные опции, функция вызова меню расположена в правом верхнем углу экрана. Для возврата на главный экран используется кнопка в виде логотипа приложения в левом верхнем углу экрана.

Меню, вызванное на главном экране, позволяет перейти к настройкам приложения, открыть веб-справку, содержащую подробное описание всех его настроек и функций, а также открыть экран с информацией о приложении.

На экране с информацией о приложении вы можете ознакомиться с информацией о версии приложения, о владельце используемой лицензии и датах ее активации и окончании срока действия. Кроме того, на данном экране расположены ссылки на официальный сайт компании **«Доктор Веб»** и вашу персональную страницу на этом сайте, а также на страницы компании в социальных сетях Twitter, Facebook, ВКонтакте, Google+, Instagram, Одноклассники и канал Youtube.

Мой Dr.Web

Онлайн-сервис **Мой Dr.Web** – это ваша персональная страница на сайте компании **«Доктор Веб»**. На данной 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 данную страницу, на главном экране (см. Рисунок 2) вызовите меню приложения и выберите пункт **О программе**. На открывшемся экране нажмите **Мой Dr.Web**.

Глава 5. Функции программы

Данный раздел описывает основные возможности **Dr.Web**, позволяющие настроить антивирусную проверку и организовать защиту устройства.

Чтобы перейти на экран настроек приложения (см. Рисунок 3), на главном экране вызовите меню приложения и выберите пункт **Настройки**.

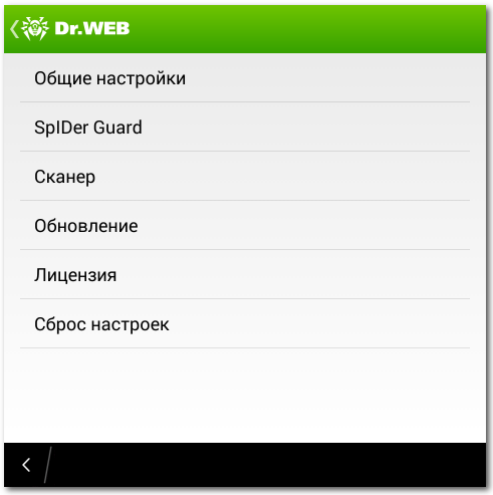


Рисунок 3. Настройки приложения

Сброс настроек

Вы можете в любой момент сбросить пользовательские настройки приложения и восстановить стандартные настройки. Для этого выполните следующие действия:

1. На экране настроек (см. Рисунок 3) в разделе **Сброс настроек** выберите пункт **Восстановить настройки**.
2. Подтвердите возврат к настройкам по умолчанию.

Постоянная антивирусная защита

Постоянная проверка файловой системы в режиме реального времени осуществляется при помощи компонента **SpIDer Guard**. Он сканирует все файлы при попытке их сохранения во внутренней памяти устройства, защищая тем самым систему от появления угроз безопасности.

Включение постоянной защиты

При первом запуске **Dr.Web** постоянная защита автоматически включается после принятия Лицензионного соглашения. Чтобы выключить или снова включить ее, нажмите на раздел **SpIDer Guard** на главном экране приложения.

При включении **SpIDer Guard** начинает защищать систему. Он продолжает работать независимо от того, запущено приложение или нет.

При обнаружении угроз безопасности будет открыт список обнаруженных угроз, который может быть закрыт только после того, как к каждой из угроз будет применено какое-либо действие. На экране блокировки отображается уведомление о найденных угрозах, при нажатии на которое будет открыт список угроз.

Работа **SpIDer Guard** будет остановлена в случае полной очистки внутренней памяти вашего устройства. В этом случае для восстановления постоянной антивирусной защиты требуется заново открыть **Dr.Web**.

Настройки SpIDer Guard

Для доступа к настройкам **Dr.Web** на главном экране вызовите меню приложения и выберите пункт **Настройки**. Чтобы настроить работу **SpIDer Guard**, на экране настроек (см. Рисунок 3) выполните следующие действия:

- чтобы включить проверку файлов в архивах, установите флажок **Файлы в архивах** в разделе **SpIDer Guard**;

По умолчанию проверка архивов выключена. 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- и *.bar-файлы в любом случае, независимо от установленного значения параметра **Файлы в архивах**.

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

Статистика

Приложение регистрирует события, связанные с работой **SpIDer Guard** (включение/выключение, результаты проверки внутренней памяти устройства, устанавливаемых приложений, обнаружение угроз безопасности). Действия приложения и, в частности, **SpIDer Guard** отображаются в разделе **Действия** на вкладке **Статистика**, отсортированные по дате.

