Dr.WEB®

Антивирус
для Symbian OS

Защити созданное

Руководство пользователя

Dr.Web для Symbian
Версия 6.00.3
Руководство пользователя
25.01.2013

«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 6

- Используемые обозначения 7
- Основные функции программы 8
- Комплектация 9

Глава 2. Лицензирование 10

- Лицензионный ключевой файл 10
- Получение ключевого файла 11
- Использование ключевого файла 13
- Продление лицензии 14

Глава 3. Установка и удаление 15

- Системные требования 15
- Установка приложения 15
- Удаление приложения 17

Глава 4. Приступая к работе 18

- Запуск и завершение программы 18
- Интерфейс 19
- Справочная система 20

Глава 5. Функции программы 21

- Постоянная антивирусная защита 21
- Проверка по запросу пользователя 23
- Нейтрализация вредоносных объектов 27
- Карантин 28
- Антиспам 29

Черные и белые списки 31

Обновление вирусных баз 33

Регистрация событий 34

Приложения 36

Приложение А. Техническая поддержка 36

Предметный указатель 37

Глава 1. Введение

Благодарим вас за выбор программы **Dr.Web для Symbian**. Данный антивирусный продукт надежно защищает телефоны и коммуникаторы, работающие под управлением операционной системы Symbian Series 60, от вирусов, созданных специально для мобильных устройств, и спама. В программе применены наиболее передовые разработки и технологии **«Доктор Веб»** по обнаружению и обезвреживанию вредоносных объектов, представляющих угрозу функционированию устройства и информационной безопасности пользователя.

Настоящее руководство призвано помочь пользователям мобильных устройств установить и настроить **Dr.Web для Symbian**, а также ознакомиться с основными функциями программы.

В приложении также представлена информация о службе технической поддержки.

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.
Знак «плюс» (+)	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Основные функции программы

Dr.Web для Symbian - это надежное антивирусное решение, обеспечивающее защиту мобильных устройств, работающих под управлением операционной системы Symbian Series 60, от различных вредоносных объектов и спама. Приложение выполняет следующие функции:

- постоянную защиту мобильного устройства в режиме реального времени;
- сканирование всей файловой системы устройства или отдельных файлов и папок по запросу пользователя;
- сканирование файлов и папок на картах памяти;
- проверка архивов и всех современных мобильных инсталляторов (zip, cab, sis, jar, rar);
- удаление обнаруженных опасных объектов или перемещение их в карантин;
- фильтрацию входящих телефонных звонков и SMS-сообщений на основе настраиваемых черного и белого списков;
- ведение детализированных отчетов о сканировании системы;
- обновление **вирусных баз Dr.Web** через интернет-соединение;
- обеспечение доступа к контекстной справке из любого окна программы.

Удобный графический интерфейс программы позволяет полностью настроить параметры ее работы с учетом требований пользователя и установить оптимальный уровень защиты мобильного устройства.

Комплектация

Dr.Web для Symbian можно приобрести как через интернет-магазин по адресу http://estore.drweb.com/, так и у официальных партнеров **«Доктор Веб»**.

Комплект поставки **Dr.Web для Symbian** включает в себя установочный файл **DrWebs60.sis** и файл с данным руководством **drweb-symbian-s60-ru.pdf**.

Глава 2. Лицензирование

Права пользователя на использование **Dr.Web для Symbian** регулируются при помощи специального файла, называемого *ключевым файлом*.

Лицензионный ключевой файл

Ключевой файл содержит, в частности, следующую информацию:

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

Существует два типа ключевых файлов:

- *Лицензионный ключевой файл*, который приобретается вместе с программой **Dr.Web для Symbian** и позволяет как пользоваться продуктом, так и получать техническую поддержку. Параметры, регулирующие права пользователя, для такого ключевого файла установлены в соответствии с пользовательским договором. В такой файл также заносится информация о пользователе и продавце продукта.
- *Демонстрационный ключевой файл*, который используется для ознакомления с продуктом. Такой ключевой файл обеспечивает полную функциональность основных компонентов, но имеет ограниченный срок действия и не предусматривает оказания поддержки.

Ключевой файл является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- ключ распространяется на все используемые программой модули;
- целостность ключа не нарушена.

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

Редактирование ключевого файла делает его недействительным! Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Получение ключевого файла

Вы можете получить лицензионный ключевой файл одним из следующих способов:

- в виде ZIP-архива по электронной почте;
- загрузив его с сервера компании **«Доктор Веб»** на мобильное устройство через Интернет-соединение, используя Менеджер лицензий;
- вместе с дистрибутивом продукта, если лицензионный файл был включен в состав дистрибутива при его комплектации;
- на отдельном носителе в виде файла с расширением .key.

