Dr.WEB®

# Антивирус для Windows Mobile

Защити созданное

## Руководство пользователя

**Dr.Web® для Windows Mobile**
**Версия 6.00.1**
**Руководство пользователя**
**02.11.2011**

«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

# 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 справке. |
| **Зеленое и полужирное начертание** | Наименования продуктов компании **«Доктор Веб»** или их компонентов. |
| Зеленое и подчеркнутое начертание | Ссылки на страницы справки и веб-сайты. |
| `Моноширинный шрифт` | Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением. |
| *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 плюса | Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT. |
| Восклицательный знак | Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях. |

# Глава 1. Введение

Благодарим вас за выбор программы **Антивирус Dr.Web® для Windows Mobile** (далее **Антивирус Dr.Web**). Данный антивирусный продукт надежно защищает КПК и коммуникаторы, работающие под управлением операционной системы Microsoft® Windows Mobile®, от различных вирусных угроз, созданных специально для инфицирования мобильных устройств. В программе применены наиболее передовые разработки и технологии компании **«Доктор Веб»** по обнаружению и обезвреживанию вредоносных объектов, которые могут представлять угрозу функционированию устройства и его информационной безопасности.

Настоящее руководство призвано помочь пользователям мобильных устройств при установке и настройке **Антивируса Dr.Web® для Windows Mobile**, а также ознакомить пользователей с основными функциями программы. В приложениях представлена информация о других продуктах компании **«Доктор Веб»** и о службе технической поддержки.

# Основные функции программы

**Антивирус Dr.Web** представляет собой надежное антивирусное решение для пользователей мобильных устройств, работающих под управлением операционной системы Microsoft Windows Mobile. Приложение защищает устройства от информационных угроз и выполняет следующие функции:

- непрерывной защиты файловой системы устройства в режиме реального времени (проверка открываемых файлов, устанавливаемых программ, вложений во входящих электронных письмах и т.д.);
- сканирования файловой системы устройства или отдельных файлов и папок по запросу пользователя;
- сканирования архивов;
- удаления обнаруженных опасных объектов или перемещение их в карантин;
- фильтрации телефонных звонков и сообщений на основе предустановленных и настраиваемых пользовательских профилей фильтрации;
- обновления антивирусных баз **Dr.Web** через интернет-соединение;
- ведения отчетов о работе файлового монитора, проверках по запросу пользователя и фильтра звонков и сообщений;
- обеспечения доступа к контекстной справке из любого окна программы.

Удобный графический интерфейс программы позволяет полностью настроить параметры работы приложения с учетом нужд пользователя.

# Системные требования

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

- Microsoft® Windows Mobile® 2003
- Microsoft® Windows Mobile® 2003 Second Edition
- Microsoft® Windows Mobile® 5.0
- Microsoft® Windows Mobile® 6.0
- Microsoft® Windows Mobile® 6.1
- Microsoft® Windows Mobile® 6.5

**Антивирус Dr.Web** работает только на телефонах и коммуникаторах, поддерживающих управление через сенсорный экран.

# Комплектация

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

Комплект поставки **Антивируса Dr.Web® для Windows Mobile** включает в себя установочный файл drweb-wince-ru.msi, архив drweb-wince-ru-arm.cab, файл с данным руководством drweb-wince-ru.pdf.

# Глава 2. Лицензирование

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

## Получение ключевого файла

При работе в режиме централизованной защиты ключевой файл автоматически загружается с сервера и регистрируется программой при подключении **Агента** и не хранится локально на мобильном устройстве в виде файла.

Если у вас есть действующая лицензия на **Антивирус Dr.Web® для Windows**, **Dr.Web® Security Space**, **Dr.Web® Бастион для Windows**, **Антивирус Dr.Web® для Windows+Linux** или **Комплект Dr.Web «Малый бизнес»**, то вы можете использовать существующий ключевой файл для работы **Антивируса Dr.Web® для Windows Mobile**.

Вы также можете получить ключевой файл после регистрации продукта на официальном сайте компании **«Доктор Веб»** по адресу http://products.drweb.com/register/ или воспользовавшись процедурой получения ключевого файла.

### Получение ключевого файла

Для получения ключевого файла необходимо соединение с сетью Интернет по протоколу HTTP. Вы можете воспользоваться встроенным GPRS-модулем мобильного устройства или синхронизировать устройство через инфракрасный порт, Bluetooth, Wi-Fi или USB+ActiveSync/Центр устройств Windows Mobile с любым компьютером, имеющим подключение к сети Интернет.

1. Выполните одно из следующих действий:
   - в окне сообщения оповещения об отсутствии ключевого файла, нажмите **Регистрация**;
   - в главном окне программы выберите **Меню**, а затем **Получить ключ**.
2. Выберите тип ключевого файла, который вы хотите получить:
   - если у вас имеется регистрационный серийный номер, выданный вам при приобретении антивируса, выберите вариант **Лицензионный ключ**;
   - если вы устанавливаете программу с ознакомительными целями, выберите **Демоключ** и перейдите к шагу 4.
3. Введите серийный номер и нажмите кнопку **Далее**.
4. В окне ввода личных данных, необходимых для получения ключевого файла, заполните все поля и нажмите кнопку **Далее**.
5. Запускается процедура загрузки и установки ключевого файла. Протокол ее работы отображается в информационном окне:
   - если ключевой файл получен успешно, в информационном окне указывается путь размещения полученного ключевого файла;
   - если в процессе получения ключевого файла возникли ошибки, в информационном окне указывается описание проблемы.

