Dr.WEB®

Антивирус
для серверов Windows

Защити созданное

Руководство администратора

Dr.Web® Антивирус для серверов Windows
Версия 6.0
Руководство администратора
01.12.2010

«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

Dr.Web® Антивирус для серверов Windows обеспечивает многоуровневую защиту системной памяти, жестких дисков и сменных носителей от проникновений вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и различных вредоносных объектов из любых внешних источников. Важной особенностью программы **Dr.Web Антивирус для серверов** является его модульная архитектура. **Dr.Web Антивирус для серверов** использует программное ядро и вирусные базы, общие для всех компонентов и различных сред. В настоящее время, наряду с **Dr.Web Антивирус для серверов**, поставляются версии антивируса для IBM® OS/2®, Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Andorid®, Symbian®, а также ряда систем семейства Unix® (например, Linux® и FreeBSD®).

Dr.Web использует удобную и эффективную процедуру обновления вирусных баз и версий программного обеспечения через Интернет.

Dr.Web способен также обнаруживать и удалять с компьютера различные нежелательные программы (рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы, программы взлома). Для обнаружения нежелательных программ и действий над содержащими их файлами применяются стандартные средства антивирусных компонентов **Dr.Web**.

Dr.Web Антивирус для серверов может включать в себя следующие компоненты:

- **Dr.Web Сканер для Windows** – антивирусный сканер с графическим интерфейсом. Программа запускается по запросу пользователя или по расписанию и производит антивирусную проверку компьютера. Существуют также версии программы с интерфейсом командной строки (**Консольные сканеры для Windows**);
- **SpIDer Guard® для Windows** – антивирусный сторож, (называемый также монитором). Программа постоянно

находится в оперативной памяти, осуществляя проверку файлов и памяти «на лету», а также обнаруживая проявления вирусной активности;

- **Dr.Web Модуль автоматического обновления** – позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов **Dr.Web**, а также производит их автоматическую установку;
- **SpIDer Agent** – модуль управления, с помощью которого осуществляется запуск и настройка компонентов программы **Dr.Web Антивирус для серверов**.

Для организации централизованного управления антивирусной защитой в масштабе предприятия поставляется специальное средство – **Dr.Web® Enterprise Suite** (см. Приложение E).

Для провайдеров интернет-услуг защиту их клиентов от вирусов и спама обеспечивает **Dr.Web® AV-Desk** (см. Приложение F).

О чем эта документация

Настоящее руководство администратора содержит необходимые сведения по установке и эффективному использованию программы **Dr.Web® Антивирус для серверов Windows**.

Подробное описание всех элементов графического интерфейса содержится в справочной системе, доступной для запуска из любого компонента программы.

Настоящее руководство содержит подробное описание процесса установки **Dr.Web**, а также начальные рекомендации по его использованию для решения наиболее типичных проблем, связанных с вирусными угрозами. В основном рассматриваются наиболее стандартные режимы работы компонентов программы **Dr.Web Антивирус для серверов** (настройки по умолчанию).

В Приложениях содержится подробная справочная информация по настройке **Dr.Web**, предназначенная для опытных пользователей.

В связи с постоянным развитием, интерфейс программы может не совпадать с предоставленными в данном документе изображениями. Всегда актуальную справочную информацию вы можете найти по адресу http://products.drweb.com.

Используемые обозначения и сокращения

В данном руководстве используются обозначения, приведенные в таблице 1.

Таблица 1. 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 **«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 плюс («+»)	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.

Системные требования

Перед установкой **Dr.Web** следует:

- удалить с компьютера другие антивирусные пакеты для предотвращения возможной несовместимости их резидентных компонентов с резидентными компонентами **Dr.Web**;
- установить все рекомендуемые производителем операционной системы критические обновления.

Использование программы **Dr.Web Антивирус для серверов** возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
Операционная система	Одна из следующих: • Microsoft® Windows® 2000 Server с пакетом обновлений SP4 и Update Rollup 1; • Microsoft® Windows Server® 2003 с пакетом обновлений SP1; • Microsoft® Windows Server® 2008. Поддерживаются 32- и 64-битные версии операционных систем. Возможно, потребуется загрузить с сайта Microsoft и установить обновления ряда системных компонентов. **Dr.Web Антивирус для серверов** сообщит вам, при необходимости, их наименования и URL.
Место на жестком диске	Не менее 275 МБ свободного дискового пространства для установки всех компонентов **Dr.Web**, из них: • до 80 МБ занимает установочный файл; • до 97 МБ занимают временные файлы, которые будут автоматически удалены после завершения установки.
Процессор	Поддерживающий систему команд i686 и старше.

Компонент	Требование
Оперативная память	512 МБ и больше.
Прочее	Подключение к сети Интернет для обновления вирусных баз и компонентов программы **Dr.Web Антивирус для серверов**.

Проверка антивируса

Вы можете проверить работоспособность антивирусных программ, обнаруживающих вирусы по их сигнатурам, с использованием тестового файла EICAR (European Institute for Computer Anti-Virus Research).

Многими разработчиками антивирусов принято для этой цели использовать одну и ту же стандартную программу test.com. Эта программа была специально разработана для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении вируса. Программа test.com не является сама по себе вредоносной, но специально обрабатывается большинством антивирусных программ как вирус. **Dr.Web® Антивирус для серверов Windows** называет этот «вирус» следующим образом: `EICAR Test File (Not a Virus!)`. Примерно так его называют и другие антивирусные программы.

Программа test.com представляет собой 68-байтный COM-файл, в результате исполнения которого на консоль выводится текстовое сообщение EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

Файл test.com состоит только из текстовых символов, которые формируют следующую строку:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Если вы создадите файл, содержащий приведенную выше строку и сохраните его под именем test.com, то в результате получится программа, которая и будет описанным выше «вирусом».

SpIDer Guard в оптимальном режиме не определяет тестовый файл EICAR как вредоносную программу, так как он является DOS-приложением, которое не представляет угрозы для компьютера.

Лицензирование

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

Для работы программы **Dr.Web Антивирус для серверов** вам необходимо получить и установить ключевой файл.

Дополнительную информацию о сроках и типах лицензирования можно найти на официальном сайте **«Доктор Веб»** по адресу http://www.drweb.com/.

Ключевой файл

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

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование антивируса;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать антивирус).

Dr.Web Антивирус для серверов использует *лицензионный ключевой файл*, который позволяет как пользоваться продуктом, так и получать техническую поддержку. Параметры этого ключевого файла, регулирующие права пользователя, установлены в соответствии с пользовательским договором. В такой файл также заносится информация о пользователе и продавце продукта.

Ключевой файл **Dr.Web** 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 **Dr.Web Антивирус для серверов** перестает обнаруживать и обезвреживать вредоносные программы.

Получение ключевого файла

Ключевой файл поставляется в виде файла с расширением .key или в виде ZIP-архива, содержащего этот файл.

Получение ключевого файла в процессе регистрации на сайте

Регистрация на сайте и загрузка ключевого файла осуществляется по сети Интернет. Перед началом установки убедитесь, что ваш компьютер имеет действующее интернет-соединение.

Для получения лицензионного ключевого файла необходим регистрационный серийный номер продукта.

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.
2. Заполните форму со сведениями о покупателе.
3. Введите регистрационный серийный номер (находится на регистрационной карточке).
4. Сформированный ключевой файл высылается по электронной почте в виде ZIP-архива, содержащего файл с расширением .key. Также вы можете загрузить архив со страницы регистрации.

5. После получения ключевого файла установите его на вашем компьютере.

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты ключевого файла. При повторной регистрации необходимо указать те же персональные данные, которые вы ввели при первой регистрации. Допускается использовать другой адрес электронной почты – в таком случае ключевой файл будет выслан по новому адресу.

Количество запросов на получение ключевого файла ограничено – регистрация с одним и тем же серийным номером допускается не более 25 раз. Если это число превышено, ключевой файл не будет выслан. В этом случае обратитесь в службу технической поддержки (в запросе следует подробно описать ситуацию, указать персональные данные, введенные при регистрации, и серийный номер). Ключевой файл будет выслан вам службой технической поддержки по электронной почте.

Продление лицензии

В некоторых случаях, например, при окончании срока действия лицензии или при изменении характеристик защищаемой системы или требований к ее безопасности, вы можете принять решение о приобретении новой или расширенной лицензии на **Dr.Web Антивирус для серверов**. В таком случае вам потребуется заменить уже существующий и зарегистрированный в системе лицензионный ключевой файл. **Dr.Web Антивирус для серверов** поддерживает обновление лицензии «на лету», при котором не требуется переустанавливать антивирус или прерывать его работу.

Замена ключевого файла

1. Чтобы продлить лицензию, используйте Менеджер лицензий. Для приобретения новой или продления текущей лицензии вы также можете воспользоваться вашей персональной страничкой на официальном сайте компании **«Доктор Веб»**, которая открывается в окне интернет-браузера по умолчанию при выборе пункта **Мой Dr.Web** как в **Менеджере лицензий**, так и в меню SpIDer Agent.
2. Если текущий ключевой файл недействителен, **Dr.Web Антивирус для серверов** переключится на использование нового ключевого файла.

Глава 2. Установка программы

Перед установкой программы **Dr.Web Антивирус для серверов** настоятельно рекомендуется:

- установить все критические обновления, выпущенные компанией Microsoft для вашей версии операционной системы (их можно загрузить и установить с сайта обновлений компании по адресу http://windowsupdate.microsoft.com);
- проверить при помощи системных средств файловую систему и устранить обнаруженные дефекты;
- закрыть активные приложения.

Перед установкой **Dr.Web** следует удалить с компьютера другие антивирусные пакеты для предотвращения возможной несовместимости их резидентных компонентов.

Установка программы Dr.Web® Антивирус для серверов Windows

В данном разделе описывается установка программы **Dr.Web Антивирус для серверов** на компьютеры, работающие под управлением одной из следующих операционных систем:

- Microsoft® Windows® 2000 Server с пакетом обновлений SP4 и Update Rollup 1;
- Microsoft® Windows Server® 2003 с пакетом обновлений SP1;
- Microsoft® Windows Server® 2008.

Поддерживаются 32- и 64-битные версии операционных систем.

Первая установка программы Dr.Web Антивирус для серверов

Для установки **Dr.Web** необходимы права Администратора.

Установка программы **Dr.Web Антивирус для серверов** возможна в двух режимах:

1. В фоновом режиме.
2. В обычном режиме.

Установка в фоновом режиме

Для запуска установки **Dr.Web** в фоновом режиме, в командной строке введите имя исполняемого файла с необходимыми параметрами (параметры влияют на ведение отчета и перезагрузку после окончания установки):

Установка	Параметры
Без перезагрузки и без ведения отчёта	/S /V/qn
С перезагрузкой и без ведения отчёта	/S /V"/qn REBOOT=Force" или /S /V"/qn REBOOT=F"
Без перезагрузки и с ведением отчёта	/S /V"/qn /lv*\"<*путь*>\drweb-setup.log\""
С перезагрузкой и с ведением отчёта	/S /V"/qn /lv*\"<*путь*>\drweb-setup.log\" REBOOT=F" или /S /V"/qn /lv*\"<*путь*>\drweb-setup.log\" REBOOT=Force"

Например, при запуске следующей команды:

```
C:\Documents and Settings\drweb-600-winsrv-x86
/S       /V"/qn       /lv*\"%temp%\drweb-setup.
log\"REBOOT=F"
```

будет проведена установка программы **Dr.Web Антивирус для серверов**, создан файл отчета и проведена перезагрузка после установки.

Если необходимо установить **Dr.Web Антивирус для серверов** на определённом языке, то дополнительно необходимо задать следующий параметр:

/L<*код_языка*>

Например,

```
/L1049 /S /V"/qn REBOOT=Force"
```

Список языков:

Код	Язык
1033	английский
1026	болгарский
1038	венгерский
1032	греческий
1034	испанский
1040	итальянский
1028	китайский (традиционный)
2052	китайский (упрощённый)
1062	латышский
1063	литовский
1031	немецкий
1045	польский

Код	Язык
2070	португальский
1049	русский
1051	словацкий
1055	турецкий
1058	украинский
1036	французский
1061	эстонский

Независимо от выбранного языка будет дополнительно установлен английский язык.

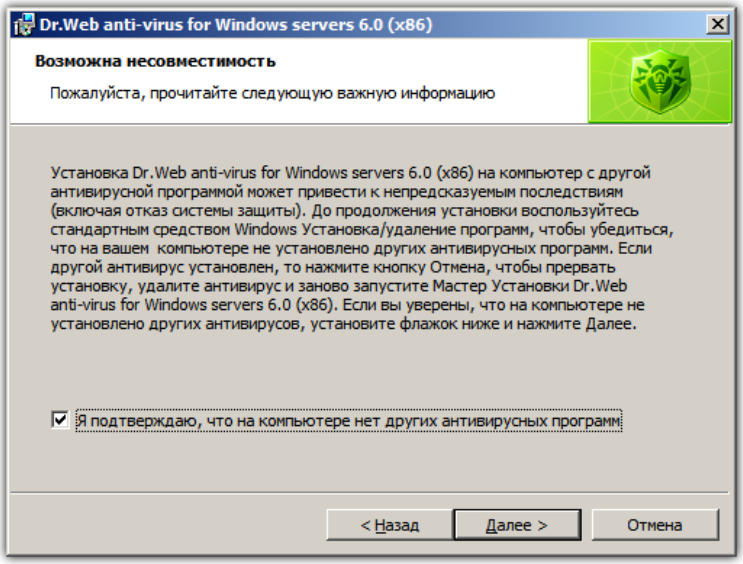
Установка в обычном режиме

Следуйте указаниям программы установки. На любом шаге до начала копирования файлов на компьютер вы можете выполнить следующее:

- чтобы вернуться к предыдущему шагу программы установки, нажмите кнопку **Назад**;
- чтобы перейти на следующий шаг программы, нажмите кнопку **Далее**;
- чтобы прервать установку, нажмите кнопку **Отмена**.

Процедура установки:

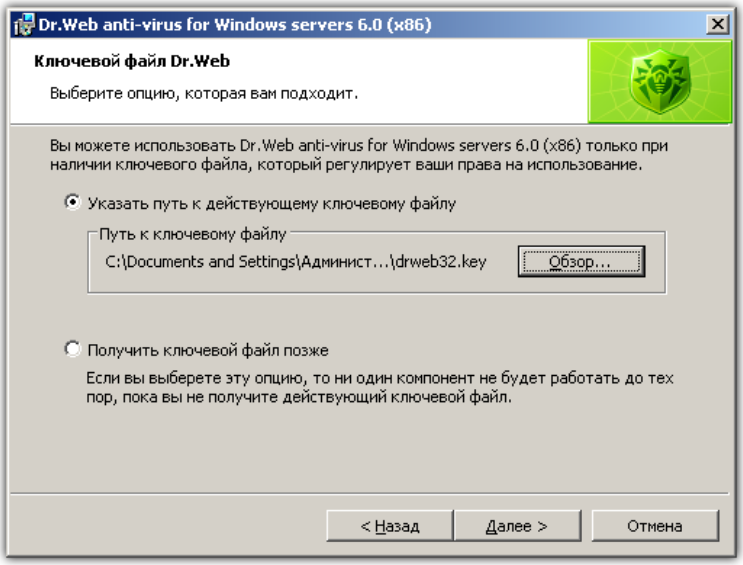
1. На первом шаге выберите язык установки, который будет использоваться в интерфейсе. Независимо от вашего выбора дополнительно будет установлен английский язык.
2. На следующем шаге ознакомьтесь с лицензионным соглашением. Для продолжения установки его необходимо принять.
3. На следующем шаге программа установки предупредит вас о возможной несовместимости программы **Dr.Web Антивирус для серверов** и иных антивирусов, установленных на вашем компьютере, и предложит удалить их. Выполните одно из следующих действий:
   - если на вашем компьютере установлены другие антивирусы, то рекомендуется нажать кнопку **Отмена** и прервать установку, удалить или дезактивировать эти антивирусы и после этого начать установку заново;
   - если на вашем компьютере не установлены другие антивирусы, для продолжения установите флажок **Я подтверждаю, что на компьютере нет других антивирусных программ** и нажмите кнопку **Далее**.



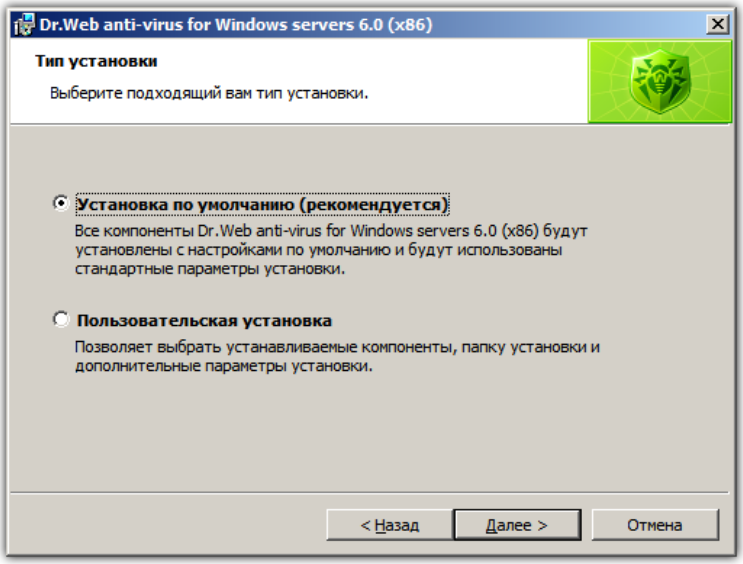
4. На шаге **Ключевой файл Dr.Web** программа установки предупредит вас о том, что для работы **Dr.Web** необходим лицензионный ключевой файл. Выполните одно из следующих действий:
   - если у вас есть ключевой файл, и он находится на жестком диске или сменном носителе, нажмите кнопку **Обзор** и выберите ключевой файл в стандартном окне открытия файла;
   - для продолжения установки без ключевого файла выберите **Получить ключевой файл позднее**. В этом случае ни один компонент программы не будет работать до тех пор, пока вы не укажете действующий ключевой файл.

   Нажмите кнопку **Далее**.

Используйте только ключевой файл варианта **Dr.Web Антивирус для серверов**. Ключевой файл должен иметь расширение .key. Если файл находится в архиве, необходимо извлечь его соответствующим архиватором.

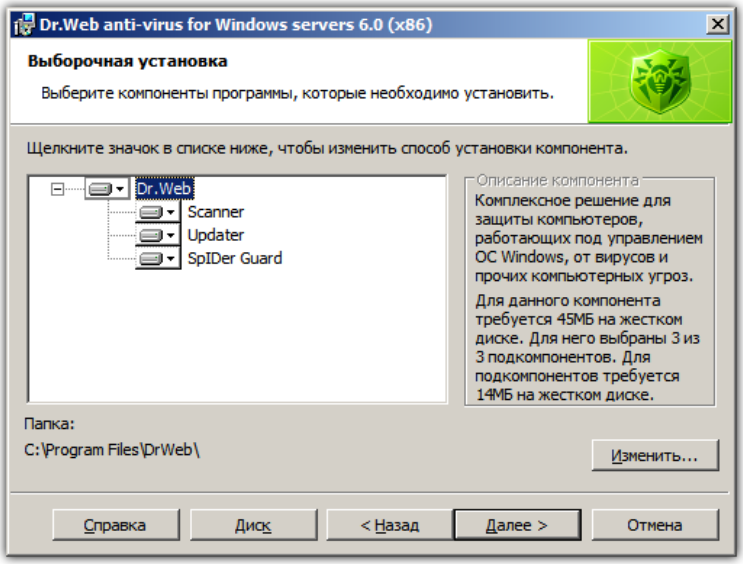


5. На следующем шаге вам будет предложено выбрать тип установки:
   - **Установка по умолчанию** предполагает установку всех компонентов, английского и русского языков интерфейса, а также всех вспомогательных программ, причем этапы установки до шага 9 будут проведены автоматически;
   - **Пользовательская установка** предназначена для опытных пользователей. В процессе пользовательской установки вам будет предложено самостоятельно выбрать устанавливаемые компоненты и некоторые дополнительные параметры установки.