Получение ключевого файла по электронной почте

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.
2. Введите регистрационный серийный номер (находится на регистрационной карточке).
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 мобильное устройство посредством программы Nokia Suite/Nokia PC Suite.

Для получения демонстрационного ключевого файла по электронной почте следует зарегистрироваться на веб-сайте http://download.drweb.com/demoreq/.

Загрузка ключевого файла на мобильное устройство

В данном случае для получения ключевого файла необходимо соединение с сетью Интернет по протоколу HTTP. Вы можете воспользоваться встроенным GPRS-модулем мобильного устройства.

В случае, если вы используете WAP-подключение, узнайте у вашего мобильного оператора о возможных ограничениях соединения и загрузки файлов.

1. В окне сообщения об отсутствии ключевого файла или в главном окне программы выберите **Функции** -> **Получить лицензию**. Запустится Менеджер лицензий.
2. Укажите тип ключевого файла, который вы хотите загрузить, выбрав соответствующий пункт в списке **Функции**.

   Вы можете загрузить лицензионный или демонстрационный ключевой файл.

   - если у вас есть серийный номер, полученный при приобретении антивируса, выберите вариант **Лицензия**;
   - если вы установили программу для ознакомительных целей, выберите вариант **Демоключ** и перейдите к шагу 4.
3. Введите серийный номер и выберите **Далее**.
4. В окне ввода личных данных, необходимых для получения ключевого файла, заполните все поля и выберите **Далее**.
5. Запустится процедура загрузки и установки ключевого файла. При необходимости, укажите точку доступа для подключения к сети Интернет.

Протокол загрузки и установки ключевого файла отображается на экране:

- если ключевой файл получен успешно, выберите **Готово** для выхода в главное окно программы;
- если в процессе получения ключевого файла возникли ошибки, в информационном окне указывается описание проблемы.

В данном случае ключ будет автоматически установлен и готов к использованию.

Дополнительную информацию о лицензировании и ключевых файлах можно найти на официальном сайте компании **«Доктор Веб»** по адресу http://www.drweb.com/.

Использование ключевого файла

Если у вас уже имеется ключевой файл, полученный по электронной почте или входящий в состав дистрибутива продукта, то для того, чтобы начать его использование, вам необходимо скопировать его в специальную папку на мобильном устройстве. Для этого вы можете воспользоваться программой Nokia Suite/ Nokia PC Suite.

Чтобы скопировать ключевой файл на устройство с установленным приложением Dr.Web для Symbian:

1. В окне сообщения приложения об отсутствии ключевого файла или в главном окне программы выберите **Функции** -> **Получить лицензию**.
2. В списке **Функции** выберите пункт **Из файла**.

3. Синхронизируйте ваше мобильное устройство с компьютером, на котором расположен ключевой файл, и с помощью программы Nokia Suite/Nokia PC Suite скопируйте ключевой файл в папку **C:\Data\DrWeb**, расположенную на мобильном устройстве.
4. Выберите **Готово** на экране мобильного устройства.

Ключевой файл будет установлен и готов к использованию.

Продление лицензии

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

Продление лицензии

Для продления лицензии воспользуйтесь процедурой получения ключевого файла. Приложение **Dr.Web для Symbian** автоматически переключится на использование нового ключевого файла.

Глава 3. Установка и удаление

Приложение **Dr.Web для Symbian** может быть установлено и удалено как с использованием программы Nokia Suite/Nokia PC Suite, так и вручную.

Системные требования

Для установки и работы **Dr.Web для Symbian** требуется, чтобы мобильное устройство работало под управлением одной из следующих операционных систем:

- Symbian 9, Series60 3rd Edition, Series60 5th Edition, Symbian[3], Symbian Belle.

Антивирус **Dr.Web для Symbian** может быть установлен только на устройствах Nokia.

Кроме того, для загрузки обновлений вирусных баз требуется соединение с сетью Интернет.

Установка приложения

Приложение **Dr.Web для Symbian** может быть установлено на ваше мобильное устройство как посредством синхронизации с компьютером с помощью программы Nokia Suite/Nokia PC Suite, так и путем запуска установочного файла непосредственно на мобильном устройстве.