# Глава 3. Установка и удаление

**Антивирус Dr.Web** может быть установлен и удален как с использованием программы ActiveSync/Центра устройств Windows Mobile, так и вручную.

## Установка с помощью синхронизации

Если для синхронизации вашего устройства с компьютером вы используете программу ActiveSync/Центр устройств Windows Mobile, то установку **Антивируса Dr.Web** можно осуществить следующим образом:

1. Синхронизируйте устройство, на которое требуется произвести установку, с вашим персональным компьютером посредством программы ActiveSync/Центра устройств Windows Mobile.
2. Запустите файл drweb-wince-ru.msi.

В случае работы **Dr.Web® для Windows Mobile** в режиме централизованной защиты, чтобы не проходить авторизацию на сервере вручную после установки, вы можете создать и запустить конфигурационный bat-файл, который должен находиться в одном каталоге с файлом drweb-wince-ru.msi. Конфигурационный файл имеет следующую структуру:

```
msiexec.exe /i drweb-wince-ru.msi SERVER="10.3.0.76"
ID="c00a76b5-d11d-b211-aaad-e409beb1d587"
PASS="12345678"
```

Укажите IP-адрес сервера централизованной защиты, идентификатор и пароль, полученные у администратора антивирусной сети.

Если вы запустили установку с помощью bat-файла, не закрывайте уведомление о процессе установки на персональном компьютере до полного завершения установки **Dr.Web® для Windows Mobile**.

3. Откроется окно мастера установки. Нажмите кнопку **Далее.**
4. Укажите папку на компьютере, в которую вы хотите записать файлы, необходимые для установки **Антивируса Dr.Web** на устройство. Для этого введите путь к папке в соответствующем поле или нажмите кнопку **Обзор**, выберите необходимую папку и нажмите кнопку **ОК**. Ниже при помощи переключателя выберите, кому будет доступна установка программы. Нажмите **Далее** для продолжения.
5. Появится окно, в котором говорится, что мастер установки готов установить программу. Если вам необходимо изменить какие-либо настройки мастера, то нажмите кнопку **Назад**. Если вы хотите начать установку, то нажмите **Далее**.
6. После окончания копирования файлов в указанную папку откроется окно программы ActiveSync/Центра устройств Windows Mobile **Установка и удаление программ** и начнется установка **Антивируса Dr.Web** на устройство.
7. На экране карманного компьютера появится окно с ходом установки программы.

8. Программа попытается запустить *монитор*. Однако без действующего ключевого файла запуск данного компонента невозможен. На экране карманного компьютера появится предупреждение о невозможности запуска монитора. Нажмите кнопку **Закрыть**, чтобы закрыть это предупреждение, или кнопку **Регистрация**, чтобы перейти к процедуре получения ключевого файла.
9. По окончании нажмите кнопку **ОК**.
10. Для дальнейшей работы с приложением перенесите необходимый ключевой файл в папку установки **Антивируса Dr.Web** или воспользуйтесь процедурой получения ключевого файла, если у вас нет действительного ключевого файла.

# Установка без синхронизации

Для установки **Антивируса Dr.Web** без использования синхронизации с компьютером сделайте следующее:

1. Скопируйте архив drweb-wince-ru-arm.cab на устройство, подключив его к вашему персональному компьютеру либо воспользовавшись картой памяти.
2. Запустите скопированный файл на устройстве.
3. На экране карманного компьютера появится окно с ходом установки программы.
4. Программа попытается запустить *монитор*. Однако без действующего ключевого файла запуск данного компонента невозможен. На экране карманного компьютера появится предупреждение о невозможности запуска монитора. Нажмите кнопку **Закрыть**, чтобы закрыть это предупреждение, или кнопку **Регистрация**, чтобы перейти к процедуре получения ключевого файла.
5. По окончании нажмите кнопку **ОК**.
6. Для дальнейшей работы с приложением перенесите необходимый ключевой файл в папку установки **Антивируса Dr.Web** или воспользуйтесь процедурой получения ключевого файла, если у вас нет действительного ключевого файла.

В случае работы **Dr.Web® для Windows Mobile** в режиме централизованной защиты, необходимо пройти авторизацию на Сервере. Чтобы не проходить авторизацию вручную после установки, вы можете скопировать конфигурационный файл agent.cfg на защищаемое устройство в директорию установки приложения \Program Files\DrWeb перед началом установки. Файл agent.cfg имеет следующую структуру:

SERVER = 10.3.0.76 ID = c01e2b55-d21d-b211-8d64-dc0d9c68edba PASS = 12345678

Укажите IP-адрес сервера централизованной защиты, идентификатор и пароль, полученные у администратора антивирусной сети.