Проверка по запросу пользователя

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

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

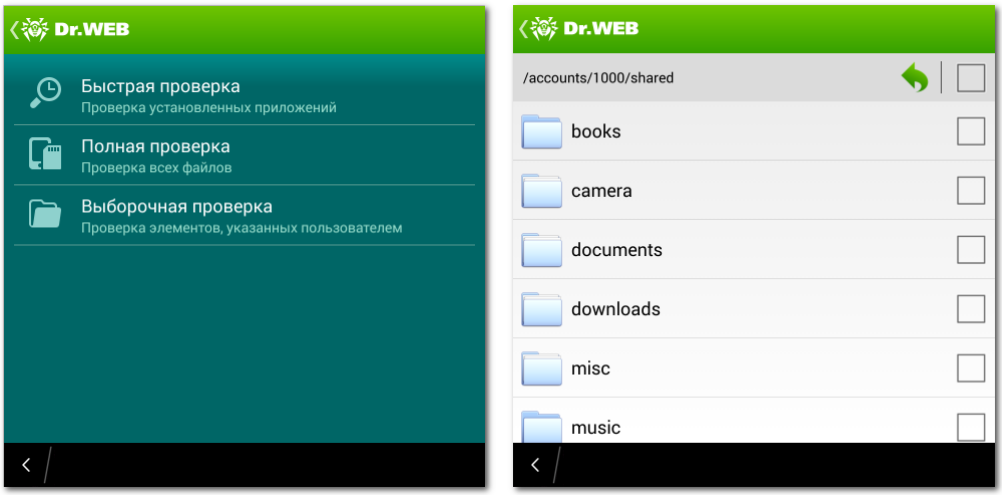
Проверка

Чтобы проверить систему, на главном экране выберите пункт **Сканер** и в открывшемся окне (см. Рисунок 4) выполните одно из следующий 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 необходимые объекты в появившемся списке объектов файловой системы (см. Рисунок 5) и нажмите кнопку **Проверить**. При выборе объектов в списке вы можете использовать расположенные над списком справа опции выбора всех элементов списка и перехода на один уровень вверх для навигации между папками.

По окончании сканирования на экран выводится список обнаруженных угроз и предлагается

выбрать действия по их обезвреживанию.



Рисунки 4 и 5. Сканер Dr.Web и окно выбора объектов сканирования

Отправка подозрительных файлов в антивирусную лабораторию «Доктор Веб»

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

1. Нажмите и удерживайте файл в списке объектов файловой системы (см. Рисунок 5), затем нажмите **Отправить в лабораторию**.
2. На следующем экране введите адрес вашей электронной почты, если вы хотите получить результаты анализа отправленного файла.
3. Выберите одну из категорий для вашего запроса:
   - **Подозрение на вирус**, если вы считаете, что файл представляет угрозу;
   - **Ложное срабатывание** или **Ложное срабатывание Origins Tracing**, если вы считаете, что файл был ошибочно отнесен к угрозам.

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

> В антивирусную лабораторию **«Доктор Веб»** могут быть отправлены ZIP-архивы, размер которых не превышает 10 МБ.

Настройки Сканера Dr.Web

Для доступа к настройкам **Сканера Dr.Web** на главном экране вызовите меню приложения, выберите пункт **Настройки**. Доступны следующие настройки:

- чтобы включить проверку файлов в архивах, установите флажок **Файлы в архивах** в разделе **Сканер**;

По умолчанию проверка архивов выключена. 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- и *.bar-файлы в любом случае, независимо от установленного значения параметра **Файлы в архивах**.

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

Статистика

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

Нейтрализация угроз

Просмотр списка угроз

В случае обнаружения угроз безопасности будет открыт список обнаруженных угроз, который может быть закрыт только после того, как к каждой из угроз будет применено какое-либо действие. На экране блокировки отображается уведомление о найденных угрозах, при нажатии на которое будет открыт список угроз.

Для каждой угрозы в списке показывается следующая информация:

- имя угрозы;
- путь к файлу, содержащему угрозу.

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

Применение действий к угрозам

Нажмите на угрозу в списке и выберите одно из доступных действий:

- **Удалить** – угроза полностью удаляется из внутренней памяти устройства;
- **В карантин** – угроза перемещается в специальную папку, где она изолируется от остальной системы;

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

- **Пропустить** – приложение не производит никаких операций над угрозой, оставляя ее нетронутой;
- **Сообщить о ложном срабатывании** – вам будет предложено отправить угрозу в антивирусную лабораторию **«Доктор Веб»** с сообщением о том, что она не представляет опасности и была ошибочно отнесена антивирусом к подозрительным объектам. Чтобы получить результаты анализа отправленного файла, укажите адрес своей электронной почты в соответствующем поле и нажмите кнопку **Отправить**.

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

Вы можете настроить звуковые оповещения об обнаружении угроз, их удалении или перемещении в карантин. Для этого на главном экране вызовите меню приложения и выберите пункт **Настройки**, после чего в разделе **Общие настройки** на экране настроек (см. Рисунок 3) установите флажок **Звук**.