Установка с помощью Nokia Suite/Nokia PC Suite

1. Для установки программы посредством Nokia Suite/Nokia PC Suite синхронизируйте ваше мобильное устройство с персональным компьютером:
   - в случае использования Nokia Suite дважды щелкните по установочному файлу приложения **DrWebs60.sis** или перетащите установочный файл на изображение устройства, на которое вы хотите произвести установку, в области устройств;
   - в случае использования Nokia PC Suite запустите мастер установки приложений, после чего укажите путь, по которому установочный файл **DrWebs60.sis** расположен на компьютере. В нижней части окна мастера установки вы можете ознакомиться с информацией об устанавливаемом приложении.

     Нажмите кнопку  для установки выбранного приложения на мобильное устройство.
2. На экране мобильного устройства откроется окно с предложением установить программу. Выберите **OK**/**Да.** В окне с информацией об устанавливаемой программе (версия программы, поставщик, сертификат) выберите **OK**/**Продолжить**.
3. Далее может открыться окно с предложением выбрать язык приложения. Вы можете выбрать один из следующих языков:
   - английский;
   - русский;
   - французский;
   - китайский (упрощенный).

   Выберите **Продолжить**.
4. На шаге **Куда установить** выберите память телефона или съемную карту для установки приложения.
5. Программа **Dr.Web для Symbian** будет установлена на мобильное устройство.

6. При использовании Nokia PC Suite по окончании установки нажмите **Готово** в окне мастера установки.

Установка программы средствами операционной системы

1. Для установки **Dr.Web для Symbian** без помощи Nokia Suite/Nokia PC Suite перенесите установочный файл программы (**DrWebs60.sis**) на мобильное устройство, например, посредством его подключения к персональному компьютеру или с помощью карты памяти.
2. Выберите в меню мобильного устройства **Средства** -> **Диспетчер приложений**. Далее выберите в списке доступных для установки приложений **Dr.Web**.
3. Перед установкой выберите **Функции** -> **Показать сведения** для просмотра информации о программе, ее поставщике и сертификате, после чего выберите **Функции** -> **Установить**.
4. Далее следуйте инструкциям по установке приложения с помощью Nokia Suite/Nokia PC Suite, начиная с шага 3.

Программа **Dr.Web для Symbian** установлена на ваше мобильное устройство. Для дальнейшей работы с приложением вам необходимо получить ключевой файл.

Удаление приложения

Приложение **Dr.Web для Symbian** может быть полностью удалено с мобильного устройства средствами операционной системы.

Удаление антивируса

1. В меню мобильного устройства выберите **Средства** -> **Диспетчер приложений**.
2. Выберите в списке установленных приложений **Dr.Web**, после чего выберите **Функции** -> **Удалить**.
3. Подтвердите удаление выбранной программы. Операционная система удалит программу с устройства.

Глава 4. Приступая к работе

Данный раздел описывает процедуру запуска и выхода из приложения **Dr.Web для Symbian**, а так же его пользовательский интерфейс и систему контекстной справки.

Запуск и завершение программы

Запуск программы

Для запуска программы откройте список установленных на мобильном устройстве приложений. В списке выберите **Dr. Web**. Откроется главное окно программы.

Выход из программы

Для завершения работы с приложением в главном окне программы (см. Интерфейс) выберите **Выйти**.

Интерфейс

Главное окно **Dr.Web для Symbian** содержит четыре раздела, предоставляющие доступ к основным функциям приложения (см. Рисунок 1):

- **Полная проверка** – запускает сканирование всей файловой системы;
- **Выборочная проверка** – позволяет выбрать отдельные файлы и папки для проверки;
- **Журналы** – позволяет просмотреть журналы регистрации событий компонентов программы, а также список файлов, помещенных в карантин;
- **Настройки** – открывает окно настроек приложения.

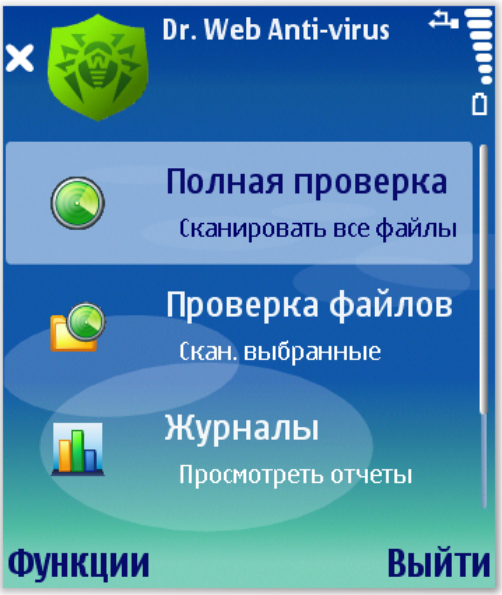

Рисунок 1. Главное окно приложения.