# Повторная установка и удаление

С использованием программы ActiveSync/Центра устройств Windows Mobile вы можете восстановить поврежденную установку или полностью удалить **Антивирус Dr.Web** с устройства.

### Удаление и восстановление антивируса с помощью ActiveSync/Центра устройств Windows Mobile

1. Синхронизируйте устройство с вашим персональным компьютером с использованием программы ActiveSync/ Центра устройств Windows Mobile.
2. Выполните одно из следующих действий:
   - запустите установочный файл drweb-wince-ru.msi и выберите тип операции;
   - в главном окне программы ActiveSync выберите пункт **Установка и удаление программ** в меню **Сервис** на панели инструментов, а затем в открывшемся окне установите/снимите флажок **Doctor Web, Ltd. Dr. Web Anti-virus** в списке установленных программ и нажмите кнопку **OK**.

- в главном окне Центра устройств Windows Mobile наведите курсор мыши на надпись **Программы и службы**, затем во всплывающем меню щелкните по ссылке **Дополнительно** и нажмите кнопку **Установка и удаление программ**. В открывшемся окне снимите флажок **Doctor Web, Ltd. Dr.Web Anti-virus** в списке установленных программ и нажмите кнопку **ОК**.

3. При удалении антивируса, программа предупредит вас о том, что приложение **Антивирус Dr.Web® для Windows Mobile** будет удалено. Нажмите кнопку **ОК** для продолжения.

Если на персональном компьютере, с которым синхронизировано ваше устройство, программа ActiveSync не установлена, то вы можете удалить **Антивирус Dr.Web** вручную при помощи средств операционной системы Microsoft Windows Mobile.

### Удаление антивируса средствами операционной системы

1. В меню **Пуск** операционной системы устройства выберите пункт **Настройки** и переключитесь на вкладку **Система**.
2. Запустите утилиту **Удаление программ**, в списке установленных программ выберите **Dr.Web Anti-virus** и нажмите кнопку **Удалить**. Операционная система удалит **Антивирус Dr.Web** с устройства.

# Глава 4. Приступая к работе

Данный раздел описывает процедуру запуска и выхода из **Антивируса Dr.Web**, а также его пользовательский интерфейс и систему контекстной справки.

## Запуск и выход из программы

**Антивирус Dr.Web** по умолчанию устанавливается в папку \Program Files\DrWeb.

### Запуск программы

Выполните одно из следующих действий:

- чтобы запустить **Антивирус Dr.Web**, нажмите на значок файла DrWeb.exe, расположенный в каталоге установки;
- чтобы запустить **Антивирус Dr.Web** не открывая Проводник файловой системы, выберите пункт **Программы** в меню **Пуск** и в открывшемся окне нажмите на значок программы **Dr.Web Anti-virus**.

### Перевод в фоновый режим

Чтобы перевести приложение в фоновый режим и вернуться к работе с устройством, нажмите кнопку выхода из программы в верхнем правом углу. Приложение не выгружается из памяти.

### Выход из программы

Чтобы завершить работу с приложением, нажмите кнопку **Выход** в главном окне программы (см. Интерфейс). Приложение выгружается из памяти.

Для повторного запуска приложения или вывода приложения из

фонового режима вы можете воспользоваться значком программы **Dr.Web Anti-virus** в разделе недавно запущенных программ меню **Пуск**. При первом запуске **Антивирус Dr.Web** открывается на главном окне. При повторной активации приложения оно открывается на последнем активном окне, из которого приложение было переведено в фоновый режим.

# Интерфейс

Главное окно **Антивируса Dr.Web** состоит из трех кнопок, предоставляющих 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;
- **Настройки** – открывает окно настроек приложения.


**Рисунок 1. Главное окно приложения.**

В панели инструментов в нижней части главного окна находятся кнопки **Выход** (для завершения работы приложения) и **Меню** (для доступа к основному меню приложения).

Внешний вид интерфейса приложения можно настроить, изменяя параметры шрифта. Размер шрифта для текста в устройстве настраивается в разделе **Экран** настроек операционной системы и по умолчанию не влияет на размер текста в приложении.

## Настройки интерфейса

1. Чтобы размер текста в **Антивирусе Dr.Web** зависел от настроек операционной системы, установите флажок **Использовать системный размер шрифта** на вкладке **Интерфейс** настроек приложения (см. Рисунок 2).
2. Здесь же, вы можете включить функцию ClearType, сглаживающую края шрифтов. Для этого установите соответствующий флажок.
3. При необходимости измените язык интерфейса.