Выберите необходимый тип установки и нажмите кнопку **Далее**.

6. Если вы выбрали режим установки по умолчанию, то перейдите к описанию шага 9. Если вы выбрали режим **Пользовательской установки**, то в открывшемся окне выберите устанавливаемые компоненты, при необходимости измените каталог установки и нажмите кнопку **Далее**.

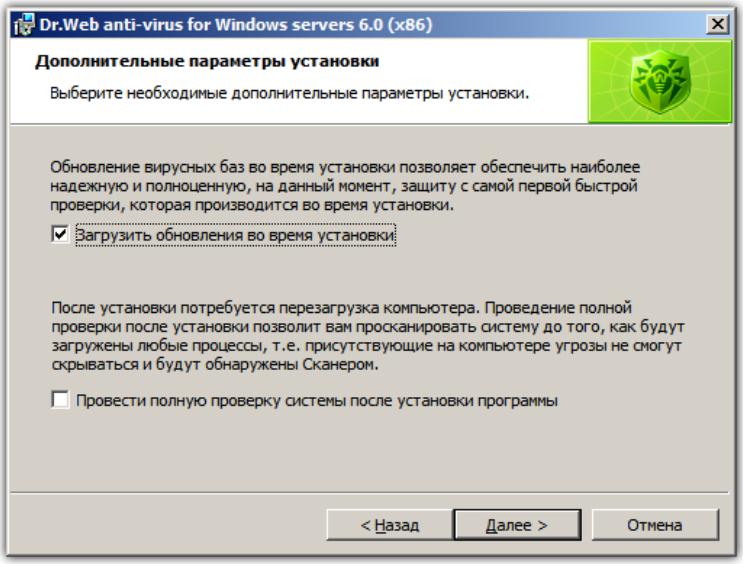


7. На следующем шаге вам будет предложено настроить создание ярлыков для запуска программы **Dr.Web Антивирус для серверов**. Укажите необходимые пункты и нажмите кнопку **Далее**.

8. На следующем шаге вам будет предложено выбрать дополнительные параметры установки. При необходимости выполните следующие действия:

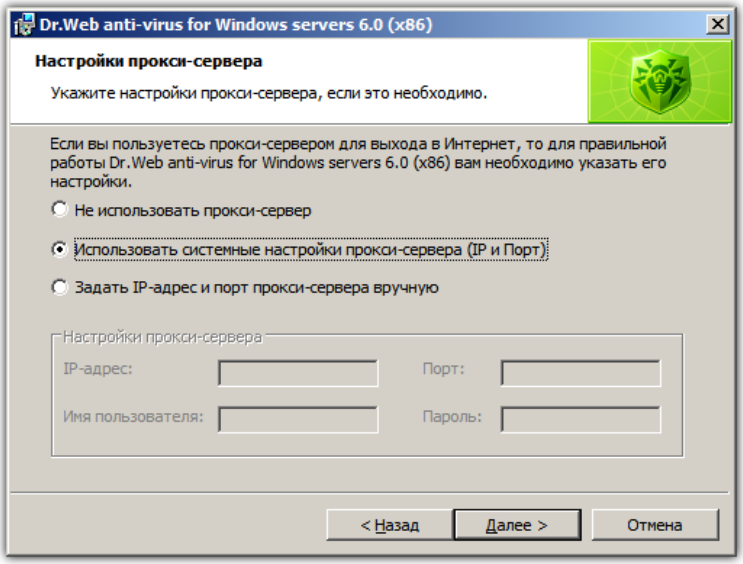
   - чтобы в процессе установки были загружены актуальные вирусные базы, установите флажок **Загрузить обновления во время установки**;
   - чтобы провести полную проверку файловой системы компьютера после установки Dr.Web, установите флажок **Провести проверку системы после установки программы**.

   Нажмите кнопку **Далее**.

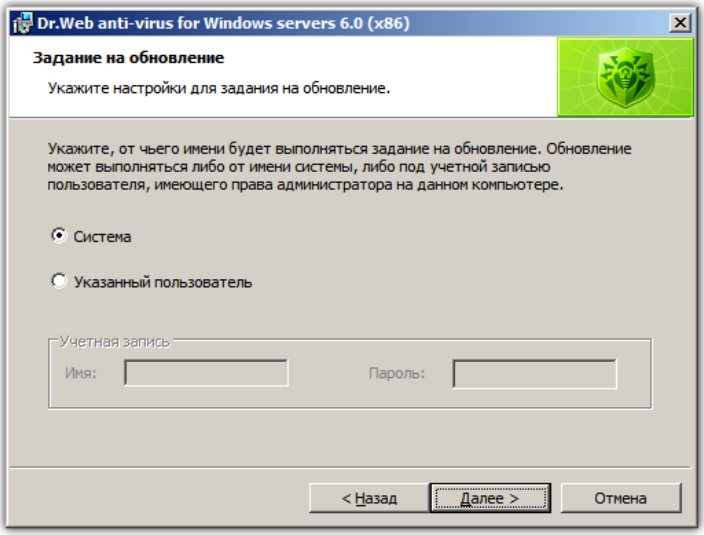


9. На следующем шаге вам будет предложено указать настройки подключения к прокси-серверу. Выберите один из следующих вариантов:
   - если для выхода в Интернет прокси-сервер не используется, выберите **Не использовать прокси-сервер**;
   - если для выхода в Интернет вы используете текущие настройки прокси-сервера, выберите пункт **Использовать системные настройки прокси-сервера (IP и Порт)**;
   - если вы хотите задать настройки прокси-сервера, выберите пункт **Задать IP-адрес и порт прокси-сервера вручную** и укажите необходимые параметры.

   Нажмите кнопку **Далее**.



10. На этом шаге укажите, от чьего имени будет выполняться задание на обновление.



11. Откроется информационное окно с сообщением о готовности к установке. Вы можете выполнить одно из следующих действий:
    - чтобы запустить процесс копирования файлов, нажмите кнопку **Установить**;
    - чтобы изменить параметры установки, нажмите кнопку **Назад**.
12. Если в процессе установки вы указали действующий ключевой файл и на шаге 8 установили флажок **Загрузить обновления во время установки**, то будет выполнен процесс обновления вирусных баз и других компонентов программы **Dr.Web Антивирус для серверов**. Обновление проводится автоматически и не требует дополнительных действий.
13. По завершении установки **Сканер** запустится и проведет быстрое сканирование. В случае обнаружения инфицированных файлов выберите необходимые действия для этих объектов. После завершения проверки выключите **Сканер**.

Известна проблема несовместимости **Сканера** с программой WindowBlinds, позволяющей настраивать элементы графического интерфейса операционных систем семейства Windows. Для корректной работы антивируса необходимо отключить возможность изменения интерфейса **Dr.Web** в настройках программы WindowBlinds, добавив файл drweb32w.exe в список исключаемых программ.

14. Для завершения процесса установки выполните перезагрузку компьютера.

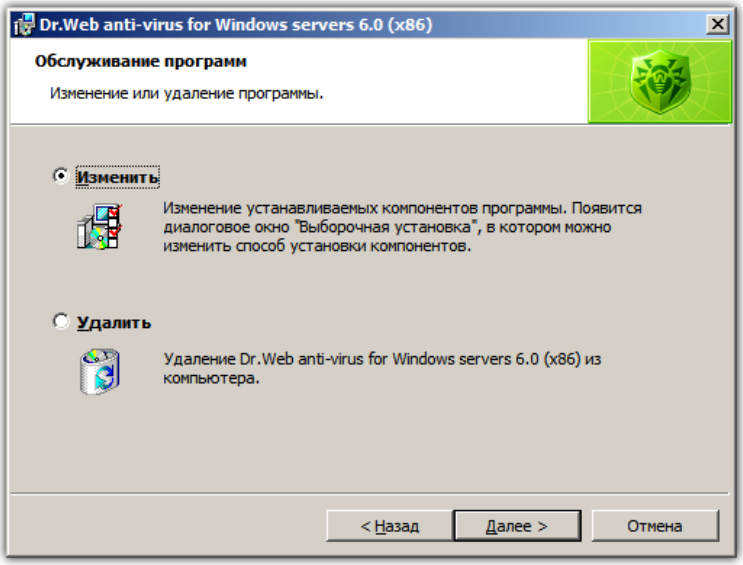
Повторная установка и удаление программы Dr.Web Антивирус для серверов

С помощью программы установки **Dr.Web** вы можете также:

- изменить состав установленных компонентов;
- удалить все установленные компоненты с компьютера.

Изменение и удаление программы

1. Чтобы запустить установку, запустите исполняемый файл программы.
2. Выберите язык работы программы.
3. В открывшемся окне выберите режим работы программы установки:
   - чтобы изменить состав устанавливаемых компонентов, выберите вариант **Изменить**;
   - чтобы удалить все установленные компоненты, выберите пункт **Удалить**.



4. Для удаления программы **Dr.Web Антивирус для серверов** или изменения состава компонентов программе установки потребуется отключить модуль самозащиты. Для этого введите код, изображенный в открывшемся окне.
5. При необходимости по просьбе программы перезагрузите компьютер для завершения процедуры удаления или изменения состава компонентов.

Глава 3. Приступая к работе

Программа установки по умолчанию устанавливает на компьютер следующие компоненты антивирусной защиты:

- **Сканер** для среды Windows (с GUI-интерфейсом и консольную версию);
- сторож **SpIDer Guard**;
- модуль управления **SpIDer Agent**.

В обязательном порядке устанавливается модуль автоматического обновления и ряд дополнительных утилит.

Компоненты антивирусной защиты используют общие вирусные базы и единые алгоритмы обнаружения вирусов в проверяемых объектах. Однако методика выбора объектов для проверки существенно различается, что позволяет использовать эти компоненты для организации существенно разных, взаимодополняющих стратегий защиты компьютера.

Так, **Сканер для Windows** проверяет (по команде пользователя или автоматически, по расписанию) определенные файлы (все файлы, выбранные логические диски, каталоги и т. д.). При этом по умолчанию проверяется также оперативная память и все файлы автозапуска. Так как время запуска задания выбирается пользователем, можно не опасаться нехватки вычислительных ресурсов для других важных процессов.

Сторож SpIDer Guard постоянно находится в памяти компьютера и перехватывает обращения к объектам файловой системы. По умолчанию программа проверяет на наличие вирусов открываемые файлы на сменных носителях и запускаемые, создаваемые или изменяемые файлы на жестких дисках. Благодаря менее детализированному способу проверки программа практически не создает помех другим процессам на компьютере, однако, это осуществляется за счет незначительного снижения надежности обнаружения вирусов.

Достоинством программы является непрерывный, в течение всего

времени работы компьютера, контроль вирусной ситуации. Кроме того, некоторые вирусы могут быть обнаружены только сторожем по специфичным для них действиям.

Для организации эффективной антивирусной защиты можно рекомендовать следующую схему использования компонентов **Dr.Web**:

- произвести сканирование всей файловой системы компьютера с предусмотренными по умолчанию (максимальными) настройками подробности сканирования;
- сохранить настройки системного сторожа по умолчанию;
- периодически, по мере обновления вирусных баз, повторять полное сканирование компьютера (не реже раза в неделю);
- в случае временного отключения сторожа, если в этот период компьютер подключался к Интернету или производилась загрузка файлов со сменного носителя, провести полное сканирование немедленно.

Антивирусная защита может быть эффективной только при условии своевременного (желательно, ежечасного) получения обновлений вирусных баз и других файлов **Dr.Web** (см. Глава 4. Автоматическое обновление).

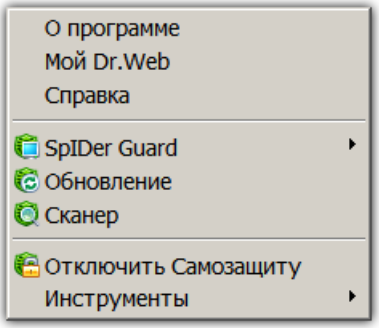
Использование компонентов программы **Dr.Web Антивирус для серверов** подробнее описано в следующих разделах.

Модуль управления SpIDer Agent

После установки **Dr.Web** в область уведомлений Windows добавляется значок **SpIDer Agent** .

При наведении курсора мыши на значок появляется всплывающая подсказка с информацией о запущенных компонентах, а также датой последнего обновления антивируса и количеством записей в вирусных базах. Также, в соответствии с настройками, над значком **SpIDer Agent** могут появляться различные подсказки-уведомления.

С помощью контекстного меню значка модуля управления осуществляется запуск и настройка компонентов программы **Dr.Web Антивирус для серверов**.



Пункт **О программе** открывает окно с информацией о версиях компонентов программы **Dr.Web Антивирус для серверов**, а также о вирусных базах.

Пункт **Мой Dr.Web** открывает вашу персональную страницу на сайте компании **«Доктор Веб»**. На данной странице вы сможете получить информацию о вашей лицензии (срок действия, серийный номер), продлить срок ее действия, задать вопрос службе поддержки и многое другое.

Пункт **Справка** открывает файл справки программы **Dr.Web**

Антивирус для серверов.

Пункты **SpIDer Guard**, **Обновление** открывают доступ к настройкам и управлению соответствующих компонентов.

Пункт **Сканер** запускает **Сканер Dr.Web**, который автоматически начинает быструю проверку компьютера.

Пункт **Отключить/Включить Самозащиту** позволяет отключить/включить защиту файлов, веток реестра и запущенных процессов **Dr.Web** от повреждений и удаления.

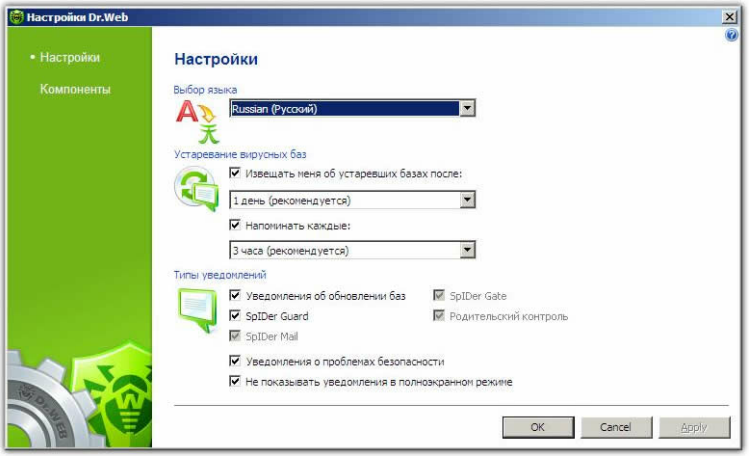
Чтобы отключить самозащиту:

- выберите в меню **SpIDer Agent** пункт **Отключить Самозащиту**;
- введите код подтверждения.

В меню **SpIDer Agent** пункт **Отключить Самозащиту** заменится на пункт **Включить Самозащиту**.

Пункт **Инструменты** открывает меню, предоставляющее доступ:

- к **Менеджеру лицензий** (см. раздел Менеджер лицензий);
- к настройкам самого **SpIDer Agent**.

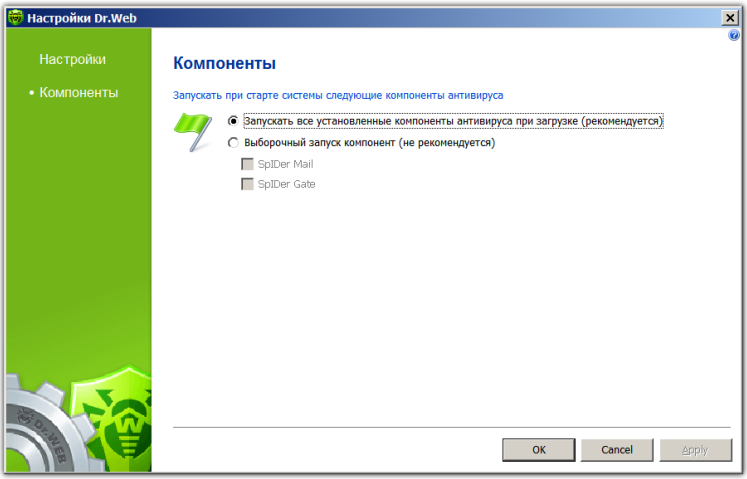


В окне настроек **SpIDer Agent** производится выбор языка интерфейса программы **Dr.Web Антивирус для серверов**. Если в выпадающем списке вы выберете язык, который не был установлен, **Dr.Web** предложит его установить.

Также в этом окне в первом разделе производится настройка типов подсказок-уведомлений, появляющиеся в виде всплывающего окна над значком **SpIDer Agent** в области уведомлений Windows. Компоненты, перечисленные в окне настроек, посылают уведомления в случае срабатывания соответствующей защиты. Также уведомление может появляться при каждом обновлении вирусных баз и в том случае, если сканирование системы не проводилось более 7 дней (флаг **Уведомления о проблемах безопасности**).

В разделе **Компоненты** вы можете выбрать один из вариантов:

- **Запускать все установленные компоненты антивируса при загрузке (рекомендуется)**;
- **Выборочный запуск компонентов (не рекомендуется)**. В этом режиме вы можете отключить автоматический запуск некоторых компонентов;



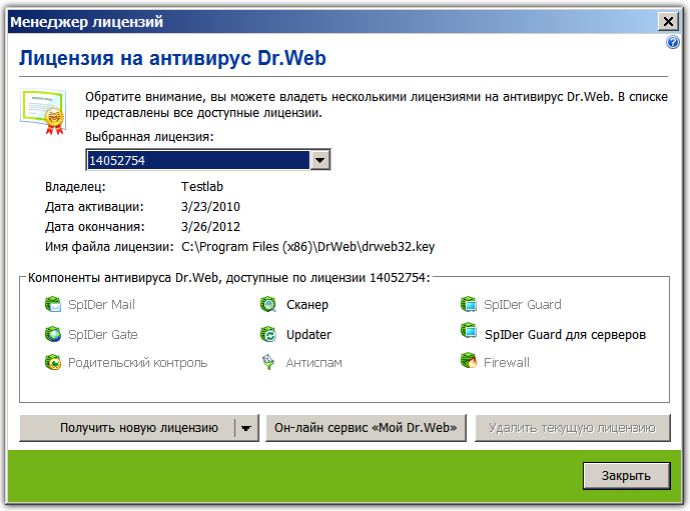
- к стандартному заданию операционной системы Windows, которое определяет периодичность и параметры обновления **Dr.Web** (пункт **Планировщик**);
- к **Карантину** (см. Карантин);
- к созданию отчёта.

При обращении в службу технической поддержки компании **«Доктор Веб»** вы можете сформировать отчёт о вашей операционной системе и работе **Dr.Web**. Для настройки параметров, в открывшемся окне нажмите **Особые параметры формирования отчёта**. Отчёт будет сохранён в виде архива в каталоге DoctorWeb, расположенном в папке профиля пользователя `%USERPROFILE%`.

Менеджер лицензий

Менеджер лицензий в доступном виде отображает информацию, содержащуюся в имеющихся у вас ключевых файлах программы **Dr.Web Антивирус для серверов**.

Чтобы открыть это окно, в контекстном меню значка **SpIDer Agent** в области уведомлений Windows выберите пункт **Инструменты**, а затем пункт **Менеджер лицензий.**



В группе **Компоненты** выделены те компоненты, с которыми согласно лицензии работает **Dr.Web Антивирус для серверов**.

Установка полученного ключевого файла

1. Нажмите кнопку **Получить новую лицензию**. В выпадающем списке выберите **указав путь к файлу на диске**.
2. Укажите путь до ключевого файла. Если вы получили ключевой файл в виде ZIP-архива, распаковывать его необязательно.

3. **Dr.Web Антивирус для серверов** автоматически начнет использовать ключевой файл.

