



для Windows

Руководство пользователя

Версия 5.0.1

© 2009 ООО "Доктор Веб". Все права защищены

Материалы, приведенные в данном документе, являются собственностью ООО "Доктор Веб" и могут быть использованы исключительно для личных целей приобретателя продукта. Ни какая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

ТОВАРНЫЕ ЗНАКИ

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt! и логотипы Dr.WEB и Dr.WEB INSIDE являются зарегистрированными товарными знаками ООО "Доктор Веб". Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Ни при каких обстоятельствах ООО "Доктор Веб" и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

**ООО "Доктор Веб" Dr.Web® для Windows
Руководство пользователя
02.02.2009.**

*ООО "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.

ООО "Доктор Веб"

ООО "Доктор Веб" - российский разработчик средств информационной безопасности.

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

Антивирусные продукты ООО "Доктор Веб" разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ и 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	7
О чем эта документация	10
Используемые обозначения и сокращения	11
Системные требования	13
Лицензионный ключевой файл	15
Глава 2. Установка Dr.Web для Windows	19
Установка на ПК под управлением Microsoft® Windows® 2000(SP4)/XP/2003/Vista/2008	21
Первая установка Dr.Web для Windows	21
Обновление Dr.Web для Windows	27
Повторная установка и удаление программного комплекса	28
Установка на ПК под управлением Microsoft® Windows® 95/98/NT(SP6a)/Me	30
Первая установка Dr.Web для Windows	30
Повторная установка и удаление программного комплекса	35
Получение ключевого файла	37
Глава 3. Приступая к работе	40
Состав и функции установленных компонентов	40
Модуль управления SpIDer Agent	44
Менеджер лицензий	46
Сканер для Windows	47
Общие сведения	47
Запуск Сканера	48



Действия при обнаружении вирусов	52
Настройка параметров программы	55
Сканирование в режиме командной строки	60
SpIDer Guard для Windows	63
Общие сведения	63
Управление сторожем SpIDer Guard	64
Настройка режима запуска SpIDer Guard	67
Основные настройки сторожа	69
SpIDer Mail для рабочих станций Windows	76
Общие сведения	76
Управление почтовым сторожем SpIDer Mail	78
Основные настройки почтового сторожа	79
SpIDer Gate Dr.Web	88
Общие сведения	89
Управление SpIDer Gate	89
Настройка SpIDer Gate	90
Модуль Родительского контроля	93
Общие сведения	93
Настройка параметров модуля	94
Планировщик для Windows	97
Задания на сканирование и обновление	101
Глава 4. Автоматическое обновление	104
Принцип работы модуля автоматического обновления	104
Запуск модуля автоматического обновления	107
Приложения	109



Приложение А. Различия между Dr.Web для Windows и Dr.Web для Windows Server	109
Приложение В. Дополнительные параметры командной строки	111
Параметры командной строки для Сканеров	111
Параметры командной строки для модуля автоматического обновления	117
Коды возврата	120
Приложение С. Настраиваемые параметры компонентов Dr.Web	122
Параметры Windows-версий Сканера, сторожа, Планировщика и модуля автоматического обновления	123
Параметры SpIDer Mail для рабочих станций Windows	137
Приложение D. Вредоносные программы и способы их обезвреживания.	142
Классификация вредоносных программ и других компьютерных угроз	142
Действия, применяемые к вредоносным программам	149
Приложение Е. Принципы именования вирусов	151
Приложение F. Защита корпоративной сети с помощью Dr.Web® Enterprise Suite	157
Приложение G. Dr.Web® AV-Desk для провайдеров интернет-услуг.	163



Глава 1. Введение

Dr.Web® для Windows представляет собой мощное антивирусное средство, регулярно показывающее лучшие результаты в использовании и при независимом тестировании. Важной особенностью комплекса является его модульная архитектура. Антивирус использует программное ядро и вирусные базы, общие для всех компонентов и различных сред. В настоящее время, наряду с **Dr.Web® для Windows**, поставляются версии антивируса для MS-DOS®, IBM® OS/2®, Novell® NetWare®, а также ряда Unix®-подобных систем (например, Linux® и FreeBSD®).

Программный комплекс поставляется в двух вариантах:

- **Dr.Web® для Windows (Dr.Web для рабочих станций);**
- **Dr.Web® для Windows Server (Dr.Web для серверов).**

Всюду, где не указано иное, описание в равной степени относится к обоим вариантам. В этих случаях будет употребляться сокращенное обозначение **Dr.Web**.