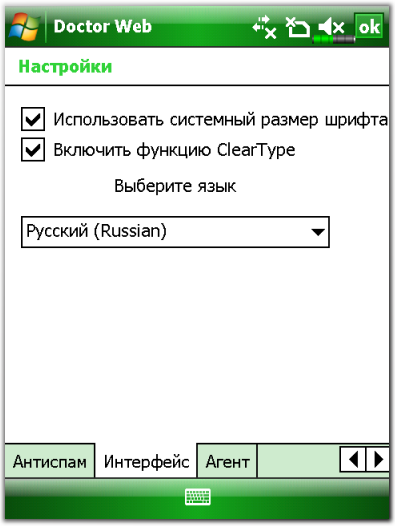


**Рисунок 2. Окно Настройки. Вкладка Интерфейс.**

# Справочная система

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

### Вызов справки

Для вызова справки зайдите в меню **Пуск** и выберите пункт **Справка**.

# Режим работы

**Антивирус Dr.Web** может функционировать в сети, контролируемой **Центром Управления Dr.Web**. Для антивирусной защиты в таком централизованном режиме вам не потребуется устанавливать дополнительные программные модули или удалять установленный **Антивирус Dr.Web**.

В режиме централизованной защиты дополнительно осуществляются следующие функции:

- обновление и настройка компонентов антивирусного пакета **Dr.Web** согласно инструкциям, полученным из **Центра Управления Dr.Web**, а также передача результатов выполнения заданий **Центру Управления Dr.Web**;
- загрузка лицензионного ключа и управление правами для настройки компонентов программы и включения/выключения **Монитора**;
- передача **Центру Управления Dr.Web** сообщений о возникновении заранее оговоренных событий (например, обнаружение инфицированных объектов, запуск **Сканера** и т.п.) в работе программы.

В режиме централизованной защиты пользователь может осуществлять следующие действия:

- запускать при необходимости сканирование компьютера;
- изменять настройки отдельных компонентов **Антивируса Dr.Web**, в том числе, отключать режим централизованной защиты.

Для подключения к антивирусной сети используется специальный модуль - **Агент**. Включить и настроить работу **Агента** можно на вкладке **Агент** (см. Рисунок 3) настроек программы.

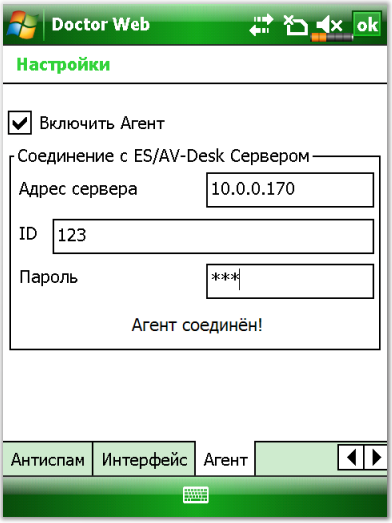


**Рисунок 3. Окно Настройки. Вкладка Агент.**

## Настройка режима централизованной защиты

1. Обратитесь к администратору антивирусной сети компании или IT-провайдера за параметрами подключения к **Центру Управления Dr.Web** (серверу централизованной защиты).
2. На вкладке **Агент** установите флажок **Включить Агент**.
3. В разделе **Соединение с ES/AV-Desk Сервером** введите IP-адрес сервера, укажите идентификатор и пароль, полученные у администратора антивирусной сети.

4. **Агент** получит настройки и права, указанные на сервере. Далее **Агент** будет работать вне зависимости от наличия соединения с **Центром Управления Dr.Web**.

В режиме централизованной защиты значения параметров сервера Administration\Configure Dr.Web Enterprise Server\Compression и Administration\Configure Dr.Web Enterprise Server\Encryption должны быть **No** или **Possible**. Если значение любого из этих параметров будет **Yes**, то соединение с сервером установлено не будет.

## Просмотр журнала Агента

Для доступа к журналу нажмите кнопку **Меню** в главном окне и выберите пункт **Журнал событий Агента**.

# Глава 5. Функции программы

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

В случае работы в режиме централизованной защиты настройки программы доступны только при наличии у пользователя прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.

## Постоянная антивирусная защита

Основной функцией, реализованной в **Антивирусе Dr.Web**, является постоянная проверка файловой системы в режиме реального времени. Это достигается 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.

По умолчанию **Монитор** автоматически активируется при установке и сразу начинает защищать файловую систему вашего устройства. Он продолжает работать независимо от того, запущено приложение или нет. Признаком активности монитора является значок **Монитора**  в нижней части экрана **Сегодня**. Нажав на данный значок, вы можете перейти к окну статистики файлового монитора.

Для файлового монитора в **Антивирусе Dr.Web** реализована возможность просмотра статистики его работы, а также журнал событий **Монитора**, в котором автоматически регистрируются все события, связанные с его работой, отсортированные по дате.

### Просмотр статистики Монитора

Выполните одно из следующих действий:

- нажмите кнопку **Меню** в главном окне программы и выберите пункт **Статистика Монитора**;
- если доступно, на командной панели экрана **Сегодня** (начальный экран) нажмите значок **Монитора**  .

### Просмотр журнала Монитора

Для доступа к журналу нажмите кнопку **Меню** в главном окне программы и выберите пункт **Журнал событий Монитора**.