Для того чтобы удалить ключевой файл из списка, нажмите кнопку **Удалить текущую лицензию**. Последний используемый ключ не может быть удален.

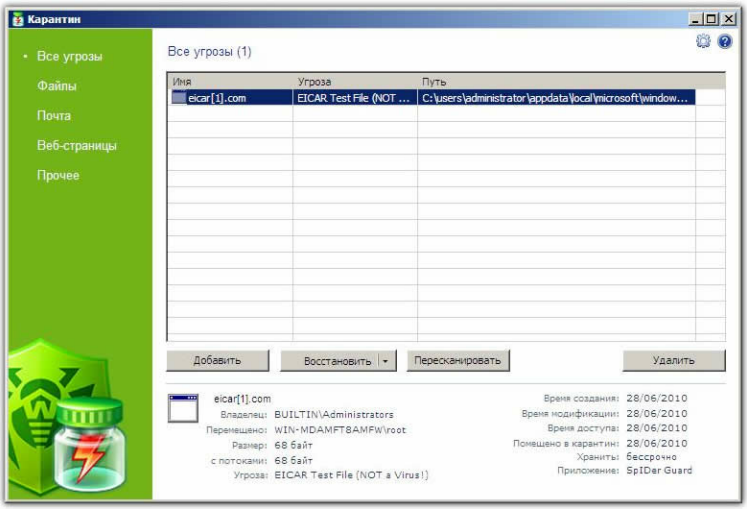
При работе программы ключевой файл по умолчанию должен находиться в каталоге установки. Программа регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа, не модифицируйте ключевой файл.

При отсутствии действительного ключевого файла активность всех компонентов блокируется.

Карантин

Это окно содержит данные о содержимом **Карантина Dr.Web**, который служит для изоляции файлов, подозрительных на наличие вредоносных объектов. Папки **Карантина** создаются отдельно на каждом логическом диске, где были обнаружены подозрительные файлы. При обнаружении зараженных объектов на съемном носителе, если запись на носителе возможна, на нём создается папка Карантин и в неё переносится зараженный объект.

Для просмотра и редактирования содержимого карантина выберите в разделе **Инструменты** контекстного меню **SpIDer Agent** пункт **Карантин**.



В центральной части окна отображается таблица с информацией о состоянии карантина, включающая следующие поля:

- **Имя** – список имен объектов, находящихся в карантине;
- **Угроза** – классификация вредоносной программы, определяемая программой **Dr.Web Антивирус для серверов** при автоматическом перемещении объекта в

карантин;

- **Путь** – полный путь, по которому находился объект до перемещения в карантин.

В нижней части окна карантина отображается подробная информация о выделенных объектах карантина. Вы можете включить отображение столбцов с подробной информацией об объекте, аналогичной данным в нижней части окна.

Настройка отображения столбцов

1. Чтобы задать параметры отображения информации в таблице **Карантина**, щелкните правой кнопки мыши по заголовку таблицы и выберите пункт **Настроить колонки**.
2. В открывшемся окне установите флажки напротив тех пунктов, которые вы хотите включить в таблицу объектов. Чтобы исключить столбцы из таблицы объектов, снимите флажки напротив соответствующих пунктов. Также вы можете выполнить одно из следующих действий:
   - чтобы установить флажки напротив всех объектов сразу, нажмите кнопку **Отметить все**;
   - чтобы снять все флажки, нажмите кнопку **Снять отметки**.
3. Для изменения порядка следования столбцов в таблице выберите соответствующий столбец в списке и нажмите на одну из следующих кнопок:
   - **Вверх** – для перемещения столбца ближе к началу таблицы (вверх по списку в настройках и левее в таблице объектов).
   - **Вниз** – для перемещения столбца ближе к концу таблицы (вниз по списку в настройках и правее в таблице объектов).
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Боковая панель слева служит для фильтрации объектов карантина, которые будут отображены. При нажатии на соответствующий пункт, в центральной части окна будут показаны все объекты карантина или только заданные группы

объектов: файлы, почтовые объекты, веб-страницы или все остальные объекты, не попадающие в данные категории.

В окне карантина файлы могут видеть только те пользователи, которые имеют права доступа к этим файлам.

В окне карантина доступны следующие кнопки управления:

- **Добавить** – добавить файл в карантин. В открывшемся браузере по файловой системе выберите нужный файл;
- **Восстановить** – переместить файл из карантина и восстановить первоначальное местоположение файла на компьютере (восстановить файл под тем же именем и в папку, в которой он находился до перемещения в карантин).

Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

В выпадающем меню вы можете выбрать вариант **Восстановить в** – переместить файл под заданным именем в папку, указанную администратором;

- **Пересканировать** – сканировать файл из карантина повторно;
- **Удалить** – удалить файл из карантина и из системы.

Для работы одновременно с несколькими файлами выберите необходимые файлы, удерживая клавиши SHIFT или CTRL, затем щелкните правой кнопкой мыши в на любой строчке таблицы и выберите необходимое действие.

Для настройки свойств **Карантина** нажмите кнопку  в окне **Карантина**. Откроется окно **Свойства карантина**, в котором вы можете изменять следующие параметры:

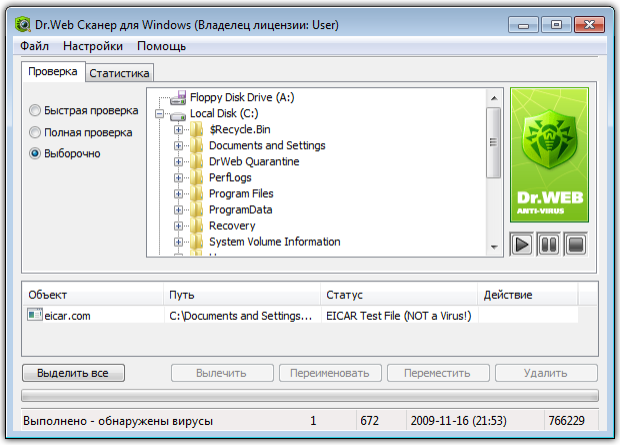
- в разделе **Задать размер карантина** вы можете управлять объемом дискового пространства, занимаемого папкой **Карантина**;

- в разделе **Вид** вы можете установить флаг **Показывать резервные копии**, чтобы отобразить в таблице объектов резервные копии файлов, находящихся в **Карантине**.

Резервные копии создаются автоматически при перемещении файлов в **Карантин**. Даже при хранении файлов в **Карантине** бессрочно, их резервные копии сохраняются временно.

Сканер для Windows

По умолчанию **Сканер** производит антивирусное сканирование всех файлов с использованием как вирусных баз, так и эвристического анализатора (алгоритма, позволяющего с большой вероятностью обнаруживать неизвестные программе вирусы на основе общих принципов их создания). Исполняемые файлы, упакованные специальными упаковщиками, при проверке распаковываются. Проверяются файлы в архивах всех основных распространенных типов (ACE (до версии 2.0), ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP), файловых контейнерах (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM), а также файлы в составе писем в почтовых ящиках почтовых программ (формат писем должен соответствовать RFC822).



Dr.Web в случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом по умолчанию выводит пользователю сообщения об этом в специальном поле отчета в нижней части главного окна.

Запуск Сканера

Сканер устанавливается как обычное приложение Windows и запускается по команде пользователя (или по расписанию, см. Задания на скранирование и обновление).

Запуск Сканера

Рекомендуется запускать **Сканер** от имени пользователя, обладающего правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут подвергнуты проверке.

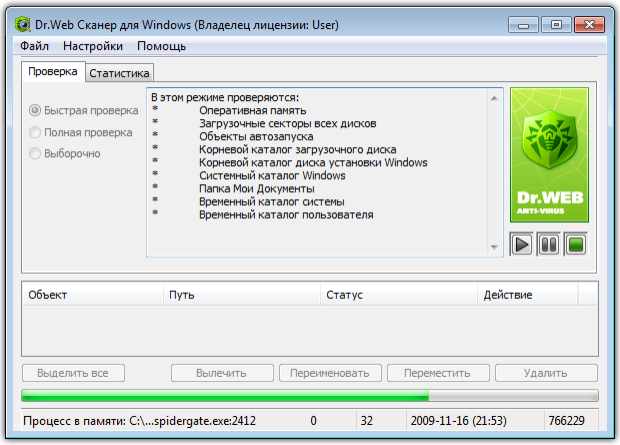
1. Для запуска Сканера используйте одно из следующих средств:
   - значок **Сканера** на Рабочем столе;
   - пункт **Сканер** контекстного меню значка **SpIDer Agent** (см. Модуль управления SpIDer Agent);
   - пункт меню **Сканер Dr.Web** в папке Dr.Web Главного меню Windows (открывается по кнопке **Пуск**);
   - специальную команду операционной системы Windows (подробнее см. п. Сканирование в режиме командной строки).

   Чтобы запустить **Сканер** с настройками по умолчанию для проверки какого-либо файла или каталога, воспользуйтесь одним из следующих способов:

   - выберите в контекстном меню значка файла или каталога (на Рабочем столе или в Проводнике операционной системы Windows) пункт **Проверить Dr.Web**;
   - перетащите значок файла или каталога на значок или открытое Главное окно **Сканера**.
2. После запуска программы открывается ее главное окно.

   Если вы запускаете **Сканер** на проверку файла или каталога, то после этого немедленно начинается сканирование выбранного объекта. В противном случае,

при настройках по умолчанию, немедленно после запуска программы производится быстрое сканирование. Сканирование остальных объектов файловой системы производится по запросу пользователя.



3. На выбор предоставляется три возможных режима проверки: **Быстрая**, **Полная** и **Выборочно**. В центральной части окна в зависимости от выбранного режима отображается информация о проверяемых объектах, либо файловая структура, представленная в виде иерархического дерева (в случае выборочной проверки).

   Во время *быстрой проверки* проверяются:

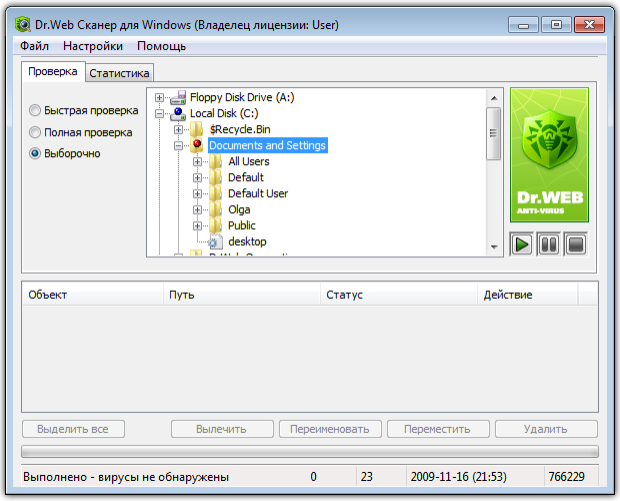
   - оперативная память;
   - загрузочные секторы всех дисков;
   - объекты автозапуска;
   - корневой каталог загрузочного диска;
   - корневой каталог диска установки Windows;
   - системный каталог Windows;
   - папка Мои Документы;
   - временный каталог системы;
   - временный каталог пользователя.

В режиме *полной проверки* производится полное сканирование оперативной памяти, всех жестких дисков и сменных носителей (включая загрузочные секторы).

В режиме *выборочной проверки* пользователю предоставляет возможность выбирать любые файлы и папки для антивирусной проверки.

4. Если вы выбрали выборочный режим проверки, в иерархическом списке выберите объекты для проверки. В случае полной или быстрой проверки выбирать объекты не требуется. На рисунке изображена ситуация, в которой выбрана для сканирования папка Documents and Settings на логическом диске C.

По умолчанию наряду с выбранными объектами также будут проверяться подкаталоги всех выбранных каталогов и логических дисков, а также загрузочные секторы всех логических дисков, на которых выбран хотя бы один каталог или файл, а также главные загрузочные секторы соответствующих физических дисков.



При быстрой и полной проверке **Сканер** определит, не был ли изменен HOSTS-файл (текстовый файл, который содержит базу данных доменных имен и используется при их трансляции в сетевые адреса узлов). HOSTS-файл может подвергнуться воздействию вредоносных программ (например, с целью перенаправить пользователя на определённый сайт). В том случае, если HOSTS-файл был изменен, **Сканер** предложит восстановить его исходное состояние. Это позволит устранить несанкционированное изменение файла вредоносным программным обеспечением.

5. Для того чтобы приступить к сканированию, нажмите кнопку **Старт** в правой части главного окна.

В случае запуска **Сканера** на портативном компьютере, работающем от батареи, появится предупреждение, информирующее вас об оставшемся заряде батареи. Вы можете отключить проверку режима питания вашего ноутбука на вкладке **Общие** окна настроек **Сканера**. Подробнее об изменении остальных настроек программы см. Настраиваемые параметры программы.

6. После начала сканирования в правой части окна становятся доступными кнопки **Пауза** и **Стоп**. На любом этапе проверки вы можете сделать следующее:
   - чтобы приостановить проверку, нажмите кнопку **Пауза**. Для того чтобы возобновить проверку после паузы, снова нажмите кнопку **Старт**;
   - чтобы полностью остановить проверку, нажмите кнопку **Стоп**.

Если сканирование системы не проводится более 7 дней, выводится уведомление (см. настройки SpIDer Agent).

Действия при обнаружении вирусов

По умолчанию **Сканер** лишь информирует пользователя обо всех зараженных и подозрительных объектах. Вы можете использовать программу для того, чтобы попытаться восстановить функциональность зараженного объекта (*вылечить* его), а при невозможности – чтобы устранить исходящую от него угрозу (*удалить* объект), а также удалить вредоносные процессы из системы.

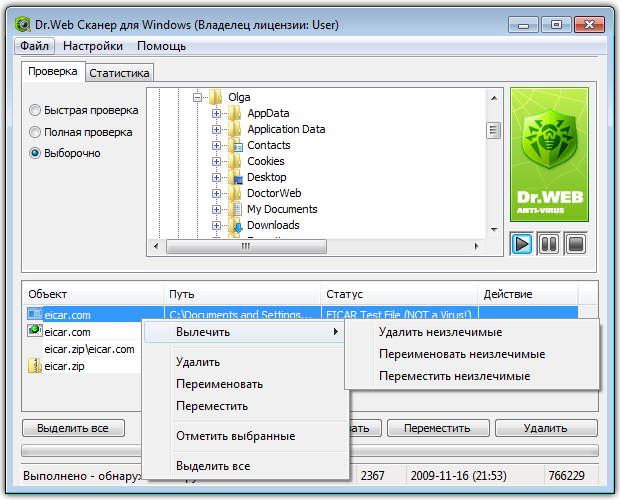
Выбор действия

1. Выберите один или несколько зараженных объектов. Вы можете указать действие сразу для всех или нескольких объектов в списке отчета. Чтобы выделить все объекты, нажмите кнопку **Выделить все**.

   Для выделения объектов в списке отчета вы можете использоваться следующие клавиши и комбинации клавиш:

   - INSERT – выделить объект;
   - CTRL+A – выделить все;
   - клавиша умножения (*) на цифровой клавиатуре – выделить все или полностью снять выделение.

2. Щелкните правой клавишей мыши по одной из выбранных строк отчета. В открывшемся контекстном меню выберите действие, которое вы хотите предпринять. Также вы можете воспользоваться одной из соответствующих кнопок, расположенных непосредственно под полем отчета.



3. При выборе варианта **Вылечить** необходимо также выбрать действие, которое будет предпринято в случае невозможности лечения.

   Переименование производится путем замены расширения файла, по умолчанию первый символ расширения заменяется на символ #.

   Перемещение производится в каталог, заданный в настройках программы, по умолчанию это подкаталог каталога установки программы с названием infected.!!!.

   Удалить — удалить инфицированный объект.

   Существуют следующие ограничения:

   - лечение подозрительных объектов невозможно;
   - перемещение, переименование или удаление объектов, не являющихся файлами (например, загрузочных секторов), невозможно;

- любые действия для отдельных файлов внутри архивов, контейнеров или в составе писем невозможны – действие в таких случаях применяется только ко всему объекту целиком.

Подозрительные файлы, перемещенные в каталог infected.!!!, рекомендуется передавать для дальнейшего анализа в антивирусную лабораторию **«Доктор Веб»**, используя специальную форму на веб-сайте http://vms.drweb.com/sendvirus/.

По умолчанию при выборе действия **Удалить** для файловых архивов, контейнеров или почтовых ящиков программа выдает предупреждение о возможной потере данных.

4. После выполнения выбранного вами действия антивирус добавляет в колонку **Действие** поля отчета сообщение о результате операции.

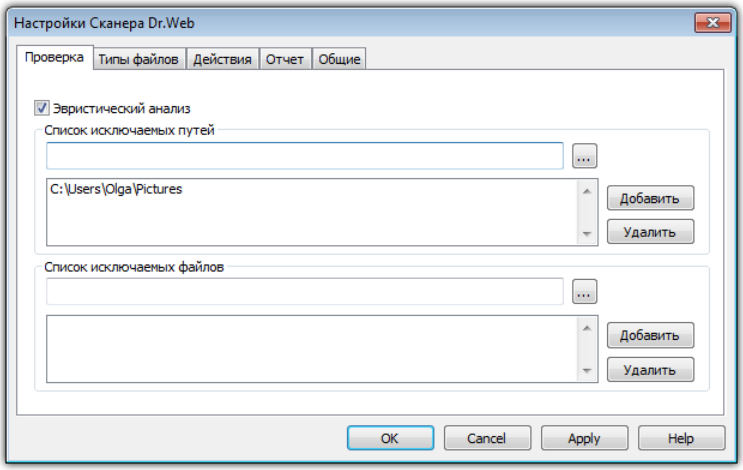
   В некоторых случаях, выбранное вами действие не может быть выполнено немедленно. В этом случае в поле отчета **Сканера** в колонке **Действие** появляется запись **Будет излечен после рестарта**, **Будет удален после рестарта** или **Будет переименован после рестарта** в зависимости от выбранного действия. Указанное действие будет реально выполнено только после перезагрузки компьютера, т. е. это будет отложенное действие. Поэтому при обнаружении таких объектов рекомендуется провести перезагрузку системы сразу после окончания сканирования. При необходимости вы можете настроить автоматическую перезагрузку операционной системы для завершения лечения (см. Настраиваемые параметры программы).

Подробный отчет о работе программы сохраняется в виде файла отчета. По умолчанию он размещается в подпапке DoctorWeb, расположенной в папке профиля пользователя `%USERPROFILE%` и именуется drweb32w.log.

Настройка параметров программы

Рекомендуется запускать **Сканер** от имени пользователя, обладающим правами администратора. В противном случае пользовательские настройки не будут сохранены при выходе из системы.

Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.



Изменение настроек программы

1. Чтобы вызвать **Настройки** программы, выполните одно из следующих действий:
   - выберите в главном меню программы пункт **Настройки**, после чего в открывшемся подменю выберите пункт **Изменить настройки**;
   - убедившись, что окно **Сканера** активно, нажмите F9.

   Откроется окно настроек, содержащее несколько вкладок.

2. Внесите необходимые изменения. При необходимости нажимайте кнопку **Применить** перед переходом на другую вкладку.
3. Для более подробной информации о настройках, задаваемых на каждой вкладке, воспользуйтесь кнопкой **Справка**.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

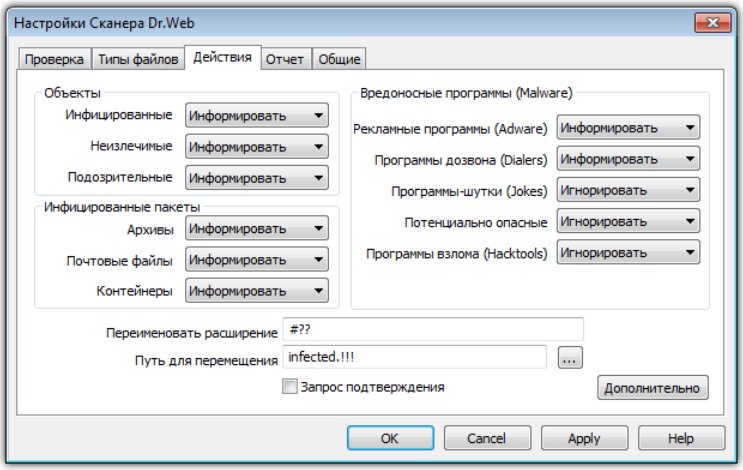
Ниже описываются часто используемые случаи изменения настроек по умолчанию.