Компоненты и конфигурационные файлы **Dr.Web** для серверов разработаны специально для осуществления эффективной антивирусной защиты файлового сервера, с учетом его высокой загруженности, круглосуточной работы и нежелательности частого вмешательства пользователя (администратора сервера).

Dr.Web использует удобную и эффективную процедуру обновления вирусных баз и обновления 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® для Windows в зависимости от типа лицензии 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. Существует также версия программы с интерфейсом командной строки (**Dr. Web Консольный сканер для Windows**);
- **SpIDer Guard® для Windows** – антивирусный сторож, (называемый также монитором). Программа постоянно находится в оперативной памяти, осуществляя проверку файлов "на лету", а также обнаруживая проявления вирусной активности;
- **SpIDer Mail® для рабочих станций Windows** – почтовый антивирусный сторож. Программа перехватывает обращения любых почтовых клиентов компьютера к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP (под IMAP4 имеется в виду IMAPv4rev1), обнаруживает и обезвреживает почтовые вирусы до получения писем почтовым клиентом с сервера или до отправки письма на почтовый сервер. В том случае, если система **Dr. Web** работает с лицензией на программный пакет "**Dr.Web Security Space**", почтовый сторож также может осуществлять проверку корреспонденции на спам с помощью спам-фильтра Vade Retro. Компонент **SpIDer Mail** не входит в состав **Dr.Web для Windows Server**;
- **SpIDer Gate** – антивирусный HTTP-сторож. При настройках по умолчанию **SpIDer Gate** автоматически проверяет входящий и исходящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы. Компонент не входит в состав **Dr.Web для Windows Server**.
- **Родительский контроль**. С помощью данного компонента осуществляется ограничение доступа пользователя к ресурсам, содержащимся как локально, на самом ПК, так и в сети. Компонент не входит в состав **Dr.Web для Windows Server**.
- **Dr.Web Модуль автоматического обновления** – позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов комплекса, а



также производит их автоматическую установку; незарегистрированным пользователям дает возможность зарегистрироваться или получить демонстрационный ключ. Кроме того, с помощью модуля автоматического обновления зарегистрированные пользователи могут продлить срок действия лицензии (при наличии серийного номера продления). Незарегистрированным пользователям модуль автоматического обновления дает возможность зарегистрироваться, а также получить лицензионный (при наличии серийного номера) или демонстрационный ключ (см. п. [Получение ключевого файла](#)).

- **SpIDer Agent** – модуль управления, с помощью которого осуществляется запуск и настройка компонентов Антивируса.

В состав **Dr.Web для Windows** входят также **Планировщик заданий** для Windows 95/98/Me, сканер для среды DOS и ряд вспомогательных программ.

Для организации централизованного управления антивирусной защитой в масштабе предприятия поставляется специальное средство – **Dr.Web® Enterprise Suite**. Подробнее об этом программном комплексе см. [Приложение F](#).

Для провайдеров интернет-услуг защиту их клиентов от вирусов и спама обеспечивает **Dr.Web® AV-Desk**. Подробнее о данном программном комплексе см. [Приложение G](#).



О чем эта документация

Настоящее руководство пользователя содержит необходимые сведения по установке и эффективному использованию антивирусного программного комплекса **Dr.Web® для Windows**.

Подробное описание всех элементов графического интерфейса содержится в справочной системе комплекса, 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 комплекса (настройки по умолчанию).

В Приложениях содержится подробная справочная информация по настройке антивирусного комплекса, предназначенная для опытных пользователей.



Используемые обозначения и сокращения

В данном руководстве используются следующие обозначения:

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в справке.
Зеленое и полужирное начертание	Наименования продуктов ООО "Доктор Веб" или их компонентов.
<u>Зеленое и подчеркнутое начертание</u>	Ссылки на страницы справки и веб-сайты.
Моноширинный шрифт	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
<i>Курсив</i>	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак плюса	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

В тексте руководства будут употребляться без расшифровки следующие сокращения:



- GUI – графический пользовательский интерфейс (Graphical User Interface), GUI-версия программы – версия, использующая средства GUI,
- ПК – персональный компьютер,
- ОС – операционная система.



Системные требования

Для установки **Dr.Web для Windows**, в зависимости от состава компонентов, требуется до 55 Мбайт на жестком диске.

Сканер (GUI-версия и консольная версия для Windows) и сторож **SpIDer Guard** работают на ПК под управлением Microsoft® Windows® 95/98/Me или Windows® NT(SP6a)/2000(SP4)/XP/2003/Vista/2008.

SpIDer Mail работает на ПК под управлением Microsoft® Windows® 95/98/Me или Microsoft® Windows® NT(SP6a)/2000(SP4)/XP/Vista.