Обновление

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

На главном экране приложения в разделе **Обновление** отображается дата последнего обновления вирусных баз приложения.

Обновление

1. Чтобы обновить вирусные базы, на главном экране приложения нажмите на раздел с информацией об обновлениях.
2. Обновление запустится автоматически.

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 обновляется сразу же, как только специалисты антивирусной лаборатории **«Доктор Веб»** обнаруживают новые угрозы, иногда – до нескольких раз в час.

Настройка обновлений

По умолчанию обновления загружаются в автоматическом режиме с периодичностью четыре раза в сутки. В разделе **Обновление** на экране настроек (см. Рисунок 3) вы можете разрешить/запретить использование мобильных сетей при загрузке обновлений. Чтобы не использовать при загрузке обновлений мобильные сети, установите флажок **Не использовать Мобильный интернет при загрузке обновлений**. Если активные сети Wi-Fi не будут обнаружены, вам будет предложено воспользоваться сетями 3G или GPRS. Изменение данной настройки не влияет на использование мобильных сетей остальными функциями приложения и мобильного устройства.

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

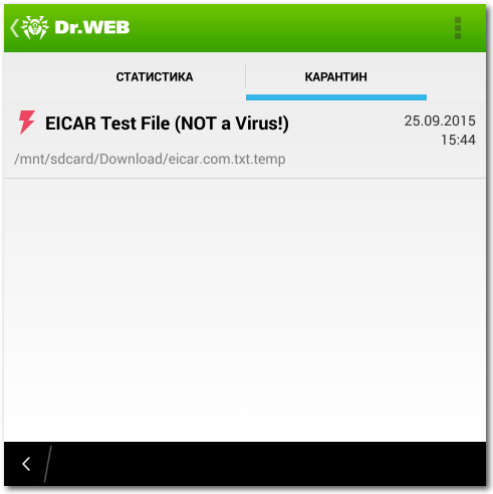
Карантин

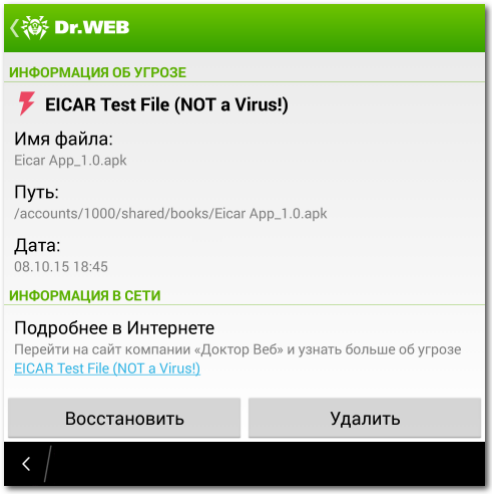
Для обнаруженных угроз в **Dr.Web** реализована функция перемещения в карантин – особую папку, предназначенную для их изоляции и безопасного хранения.

Работа с угрозами в карантине

1. Чтобы просмотреть список угроз, перемещенных в карантин, на главном экране вызовите меню приложения и выберите пункт **Карантин**.
2. Откроется список всех угроз, находящихся в карантине (см. Рисунок 6).
3. Нажав на угрозу в списке, вы можете просмотреть следующую информацию о ней (см. Рисунок 7):
   - имя файла;
   - путь к файлу;
   - дата перемещения в карантин.

   Кроме того, вы можете перейти по ссылке в разделе **Информация в сети** для просмотра более подробной информации о подобном типе угроз в Интернете на сайте компании **«Доктор Веб»**.
4. Вы можете применить к каждой угрозе одно из следующих действий:
   - **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.





Рисунки 6 и 7. Карантин

Размер карантина

Вы можете просмотреть информацию о размере памяти, занимаемой карантином, и свободном месте во внутренней памяти устройства. Для этого на вкладке **Карантин** вызовите меню приложения и выберите пункт **Размер карантина**.

Статистика

В **Dr.Web** реализовано ведение статистики обнаруженных угроз и действий приложения. Для просмотра статистики работы приложения на главном экране откройте меню приложения и

выберите пункт **Статистика**.

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

- раздел **За все время**, в котором содержится информация об общем количестве проверенных файлов, обнаруженных и обезвреженных угроз;
- раздел **Действия**, в котором содержится информация о начале/окончании проверки **Сканером Dr.Web**, включении/выключении **SpIDer Guard**, обнаруженных угрозах и действиях по их обезвреживанию. Нажмите на название угрозы, чтобы перейти к ее описанию на сайте компании **«Доктор Веб»**.