Настройки по умолчанию являются оптимальными для режима, в котором сканирование производится по запросу пользователя. Программа производит наиболее полное и подробное сканирование выбранных объектов, информируя пользователя обо всех зараженных или подозрительных объектах и предоставляя ему возможность назначать действия программы по отношению к ним. Исключением являются объекты, содержащие программы-шутки, потенциально опасные программы и программы взлома: по умолчанию они игнорируются.

Однако когда сканирование производится без участия пользователя, оптимальны настройки, обеспечивающие *автоматическую* реакцию программы на обнаружение зараженных объектов.

Настройка реакции программы на обнаружение зараженных объектов

1. Перейдите в окне настроек на вкладку **Действия**.



2. Выберите в выпадающем списке **Инфицированные объекты** реакцию программы на обнаружение инфицированного объекта.
3. Выберите в выпадающем списке **Неизлечимые объекты** реакцию программы на обнаружение неизлечимого объекта. Это действие аналогично рассмотренному в предыдущем пункте, с той разницей, что вариант **Вылечить** отсутствует.
4. Выберите в выпадающем списке **Подозрительные объекты** реакцию программы на обнаружение подозрительного объекта (полностью аналогично предыдущему пункту).
5. Аналогично настраивается реакция программы на обнаружение объектов, содержащих рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.
6. Аналогично настраиваются автоматические действия

программы при обнаружении вирусов или подозрительного кода в файловых архивах, контейнерах и почтовых ящиках. Действия по отношению к вышеуказанным объектам выполняются над всем объектом, а не только над зараженной его частью. По умолчанию во всех этих случаях предусмотрено информирование.

7. Снимите флаг **Запрос подтверждения**, чтобы программа выполняла предписанное действие без предварительного запроса.
8. В случаях, когда в качестве реакции программы задано переименование, программа по умолчанию заменяет первый символ расширения имени файла на #. При необходимости вы можете изменить маску переименования расширения файла. Для этого введите нужное значение маски переименования в поле ввода **Переименовать расширение**.
9. В случаях, когда в качестве реакции программы задано перемещение, программа по умолчанию перемещает файл в подкаталог infected.!!! каталога установки программы. При необходимости вы можете задать другое имя каталога в поле ввода **Путь для перемещения**.
10. Для успешного завершения лечения некоторых зараженных (инфицированных) файлов требуется перезагрузка операционной системы. Параметры перезагрузки системы вы можете настроить в окне **Настройки лечения**. Откройте это окно, нажав кнопку **Дополнительно**, расположенную в правом нижнем углу вкладки. Вы можете выбрать один из вариантов:

    - **Перезагружать систему автоматически, если необходимо**. Этот режим может привести к потере несохраненных данных;
    - **Не перезагружать систему автоматически**. В случае выбора этого варианта рекомендуется установить флаг **Предлагать перезагрузку в случае необходимости**, для того чтобы корректно завершать лечение инфицированных файлов в удобное для вас время.

Вкладка Типы файлов

На этой вкладке задаются дополнительные ограничения на состав файлов, подлежащих сканированию в соответствии с заданием на сканирование, а также указывается, проводится ли проверка почтовых файлов и архивов.

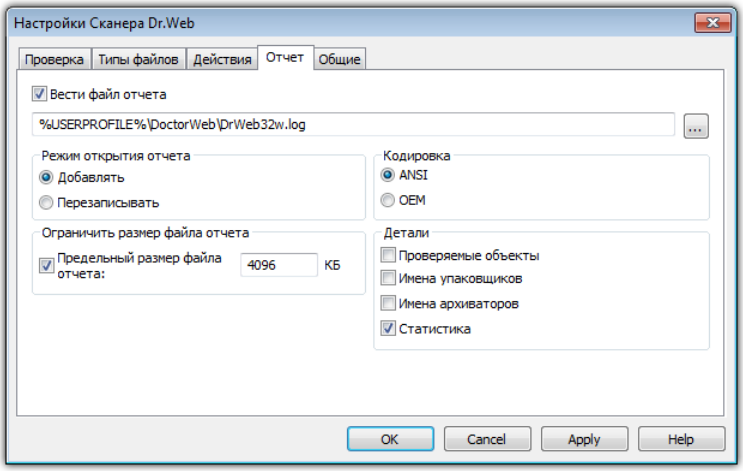
В группе кнопок выбора **Режим проверки** задается способ отбора проверяемых файлов:

- вариант **Все файлы** обеспечивает максимальную защиту (выбран по умолчанию);
- варианты **Выбранные типы** и **Заданные маски** предписывают проверять только файлы, расширения или имена которых соответственно входят в список, задаваемый в правой части вкладки. По умолчанию список включает расширения основных типов файлов, могущих быть носителями вирусов, и основных типов файловых архивов. Вы можете отредактировать этот список.

На этой вкладке задается также режим проверки **Файлов в архивах** и **Почтовых файлов**. По умолчанию проверяются и файловые архивы, и почтовые ящики.

Вкладка Отчет

На этой вкладке вы можете настроить параметры ведения файла отчета.



Большинство параметров, заданных по умолчанию, следует сохранить, однако по мере накопления опыта работы с отчетом вы можете изменить степень детальности протоколирования событий (в отчет всегда включаются сведения о зараженных и подозрительных объектах; сведения о проверке упакованных файлов и архивов и сведения об успешной проверке остальных файлов по умолчанию не включаются).

Вы можете предписать программе отображать в отчете сведения о проверке всех файлов, независимо от исхода – для этого установите флаг **Проверяемые объекты** (это значительно увеличит объем отчета).

Вы можете предписать программе отображать имена архиваторов (установите флаг **Имена архиваторов**) или упаковщиков исполняемых файлов (установите флаг **Имена упаковщиков**).

Вы можете отменить установленное по умолчанию ограничение максимального размера файла отчета (снимите флаг **Предельный размер**) или ввести собственное значение лимита длины файла в поле ввода рядом с флагом.

Вкладка Общие

На этой вкладке задаются параметры взаимодействия программы с операционной системой, а также звуковые реакции программы на различные события.

Флажок **Автосохранение** настроек предписывает программе сохранять измененные настройки при завершении работы **Сканера Dr.Web**. В противном случае изменения в настройках сохраняются, только если пользователь явно потребовал этого (пункт **Сохранить настройки** в меню **Настройки** главного окна **Сканера Dr.Web**). Данный режим задан по умолчанию.

Флажок **Проверять работу от батареи** позволяет проверять перед началом сканирования, работает ли ноутбук от батареи. Опция доступна только для портативных компьютеров (ноутбуков).

Бегунок **Приоритет проверки** позволяет изменить приоритет процесса сканирования в системе.

Сканирование в режиме командной строки

Вы можете запускать программу **Dr.Web Сканер для Windows** в режиме командной строки. Такой способ позволяет задать настройки текущего сеанса сканирования и перечень сканируемых объектов в качестве параметров вызова. Именно в таком режиме возможен автоматический вызов **Сканера** по расписанию.

Синтаксис команды запуска следующий:

[<*путь_к_программе*>] `drweb32w` [<*объекты*>] [<*ключи*>]

Список объектов сканирования может быть пуст или содержать несколько элементов, разделенных пробелами.

Наиболее распространенные следующие варианты указания объектов сканирования:

- `*` – сканировать все жесткие диски;
- `C:` – сканировать диск `C:` ;
- `D:\games` – сканировать файлы в каталоге;
- `C:\games\*` – сканировать все файлы и подкаталоги каталога C:\games.

Параметры – ключи командной строки, которые задают настройки программы. При их отсутствии сканирование выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их).

Каждый параметр этого типа начинается с символа `/`, ключи разделяются пробелами.

Ниже приведено несколько наиболее часто используемых ключей. Полный их список содержится в Приложении А.

- `/cu` – лечить инфицированные объекты.
- `/icm` – перемещать неизлечимые файлы (в каталог по умолчанию), `/icr` – переименовывать (по умолчанию).
- `/qu` – закрыть окно **Сканера** по окончании сеанса.
- `/go` – не выдавать никаких запросов.

Последние два параметра особенно полезны при автоматическом запуске **Сканера** (например, по расписанию).

С такими же параметрами может использоваться **Dr.Web Консольный сканер для Windows DrWebWcl**. В этом случае вместо `drweb32w` необходимо набрать имя команды `drwebwcl`.

Консольный сканер DrWebWcl по умолчанию использует те же настройки, что и **GUI-версия Сканера**. Параметры, заданные средствами графического интерфейса **Сканера** (см. п. Настройка параметров программы), используются также при сканировании в режиме командной строки, если иные значения параметров не были заданы в виде ключей. Некоторые настройки **Сканера** могут задаваться только в конфигурационном файле программы. (См. Приложение В).

Консольный сканер DWScancl

Также в состав компонентов **Dr.Web Антивирус для серверов** входит **Консольный сканер DWScancl**. В отличие от **Консольного сканера DrWebWcl**, он предоставляет пользователю расширенные возможности настройки (большее количество параметров) и рассчитан на многопроцессорные системы.

Файлы, подозрительные на наличие вредоносных объектов, **Консольный сканер DWScancl** помещает не в каталог infected.!!!, а в **Карантин**.

Чтобы запустить **Консольный сканер DWScancl**, воспользуйтесь следующей командой:

[*<путь_к_программе>*] `dwscancl` [*<ключи>*] [*<объекты>*]

Список объектов сканирования может быть пуст или содержать несколько элементов, разделенных пробелами.

Список ключей **Консольного сканера DWScancl** содержится в Приложении А.

SpIDer Guard для Windows

По умолчанию **SpIDer Guard** запускается автоматически при каждой загрузке операционной системы, при этом запущенный сторож **SpIDer Guard** не может быть выгружен в течение текущего сеанса работы операционной системы. При необходимости приостановить на некоторое время работу сторожа (например, при выполнении критически чувствительного к загрузке процессора задания в реальном масштабе времени) выберите в меню **SpIDer Guard** контекстного меню модуля управления пункт **Отключить**.

Временное отключение мониторинга доступно только пользователю, обладающему правами администратора.

При настройках по умолчанию сторож «на лету» проверяет на жестком диске – только создаваемые или изменяемые файлы, на сменных носителях – все открываемые файлы. Кроме того, сторож постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при их обнаружении блокирует эти процессы.

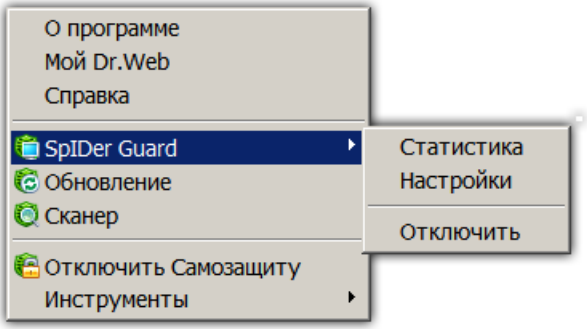
Сторож в пакете программы **Dr.Web Антивирус для серверов** при обнаружении зараженных объектов применяет к ним действия согласно установленным настройкам.

Соответствующим изменением настроек вы можете задать автоматическую реакцию программы на вирусные события. Пользователь сможет следить за ней с помощью окна статистики и файла отчета.

Возможна несовместимость **Dr.Web Антивируса для серверов** с MS Exchange Server. В случае возникновения проблем, добавьте базы данных и журнал транзакций MS Exchange Server в список исключений **SpIDer Guard**.

Управление сторожем SpIDer Guard

В меню **SpIDer Guard** сосредоточены основные средства настройки и управления сторожем.



Пункт **Статистика** открывает окно, содержащее сведения о работе сторожа в течение текущего сеанса (количество проверенных, зараженных и подозрительных объектов, предпринятые действия и др.).

Пункт **Настройки** открывает доступ к основной части настраиваемых параметров программы (подробнее см. п. Основные настройки сторожа).

Пункт **Отключить** позволяет временно отключить **SpIDer Guard** (доступно только пользователю, имеющему права администратора данного компьютера).

Основные настройки сторожа

Основные настраиваемые параметры сторожа сосредоточены в разделах окна **Настройки SpIDer Guard** (см. ниже). Для того чтобы получить справку о параметрах, задаваемых в каком-либо разделе, перейдите в этот раздел и нажмите кнопку **Справка** .

По окончании редактирования настроек нажмите кнопку **ОК**, чтобы сохранить изменения, или кнопку **Отмена**, чтобы отказаться от внесенных изменений.

Ниже описываются некоторые наиболее часто изменяемые настройки программы.

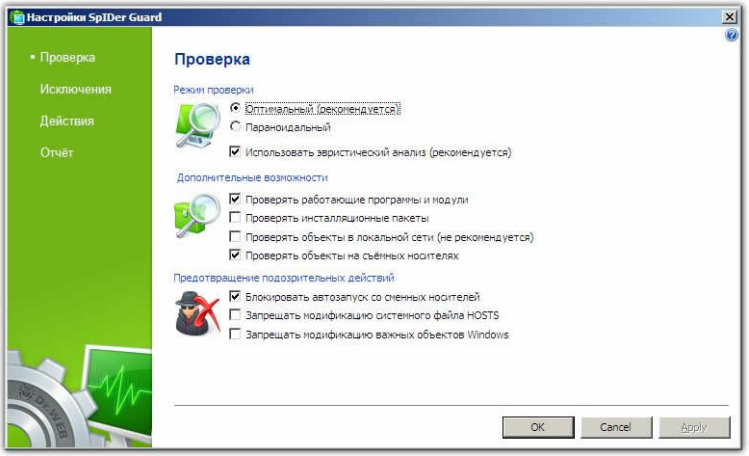
Раздел Проверка

По умолчанию установлен режим проверки **Оптимальный**: сканирование на жестких дисках – только запускаемых, создаваемых или изменяемых файлов, на сменных носителях – всех открываемых файлов.

В оптимальном режиме **SpIDer Guard** не определяет DOS-приложения (например, тестовый файл EICAR) как вредоносную программу, так как они не представляют угрозы для компьютера.

В режиме **Параноидальный** производится проверка всех открываемых, создаваемых или изменяемых файлов на жестких дисках, сменных носителях и сетевых дисках .

Флажок **Использовать эвристический анализ** включает режим эвристического анализатора (режим поиска неизвестных вирусов на основании анализа структуры файла).



Группа настроек **Дополнительные возможности** позволяет задать параметры проверки «на лету», которые будут применяться вне зависимости от выбранного режима работы сторожа **SpIDer Guard**.

Здесь вы можете задать проверку:

- файлов запускаемых процессов вне зависимости от их расположения;
- установочных файлов;
- файлов на сетевых дисках;
- файлов и загрузочных секторов на съемных носителях.

Некоторые внешние накопители (в частности, мобильные винчестеры с интерфейсом USB) могут представляться в системе как жесткие диски. Поэтому такие устройства следует использовать с особой осторожностью, проверяя на вирусы при подключении к компьютеру с помощью антивирусного **Сканера**.

Отказ от проверки архивов в условиях постоянной работы сторожа не ведет к проникновению вирусов на компьютер, а лишь откладывает момент их обнаружения. При распаковке зараженного архива (открытии зараженного письма) будет сделана попытка записать инфицированный объект на диск, при этом сторож его неминуемо обнаружит.

Группа настроек **Предотвращение подозрительных действий** позволяет запретить некоторые действия, которые могут привести к заражению вашего компьютера.

Если при установке важных обновлений от Microsoft возникают проблемы, снимите флаг **Запрещать модификацию важных объектов Windows**.

Задание исключений

В разделе **Исключения** задается список каталогов и файлов, исключаемых из проверки.

В поле **Список исключаемых путей и файлов** приводится список каталогов и файлов, которые не проверяются сторожем **SpIDer Guard**. В таком качестве могут выступать каталоги карантина, рабочие каталоги некоторых программ, временные файлы (файлы подкачки) и т. п.

По умолчанию список пуст. Вы можете добавить к исключениям конкретные каталоги и файлы или использовать маски, чтобы запретить проверку определенной группы файлов.

Вы можете формировать список исключений следующим образом:

- чтобы указать конкретный существующий каталог или файл, нажмите кнопку **Обзор** и выберите каталог или файл в стандартном окне открытия файла. Вы также можете вручную ввести полный путь к файлу или каталогу в поле ввода;
- чтобы исключить из проверки все файлы или каталоги с определенным именем, введите это имя в поле ввода. Указывать путь к каталогу или файлу при этом не требуется;
- чтобы исключить из проверки файлы или каталоги определенного вида, введите определяющую их маску в поле ввода. Маска задает общую часть имени объекта. При этом:
  - символ «*» заменяет любую, возможно пустую последовательность символов;
  - символ «?» заменяет любой, но только один символ;
  - остальные символы маски ничего не заменяют и означают, что на данном месте в имени файла или каталога должен находиться именно этот символ.

  Пример:

  - отчет*.doc – маска, задающая все документы Microsoft Word, название которых начинается с подстроки «отчет», например, файлы отчет-февраль.doc, отчет121209.doc и т.д.;
  - *.exe – маска, задающая все исполняемые файлы с расширением EXE, например, setup.exe, iTunes.exe и т. д.;
  - photo????09.jpg – маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных символа, например, photo121209.jpg, photomama09.jpg или photo----09.jpg.

Кнопка **Добавить** позволяет добавить к списку исключение, указанное в поле ввода.

Кнопка **Удалить** позволяет удалить из списка выбранное исключение.

Настройка действий

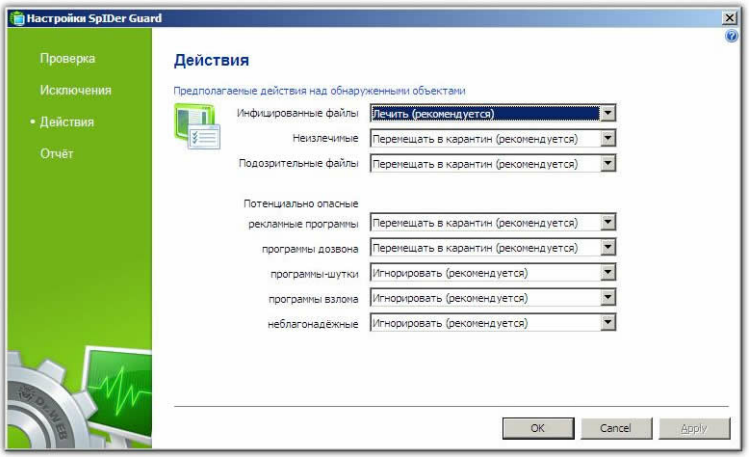
В разделе **Действия** вы можете настроить автоматические действия сторожа с зараженными объектами.

Состав доступных реакций зависит от типа вирусного события.

Реакции **Лечить**, **Перемещать в карантин, Игнорировать** и **Удалить** аналогичны таким же реакциям **Сканера**.

Изменение настроек сторожа

1. В окне **Настройки SpIDer Guard** выберите раздел **Действия**.



2. Выберите в выпадающем списке **Инфицированные** объекты реакцию программы на обнаружение инфицированного объекта. Рекомендуется установить действие **Лечить**.
3. Выберите в выпадающем списке **Неизлечимые объекты** реакцию программы на обнаружение неизлечимого

объекта. Рекомендуется установить действие **Перемещать в карантин**. Дальнейшие действия с перемещенными файлами рассмотрены в п. Действия при обнаружении вирусов.