Кроме того, в нижней части экрана расположены кнопки **Выйти** (для выхода из программы) и **Функции** (для доступа к дополнительным функциям приложения).

Значок приложения в верхней части окна может информировать о следующем:

Изображение	Комментарий
	Отсутствует ключевой файл. Для работы **Dr.Web для Symbian** вам необходимо воспользоваться процедурой получения ключевого файла.
	Вирусные базы программы устарели. Воспользуйтесь процедурой обновления вирусных баз.

Справочная система

В программе **Dr.Web для Symbian** реализована контекстная справочная система, доступная из любого активного окна приложения.

Вызов справки

Для вызова справки в любом окне программы нажмите кнопку **Справка** или выберите **Функции** -> **Справка**. Справка откроется на описании активного окна программы.

Глава 5. Функции программы

В данном разделе описаны основные возможности программы **Dr.Web для Symbian**, позволяющие настроить антивирусную проверку, а также фильтрацию SMS-сообщений и поступающих звонков для защиты мобильного устройства от вирусов и спама.

Постоянная антивирусная защита

Основной функцией, реализованной в **Dr.Web для Symbian**, является постоянная проверка файловой системы в режиме реального времени. Она осуществляется при помощи программного средства, называемого *файловым монитором*. Он постоянно находится в памяти устройства и сканирует все файлы, к которым вы осуществляете доступ, защищая тем самым систему от появления вредоносных объектов.

Включить монитор можно в разделе **Настройки** -> **Монитор**. Для этого выберите соответствующее значение настройки **Постоянная защита**. При включении монитор сразу начинает защищать систему. Он продолжает работать независимо от того, запущено приложение или нет.

При обнаружении угроз безопасности монитором на экране мобильного устройства появляется сообщение с информацией об обнаруженных угрозах и предлагается перейти к списку угроз, чтобы выбрать действия для их обезвреживания.

Настройка монитора

Чтобы настроить работу файлового монитора, в главном окне программы выберите **Настройки**, затем выберите раздел **Монитор** в списке разделов настроек приложения (см. Рисунок 2). Вы можете настроить следующие параметры:

- включить/выключить автоматический запуск работы монитора и **Антиспама** после перезагрузки устройства. Для этого выберите соответствующее

значение настройки **Автозапуск при перезагрузке**.

- включить/выключить проверку архивов ZIP, CAB, SIS, RAR - для этого установите значения **Проверять**/**Не проверять** для соответствующих настроек;
- включить/выключить регистрацию событий в отладочном журнале событий монитора. Отладочный журнал необходимо отправить в техническую поддержку **«Доктор Веб»** в случае возникновения проблем при работе с приложением.

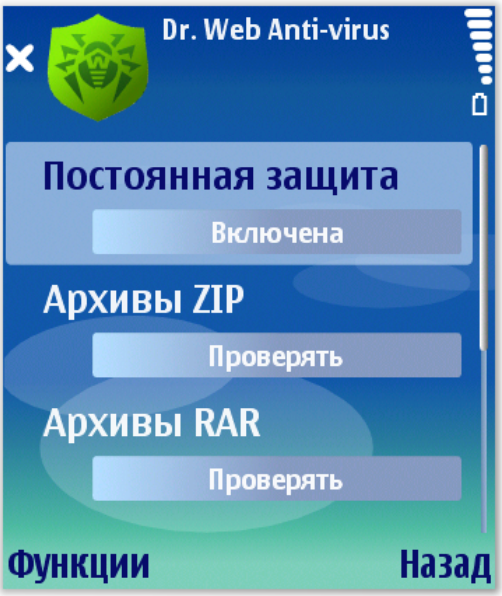

Рисунок 2. Окно настроек монитора.

Для файлового монитора в **Dr.Web для Symbian** реализована возможность просмотра статистики его работы, а также ведение журнала событий, в котором автоматически регистрируются все события, связанные с работой монитора (запуск/остановка, обнаружение угроз безопасности, невозможность проверки какого-либо файла и т.д.), отсортированные по дате.

Статистика монитора

Для доступа к статистике монитора в главном окне программы выберите **Функции** -> **Статистика монитора**. В окне статистики отображается следующая информация:

- общее количество объектов, проверенных монитором;
- количество обнаруженных угроз;
- количество обезвреженных угроз;
- количество ошибок при проверке;
- информация об вирусных базах (дата последнего обновления и количество вирусных записей);

Выберите **ОК**, чтобы закрыть окно статистики.