### Настройка монитора

Чтобы настроить монитор, на вкладке **Монитор** окна настроек приложения (см. Рисунок 4) выполните следующие действия:

- чтобы отключить файловый монитор, откройте окно **Настройки** и снимите флажок **Включить монитор** на вкладке **Монитор**;
- чтобы настроить добавление в журнал событий **Монитора** записей о начале и окончании его работы, а также о неудавшихся проверках, установите соответствующие флажки в группе **События** в журнале монитора;
- чтобы настроить проверку файлов в архивах определенных типов, выберите соответствующие флажки в группе **Скан.файлы в архивах**.

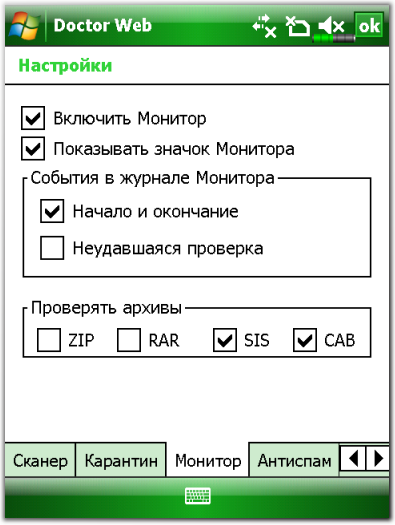


**Рисунок 4. Окно Настройки. Вкладка Монитор.**

# Проверка по запросу пользователя

**Антивирус Dr.Web** позволяет производить полное сканирование файловой системы или проверять отдельные файлы и папки по запросу пользователя. При этом по умолчанию проверяются файлы, расположенные на съемных носителях (картах памяти устройства), включая файлы в архивах.

В приложении реализовано ведение журнала событий **Сканера**, отвечающего за проверку устройства по запросу пользователя, в котором регистрируются все события, связанные с его работой (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 нажмите кнопку **Меню** в главном окне и выберите пункт **Журнал событий Сканера**.

### Настройка сканера

Чтобы настроить **Сканер**, на вкладке **Сканер** окна настроек приложения (см. Рисунок 5) выполните следующие действия:

- чтобы включить проверку файлов на карте памяти, установить флажок **Проверять файлы на картах памяти**;
- чтобы включить проверку файлов "прошивки" (программного обеспечения, встроенного в устройство производителем), установите флажок **Проверять файлы "прошивки"**;
- чтобы настроить регистрацию записей о начале и окончании работы **Сканера** в журнале событий **Сканера**, а также о неудавшихся проверках, установите соответствующие флажки в группе настроек **События в журнале сканера**;
- чтобы настроить проверку файлов в архивах определенных типов, выберите соответствующие флажки в группе настроек **Проверять архивы**.

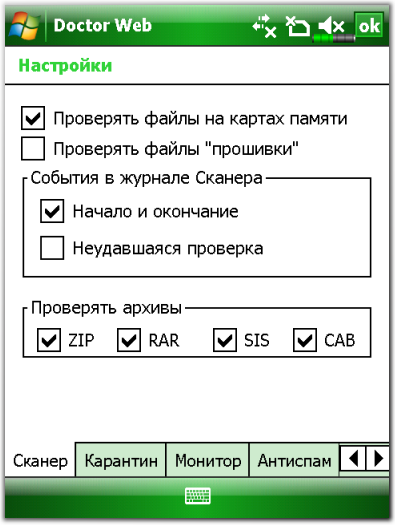


**Рисунок 5. Окно Настройки. Вкладка Сканер.**

Настоятельно рекомендуется периодически пользоваться функцией сканирования файловой системы, например, на случай если **Монитор** какое-то время был неактивен.

## Сканирование

Чтобы провести сканирование системы, в главном окне программы (см. Рисунок 1) выполните одно из следующий действий:

- чтобы запустить сканирование всех файлов системы, нажмите кнопку **Полная проверка**;
- чтобы проверить только критические файлы и папки, нажмите кнопку **Выборочная проверка**, выберите необходимые объекты в появившемся списке объектов файловой системы (см. Рисунок 6) и нажмите кнопку **Старт**.

По окончании сканирования на экран выводится отчет об обнаруженных опасных объектах и предлагаются варианты действий над ними.

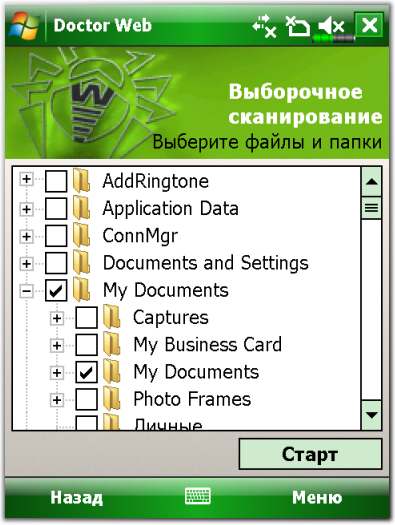


**Рисунок 6. Окно выбора объектов сканирования.**

# Нейтрализация вредоносных объектов

**Антивирус Dr.Web** предоставляет пользователю выбор из двух действий по обезвреживанию вредоносных объектов:

- **Удаление** – объект полностью удаляется из памяти устройства;
- **Карантин** – опасный объект перемещается в специальную папку, где он изолируется от остальной системы.