4. Выберите в выпадающем списке **Подозрительные объекты** реакцию программы на обнаружение подозрительного объекта. Рекомендуется установить действие **Игнорировать** или **Перемещать в карантин**.
5. Выберите в выпадающих списках **Потенциально опасные рекламные программы** и **Программы дозвона** реакцию программы на обнаружение подозрительного объекта. Рекомендуется установить действие **Перемещать в карантин**.
6. Аналогично настраивается реакция программы на обнаружение объектов, содержащих рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома. Рекомендуется установить действие **Игнорировать**.
7. Нажмите кнопку **ОК**.

Раздел Отчет

В этом разделе вы можете задать одну из следующих степеней детальности ведения отчета:

- **Стандартный** – в данном режиме в отчете фиксируются только наиболее значимые события, такие как проведение обновлений, запуск и остановка сторожа **SpIDer Guard** и вирусные события. Данный режим ведения отчета походит для большинства применений;
- **Расширенный** – в данном режиме в отчете помимо общих событий фиксируются данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых составных объектов (архивов, файлов электронной почты или файловых контейнеров);
- **Отладочный** – в данном режиме в отчете фиксируется максимальное количество информации о работе сторожа **SpIDer Guard**, что может привести к значительному увеличению файла отчета.

Задания на сканирование и обновление

При установке **Dr.Web** в системном расписании (папка **Назначенные задания**) автоматически создается задание на обновление вирусных баз и других файлов пакета, а также задание на проведение антивирусного сканирования (оно по умолчанию выключено).

Пункт **Планировщик** в разделе **Инструменты** контекстного меню **SpIDer Agent** открывает стандартный планировщик заданий Windows.

В нижней части окна на вкладке **Общие** указываются общие сведения о задании, а также параметры безопасности. На вкладках **Триггеры** и **Условия** – различные условия, при которых осуществляется запуск задания. Просмотреть историю событий можно на вкладке **Журнал**.

Вы также можете создавать собственные задания на обновление и антивирусное сканирование, а также удалять и редактировать существующие. Подробнее о работе с системным расписанием см. справочную систему и документацию операционной системы Windows.

Глава 4. Автоматическое обновление

Для современных компьютерных вирусов характерна огромная скорость распространения. В течение нескольких дней, а иногда и часов, вновь появившийся вирус может заразить миллионы компьютеров по всему миру.

Разработчики **Dr.Web** непрерывно пополняют вирусные базы новыми вирусными записями. После установки таких дополнений **Dr.Web** способен обнаруживать новые вирусы, блокировать их распространение, а в ряде случаев – излечивать зараженные файлы.

Время от времени пополняются антивирусные алгоритмы, реализованные в виде исполняемых файлов и программных библиотек **Dr.Web**. Благодаря опыту эксплуатации антивируса исправляются обнаруженные в программах ошибки, совершенствуется система помощи и документация.

Для ускорения и облегчения получения и установки обновлений вирусных баз и других файлов служит специальный компонент – **Dr.Web Модуль автоматического обновления для Windows**.

Принцип работы модуля автоматического обновления

Работа модуля обновления определяется структурой вирусных баз и методикой обновления баз и программы **Dr.Web Антивирус для серверов** в целом:

- в состав **Dr.Web** входит основная вирусная база (файл drwebase.vdb) и ее расширения (файлы drw50000.vdb, drw50001.vdb, drw50002.vdb, drw50003.vdb идrw50004.vdb). Все вместе они содержат вирусные записи, известные в момент выпуска данной версии **Dr.Web** (подробнее о

версии см. ниже);

- раз в неделю выпускаются еженедельные дополнения – файлы с вирусными записями для обнаружения и обезвреживания вирусов, выявленных за время, прошедшее с выпуска предыдущего еженедельного обновления. Еженедельные дополнения представлены файлами, наименование которых выглядит так: drwXXXYY.vdb, где XXX – номер текущей версии антивируса (без разделительной точки), а YY – порядковый номер еженедельного дополнения. Нумерация еженедельных дополнений начинается с номера 05, т.е. первое дополнение баз названо drw50005.vdb;
- по мере необходимости (обычно несколько раз в сутки) выпускаются горячие дополнения, содержащие вирусные записи для обнаружения и обезвреживания всех вирусов, выявленных после выхода последнего еженедельного дополнения. Эти дополнения выпускаются в виде файла с именем drwtoday.vdb. В конце дня содержимое этого файла добавляется в файл накопительного обновления drwdaily. vdb. Содержимое файла drwdaily.vdb в конце недели выпускается в виде очередного еженедельного обновления;
- в состав программы **Dr.Web Антивирус для серверов** входят дополнительные базы вредоносных программ drwnasty.vdb и drwrisky.vdb. Записи, предназначенные для обнаружения рекламных программ и программ дозвона, включаются в состав вирусной базы drwnasty.vdb. Записи для обнаружения программ-шуток, потенциально опасных программ и программ несанкционированного доступа включаются в состав вирусной базы drwrisky.vdb;
- время от времени выпускаются кумулятивные дополнения баз вредоносных программ. Горячие дополнения для этих баз могут выпускаться значительно реже, чем для основной вирусной базы;
- независимо от дополнений вирусных баз, время от времени выпускаются обновления прочих файлов;
- время от времени выпускаются радикальные обновления программ антивирусной защиты. Данное действие оформляется как издание новой версии антивируса. При этом все известные на данный момент вирусные записи включаются в состав новой главной вирусной базы. При

установке новой версии удаляются старые вирусные базы.

Таким образом, структура вирусных баз будет следующей:

- основная вирусная база drwebase.vdb;
- расширения основной вирусной базы drw50000.vdb, drw50001.vdb, drw50002.vdb, drw50003.vdb и drw50004.vdb;
- еженедельные дополнения (drw50005.vdb, drw50006.vdb и т. д.);
- горячее дополнение drwtoday.vdb;
- накопительное дополнение drwdaily.vdb;
- дополнительные базы вредоносных программ drwnasty.vdb и drwrisky.vdb;
- кумулятивные дополнения баз вредоносных программ (dwn50001.vdb, dwn50002.vdb и т. д. и dwr50001.vdb, dwr50002.vdb и т. д.);
- горячие дополнения баз вредоносных программ dwntoday. vdb и dwrtoday.vdb.

Для получения и установки дополнений вирусных баз и обновления в целом служит модуль автоматического обновления, описываемый ниже (см. п. Запуск модуля автоматического обновления).

Для использования модуля автоматического обновления необходимо иметь доступ в Интернет.

Обновление **Dr.Web** должно производиться при наличии у пользователя полномочий администратора.

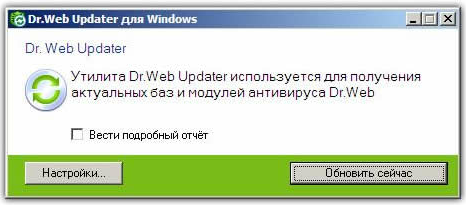
Запуск модуля автоматического обновления

Модуль автоматического обновления можно запустить одним из следующих способов:

- автоматически, по расписанию (см. п. Задание на сканирование и обновление);
- в режиме командной строки вызовом исполняемого файла drwebupw.exe из каталога установки программы;
- выбором пункта **Обновление** контекстного меню значка **SpIDer Agent**;
- нажатием кнопки **Обновить** раскрывающегося меню **Файл** в главном окне **Сканера**;
- нажатием F8 при активном окне **Сканера**.

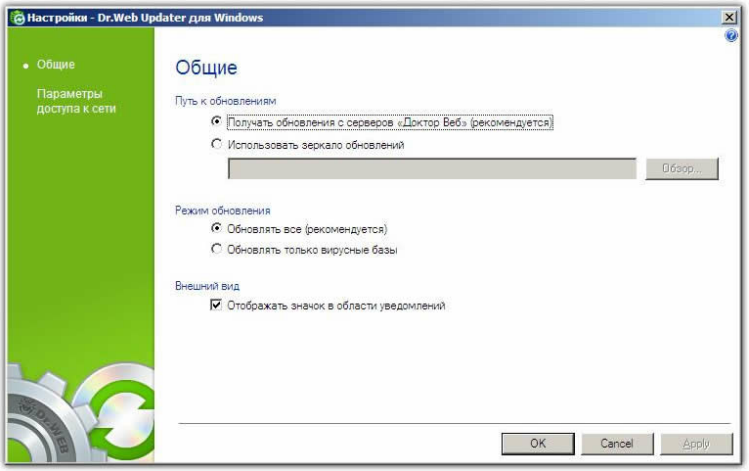
Если вы запускаете модуль **Dr.Web Updater** через меню **SpIDer Agent** или в режиме командной строки, появится диалоговое окно, в котором вы можете либо запустить обновление, либо настроить необходимые параметры. Также вы можете установить флаг **Вести подробный отчёт**, для того чтобы отчёт об изменениях был детальным. Отчет записывается в файл drwebupw.log, который находится в каталоге %USERPROFILE%\DoctorWeb.

При запуске модуля обновления автоматически, отчёт записывается в файл drwebupw.log, который находится в каталоге установки.



Настройки

Чтобы получить доступ к настройкам **Dr.Web Updater**, нажмите кнопку **Настройки**. Выберите раздел **Общие**.

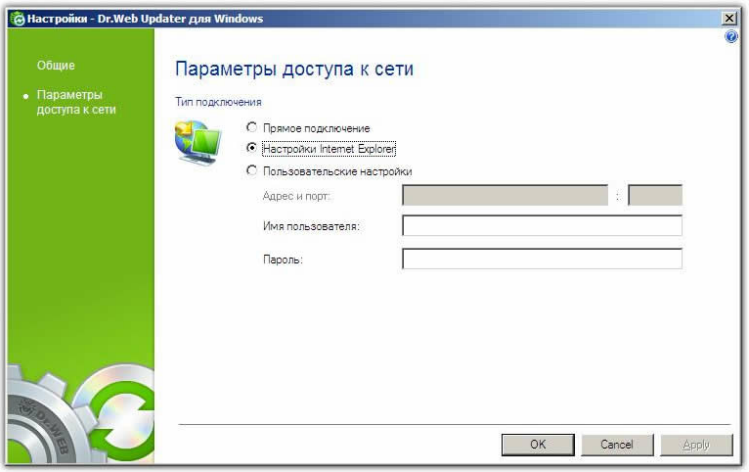


В этом разделе вы можете настроить:

- **Путь к обновлениям**. **Dr.Web Updater** может получать обновления с серверов **«Доктор Веб»** (рекомендуется) либо с зеркала обновлений. При использование зеркала обновлений укажите необходимые параметры;
- **Режим обновления**. Вы можете выбрать один из вариантов:
  - **Обновлять все (рекомендуется)**. В этом режиме будут обновляться компоненты программы **Dr.Web Антивирус для серверов**, вирусные базы и антивирусное ядро;
  - **Обновлять только вирусные базы**. В этом режиме компоненты программы **Dr.Web Антивирус для серверов** обновляться не будут;
- **Внешний вид**. По умолчанию включено отображение уведомлений об успешном обновлении компонентов и

вирусных баз. Вы можете отключить эту опцию.

В разделе **Параметры доступа к сети** вы можете указать настройки подключения к сети.



Выберите один из следующих вариантов:

- если для выхода в Интернет прокси-сервер не используется, выберите **Прямое подключение**;
- если для выхода в Интернет вы используете текущие настройки прокси-сервера, выберите пункт **Настройки Internet Explorer**;
- если вы хотите задать настройки прокси-сервера, выберите пункт **Пользовательские настройки** и укажите необходимые параметры.

Запуск обновления

При запуске обновления программа проверяет наличие лицензионного ключевого файла в каталоге установки. При отсутствии ключевого файла обновление невозможно.

При наличии ключевого файла программа проверяет на сервере www.drweb.com, не является ли ключевой файл заблокированным (блокировка файла производится в случае его дискредитации, т. е. выявления фактов его незаконного распространения). В случае блокировки обновление не производится, компоненты **Dr.Web Антивирус для серверов** могут быть заблокированы; пользователю выдается соответствующее сообщение.

В случае блокировки вашего ключевого файла свяжитесь с дилером, у которого вы приобрели **Dr.Web Антивирус для серверов**.

После успешной проверки ключевого файла происходит обновление. Программа автоматически загружает все обновленные файлы, соответствующие вашей версии **Dr.Web**, а если условия вашей подписки разрешают это, загружают новую версию (в случае ее выхода).

При обновлении исполняемых файлов и библиотек может потребоваться перезагрузка компьютера. Пользователь извещается об этом при помощи информационного окна.

Сканер может использовать обновленные базы при следующем после обновления запуске. **Сторож** периодически проверяет состояние баз и подгружает обновленные базы автоматически.

При запуске модуля автоматического обновления по расписанию или в режиме командной строки используются параметры командной строки (см. Приложение А).

Приложения

Приложение А. Дополнительные параметры командной строки

Дополнительные параметры командной строки (*ключи*) используются для задания параметров программам, которые запускаются открытием на выполнение исполняемого файла. Это относится к **Сканерам** всех версий (см. п. Сканирование в режиме командной строки) и к модулю автоматического обновления (см. Глава 4. Автоматическое обновление). При этом ключи могут задавать параметры, отсутствующие в конфигурационном файле, а для тех параметров, которые в нем заданы, имеют более высокий приоритет.

Ключи начинаются с символа / и, как и остальные параметры командной строки, разделяются пробелами.

Далее перечислены отдельно параметры командной строки для **Сканера** и для модуля автоматического обновления. Если ключ имеет модификации, они также приводятся.

Параметры перечислены в алфавитном порядке.

Параметры командной строки для Сканера

- `/?` – вывести на экран краткую справку о работе с программой и начать сканирование.
- `/@<`*имя_файла*`>` или `/@+<`*имя_файла*`>` предписывает произвести проверку объектов, которые перечислены в указанном файле. Каждый объект задается в отдельной строке файла-списка. Это может быть либо полный путь с указанием имени файла, либо строка `?boot`, означающая проверку загрузочных секторов, а для GUI-версии **Сканера** также имена файлов с маской и имена каталогов. Файл-

список может быть подготовлен с помощью любого текстового редактора вручную, а также автоматически прикладными программами, использующими **Сканер** для проверки конкретных файлов. После окончания проверки **Сканер** удаляет файл-список, если использована форма ключа без символа +.

- /AL – проверять все файлы на заданном устройстве или в заданном каталоге независимо от расширения или внутреннего формата.
- /AR – проверять файлы, находящиеся внутри архивов. В настоящее время обеспечивается проверка (без лечения) архивов ARJ, ZIP, PKZIP, ALZIP, RAR, LHA, GZIP, TAR, BZIP2, 7-ZIP, ACE и др., а также MS CAB-архивов – Windows Cabinet Files и ISO-образов оптических дисков (CD и DVD). В указанном виде (/AR) ключ задает информирование пользователя в случае обнаружения архива, содержащего зараженные или подозрительные файлы. Если ключ дополняется модификатором D, M, или R, производятся иные действия:
  - /ARD – удалять;
  - /ARM – перемещать (по умолчанию – в подкаталог infected.!!!);
  - /ARR – переименовывать (по умолчанию первая буква расширения заменяется на символ #).
  - Ключ может завершаться модификатором N, в таком случае не будет выводиться имя программы-архиватора после имени архивного файла.
- /CN – задать действие над контейнерами (HTML, RTF, PowerPoint), содержащими зараженные или подозрительные объекты. В указанном виде (/CN) ключ задает информирование пользователя в случае обнаружения такого контейнера. Если ключ дополняется модификатором D, M, или R, производятся иные действия над контейнерами:
  - /CND – удалять;
  - /CNM – перемещать (по умолчанию – в подкаталог infected.!!!);

- /CNR – переименовывать (по умолчанию первая буква расширения заменяется на символ #).
- Ключ может завершаться модификатором N, в таком случае не будет распечатываться сообщение с указанием типа контейнера.

- /CU – действия над инфицированными файлами и загрузочными секторами дисков. Без дополнительных параметров D, M или R производится лечение излечимых объектов и удаление неизлечимых файлов (если другое не задано параметром /IC). Иные действия выполняются только над инфицированными файлами:
  - /CUD – удалять;
  - /CUM – перемещать (по умолчанию – в подкаталог infected.!!!);
  - /CUR – переименовывать (по умолчанию первая буква расширения заменяется на символ #).
- /DA – проверять компьютер один раз в сутки. Дата следующей проверки записывается в файл конфигурации, поэтому он должен быть доступен для создания и последующей перезаписи.
- /EX – проверять файлы с расширениями, хранящимися в конфигурационном файле, по умолчанию или при недоступности конфигурационного файла это расширения EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

В случае если элемент списка проверяемых объектов содержит явное указание расширения файла, хотя бы и с применением специальных символов * и ?, будут проверены все файлы, заданные в данном элементе списка, а не только подходящие под список расширений.

- /FAST – предписывает произвести быстрое сканирование системы (подробно о режиме быстрого сканирования см. п. Запуск Сканера).

- /FULL – предписывает произвести полное сканирование всех жестких дисков и сменных носителей (включая загрузочные секторы).
- /GO – пакетный режим работы программы. Все вопросы, подразумевающие ожидание ответа от пользователя, пропускаются; решения, требующие выбора, принимаются автоматически. Этот режим полезно использовать для автоматической проверки файлов, например, при ежедневной (или еженедельной) проверке жесткого диска.
- /HA – производить эвристический анализ файлов и поиск в них неизвестных вирусов.
- /ICR, /ICD или /ICM – действия с зараженными файлами, вылечить которые невозможно: /ICR – переименовывать, /ICD – удалять, /ICM – перемещать.
- /INI: <*путь*> – использовать альтернативный конфигурационный файл с указанным именем или путем.
- /LNG: <*имя_файла*> или /LNG – использовать альтернативный файл языковых ресурсов (.dwl файл) с указанным именем или путем, а если путь не указан – встроенный (английский) язык.
- /ML – проверять файлы, имеющие формат сообщений e-mail (UUENCODE, XXENCODE, BINHEX и MIME). В указанном виде (/ML) параметр задает информирование пользователя в случае обнаружения зараженного или подозрительного объекта в почтовом архиве. Если параметр дополняется модификатором D, M, или R, производятся иные действия:
  - /MLD - удалять;
  - /MLM – перемещать (по умолчанию – в подкаталог infected.!!!);
  - /MLR – переименовывать (по умолчанию первая буква расширения заменяется на символ #).
  - Кроме того, параметр может завершаться дополнительным модификатором N (одновременно с этим могут быть заданы и основные модификаторы). В таком случае отключается вывод информации о почтовых файлах.
- /MW – действия со всеми видами нежелательных программ.

В указанном виде (/MW) параметр задает информирование пользователя. Если параметр дополняется модификатором D, M, R или I, производятся иные действия:

- /MWD – удалять;
- /MWM – перемещать (по умолчанию – в подкаталог infected.!!!);
- /MWR – переименовывать (по умолчанию первая буква расширения заменяется на символ #);
- /MWI – игнорировать. Действия с отдельными видами нежелательных программ определяются с помощью ключей /ADW, /DLS, /JOK, /RSK, /HCK.

- /NI – не использовать параметры, записанные в конфигурационном файле программы drweb32.ini.
- /NR – не создавать файл отчета.
- /NS – запретить возможность прерывания проверки компьютера. После указания этого параметра пользователь не сможет прервать работу программы нажатием клавиши ESC.
- /OK – выводить полный список сканируемых объектов, сопровождая незараженные пометкой **Ok**.
- /PF – запрашивать подтверждение на проверку следующей дискеты.
- /PR – выводить запрос подтверждения перед действием.
- /QU – Сканер выполняет проверку указанных в командной строке объектов (файлов, дисков, каталогов), после чего автоматически завершает работу (только для GUI-версии **Сканера**).
- /RP<*имя_файла*> или /RP+<*имя_файла*> – записать отчет о работе программы в файл, имя которого указано в ключе. При отсутствии имени записать в файл по умолчанию. При наличии символа + файл дописывается, при отсутствии – создается заново.
- /SCP: <*n*> – задает приоритет выполнения сканирования. <*n*> может принимать значения от 1 до 50 включительно.
- /SD – проверять подкаталоги.
- /SHELL – для GUI-версии **Сканера**. Отменяет показ

заставки, отключает проверку памяти и файлов автозагрузки. Этот режим позволяет использовать GUI-версию **Сканера** вместо консольной для проверки только тех объектов, которые перечислены в параметрах командной строки.