Просмотр журнала монитора

Для доступа к журналу выберите **Журналы** в главном окне и откройте вкладку **Монитор**.

Проверка по запросу пользователя

Проверка системы по запросу пользователя осуществляется с помощью специального компонента - *сканера*. **Dr.Web для Symbian** позволяет производить полное сканирование файловой системы мобильного устройства или проверять отдельные файлы и папки.

Сканирование

Чтобы проверить систему, в главном окне программы (см. Рисунок 1) выполните одно из следующий действий:

- чтобы запустить сканирование всех файлов системы (согласно настройкам программы), выберите **Полная проверка**;
- чтобы проверить только критические файлы и папки, выберите **Проверка файлов**, укажите необходимые объекты в появившемся списке объектов файловой системы (см. Рисунок 3). Для выделения объектов вы можете использовать опции **Выделить**/**Отменить** списка **Функции**. Затем выберите **Начать**.

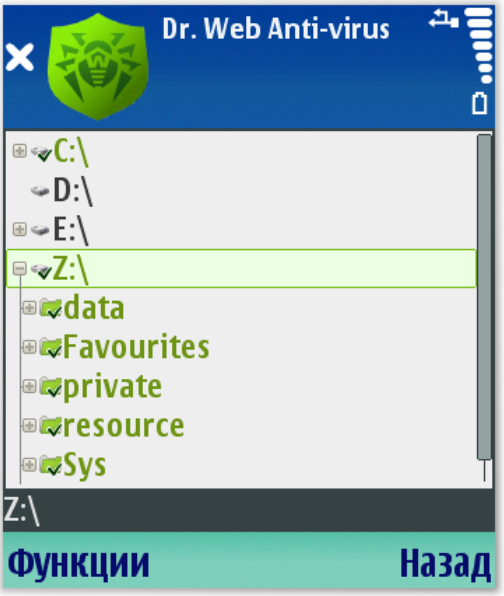

Рисунок 3. Окно выбора объектов сканирования.

В ходе сканирования на экране отображается информация об общем времени проверки, количестве и суммарном размере проверенных файлов, а также имя проверяемого в данный момент файла (при соответствующих настройках отображения, см. Рисунок 4).

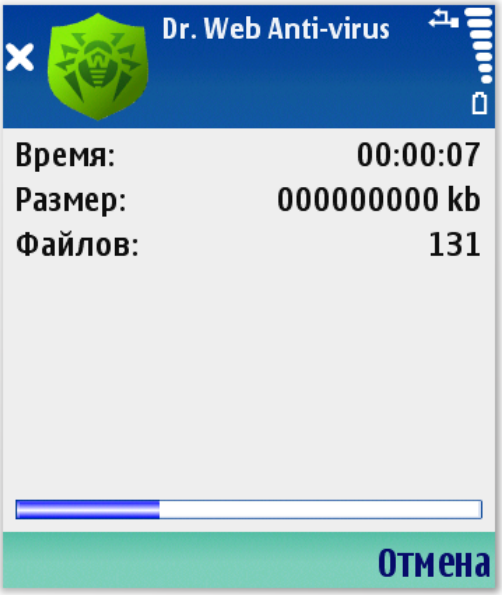

Рисунок 4. Окно проверки.

По окончании сканирования вы можете просмотреть список обнаруженных опасных объектов и выбрать варианты действий над ними (см. Нейтрализация вредоносных объектов).

Настройка сканирования

Чтобы настроить работу сканера, в главном окне программы выберите **Настройки**, затем выберите раздел **Сканер** в списке разделов настроек приложения. Вы можете изменить следующие параметры работы сканера:

- **Ошибки чтения** - позволяет записывать/не записывать ошибки чтения проверяемых файлов в журнал событий сканера;
- **Время проверки** - позволяет записывать/не записывать время начала и окончания сканирования в журнал событий сканера;

- **ROM** - отвечает за включение/выключение проверки файлов "прошивки" (программного обеспечения, встроенного в устройство производителем);
- **Карты памяти** - отвечает за включение/выключение проверки файлов и папок на картах памяти, установленных на вашем мобильном устройстве.

Кроме того, в разделе **Интерфейс** вы можете включить или отключить отображение имени проверяемого файла и общего размера проверенных файлов в окне сканирования. Для этого выберите одно из значений настройки **Проверка: инф. о файле**:

- **полная информация** - означает, что в окне проверки при сканировании будет отображаться имя проверяемого в данный момент файла, а также суммарный размер проверенных файлов;
- **частичная информация** - означает, что имя проверяемого файла и суммарный размер проверенных файлов не будут показаны.