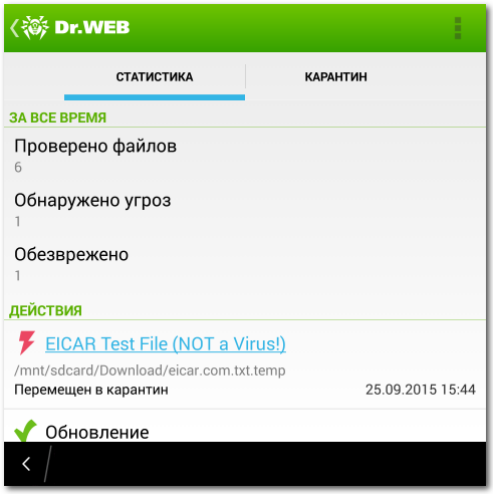


Рисунок 8. Статистика

Очистка статистики

Чтобы удалить всю собранную статистику работы приложения, вызовите меню приложения и выберите пункт **Очистить статистику**.

Журнал событий

Приложением предусмотрено ведение журнала событий, который может быть сохранен во внутренней памяти устройства для анализа в случае возникновения проблем при работе с приложением.

Чтобы сохранить журнал событий:

1. На вкладке **Статистика** вызовите меню приложения и выберите пункт **Сохранить журнал**.
2. Журнал сохраняется в файле DrWeb_Log.txt, расположенном в папке **downloads** во внутренней памяти устройства.

Помощь в решении проблем безопасности

Dr.Web позволяет провести диагностику и анализ безопасности вашего устройства и устранить выявленные проблемы и уязвимости с помощью специального компонента – **Аудитора безопасности**. Данный компонент начинает работать автоматически после первого запуска приложения и регистрации лицензии. Количество обнаруженных проблем отображается в разделе **Аудитор безопасности** на главном экране приложения.

Если в результате анализа системы **Аудитор безопасности** не обнаружит каких-либо проблем и уязвимостей, соответствующий раздел не будет отображен на главном экране приложения.

Возможные проблемы и способы их устранения

Чтобы просмотреть список обнаруженных проблем безопасности (см. Рисунок 9), нажмите на раздел **Аудитор безопасности** на главном экране приложения.

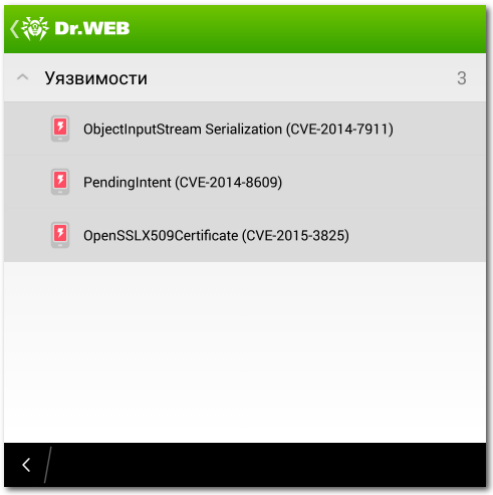


Рисунок 9. Список проблем безопасности, обнаруженных на устройстве

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

Скрытые администраторы устройства

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

Если вы не знаете, почему приложение скрывает свое присутствие в списке администраторов устройства, рекомендуем удалить его. Чтобы удалить приложение, нажмите кнопку **Удалить** на экране с подробной информацией о проблеме, связанной с данным приложением.

Уязвимости

Dr.Web позволяет обнаружить в системе устройства такие уязвимости, как Master Key (#8219321), Extra Field (#9695860), Name Length Field (#9950697), Fake ID (#13678484), ObjectInputStream Serialization (CVE-2014-7911), PendingIntent (CVE-2014-8609), Android Installer Hijacking, OpenSSLX509Certificate (CVE-2015-3825), Stagefright. Воспользовавшись данными уязвимостями, злоумышленники могут добавить программный код в ряд приложений, в результате чего данные приложения могут начать выполнять функции, представляющие угрозу безопасности устройства. **Dr.Web** также выявляет наличие в системе уязвимости Heartbleed – ошибки в криптографическом программном обеспечении OpenSSL, позволяющей злоумышленникам получить доступ к конфиденциальным данным пользователя.

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

Приложения, использующие уязвимость Fake ID

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

Приложения

Данный раздел содержит дополнительную информацию о работе с **Dr.Web**:

Приложение А. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу http://download.drweb.com/doc/;
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/show_faq/;
- посетить форумы **Dr.Web** по адресу http://forum.drweb.com/;
- задать вопрос или ознакомиться со списком часто задаваемых вопросов на вашей персональной странице Мой Dr.Web.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела http://support.drweb.com/.

Найти ближайшее к вам представительство **«Доктор Веб»** и всю контактную информацию, необходимую пользователю, вы можете по адресу http://company.drweb.com/contacts/moscow.

Предметный указатель

Предметный указатель