- `/SO` – включить звуковое сопровождение.
- `/SPR`, `/SPD` или `/SPM` – действия с подозрительными файлами:
  - `/SPR` – переименовывать,
  - `/SPD` – удалять,
  - `/SPM` – перемещать.
- `/SS` – по окончании работы сохранить режимы, заданные при текущем запуске программы, в конфигурационном файле.
- `/ST` – задает скрытый режим работы GUI-версии **Сканера**. Программа работает, не открывая никаких окон и самостоятельно завершаясь. Но если в процессе сканирования были обнаружены вирусные объекты, по завершении работы будет открыто обычное окно **Сканера**. Такой режим работы **Сканера** предполагает, что список проверяемых объектов задается в командной строке.
- `/TB` – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.
- `/TM` – выполнять поиск вирусов в оперативной памяти (включая системную область операционной системы Windows, только для **Сканеров для Windows**).
- `/TS` – выполнять поиск вирусов в файлах автозапуска (по папке Автозагрузка, системным .ini файлам, реестру операционной системы Windows).
- `/UPN` – при проверке исполняемых файлов, упакованных специальными программами-упаковщиками, не выводить в файл отчета названия программ, использованных для упаковки.
- `/WA` – не завершать работу программы до нажатия на любую клавишу, если обнаружены вирусы или подозрительные объекты (только для **консольных Сканеров**).

Режимы, установленные по умолчанию (если отсутствует или не используется конфигурационный файл) приведены в таблице 2.

Некоторые параметры допускают задание в конце символа "–". В такой "отрицательной" форме параметр означает отмену соответствующего режима. Такая возможность может быть полезна в случае, если этот режим включен по умолчанию или по выполненным ранее установкам в конфигурационном файле. Список параметров командной строки, допускающих "отрицательную" форму:
`/ADW /AR /CU /DLS /FN /FAST /FULL /HCK /JOK /HA /IC /ML /MW /OK /PF /PR /RSK /SD /SO /SP /SS /TB /TM /TS /WA`

Для параметров `/CU`, `/IC` и `/SP` "отрицательная" форма отменяет выполнение любых действий, указанных в описании этих параметров. Это означает, что в отчете будет фиксироваться информация о зараженных и подозрительных объектах, но никаких действий над этими объектами выполняться не будет.

Для параметров `/INI` и `/RP` "отрицательная" форма записывается в виде `/NI` и `/NR` соответственно.

Для параметров `/AL` и `/EX` не предусмотрена "отрицательная" форма, однако задание одного из них отменяет действие другого.

Если в командной строке встречаются несколько взаимоисключающих параметров, то действует последний из них.

Параметры для Консольного Сканера DWScancl

- /AR – проверять архивы.
- /AC – проверять контейнеры.
- /AFS – использовать прямой слеш при указании вложенности внутри архива.
- /ARC: <*n*> – максимальный уровень сжатия. Если **Консольный сканер** определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка не производится.
- /ARL: <*n*> – максимальный уровень вложенности проверяемого архива.
- /ARS: <*n*> – максимальный размер проверяемого архива.
- /ART: <*n*> – порог проверки уровня сжатия (минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия).
- /ARX:<*n*> – максимальный размер проверяемых объектов в архивах.
- /BI – вывести информацию о вирусных базах.
- /DR – рекурсивно сканировать директории (проверять поддиректории).
- /E:<*n*> – использовать указанное количество движков.
- /FL:<*имя_файла*> – сканировать пути, указанные в файле.
- /FR:regexpr – сканировать файлы по регулярному выражению.
- /FM:masks – сканировать файлы по маске.
- /H or /? – вывести на экран краткую справку о работе с программой.
- /HA – производить эвристический анализ файлов и поиск в них неизвестных вирусов.
- /KEY:<*ключевой_файл*> – указать путь к ключевому файлу. Параметр необходим в том случае, если ключевой файл находится не в той же директории, что и **Консольный сканер**.

- /LN – сканировать файлы, на которые указывают ярлыки.
- /LS – сканировать под учетной записью LocalSystem.
- /MA – проверять почтовые файлы.
- /MC:<*число*> – установить максимальное число попыток вылечить файл.
- /NB – не создавать резервные копии вылеченных/удалённых файлов.
- /NI[:X] – уровень использования ресурсов системы. Определяет количество памяти используемой для сканирования и системный приоритет задачи сканирования.
- /NT – сканировать NTFS-потоки.
- /OK – выводить полный список сканируемых объектов, сопровождая незараженные пометкой **Ok**.
- /P:<*приоритет*> – приоритет запущенной задачи сканирования в общей очереди задач на сканирование:
  - 0 – низший.
  - L – низкий.
  - N – обычный. Приоритет по умолчанию.
  - H – высший.
  - M – максимальный.
- /PAL:level – уровень вложенности упаковщиков (по умолчанию – 1000).
- /RA:file.log – дописать отчет о работе программы в указанный файл.
- /RP:file.log – записать отчет о работе программы в указанный файл.
- /RPC:<*секунды*> – таймаут соединения с ScanEngine (по умолчанию – 30 секунд).
- /RPCD – использовать динамический идентификатор RPC.
- /RPCE – использовать динамический целевой адрес RPC.
- /RPCE:<*целевой_адрес*> – использовать указанный целевой адрес RPC.
- /RPCH:<*имя_хоста*> – использовать указанное имя хоста для вызовов RPC.
- /RPCP:<*протокол*> – использовать указанный протокол

RPC (lpc,np,tcp).

- /QL – вывести список всех файлов, помещённых в карантин на всех дисках.
- /QL:drive – вывести список всех файлов, помещённых в каранатин на указанном логическом диске.
- /QR[:[d][:p]] – удалить файлы с указанного диска <*d*>, находящие в карантие дольше <p> дней. Если <d> и <p> не указаны, то будут удалены все файлы, находящиеся в карантине, со всех логических дисков.
- /QNA – выводить пути в двойных кавычках.
- /REP – сканировать по символьным ссылкам.
- /SCC – выводить содержимое составных объектов.
- /SCN – выводить название контейнера.
- /SPN – выводить название упаковщика.
- /SLS – выводить логи на экран.
- /SPS – отображать процесс проведения сканирования.
- /SST – выводить время сканирования файла.
- /TB – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.
- /TM – выполнять поиск вирусов в оперативной памяти (включая системную область Windows).
- /TS – выполнять поиск вирусов в файлах автозапуска (по папке Автозагрузка, системным ini-файлам, реестру Windows).
- /TR – сканировать системные точки восстановления.
- /W:<*секунды*> – максимальное время сканирования.
- /WCL – вывод, совместимый с drwebwcl.
- /X: S[:R] – по окончании сканирования перевести машину в указанный режим: выключение/перезагрузка/ждущий режим/спящий режим.

Задание действий с различными объектами (C - вылечить, Q - переместить в карантин, D - удалить, I - игнорировать, R - информировать. По умолчанию для всех - информировать):

- /AAD:<*действие*> – действия для рекламных программ

(возможные действия: DQIR)

- /AAR:<*действие*> – действия с архивами (возможные действия: DQIR)
- /ACN:<*действие*> – действия с контейнерами (возможные действия: DQIR)
- /ADL:<*действие*> – действия с программами дозвона (возможные действия: DQIR)
- /AHT:<*действие*> – действия с программами взлома (возможные действия: DQIR)
- /AIC:<*действие*> – действия с неизлечимыми файлов (возможные действия: DQR)
- /AIN:<*действие*> – действия с инфицированными файлов (возможные действия: CQIR)
- /AJK:<*действие*> – действия с программами-шутками (возможные действия: DQIR)
- /AML:<*действие*> – действия с почтовыми файлами (возможные действия: QIR)
- /ARW:<*действие*> – действия с потенциально опасными файлами (возможные действия: DQIR)
- /ASU:<*действие*> – действия с подозрительными файлами (возможные действия: DQIR)

Параметры командной строки для модуля автоматического обновления

При запуске модуля автоматического обновления через Планировщик Windows или в режиме командной строки вы можете ввести следующие параметры командной строки:

- `/DBG` – вести подробный отчет.
- `/DIR`: *<каталог>* – переназначение каталога, в который устанавливаются файлы обновления; по умолчанию это каталог, из которого модуль обновления был запущен.
- `/INI`: *<путь>* – использовать альтернативный конфигурационный файл с указанным именем или путем.
- `/GO` – пакетный режим работы, без диалоговых остановок.
- `/LNG`: *<имя_файла>* – имя файла языковых ресурсов; если не указано, использовать английский язык.
- `/NI` – не использовать параметры, записанные в конфигурационном файле программы drweb32.ini.
- `/NR` – не создавать файл отчета.
- `/PASS`: *<пароль пользователя http-сервера>* – пароль пользователя сервера обновлений.
- `/PPASS`: *<пароль пользователя прокси>* – пароль пользователя проксисервера.
- `/PUSER`: *<имя пользователя прокси>* – имя пользователя прокси-сервера.
- `/PURL`: *<адрес прокси>* – адрес проксисервера.
- `/QU` – принудительно закрывать модуль обновления после окончания сеанса обновления независимо от того, успешно оно прошло или нет. Успешность обновления можно проверить по коду возврата программы `drwebupw.exe` (например, из bat-файла по значению переменной `errorlevel`: 0 – успешно, другие значения – неуспешно).
- `/RP`*<имя_файла>* или `/RP+`*<имя_файла>* – записать отчет о работе программы в файл, имя которого указано в ключе. При отсутствии имени записать в файл по умолчанию. При наличии символа «+» файл дописывается, при отсутствии –

создается заново.

- /SETTINGS – отобразить окно настроек модуля автоматического обновления.
- /SO – включить звуковое сопровождение (только при возникновении ошибки).
- /ST – запускать модуль обновления в невидимом окне (stealth mode).
- /UA – загрузка всех файлов, заявленных в списке обновления, независимо от используемой системы и установленных компонентов. Режим предназначен для получения полной локальной копии серверной области обновления **Dr.Web**; этот режим нельзя использовать для обновления антивируса, установленного на компьютере.
- /UPM: <*режим прокси*> – режим использования проксисервера; может принимать следующие значения:
  - direct – не использовать прокси-сервер,
  - ieproxy – использовать системные настройки,
  - userproxy – использовать настройки, задаваемые пользователем (на вкладке Обновление панели настроек **Dr.Web** или ключами /PURL /PUSER /PPASS).
- /URL: <url сервера обновления> – допускаются только UNC-пути.
- /URM: <*режим*> – режим перезагрузки после обновления; может принимать следующие значения:
  - prompt – по окончании сеанса обновления в случае необходимости перезагрузки выдавать запрос,
  - noprompt – в случае необходимости перезагружаться без выдачи запроса,
  - force – перезагружать принудительно всегда (независимо от того, требуется это для обновления или нет),
  - disable – запретить перезагрузку.
- /UPD – обычное обновление.
- /USER: <*имя пользователя http-сервера*> – имя пользователя сервера обновлений.

- /UVB – обновлять только вирусные базы и ядро drweb32.dll (отменяет действие ключа /UA, если он задан).

Режимы, установленные по умолчанию (если отсутствует или не используется конфигурационный файл) приведены в таблице 2.

Параметр /SO допускает задание в конце символа "–". В такой "отрицательной" форме параметр означает отмену соответствующего режима. Такая возможность может быть полезна в случае, если этот режим включен по выполненным ранее установкам в конфигурационном файле.

Для параметров /INI и /RP "отрицательная" форма записывается в виде /NI и /NR соответственно.

Если в командной строке встречаются несколько взаимоисключающих параметров, то действует последний из них.

Коды возврата

Возможные значения кода возврата и соответствующие им события следующие:

Код возврата	Событие
0	OK, не обнаружено вирусов или подозрений на вирусы
1	обнаружены известные вирусы
2	обнаружены модификации известных вирусов
4	обнаружены подозрительные на вирус объекты
8	в архиве, контейнере или почтовом ящике обнаружены известные вирусы
16	в архиве, контейнере или почтовом ящике обнаружены модификации известных вирусов
32	в архиве, контейнере или почтовом ящике обнаружены подозрительные на вирус объекты
64	успешно выполнено лечение хотя бы одного зараженного вирусом объекта
128	выполнено удаление/переименование/перемещение хотя бы одного зараженного файла

Результирующий код возврата, формируемый по завершению проверки, равен сумме кодов тех событий, которые произошли во время проверки (и его слагаемые могут однозначно быть по нему восстановлены).

Например, код возврата 9 = 1 + 8 означает, что во время проверки обнаружены известные вирусы (вирус), в том числе в архиве; обезвреживание не проводилось; больше никаких "вирусных" событий не было.

Приложение В. Настраиваемые параметры компонентов Dr.Web

Настраиваемые параметры компонентов программы **Dr.Web Антивирус для серверов** (за исключением **SpIDer Guard**) хранятся, главным образом, в конфигурационном файле программы (файле drweb32.ini, расположенном в каталоге установки). Этот файл имеет текстовый формат и разделяется на секции, соответствующие отдельным компонентам. Каждый параметр какого-либо компонента представляется в соответствующей секции строкой вида: *<параметр> = <значение>*.

Изменение значений параметров осуществляется одним из следующих способов:

- средствами интерфейса соответствующих программ (**Сканера**). Наиболее важные из таких настроек были приведены выше;
- заданием параметров командной строки при вызове программ из режима командной строки или по расписанию (для **Сканера** различных версий). Подробнее об этой возможности см. Приложение А.
- непосредственным редактированием конфигурационного файла в любом текстовом редакторе.

Непосредственное редактирование конфигурационного файла может быть рекомендовано только опытным пользователям. Использование этой возможности без ясного понимания устройства **Dr.Web** может снизить качество защиты и даже привести к полной неработоспособности некоторых программ.

Перед редактированием конфигурационного файла следует деактивировать сторож, как указано в соответствующих разделах.

Параметры Windows-версий Сканера и модуля автоматического обновления

В колонках таблицы 2 приведены следующие сведения для каждого параметра:

- наименование параметра,
- наименования компонентов, использующих параметр,
- наименование параметра в конфигурационном файле,
- значения параметра,
- ключи командной строки.

Наименование параметра указывается либо в соответствии с интерфейсом (в этом случае оно дается полужирным шрифтом), либо как условное наименование, если ему нет аналога в интерфейсе (тогда оно дается светлым шрифтом).

В данной таблице наименование компонента «Сканер» подразумевает под собой обе версии **Сканера** («**Сканер-GUI**» и «**Сканер-консольный**»).

Если для отдельного режима нет соответствующего ему параметра конфигурационного файла, то значения параметра указаны в скобках и относятся к состоянию диалогового элемента интерфейса или к заданному ключу командной строки.

Значения по умолчанию для **Сканера** и модуля автоматического обновления выделены полужирным шрифтом, для всех компонентов – полужирным курсивом.

Ключи командной строки, соответствующие данному параметру, описываются сокращенно, без большинства модификаторов. Более подробная информация о ключах приведена в Приложении А.

Таблица 2. Настраиваемые параметры Windows-версий Сканера, сторожа и модуля автоматического обновления

Наименование	Компоненты	Параметр конф. файла	Значения	Ключи
Режим проверки	Сканер	ScanFiles	**All** ByType ByMasks	/AL /EX
Быстрая проверка системы	Сканер			/FAST
Полная проверка системы	Сканер			/FULL
Приоритет выполнения сканирования, от 1 до 50	Сканер			/SCP
Эвристический анализ	Сканер	HeuristicAnalysis	**Yes** / No	/HA
Проверять память	Сканер	TestMemory	**Yes** / No	/TM
Проверять файлы автозагрузки	Сканер	TestStartup	**Yes** / No	/TS
Проверять загрузочные секторы	Сканер	TestBootSectors	**Yes** / No	/TB
Проверять подкаталоги	Сканер	ScanSub Directories	**Yes** / No	/SD
Проверка нескольких дискет	Сканер	PromptFloppy	**Yes** / No	/PF
Файлы в архивах	Сканер	CheckArchives	**Yes** / *No*	/AR

Наименование	Компо-ненты	Параметр конф. файла	Значения	Клю чи
Почтовые файлы	Сканер	CheckEMailFiles	**Yes** / *No*	/ML
Макс. длина распакованного из архива файла, подлежащего проверке, Кбайт	Сканер-консольный	MaxFileSizeTo Extract	*(не задано)*	
Макс. коэффициент сжатия файла в архиве	Сканер-консольный	MaxCompression Ratio	*(не задано)*	
Нижний порог срабатывания параметра MaxCompression Ratio, Кбайт	Сканер-консольный	Compression CheckThreshold	*(не задано)*	
Список расширений	Сканер	FilesTypes	**(см. после табл.)**	
Список масок	Сканер	UserMasks	**(см. после табл.)**	
Список исключаемых путей	Сканер	ExcludePaths	**(пусто)**	
Список исключаемых файлов	Сканер	ExcludeFiles	**(пусто)**	
Проверять жесткие диски (при сканировании с параметром командной строки * и при нажатии кнопки **Выделить диски**)	Сканер	ScanHDD	**Yes** / No	

Наименование	Компо-ненты	Параметр конф. файла	Значения	Клю чи
Проверять дискеты (при сканировании с параметром командной строки * и при нажатии кнопки **Выделить диски**)	Сканер	ScanFDD	Yes / **No**	
Проверять компакт-диски (при сканировании с параметром командной строки * и при нажатии кнопки **Выделить диски**)	Сканер	ScanCD	Yes / **No**	
Проверять сетевые диски (при сканировании с параметром командной строки * и при нажатии кнопки **Выделить диски**)	Сканер	ScanNet	Yes / **No**	
Запрос подтвержде-ния	Сканер	PromptOnAction	**Yes** / No	/PR
Переимено-вать расширение	Сканер	RenameFilesTo	**#??**	
Имя каталога карантина	Сканер	MoveFilesTo	infected.!!!	