Если для данной настройки интерфейса выбрано значение **полная информация**, скорость антивирусной проверки снижается.

Для сохранения сделанных изменений в текущем разделе и возврату к списку разделов выберите **Назад**. Для возврата к главному окну приложения выберите **Назад** в окне списка разделов настроек.

В приложении **Dr.Web для Symbian** реализовано ведение журнала событий сканера, отвечающего за антивирусную проверку устройства. В журнале регистрируются все события, связанные с работой сканера (запуск и остановка процесса сканирования, обнаружение вредоносных объектов, невозможность проверки какого-либо файла и т.д.), отсортированные по дате.

Просмотр журнала сканера

Для доступа к журналу выберите **Журналы** в главном окне и откройте вкладку **Сканер**.

Нейтрализация вредоносных объектов

По окончании полной или выборочной проверки файловой системы **Dr.Web для Symbian** предоставляет пользователю возможность выбрать одно из следующих действий по обезвреживанию вредоносных объектов:

- **Удалить** – объект полностью удаляется из памяти устройства;
- **Карантин** – опасный объект перемещается в специальную папку, где он изолируется от остальной системы.
- **Игнорировать** – объект временно пропускается и остается в файловой системе. При следующей проверке проигнорированные объекты будут обнаружены повторно.

Для того, чтобы применить необходимое действие к объектам, выберите соответствующую опцию в списке **Функции**.

Вы также можете просмотреть информацию об объекте, выделив его и выбрав **Функции** -> **Подробнее**.

Оставляйте найденные объекты в файловой системе только в том случае, если вы абсолютно уверены в том, что они не являются вредоносными.

Карантин

Для изоляции и безопасного хранения вредоносных объектов в программе **Dr.Web для Symbian** реализована функция перемещения таких объектов в карантин – особую папку, расположенную на системном диске мобильного устройства.

Обработка объектов в карантине

1. Чтобы просмотреть список объектов, перемещенных в карантин, в главном окне программы выберите **Функции** -> **Карантин**.
2. Откроется список всех объектов, находящихся в карантине (см. Рисунок 5).
3. Выберите один или несколько файлов в списке. Для выделения одного объекта или всех объектов в списке, а также для снятия выделения, вы можете воспользоваться соответствующими опциями в списке **Функции**.
4. В списке **Функции** выберите одно из следующих действий:
   - **Восстановить** – возвращает файл в ту папку, в которой он находился до перемещения (используйте данную функцию только если вы уверены, что объект безопасен);
   - **Удалить** – удаляет файл из карантина и из системы;

   Для просмотра информации об объекте из списка выделите его и выберите **Функции** -> **Подробнее**.

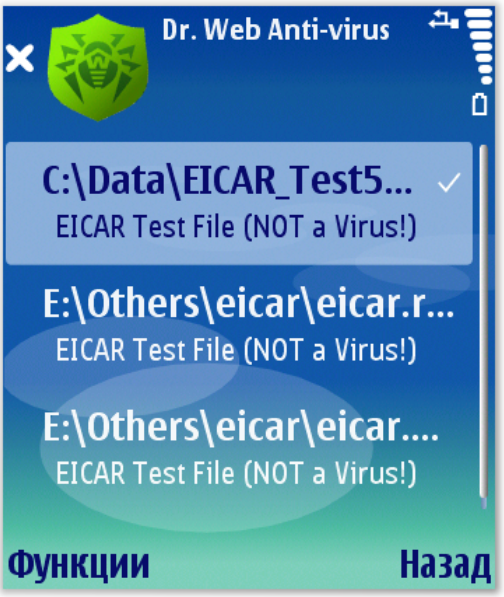

Рисунок 5. Карантин.

Антиспам

Антиспам осуществляет фильтрацию SMS-сообщений и телефонных звонков, позволяя в автоматическом или ручном режиме блокировать нежелательные сообщения и звонки, в частности, рекламные рассылки, а также звонки и сообщения с неизвестных номеров. Фильтрация сообщений осуществляется на основе черного и белого списков.

Настройка Антиспама

Чтобы настроить работу **Антиспама**, выберите пункт **Антиспам** в разделе настроек приложения, а затем выберите вкладку **Параметры**.

Вы можете настроить следующие параметры фильтрации SMS-сообщений и телефонных звонков:

- **Автозапуск при перезагрузке** - позволяет включить/выключить автоматический запуск работы **Антиспама** (фильтрации SMS и звонков) и файлового монитора после перезагрузки устройства;

Для корректной работы **Антиспама** рекомендуется установить значение **Включить** для данной настройки.