Помимо действий по обезвреживанию, вы можете выбрать действие **Игнорирование**, при котором приложение не производит никаких операций над опасным объектом, оставляя его нетронутым.

При обнаружении вредоносного объекта файловым монитором на экране устройства сразу появляется окно, предлагающее пользователю выбрать действие, которое следует предпринять по отношению к объекту. Сканер предлагает выбор действий для обнаруженных объектов только после окончания сканирования.

# Антиспам

**Антиспам** осуществляет фильтрацию 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 предустановленных и пользовательских профилей фильтрации.

В приложении реализовано ведение журнала событий компонента **Антиспам**, отвечающего за фильтрацию звонков и сообщений. В журнале регистрируются все события, связанные с фильтрацией (запуск и остановка **Антиспама**, блокирование звонков и сообщений и т.д.), отсортированные по дате.

## Просмотр журнала Антиспама

Для доступа к журналу нажмите кнопку **Меню** в главном окне и выберите пункт **Журнал событий Антиспама**.

## Настройка Антиспама

Чтобы настроить работу компонента **Антиспам**, на вкладке **Антиспам** окна настроек приложения (см. Рисунок 7) выполните следующие действия:

1. Чтобы включить фильтры входящих SMS/MMS-сообщений и/или звонков, в разделе настроек **Входящие** установите флажки **Включить фильтр SMS/MMS** и/или **Включить фильтр звонков** соответственно.
2. Выберите профиль фильтрации в выпадающем списке. Вы можете выбрать один из предустановленных профилей - **Блокировать всё**, **Блокировать по чёрному списку**, **Пропускать номера из Контактов**, или же

пользовательский профиль.

3. Чтобы включить фильтр исходящих SMS-сообщений, в разделе настроек **Исходящие** установите флажок **Включить фильтр SMS**. В данном случае при отправке сообщения будет выдаваться запрос для подтверждения/запрета передачи.
4. Чтобы разрешить передачу SMS-сообщений на номера из списка Контакты без подтверждения, установите флажок **Пропускать Контакты**.
5. Создайте список исключений для фильтра исходящих сообщений.

Для устройств, работающих под управлением операционных систем Windows Mobile 2003 или Windows Mobile 2003 SE, при выборе профилей фильтрации **Пропускать номера из Контактов** в разделе **Входящие** и/или **Пропускать Контакты** в разделе **Исходящие**, в случае изменения данных контактов телефонной книги, расположенных в памяти телефона, необходимо в настройках **Антивируса Dr.Web** открыть вкладку **Антиспам** и нажать кнопку **ОК**, чтобы сделанные изменения были учтены при фильтрации звонков и сообщений.

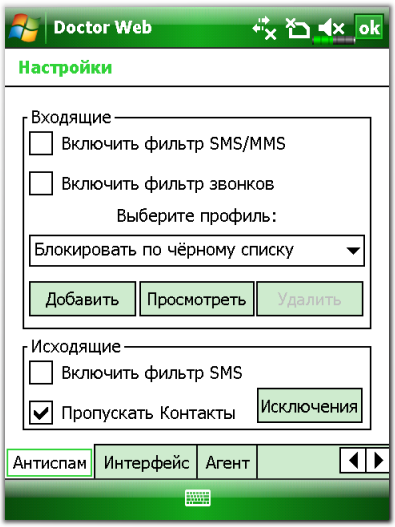


**Рисунок 7. Окно Настройки. Вкладка Антиспам.**

## Профили фильтрации входящих звонков и сообщений

Для фильтрации входящих звонков и сообщений предусмотрены следующие профили:

- **Блокировать всё** - при выборе данного профиля все входящие звонки и сообщения будут заблокированы;
- **Блокировать по чёрному списку** - при выборе данного профиля все входящие звонки и сообщения с номеров из черного списка будут заблокированы. При этом, звонки и сообщения с других номеров будут пропущены.
- **Пропускать номера из Контактов** - при выборе данного профиля будут пропущены только входящие звонки и сообщения с номеров из списка Контакты.

## Создание пользовательского профиля

Помимо предустановленных неизменяемых профилей, **Антивирус Dr.Web** предоставляет возможность создания неограниченное количество пользовательских профилей фильтрации, для каждого из которых может быть задан отдельный список номеров и определены действия программы для входящих звонков и сообщений с номеров из данного списка.

Чтобы создать новый профиль, нажмите кнопку **Добавить** под списком выбора профилей фильтрации. Откроется окно **Новый профиль**. Введите имя профиля и определите способ фильтрации при выборе данного профиля:

- **Использовать как белый список** - чтобы принимать все звонки и сообщения с номеров из списка профиля;
- **Добавить в черный список** - для того, чтобы звонки и сообщения с номеров из списка данного профиля были заблокированы дополнительно к звонкам и сообщениям с номеров из черного списка.