Наименование	Компоненты	Параметр конф. файла	Значения	Ключи
Список путей к вирусным базам	Сканер	VirusBase	*.vdb	
Путь к каталогу временных файлов компонента	Сканер	TempPath	**%TMP%, %TEMP%, каталог установки**	
Действия со всеми видами нежелательных программ	Сканер		Информировать	/MW
Инфицированные объекты	Сканер	InfectedFiles	**Report** **Cure** Delete Rename Move	/CU
Неизлечимые объекты	Сканер	IncurableFiles	**Report** Delete Rename **Move**	/IC
Подозрительные объекты	Сканер	SuspiciousFiles	**Report** Delete Rename **Move**	/SP
Инфицированные архивы	Сканер	ActionInfected Archive	**Report** Delete Rename **Move**	/AR
Инфицированные почтовые файлы	Сканер	ActionInfected Mail	**Report** Delete Rename **Move**	/ML
Рекламные программы	Сканер	ActionAdware	**Report** Delete Rename **Move** Ignore	/ADW

Наименование	Компо-ненты	Параметр конф. файла	Значения	Клю чи
Программы дозвона	Сканер	ActionDialers	**Report** Delete Rename **Move** Ignore	/DLS
Программы-шутки	Сканер	ActionJokes	Report Delete Rename Move **Ignore**	/JOK
Потенциально опасные программы	Сканер	ActionRiskware	Report Delete Rename Move **Ignore**	/RSK
Программы взлома	Сканер	ActionHacktools	Report Delete Rename Move **Ignore**	/HCK
Разрешить удаление архивов без запроса предупреждения	Сканер	EnableDelete ArchiveAction	Yes / **No**	
Вести файл отчета	Сканер, модуль обновления	LogToFile	**Yes** / No	/RP /NR
Имя файла отчета	Сканер	LogFileName	**drweb32w.log** *spider.log* *spidernt.log*	/RP
Имя файла отчета	Модуль обновления		**drwebupw.log**	/RP
Режим открытия отчета	Сканер, модуль обновления	OverwriteLog	Yes / **No**	/RP

Наименование	Компоненты	Параметр конф. файла	Значения	Ключи
Кодировка отчета	Сканер, модуль обновления	LogFormat	**ANSI** OEM	
Проверяемые объекты в отчете	Сканер	LogScanned	**Yes / No**	/OK
Имена упаковщиков в отчете	Сканер	LogPacked	*Yes* / **No**	
Имена архиваторов в отчете	Сканер	LogArchived	*Yes* / **No**	
Статистика в отчете	Сканер	LogStatistics	**Yes** / No	
Предельный размер файла отчета	Сканер, модуль обновления	LimitLog	Yes / **No**	
Предельный размер файла отчета, Кбайт	Сканер, модуль обновления	MaxLogSize	**512** **8192**	
Закрыть окно после сеанса	Сканер, модуль обновления		Yes / **No**	/QU
Ожидать нажатия на клавишу (после завершения сканирования в случае обнаружения вирусов)	Сканер-консольный	WaitAfterScan	(Вкл./ **Выкл.**)	/WA
Исполнять в пакетном режиме	Сканер, модуль обновления		(Вкл./ **Выкл.**)	/GO
Запретить прерывание пользователем	Сканер		(Вкл./ **Выкл.**)	/NS

Наименование	Компо-ненты	Параметр конф. файла	Значения	Клю чи
Проверять один раз в сутки	Сканер		(Вкл./ **Выкл**.)	/DA
Проверять только явно заданные объекты	Сканер-GUI		(Вкл./ **Выкл**.)	/ SHEL L
Не открывать окон (режим stealth)	Сканер-GUI		(Вкл./ **Выкл**.)	/ST
Использовать альтернативный конфиг. файл. Не использовать никакого конфиг. файла	Сканер, модуль обновления		(Вкл./ **Выкл**.)	/INI /NI
Использовать собственный файл подкачки	Сканер	UseDiskForSwap	**Yes** / No	
Отображать индикатор работы (прогресс-индикатор)	Сканер	ShowProgressBar	**Yes** / No	
Звуки	Сканер, модуль обновления	PlaySounds	Yes / **No**	/SO
Опасность (звук)	Сканер	AlertWav	alert.wav	
Исцелен (звук)	Сканер	CuredWav	cured.wav	
Удален (звук)	Сканер	DeletedWav	deleted.wav	
Переименован (звук)	Сканер	RenamedWav	renamed.wav	
Перемещен (звук)	Сканер	MovedWav	moved.wav	

Наименование	Компо-ненты	Параметр конф. файла	Значения	Клю чи
Конец проверки (звук)	Сканер	FinishWav	finish.wav	
Ошибка (звук)	Сканер, модуль обновления	ErrorWav	error.wav	
Автосохранение настроек при выходе	Сканер	AutoSaveSettings	**Yes** / No	/SS
Использовать настройки из реестра	Сканер-GUI		(**Вкл.**/ Выкл.)	
Приоритет проверки	Сканер	ScanPriority	**25** **50**	
Язык (Language)	Сканер, модуль обновления	LngFileName	**ru-drweb.dwl**	/LNG
Режим прокси	Сканер-GUI (настройки модуля обновления)	UpdateProxyMode	direct **ieproxy** userproxy	/UPM
Обновлять только вирусные базы и ядро *drweb32.dll*	модуль обновления	UpdateVirusBasesOnly	Yes / **No**	/UVB
Загрузка всех файлов, заявленных в списке обновления	модуль обновления	UpdateAllFiles	Yes / **No**	/UA
Режим перезагрузки при обновлении	модуль обновления	UpdateRebootMode	**prompt** noprompt force disable	/URM
Вести подробный отчет	модуль обновления		(Вкл./ **Выкл.**)	/DBG

Список расширений файлов (значение параметра `FilesTypes` конфигурационного файла) по умолчанию содержит следующие расширения: EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

Список выбранных масок (значение параметра `UserMasks` конфигурационного файла) по умолчанию состоит из значений, получаемых добавлением знака `*` и точки перед расширением из списка расширений файлов (например, "`*.exe`").

Приложение C. Вредоносные программы и способы их обезвреживания

С развитием компьютерных технологий и сетевых решений, всё большее распространение получают различные вредоносные программы, направленные на то, чтобы так или иначе нанести вред пользователям. Их развитие началось еще в эпоху зарождения вычислительной техники, и параллельно развивались средства защиты от них. Тем не менее, до сих пор не существует единой классификации всех возможных угроз, что связано, в первую очередь, с непредсказуемым характером их развития и постоянным совершенствованием применяемых технологий.

Вредоносные программы могут распространяться через Интернет, локальную сеть, электронную почту и съемные носители информации. Некоторые рассчитаны на неосторожность и неопытность пользователя и могут действовать полностью автономно, другие являются лишь инструментами под управлением компьютерных взломщиков и способны нанести вред даже надежно защищенным системам.

В данной главе представлены описания всех основных и наиболее распространенных типов вредоносных программ, на борьбу с

которыми в первую очередь и направлены разработки **«Доктор Веб»**.

Классификация вредоносных программ и других компьютерных угроз

Компьютерные вирусы

Главной особенностью таких программ является способность к внедрению своего кода в исполняемый код других программ. Такое внедрение называется инфицированием (или заражением). В большинстве случаев инфицированный файл сам становится носителем вируса, причем внедренная часть кода не обязательно будет совпадать с оригиналом. Действия большинства вирусов направлены на повреждение или уничтожение данных. Вирусы, которые внедряются в файлы операционной системы (в основном, исполняемые файлы и динамические библиотеки), активируются при запуске пораженной программы и затем распространяются, называются файловыми.

Некоторые вирусы внедряются не в файлы, а в загрузочные записи дискет, разделы жестких дисков, а также MBR (Master Boot Record) жестких дисков. Такие вирусы называются загрузочными, занимают небольшой объем памяти и пребывают в состоянии готовности к продолжению выполнения своей задачи до выгрузки, перезагрузки или выключения компьютера.

Макровирусы – это вирусы, заражающие файлы документов, используемые приложениями Microsoft Office и другими программами, допускающими наличие макрокоманд (чаще всего на языке Visual Basic). Макрокоманды – это встроенные программы (макросы) на полнофункциональном языке программирования. Например, в Microsoft Word эти макросы могут автоматически запускаться при открытии любого документа, его закрытии, сохранении и т.д.

Вирусы, которые способны активизироваться и выполнять заданные вирусописателем действия, например, при достижении компьютером определенного состояния называются резидентными.

Большинство вирусов обладают той или иной защитой от

обнаружения. Способы защиты постоянно совершенствуются и вместе с ними разрабатываются новые технологии борьбы с ними.

Например, шифрованные вирусы шифруют свой код при каждом новом заражении для затруднения его обнаружения в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры.

Существуют также полиморфные вирусы, использующие помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур.

Стелс вирусы (вирусы-невидимки) - вирусные программы, предпринимающие специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в зараженных объектах. Такой вирус снимает перед заражением характеристики инфицируемой программы, а затем подсовывает старые данные программе, ищущей изменённые файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на ассемблере, высокоуровневых языках программирования, скриптовых языках и т.д.) и по поражаемым операционным системам.

Компьютерные черви

В последнее время, черви стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны размножать свои копии, но они не могут заражать другие компьютерные программы. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через сеть Интернет) и рассылает свои функциональные копии в другие компьютерные сети. Причем для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

Черви не всегда целиком состоят из одного файла (тела червя). У

многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в ОЗУ и «догружает» по сети непосредственно само тело в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс ОЗУ). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения, черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

Троянские программы (троянские кони, трояны)

Этот тип вредоносных программ не способен к саморепликации. Трояны подменяют какую-либо из часто запускаемых программ и выполняют её функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т.д.), либо делая возможным несанкционированное использование компьютера другим лицом, например для нанесения вреда третьему лицу.

Троянец обладает схожими с вирусом маскировочными и вредоносными функциями и даже может быть модулем вируса, но в основном троянские программы распространяются, как отдельные исполняемые файлы (выкладываются на файл-сервера, записываются на носители информации или пересылаются в виде приложений к сообщениям), которые запускаются либо самим пользователем, либо определенным процессом системы.

Руткит

Это вредоносная программа, предназначенная для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в

составе другой вредоносной программы. По сути – это набор утилит, которые взломщик устанавливает в систему, к которой получил первоначальный доступ.

По принципу своей работы руткиты условно разделяют на две группы: *User Mode Rootkits (UMR)* - работающие в режиме пользователя (перехват функций библиотек пользовательского режима), и *Kernel Mode Rootkits (KMR)* - работающие в режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет его обнаружение и обезвреживание).

Программы взлома

К данному типу вредоносных программ относятся различные инструменты, которыми злоумышленники пользуются для взлома компьютеров и сетей. Наиболее распространенными среди них являются сканеры портов, которые выявляют уязвимости в системе защиты компьютера. Помимо взломщиков, подобными программами пользуются администраторы для контроля безопасности своих сетей. Иногда к программам взлома причисляют различное распространенное ПО, которое может использоваться для взлома, а также некоторые программы, использующие методы социальной инженерии (получение конфиденциальной информации у пользователей путем введения их в заблуждение).

Шпионские программы

Этот тип вредоносных программ, предназначен для слежения за системой и отсылкой собранной информации третьей стороне - создателю или заказчику такой программы. Заказчиками шпионских программ могут быть: распространители спама и рекламы, маркетинговые агентства, скам-агентства, преступные группировки, деятели промышленного шпионажа.

Такие программы тайно закачиваются на компьютер вместе с каким-либо программным обеспечением или при просмотре определенных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя.

Побочные эффекты от присутствия шпионских программ на компьютере - нестабильная работа браузера и замедление производительности системы.

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например, в интеренет-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

Это специальные компьютерные программы, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон жертве или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

Все вышеперечисленные типы программ считаются вредоносными, т.к. представляют угрозу либо данным пользователя, либо его правам на конфиденциальность информации. К вредоносным не принято причислять программы,

не скрывающие своего внедрения в систему, программы для рассылки спама и анализаторы трафика, хотя потенциально и они могут при определенных обстоятельствах нанести вред пользователю.

Среди программных продуктов также выделяется целый класс потенциально опасных программ, которые не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. Причем, это не только программы, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К ним можно отнести различные программы удаленного общения и администрирования, FTP-сервера и т.д.

Ниже приведены некоторые виды хакерских атак и интернет-мошенничества:

- *Атаки методом подбора пароля* - специальная троянская программа вычисляет необходимый для проникновения в сеть пароль методом подбора на основании заложенного в эту программу словаря паролей или генерируя случайные последовательности символов.
- *DoS-атаки* (отказ обслуживания) и *DDoS-атаки* (распределённый отказ обслуживания) - вид сетевых атак, граничащий с терроризмом, заключающийся в посылке огромного числа запросов с требованием услуги на атакуемый сервер. При достижении определенного количества запросов (ограниченного аппаратными возможностями сервера), сервер перестает с ними справляться, что приводит к отказу в обслуживании. DDoS-атаки отличаются от DoS-атак тем, что осуществляются сразу с большого количества IP-адресов.
- *Почтовые бомбы* - один из простейших видов сетевых атак. Злоумышленником посылается на компьютер пользователя или почтовый сервер компании одно огромное сообщение, или множество (десятки тысяч) почтовых сообщений, что приводит к выводу системы из строя. В антивирусных продуктах **Dr.Web** для почтовых серверов предусмотрен специальный механизм защиты от таких атак.
- *Сниффинг* - вид сетевой атаки, также называется

"пассивное прослушивание сети". Несанкционированное прослушивание сети и наблюдение за данными, которое производятся при помощи специальной невредоносной программы - пакетного сниффера, который осуществляет перехват всех сетевых пакетов домена, за которым идет наблюдение.

- *Спуфинг* - вид сетевой атаки, заключающейся в получении обманным путем доступа в сеть посредством имитации соединения.
- *Фишинг* (*Phishing*) - технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д. При помощи спамерских рассылок или почтовых червей потенциальным жертвам рассылаются подложные письма, якобы от имени легальных организаций, в которых их просят зайти на подделанный преступниками интернет-сайт такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию, в последствии используемую злоумышленниками для кражи денег со счета жертвы и в других преступлениях.
- *Вишинг* (*Vishing*) - технология интернет-мошенничества, разновидность фишинга, отличающаяся использованием вместо электронной почты war diallers (автонабирателей) и возможностей Интернет-телефонии (VoIP).

Действия, применяемые к вредоносным программам

Существует множество различных методов борьбы с компьютерными угрозами. Для надежной защиты компьютеров и сетей продукты **«Доктор Веб»** объединяют в себе эти методы при помощи гибких настроек и комплексного подхода к обеспечению безопасности. Основными действиями для обезвреживания вредоносных программ являются:

1. *Лечение* – действие, применяемое к вирусам, червям и троянам. Оно подразумевает удаление вредоносного кода из зараженных файлов либо удаление функциональных копий вредоносных программ, а также, по возможности,

восстановление работоспособности пораженных объектов (т.е. возвращение структуры и функционала программы к состоянию, которое было до заражения). Далеко не все вредоносные программы могут быть вылечены, однако именно продукты **«Доктор Веб»** предоставляют самые эффективные алгоритмы лечения и восстановления файлов, подвергшихся заражению.

2. *Перемещение в карантин* – действие, при котором вредоносный объект помещается в специальную папку, где изолируется от остальной системы. Данное действие является предпочтительным при невозможности лечения, а также для всех подозрительных объектов. Копии таких файлов желательно пересылать для анализа в **вирусную лабораторию «Доктор Веб»**.
3. *Удаление* – эффективное действие для борьбы с компьютерными угрозами. Оно применимо для любого типа вредоносных объектов. Следует отметить, что иногда удаление будет применено к некоторым файлам, для которых было выбрано лечение. Это происходит в случае, когда весь файл целиком состоит из вредоносного кода и не содержит никакой полезной информации. Так, например, под лечением компьютерного червя подразумевается удаление всех его функциональных копий.
4. *Блокировка, переименование* – это также действия, позволяющие обезвредить вредоносные программы, при которых, однако, в файловой системе остаются их полноценные копии. В первом случае блокируются любые попытки обращения от и к вредоносному объекту. Во втором случае, расширение файла изменяется, что делает его неработоспособным.

Приложение D. Принципы именования вирусов

При обнаружении вирусного кода компоненты **Dr.Web** сообщают пользователю средствами интерфейса и заносят в файл отчета имя вируса, присвоенное ему специалистами **«Доктор Веб»**. Эти имена строятся по определенным принципам и отражают конструкцию вируса, классы уязвимых объектов, среду распространения (ОС и прикладные пакеты) и ряд других особенностей. Знание этих принципов может быть полезно для выявления программных и организационных уязвимостей защищаемой системы. Ниже дается краткое изложение принципов именования вирусов; более полная и постоянно обновляемая версия описания доступна по адресу http://vms.drweb.com/classification/.

Эта классификация в ряде случаев условна, поскольку конкретные виды вирусов могут обладать одновременно несколькими приведенными признаками. Кроме того, она не может считаться исчерпывающей, поскольку постоянно появляются новые виды вирусов и, соответственно, идет работа по уточнению классификации.

Полное имя вируса состоит из нескольких элементов, разделенных точками. При этом некоторые элементы, стоящие в начале полного имени (префиксы) и в конце (суффиксы), являются типовыми в соответствии с принятой классификацией.

Основные префиксы

Префиксы операционной системы

Нижеследующие префиксы применяются для называния вирусов, инфицирующих исполняемые файлы определенных платформ (ОС):

- `Win` – 16-разрядные программы ОС Windows 3.1,
- `Win95` – 32-разрядные программы ОС Windows 95, ОС

Windows 98, ОС Windows Me,

- WinNT – 32-разрядные программы ОС Windows NT, ОС Windows 2000, ОС Windows XP, ОС Windows Vista,
- Win32 – 32-разрядные программы различных сред ОС Windows 95, ОС Windows 98, ОС Windows Me и ОС Windows NT, ОС Windows 2000, ОС Windows XP, ОС Windows Vista,
- Win32.NET – программы в операционной среде Microsoft .NET Framework,
- OS2 – программы ОС OS/2,
- Unix – программы различных UNIX-систем,
- Linux – программы ОС Linux,
- FreeBSD – программы ОС FreeBSD,
- SunOS – программы ОС SunOS (Solaris),
- Symbian – программы ОС Symbian OS (мобильная ОС).

Заметим, что некоторые вирусы могут заражать программы одной системы, хотя сами действуют в другой.

Вирусы, поражающие файлы MS Office

Группа префиксов вирусов, поражающих объекты MS Office (указан язык макросов, поражаемых данным типом вирусов):

- WM – Word Basic (MS Word 6.0-7.0),
- XM – VBA3 (MS Excel 5.0-7.0),
- W97M – VBA5 (MS Word 8.0), VBA6 (MS Word 9.0),
- X97M – VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0),
- A97M – базы данных MS Access'97/2000,
- PP97M – файлы-презентации MS PowerPoint,
- O97M – VBA5 (MS Office'97), VBA6 (MS Office'2000), вирус заражает файлы более чем одного компонента MS Office.

Префиксы языка разработки

Группа префиксов HLL применяется для именования вирусов, написанных на языках программирования высокого уровня, таких как C, C++, Pascal, Basic и другие. Используются модификаторы,

указывающие на базовый алгоритм функционирования, в частности:

- HLLW – черви,
- HLLM – почтовые черви,
- HLLO – вирусы, перезаписывающие код программы жертвы,
- HLLP – вирусы-паразиты,
- HLLC – вирусы-спутники.

К группе префиксов языка разработки можно также отнести:

- Java – вирусы для среды виртуальной машины Java.

Троянские кони

Trojan – общее название для различных Троянских коней (троянцев). Во многих случаях префиксы этой группы используются совместно с префиксом Trojan.

- PWS – троянец, ворующий пароли,
- Backdoor – троянец с RAT-функцией (*Remote Administration Tool* – утилита удаленного администрирования),
- IRC – троянец, использующий для своего функционирования среду Internet Relayed Chat channels,
- DownLoader – троянец, скрытно от пользователя загружающий различные вредоносные файлы из Интернета,
- MulDrop – троянец, скрытно от пользователя загружающий различные вирусы, содержащиеся непосредственно в его теле,
- Proxy – троянец, позволяющий злоумышленнику анонимно работать в Интернете через пораженный компьютер,
- StartPage (синоним: Seeker) – троянец, несанкционированно подменяющий адрес страницы, указанной браузеру в качестве домашней (стартовой),
- Click – троянец, организующий перенаправление пользовательских запросов браузеру на определенный сайт (или сайты),
- KeyLogger – троянец-шпион; отслеживает и записывает

нажатия клавиш на клавиатуре; может периодически пересылать собранные данные злоумышленнику,

- AVKill – останавливает работу программ антивирусной защиты, сетевые экраны и т.п.; также может удалять эти программы с диска,
- KillFiles, KillDisk, DiskEraser – удаляют некоторое множество файлов (файлы в определенных каталогах, файлы по маске, все файлы на диске и т. п.),
- DelWin – удаляет необходимые для работы операционной системы (Windows) файлы,
- FormatC – форматирует диск C:
  синоним: FormatAll – форматирует несколько или все диски,
- KillMBR – портит или стирает содержимое главного загрузочного сектора (MBR),
- KillCMOS – портит или стирает содержимое CMOS.

Средство использования уязвимостей

- Exploit – средство, использующее известные уязвимости некоторой операционной системы или приложения для внедрения в систему вредоносного кода, вируса или выполнения каких-либо несанкционированных действий.