- **Адресная книга** – позволяет добавить контакты адресной книги в белый список или исключить их из списков;
- **SMS-фильтрация** – позволяет включить/выключить фильтрацию SMS-сообщений;
- **Контакт не в списках** – позволяет настроить действия программы для сообщений, поступающих с неизвестных номеров и номеров, не содержащихся в черном и белом списках. Вы можете выбрать одно из следующих значений:
  - **Запрашивать** – в этом случае при поступлении SMS с неизвестного номера или номера, не включенного в списки, на экран будет выведен запрос на получение/блокировку сообщения. В зависимости от выбранного действия для полученного сообщения пользователю будет предложено добавить отправителя в белый или черный список соответственно;
  - **По белому списку** – в данном случае будут приняты только сообщения с номеров, содержащихся в белом списке. Все остальные сообщения будут блокированы;

- **По черному списку** – в данном случае будут приняты все сообщения, кроме сообщений с номеров, содержащихся в черном списке.

- **Фильтрация звонков** – позволяет включить/выключить фильтрацию поступающих звонков;
- **Тип фильтра звонков** – позволяет определить метод фильтрации звонков:
  - **По белому списку** – в данном случае будут приняты только звонки с номеров, содержащихся в белом списке. Все остальные звонки будут блокированы;
  - **По черному списку** – в данном случае будут приняты все звонки, кроме звонков, поступающих с номеров из черного списка.
- **Блокировка звонков** – позволяет блокировать звонки с ответом или без ответа на них. В случае блокировки звонка без ответа звонок будет сброшен, в случае блокировки с ответом произойдет снятие трубки, после чего звонок будет сразу же завершен;
- **Номер не определен** – позволяет блокировать/пропускать звонки, номера которых не определяются.

Все события, связанные с фильтрацией сообщений и работой **Антиспама** (запуск и остановка работы компонента, информация об отфильтрованных сообщениях и звонках и т.д.), регистрируются программой **Dr.Web для Symbian** в журнале **Антиспама**.

Просмотр журнала Антиспама

Для доступа к журналу выберите **Журналы** в главном окне программы и откройте вкладку **SMS**.

Черные и белые списки

Создание и редактирование черного и белого списков осуществляется на соответствующих вкладках раздела **Настройки** -> **Антиспам**.

Добавление контакта в список

1. В разделе **Антиспам** откройте вкладку списка, в который вы хотите добавить новый контакт.
2. Выберите **Функции** -> **Добавить**, далее выберите одну из следующих опций:
   - **Номер** – в данном случае вы можете вручную ввести данные добавляемого контакта: в поле **Контакт** укажите телефонный номер или мнемоническое имя контакта;
   - **Контакт** – в данном случае вы можете выбрать контакт из адресной книги вашего мобильного устройства, например в случае, если у контакта имеется несколько номеров, и вы хотите внести все эти номера в выбранный список;
   - **Группа** – в данном случае вы можете выбрать группу из адресной книги вашего мобильного устройства.

   В поле **Описание** вы можете ввести любую информацию и комментарии о добавляемом контакте или группе.
3. Выберите **Сохранить**. Контакт будет добавлен в выбранный список.

Черный список имеет больший приоритет, поэтому если номер занесен и в черный, и в белый список, то сообщения с этого номера будут блокироваться.

Редактирование данных контакта/группы из списка

1. Выделите контакт/группу в соответствующем списке и выберите **Функции** -> **Редактировать**;
2. Измените значения полей данных контакта/группы;
3. Выберите **Сохранить**.

Удаление контакта/группы из списка

- Выделите контакт/группу в соответствующем списке и выберите **Функции** -> **Удалить**. Подтвердите удаление в открывшемся окне.

Обновление вирусных баз

Для обнаружения вредоносных объектов программа **Dr.Web для Symbian** использует специальные **вирусные базы Dr.Web**, в которых содержится информация обо всех информационных угрозах для мобильных устройств, известных специалистам **«Доктор Веб»**. Так как появляются новые вредоносные программы, то базы требуют периодического обновления. Для этого в программе реализована система обновления вирусных баз через Интернет. Модуль обновления **Dr.Web для Symbian** позволяет загружать и устанавливать новые вирусные базы приложения.

Для обновления необходимо соединение с сетью Интернет по протоколу HTTP. Вы можете воспользоваться встроенным GPRS-модулем мобильного устройства.