## Просмотр и редактирование черного списка и списков пользовательских профилей

Чтобы просмотреть черный список/список номеров пользовательского профиля фильтрации:

- в разделе **Входящие** выберите в выпадающем списке профиль **Блокировать по черному списку** или соответствующий пользовательский профиль;
- нажмите кнопку **Просмотреть**.

Чтобы добавить номер в черный список/список номеров пользовательского профиля фильтрации:

- в окне профиля нажмите кнопку **Добавить**;
- введите телефонный номер и комментарий для добавляемого номера;
- нажмите кнопку **ОК**. Номер будет добавлен в список.

Чтобы отредактировать данные для номера из черного списка/списка пользовательского профиля:

- в окне профиля нажмите кнопку **Изменить**;
- в окне **Редактирование** измените телефонный номер и/или комментарий к нему;
- нажмите кнопку **ОК**.

Чтобы удалить номер из черного списка/списка пользовательского профиля:

- выберите номер в списке в окне профиля;
- нажмите кнопку **Удалить**.

### Фильтрация исходящих сообщений

При включении фильтра исходящих SMS-сообщений перед отправкой сообщения будет выдаваться запрос на подтверждение/запрет передачи. Если на вашем устройстве включена функция Антивора, то для гарантированной передачи SMS-сообщений с информацией о телефоне в случае его потери или кражи требуется отключить фильтрацию.

Вы можете создать список номеров, на которые SMS-сообщения будут отправлены без подтверждения передачи независимо от настроек фильтра исходящих сообщений. Для этого выполните следующие действия:

1. Чтобы настроить список исключений фильтра, на вкладке **Антиспам** нажмите кнопку **Исключения** в разделе **Исходящие**.
2. Чтобы добавить номер в список исключений:
   - в окне **Пропускать номера** нажмите кнопку **Добавить**;
   - введите телефонный номер и комментарий для добавляемого номера;
   - нажмите кнопку **ОК**. Номер будет добавлен в список.
3. Чтобы отредактировать данные для номера из списка исключений:
   - в окне **Пропускать номера** нажмите кнопку **Изменить**;

- в окне **Редактирование** отредактируйте телефонный номер и/или комментарий к нему;
- нажмите кнопку **ОК**.

4. Чтобы удалить номер из списка исключений:
   - в окне **Пропускать номе**ра выберите номер в списке;
   - нажмите кнопку **Удалить**.

# Обновление антивирусных баз

Для обнаружения вредоносных объектов **Антивирус Dr.Web** использует специальные **антивирусные базы Dr.Web**, в которых содержится информация обо все информационных угрозах для мобильных устройств, известных специалистам компании **«Доктор Веб»**. Так как могут появляться новые вредоносные программы, то эти базы требуют периодического обновления. Для этого в приложении реализована система обновления антивирусных баз через Интернет. Помимо антивирусных баз, модуль скачивает и устанавливает обновления самой программы.

## Обновление

1. Чтобы обновить программу, в главном окне нажмите кнопку **Меню** и выберите пункт **Обновление**.
2. В открывшемся окне обновления нажмите кнопку **Старт**.

Для обновления необходимо соединение с сетью Интернет по протоколу HTTP. Вы можете воспользоваться встроенным GPRS-модулем мобильного устройства или синхронизировать устройство через инфракрасный порт, Bluetooth, Wi-Fi или USB+ActiveSync/Центр устройств Windows Mobile с любым компьютером, имеющим подключение к сети Интернет.

Проверить версию программы, а также версию и дату создания антивирусных баз можно в окне информации **Антивируса Dr. Web**.

### Получение информации о программе

Чтобы открыть окно с информацией об **Антивирусе Dr. Web**, в главном окне программы нажмите кнопку **Меню** и выберите пункт **О программе**.

## Работа с карантином

Для изоляции и безопасного хранения вредоносных объектов, в **Антивирусе Dr.Web** реализована функция перемещения таких объектов в карантин – особую папку, по умолчанию расположенную в каталоге установки приложения (\Program Files\DrWeb\Quarantine). Путь к карантину можно изменить.

### Изменение папки карантина

1. Чтобы изменить путь к папке карантина, нажмите кнопку **Обзор** на вкладке **Карантин** настроек приложения (см. Рисунок 8).
2. Выберите нужную папку.
3. Выберите опцию **Путь к папке карантина**.

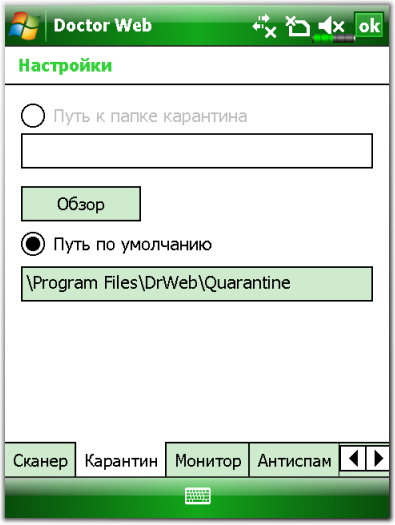


**Рисунок 8. Окно Настройки. Вкладка Карантин.**

## Обработка объектов в карантине

1. Чтобы просмотреть список объектов, перемещенных в карантин, в главном окне программы нажмите кнопку **Меню** и выберите пункт **Карантин**.
2. Откроется окно со списком всех объектов, находящихся в карантине (см. Рисунок 9).
3. Нажмите одну из следующих кнопок, чтобы применить соответствующее действие к выбранным файлам:
   - **Восстановить** – возвращает файл в ту папку, в которой он находился до перемещения (пользуйтесь данной функцией только, если вы уверены, что объект безопасен);
   - **Удалить** – удаляет файл из карантина и из системы;
   - **Закрыть** – закрывает окно **Карантин**.