Средства для сетевых атак

- Nuke – средства для сетевых атак на некоторые известные уязвимости операционных систем с целью вызвать аварийное завершение работы атакуемой системы,
- DDoS – программа-агент для проведения распределенных сетевых атак типа "отказ в обслуживании" (*Distributed Denial Of Service*),
- FDOS (синоним: Flooder) – *Flooder Denial Of Service* – программы для разного рода вредоносных действий в Сети, так или иначе использующие идею атаки типа "отказ в обслуживании"; в отличие от DDoS, где против одной цели одновременно используется множество агентов, работающих на разных компьютерах, FDOS-программа работает как отдельная, "самодостаточная" программа.

Скрипт-вирусы

Префиксы вирусов, написанных на различных языках сценариев:

- `VBS` – Visual Basic Script,
- `JS` – Java Script,
- `Wscript` – Visual Basic Script и/или Java Script,
- `Perl` – Perl,
- `PHP` – PHP,
- `BAT` – язык командного интерпретатора ОС MS-DOS.

Вредоносные программы

Префиксы объектов, являющихся не вирусами, а иными вредоносными программами:

- `Adware` – рекламная программа,
- `Dialer` – программа дозвона (перенаправляющая звонок модема на заранее запрограммированный платный номер или платный ресурс),
- `Joke` – программа-шутка,
- `Program` – потенциально опасная программа (*riskware*),
- `Tool` – программа-инструмент взлома (*hacktool*).

Разное

Префикс `generic` используется после другого префикса, обозначающего среду или метод разработки, для обозначения типичного представителя этого типа вирусов. Такой вирус не обладает никакими характерными признаками (как текстовые строки, специальные эффекты и т. д.), которые позволили бы присвоить ему какое-то особенное название.

Ранее для именования простейших безликих вирусов использовался префикс `Silly` с различными модификаторами.

Суффиксы

Суффиксы используются для именования некоторых специфических вирусных объектов:

- `generator` – объект является не вирусом, а вирусным генератором,
- `based` – вирус разработан с помощью указанного вирусного генератора или путем видоизменения указанного вируса. В обоих случаях имена этого типа являются родовыми и могут обозначать сотни и иногда даже тысячи вирусов,
- `dropper` – указывает, что объект является не вирусом, а инсталлятором указанного вируса.

Приложение Е. Защита корпоративной сети с помощью Dr.Web® Enterprise Suite

Dr.Web обеспечивает надежную, гибкую, легко настраиваемую в соответствии с пожеланиями пользователя защиту от вирусов и других нежелательных программ.

Версии **Dr.Web**, предназначенные для операционной системы Windows, а также версии для других платформ позволяют организовать надежную защиту компьютеров любой организации. Однако функционирование компьютеров в среде корпоративной сети создает особые проблемы для антивирусной защиты:

- как правило, установка ПО на компьютеры в организации производится администратором корпоративной сети. Установка антивирусов, их своевременное обновление является для такого администратора значительной дополнительной нагрузкой и требует обеспечения физического доступа к компьютерам;
- самостоятельное внесение недостаточно квалифицированными пользователями изменений в настройки антивирусной защиты (вплоть до ее отключения из-за кажущихся неудобств) создает "дыры" в защите – вирусы проникают внутрь корпоративной сети, после чего их устранение становится более сложной задачей;
- работа антивирусной защиты может быть полностью эффективной только при условии анализа ее работы квалифицированным специалистом по антивирусной безопасности – изучения протоколов, файлов, перемещенных в карантин и т. д. Данная работа затруднена в условиях, когда указанные сведения хранятся на десятках и сотнях отдельных компьютеров.

Для решения указанных задач разработан **Dr.Web Enterprise Suite** (далее **Dr.Web ES**).

Dr.Web ES решает следующие задачи:

- централизованная (без необходимости непосредственного

доступа персонала) установка антивирусных пакетов соответствующего типа на защищаемые компьютеры (рабочие станции и серверы локальной сети);

- централизованная настройка параметров антивирусных пакетов;
- централизованное обновление вирусных баз и программного обеспечения на защищаемых компьютерах;
- мониторинг вирусных событий на всех защищаемых компьютерах, а также состояния антивирусных пакетов и ОС.

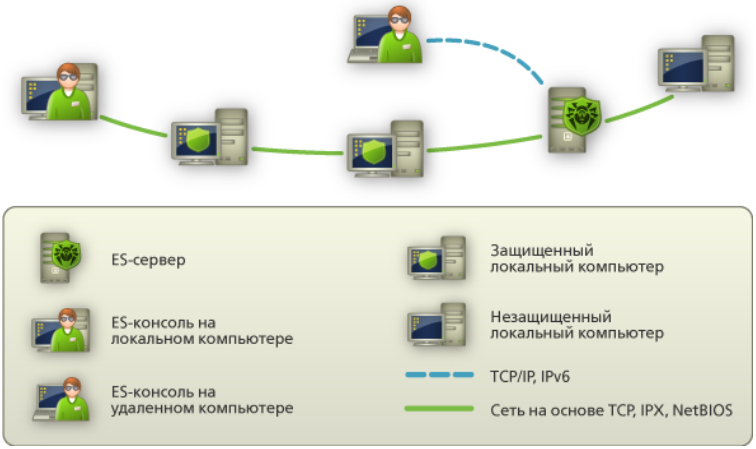
Dr.Web ES позволяет как сохранить за пользователем защищаемых компьютеров права на настройку и управление антивирусными пакетами данных компьютеров, так и гибко ограничить их, вплоть до полного запрета.

Dr.Web ES имеет архитектуру "клиент-сервер". Его компоненты устанавливаются на компьютеры локальной сети и обмениваются информацией, используя сетевые протоколы (подробнее взаимодействие компонентов **Dr.Web ES** описано ниже). Совокупность компьютеров, на которых установлены взаимодействующие компоненты **Dr.Web ES**, будем называть *антивирусной сетью*. В состав антивирусной сети входят следующие компоненты:

- *Антивирусный агент*. Этот компонент устанавливается на защищаемом компьютере, производит установку, обновление и управление антивирусным пакетом в соответствии с инструкциями, получаемыми с антивирусного сервера (см. ниже). Агент также передает на антивирусный сервер информацию о вирусных событиях и другие необходимые сведения о защищаемом компьютере;
- *Антивирусный сервер*. Этот компонент устанавливается на одном из компьютеров локальной сети. Антивирусный сервер хранит дистрибутивы антивирусных пакетов для различных операционных систем защищаемых компьютеров, обновления вирусных баз, антивирусных пакетов и антивирусных агентов, пользовательские ключи и настройки пакетов защищаемых компьютеров и передает их по запросу агентов на соответствующие компьютеры. Антивирусный сервер ведет единый журнал событий антивирусной сети и журналы по отдельным защищаемым компьютерам.

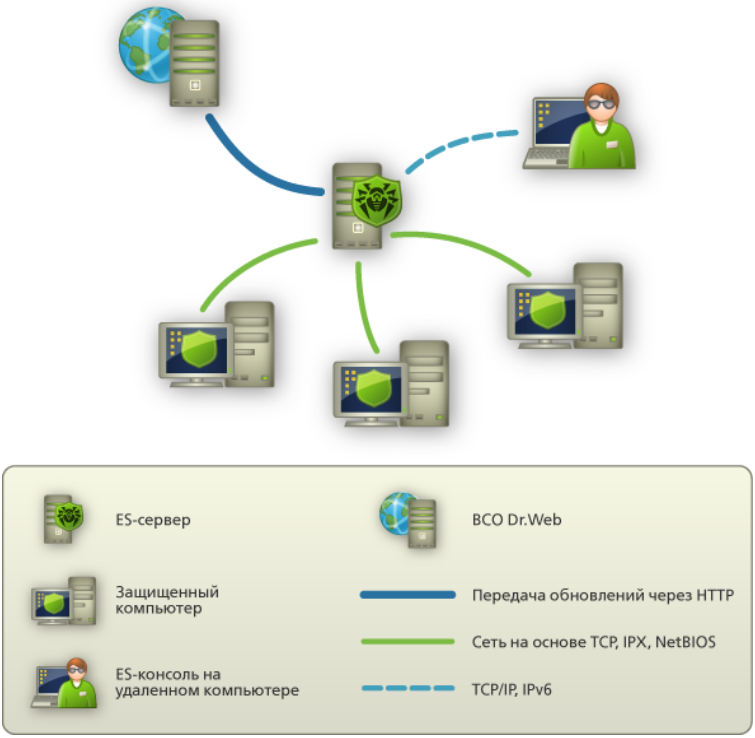
Антивирусная консоль может устанавливаться на компьютеры, не входящие в состав локальной сети; требуется только, чтобы между консолью и антивирусным сервером была связь по протоколу TCP/IP.

Ниже представлена общая схема фрагмента локальной сети, на части которой сформирована защищающая ее антивирусная сеть.



Весь поток команд, данных и статистической информации в антивирусной сети в обязательном порядке проходит через антивирусный сервер. Антивирусная консоль также обменивается информацией только с сервером; изменения в конфигурации рабочей станции и передача команд антивирусному агенту осуществляется сервером на основе команд консоли.

Таким образом, логическая структура фрагмента антивирусной сети имеет вид, представленный ниже.



От сервера к рабочим станциям и обратно (сплошная тонкая линия на рисунке) с использованием одного из поддерживаемых сетевых протоколов (TCP, IPX или NetBIOS) передаются:

- запросы агента на получение централизованного расписания и централизованное расписание данной рабочей станции;
- настройки агента и антивирусного пакета;
- запросы на очередные задания, подлежащие выполнению (сканирование, обновление вирусных баз и т. п.);
- модули антивирусных пакетов – при получении агентом задания на их установку;
- обновления ПО и вирусных баз – при выполнении задания на обновление;

- сообщения агента о конфигурации рабочей станции;
- статистика работы агента и антивирусных пакетов для записи в централизованный журнал;
- сообщения о вирусных событиях и других подлежащих фиксации событиях.

Объем трафика между рабочими станциями и сервером, в зависимости от настроек рабочих станций и их количества, может быть весьма значительным, поэтому **Dr.Web ES** предусматривает возможность компрессии трафика.

Трафик между сервером и рабочей станцией может быть зашифрован. Это позволяет избежать разглашения сведений, передаваемых по описываемому каналу, а также подмены ПО, загружаемого на рабочие станции.

Таким образом, **Dr.Web ES** позволяет:

- предельно упростить процесс установки антивирусного ПО на защищаемые компьютеры, причем в большинстве случаев (для компьютеров, работающих под управлением Windows 2000, Windows XP, Windows 2003, Windows Vista) установка может производиться централизованно, без физического доступа к компьютеру;
- централизованно настраивать антивирусное ПО и производить его обновления с минимальными трудозатратами;
- отслеживать состояние антивирусной защиты;
- при необходимости централизованно запускать или прерывать задания антивирусного ПО на компьютерах;
- собирать и изучать информацию о вирусных событиях на всех защищаемых компьютерах;
- при необходимости предоставить отдельным пользователям возможность самостоятельно настраивать антивирусное ПО;
- осуществлять управление антивирусной сетью и получение информации о ней администратором антивирусной защиты как с рабочих мест в корпоративной сети, так и удаленно через Интернет.

В крупных корпоративных сетях, насчитывающих сотни или тысячи компьютеров, целесообразно создавать средствами

Dr.Web ES антивирусную сеть с несколькими серверами. При этом между серверами выстраивается иерархическая связь, позволяющая упростить процесс передачи на рабочие станции обновлений вирусных баз и ПО и приема информации о вирусной ситуации. Администратор получает возможность изучать отчеты о работе сети как для отдельных серверов, так и сводную по всей антивирусной сети.

Dr.Web ES в условиях корпоративной сети повышает надежность антивирусной защиты и снижает расходы на ее обслуживание по сравнению с установкой на защищаемые компьютеры персональных антивирусов.

Dr.Web Enterprise Suite имеет ряд преимуществ по сравнению с аналогичными продуктами:

- высокая надежность и безопасность применяемых решений;
- легкость администрирования;
- мультиплатформенность всех компонентов;
- прекрасная масштабируемость.

Мы рекомендуем приобрести и установить **Dr.Web ES** в следующих случаях:

- ваша корпоративная сеть имеет значительный масштаб (несколько десятков компьютеров или более),
- у вас малая сеть, однако, по тем или иным причинам (специфика ПО, оборудования или квалификации персонала) вы уже используете в этой сети политику жесткого администрирования установки и настройки ПО.

Для компьютеров, не включенных в корпоративную сеть, используйте персональные антивирусы **Dr.Web для Windows** и версии **Dr.Web** для других платформ.

Приложение F. Dr.Web® AV-Desk для провайдеров интернет-услуг

Dr.Web AV-Desk позволяет упростить задачу поддержания антивирусной защиты большого числа пользователей. **Dr.Web AV-Desk** предназначен для организаций, специализирующихся на оказании различного рода интернет-услуг (провайдеры доступа в интернет (ISP), поставщики услуг приложений (ASP), а также банковских услуг (online banking) и т.д.).

AV-Desk позволяет установить антивирусные пакеты **Dr.Web** на рабочие станции клиентов организации, управлять их работой, обновлениями, оперативно отслеживать и решать проблемы, возникающие на компьютерах клиентов организации, без необходимости физического доступа к машинам или передачи инструкций пользователю.

Создание такой антивирусной сети решает ряд проблем, часто встречающихся в практике как корпоративных клиентов, так и отдельных пользователей:

- в организациях установка ПО на компьютеры, как правило, производится администратором корпоративной сети. Установка антивирусов, их своевременное обновление является для такого администратора значительной дополнительной нагрузкой и требует обеспечения физического доступа к компьютерам;
- «на дому» пользователь не всегда вовремя отслеживает вирусные события на своем компьютере или может вообще не устанавливать у себя антивирусное ПО;
- недостаточно квалифицированные пользователи могут вносить в настройки антивирусной защиты изменения (вплоть до ее отключения из-за кажущихся неудобств), которые создают "дыры" в защите, тем самым значительно снижая уровень безопасности;
- работа антивирусной защиты может быть полностью эффективной только при условии анализа ее работы квалифицированным специалистом по антивирусной безопасности – изучения протоколов, файлов,

перемещенных в карантин и т. д. В условиях организаций данная работа затруднена тем, что указанные сведения хранятся на десятках и сотнях отдельных компьютеров. В «домашних условиях» анализ работы антивируса обычно не производится.

Dr.Web AV-Desk разработан для решения этих проблем. Он обеспечивает единую и надежную комплексную антивирусную защиту рабочих станций, экономит время и усилия администраторов и освобождает пользователей от необходимости заниматься вопросами антивирусной защиты, без снижения уровня безопасности.

Dr.Web AV-Desk выполняет следующие задачи:

- простая установка ПО компонентов **Dr.Web AV-Desk** и быстрая организация антивирусной защиты,
- создание дистрибутивов с уникальными идентификаторами и передачу их пользователям для установки сервиса;
- централизованная настройка параметров антивирусных пакетов на защищаемых компьютерах сети,
- централизованное обновление вирусных баз и программного обеспечения на защищаемых компьютерах;
- мониторинг вирусных событий, а также состояния антивирусных пакетов и ОС на всех защищаемых компьютерах.

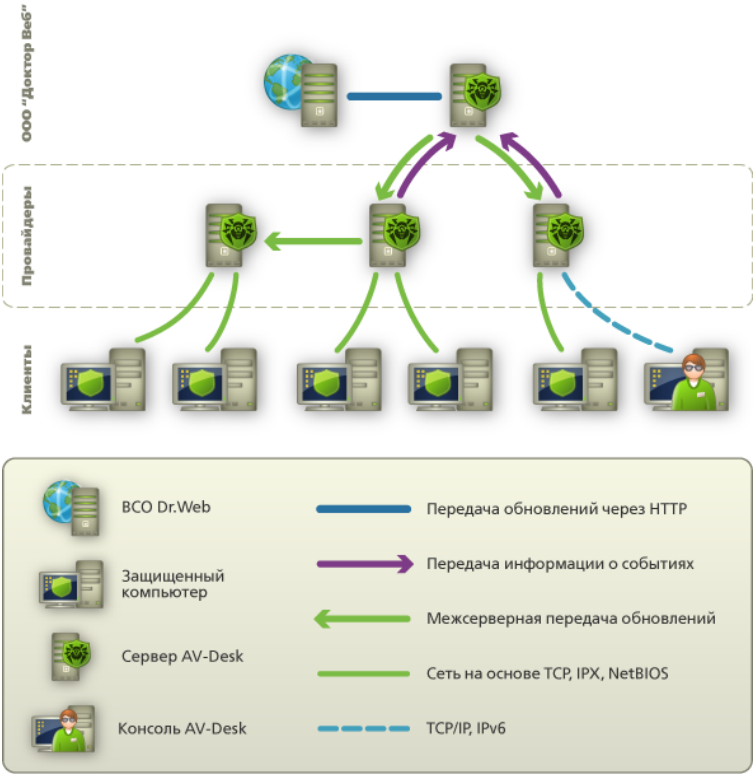
Dr.Web AV-Desk имеет архитектуру "*клиент-сервер*". В состав антивирусной сети, организованной с помощью **Dr.Web AV-Desk**, входят следующие компоненты:

- *Антивирусный сервер*. Этот компонент устанавливается на одном из компьютеров антивирусной сети. Антивирусный сервер хранит дистрибутивы антивирусных пакетов для различных операционных систем защищаемых компьютеров, скрипты веб-консоли, обновления вирусных баз, антивирусных пакетов и антивирусных агентов, пользовательские ключи и настройки пакетов защищаемых компьютеров и передает их по запросу агентов на соответствующие компьютеры. Антивирусный сервер ведет единый журнал событий антивирусной сети.
- *Веб-консоль*. Этот компонент позволяет создавать и

редактировать учетные записи пользователей, а также создавать для каждого пользователя индивидуальные дистрибутивы агента **AV-Desk**. Веб-консоль может использоваться администратором на любом компьютере, имеющем доступ в Интернет.

- *Встроенный веб-сервер*. Этот компонент устанавливается автоматически вместе с антивирусным сервером. Он представляет собой некоторое расширение стандартной веб-странички сервера и дает возможность:
  - просматривать общую информацию о сервере **AV-Desk**;
  - читать документацию;
  - просматривать репозиторий.
- *Антивирусный агент AV-Desk*. Этот компонент устанавливается на защищаемом компьютере, после чего производит на нем установку антивирусного пакета. В дальнейшем агент производит регулярные обновления установленного антивирусного ПО, передает ему команды и настройки с антивирусного сервера, а также отсылает антивирусному серверу информацию о вирусных событиях и другие необходимые сведения о защищаемом компьютере.

Ниже представлена общая схема фрагмента антивирусной сети.



Весь поток команд, данных и статистической информации в антивирусной сети в обязательном порядке проходит через антивирусный сервер. Антивирусная консоль также обменивается информацией только с сервером; изменения в конфигурации рабочей станции и передача команд антивирусному агенту осуществляется сервером на основе команд консоли.

В крупных сетях, насчитывающих сотни или тысячи компьютеров, целесообразно создавать средствами **Dr.Web AV-Desk** антивирусную сеть с несколькими серверами. При этом между серверами выстраивается иерархическая связь, позволяющая упростить процесс передачи на рабочие станции обновлений вирусных баз и ПО и приема информации о вирусной ситуации.

Администратор получает возможность изучать отчеты о работе сети как для отдельных серверов, так и сводную по всей антивирусной сети.

Dr.Web AV-Desk в условиях корпоративной сети повышает надежность антивирусной защиты и снижает расходы на ее обслуживание по сравнению с установкой на защищаемые компьютеры персональных антивирусов.

Dr.Web AV-Desk имеет ряд преимуществ по сравнению с аналогичными продуктами:

- высокая надежность и безопасность применяемых решений;
- легкость администрирования;
- мультиплатформенность всех компонентов;
- прекрасная масштабируемость.

Приложение G. Техническая поддержка

Страница службы технической поддержки компании **«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, настоятельно рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу http://solutions.drweb.com/
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/faq/
- 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 **«Доктор Веб»** и всю контактную информацию, необходимую пользователю, вы можете по адресу http://company.drweb.com/contacts/moscow.