В случае, если вы используете WAP-подключение, узнайте у вашего мобильного оператора о возможных ограничениях соединения и загрузки файлов.

Обновление вирусных баз программы

1. Чтобы обновить вирусные базы, в главном окне программы выберите **Функции** -> **Обновить**. Откроется окно модуля обновления.
2. Чтобы начать процесс обновления, выберите **Функции** -> **Обновить**.
3. По окончании загрузки и установки обновлений выберите **Готово**, чтобы закрыть окно модуля обновления.

Проверить версию программы, а также версию и дату создания вирусных баз можно в окне информации приложения **Dr.Web для Symbian**.

Получение информации о программе

Чтобы открыть окно с информацией о **Dr.Web для Symbian**, в главном окне программы выберите **Функции** -> **О программе**.

Регистрация событий

Все события, связанные с работой **Dr.Web для Symbian**, а также настройки основных компонентов хранятся в специальных файлах, расположенных на мобильном устройстве в папке C:\Data\DrWeb (см. табл. 1). Доступ к данной папке осуществляется с помощью программы Nokia Suite/Nokia PC Suite.

Таблица 1. Конфигурационные файлы и журналы регистрации событий Dr.Web для Symbian.

Имя файла	Комментарий
DrWeb.dat	Файл настроек антиспама
DrWebScanner.dat	Файл настроек сканера
DrwScannerLog.txt	Файл журнала сканера
DrWebMonLog.txt	Файл журнала монитора
DrwServerLog.txt	Файл журнала антиспама
DrwGetKeyLog.txt	Файл журнала загрузки ключевых файлов
DrwUpdaterLog.txt	Файл модуля обновления вирусных баз

Вы можете сохранить файлы настроек сканера и антиспама на компьютере, например, для возможности использования сохраненных настроек после переустановки приложения.

Файлы журналов также могут быть сохранены на компьютере для их просмотра и для отправки в техническую поддержку компании «Доктор Веб» при возникновении неполадок.

Файлы DrwGetKeyLog.txt и DrwUpdaterLog.txt служат только для отправки в техническую поддержку, так как все сообщения в них находятся в специальном техническом формате.

Приложения

Приложение А. Техническая поддержка

Страница службы технической поддержки **«Доктор Веб»** находится по адресу http://support.drweb.com/.

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/;
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/;
- попытаться найти ответ в базе знаний Dr.Web по адресу http://wiki.drweb.com/;
- посетить форумы Dr.Web по адресу http://forum.drweb.com/.

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

Предметный Указатель

D

Dr.Web для Symbian 6
- антиспам 29
- запуск 18
- интерфейс 19
- карантин 28
- комплект поставки 9
- лицензирование 10
- начало работы 18
- обновление 33
- регистрация событий 34
- системные требования 15
- справка 20
- удаление 15, 17
- установка 15
- функции 8, 21

А

антивирусная проверка 21, 23
антиспам
- журнал 29
- настройка 29
- списки контактов 31

Б

белый список 31

В

введение 6
вирусная проверка 21, 23
вирусные базы
- обновление 33

вызов справки 20

Д

демострационный ключевой файл 10

Ж

журнал
- антиспама 29
- монитора 21
- сканера 23

З

завершение программы 18
запуск программы 18

И

интерфейс 19

К

карантин 27, 28
ключевой файл
- действительность 10
- использование 13
- обновление 14
- получение 11, 12
- продление 14

комплектация 9
коплект поставки 9

Предметный Указатель

Л

лицензионный ключевой файл 10
- обновление 14
- получение 11
- продление 14

лицензирование 10

лицензия
- действительность 10
- использование 13
- обновление 14
- получение 11
- продление 14

М

монитор 21

Н

настройка
- антиспама 29
- монитора 21
- сканирования 23

нейтрализация вирусов 27

О

о программе 33

обновление
- вирусных баз 33
- лицензии 14

основные функции 8

П

получение ключевого файла 11

получение справки 20

постоянная защита
- настройка 21
- регистрация событий 21

приложения
- техническая поддержка 36

приступая к работе 18

проверка
- выборочная 23
- на вирусы 23
- на спам 29
- полная 23

продление лицензии 14

Р

регистрация событий 34
- антиспам 29
- монитор 21
- сканер 23

С

системные требования 15

сканирование
- настройка 23
- регистрация событий 23

списки контактов 31

справочная система 20

Предметный Указатель

Т

техническая поддержка 36

требования 15

У

удаление 15, 17

условные обозначения 7

установка 15

Ф

файл ключа 10

функции программы 21

Ч

черный список 31