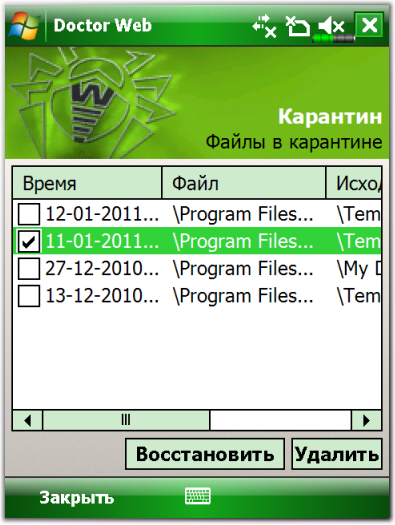


**Рисунок 9. Окно Карантин.**

# Приложения

## Приложение А. Режим централизованной защиты

**Dr.Web® для Windows Mobile** может функционировать в сети, контролируемой **Центром Управления Dr.Web**. Организация централизованной антивирусной защиты позволяет автоматизировать и упростить настройку и управление информационной безопасностью компьютеров, объединенных в единую логическую структуру (например, компьютеры одной компании, расположенные как внутри локальной сети, так и вне ее). Защищаемые компьютеры объединяются в единую *антивирусную сеть*, безопасность которой контролируется и управляется администраторами с центрального сервера (**Центра Управления Dr.Web**). Подключение к системам централизованной защиты позволяет получить гарантированно высокий уровень защиты компьютера при минимальных усилиях со стороны конечных пользователей.

### Взаимодействие компонентов антивирусной сети

Решения компании **«Доктор Веб»** по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (Рисунок 10).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз безопасности и спама *локальными антивирусными компонентами* (клиентами; в данном случае – **Dr.Web® для Windows Mobile**), которые обеспечивают антивирусную защиту и упрощают соединение с сервером централизованной защиты.

Обновление и конфигурация локальных компонентов производится через *центральный сервер*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты.

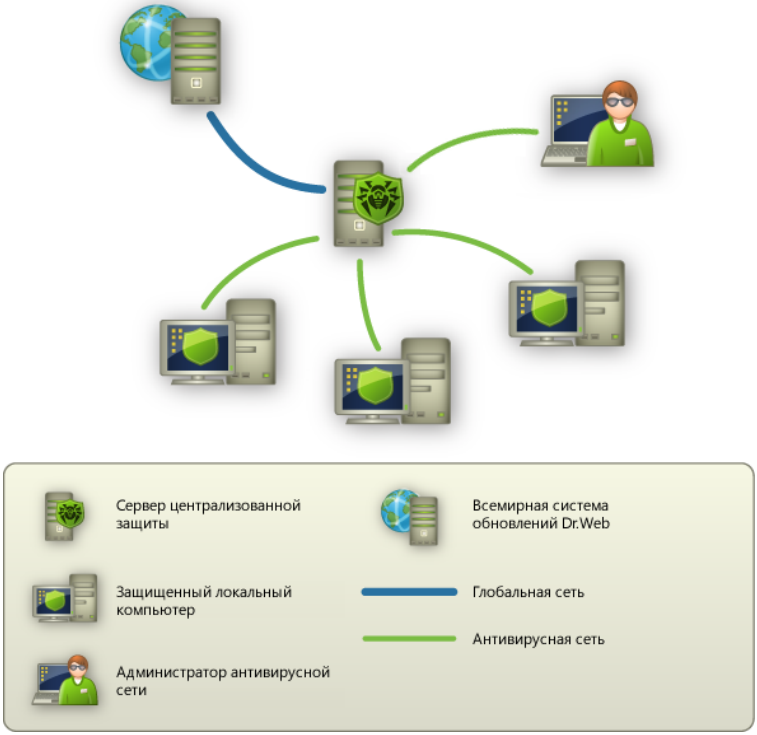


**Рисунок 10. Логическая структура антивирусной сети.**

Все необходимые обновления на сервер централизованной защиты загружаются с сервера **Всемирной системы обновлений Dr. Web**.

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется антивирусным сервером по указанию *администраторов антивирусной сети*. Администраторы управляют конфигурацией центрального сервера и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также при необходимости задают настройки работы конкретных локальных антивирусных компонентов.

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

# Предметный Указатель

# Предметный Указатель

# Предметный Указатель

## У



## Ф



## Ц



## Ч