SpIDer Gate и модуль **Родительского контроля** работают на ПК под управлением Microsoft® Windows® 2000/XP/Vista.

SpIDer Agent работает на ПК под управлением Microsoft® Windows® 2000/XP/2003/Vista/2008.



SpIDer Guard работает только в 32-разрядных системах.

Работа всех компонентов под управлением Microsoft® Windows 95 возможна только, начиная с версии Microsoft® Windows® 95 OSR2 (v.4.00.950B). Также может потребоваться загрузить с сайта Microsoft и установить обновления ряда системных компонентов. Программный комплекс сообщит вам, при необходимости, их наименования и URL.

Сканер для DOS работает под управлением MS-DOS® или в режиме командной строки Windows.

Минимальные требования к конфигурации ПК совпадают с таковыми для соответствующих ОС, однако корректная работа **SpIDer Guard** возможна только при наличии не менее 32 Мб оперативной памяти, установленной на компьютере. ПК должен



полностью поддерживать систему команд процессора i80386.



Следует установить все рекомендуемые производителем ОС критические обновления. Если поддержка ОС производителем прекращена, рекомендуется перейти на более современную версию системы.

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



Лицензионный ключевой файл

Права пользователя на использование антивируса регулируются при помощи специального файла, называемого ключевым файлом.

В ключевом файле содержится, в частности, следующая информация:

- 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).

Ключевой файл имеет расширение `.key` и при работе программ по умолчанию должен находиться в каталоге установки (см. [Первая установка антивируса Dr.Web для рабочих станций](#)).



Ключевой файл имеет формат, защищенный от редактирования. Редактирование файла делает его недействительным. Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Существует два типа ключевых файлов:

- Лицензионный ключевой файл, который приобретается вместе с программным комплексом **Dr.Web** и позволяет как пользоваться Антивирусом 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 антивируса.



- Демонстрационный ключевой файл, который используется для ознакомления с Антивирусом. Такой ключевой файл обеспечивает полную функциональность основных антивирусных компонентов, но имеет ограниченный срок действия.

Ключевой файл может поставляться в виде файла с расширением `.key` или в виде ZIP-архива, содержащего этот файл, а также в виде файла специального формата с расширением `.dwz`, используемого для распространения дополнений к пакету.

Пользователь может получить ключевой файл одним из следующих способов:

- в процессе регистрации продукта на сайте **ООО "Доктор Веб"**. На основании введенного пользователем *регистрационного серийного номера*, полученного от продавца, формируется соответствующий лицензионный ключевой файл. При отсутствии серийного номера пользователь при регистрации может получить только демонстрационный ключевой файл. Сформированный ключевой файл высылается по электронной почте, а также может быть загружен со страницы регистрации;
- через сеть Интернет на завершающей стадии процесса установки (см. [Первая установка антивируса Dr.Web для рабочих станций](#)) или при первом обновлении программного комплекса при помощи модуля автоматического обновления (см. [Глава 4. Автоматическое обновление](#)). Модуль производит регистрацию программного комплекса на сайте **ООО "Доктор Веб"**, получает и устанавливает сформированный при регистрации ключ. Данный метод можно использовать только для варианта **Dr.Web** для рабочих станций;
- вместе с дистрибутивом продукта, если ключ входит в состав дистрибутива при его комплектации;
- по электронной почте в виде файла с расширением `.dwz`. В этом случае для установки ключевого файла следует дважды щелкнуть по значку файла, присоединенного к письму;
- на отдельном носителе в виде файла с расширением `.key`. В этом случае файл необходимо скопировать в каталог



установки **Dr.Web**;

- в виде ZIP-архива, содержащего файл с расширением .key. В этом случае необходимо извлечь файл при помощи архиватора данного формата (например, WinZip или Pkunzip) и скопировать его в каталог установки **Dr.Web**.

Рекомендуется сохранять лицензионный ключевой файл до истечения срока его действия. При переустановке антивируса или в случае установки на несколько компьютеров повторная регистрация серийного номера не требуется. Используйте ключевой файл, полученный при первой регистрации.

Повторная регистрация может потребоваться в случае утраты ключевого файла. При повторной регистрации укажите те же персональные данные, введенные при первой регистрации; можно ввести только другой адрес электронной почты – в таком случае лицензионный 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.



Операционные системы семейства Microsoft® Windows®, начиная с Windows® XP, поддерживают формат сжатия файлов ZIP, для извлечения содержимого архивов данного формата сторонние программы не требуются.



При отсутствии действительного ключевого файла (лицензионного или демонстрационного) активность всех компонентов блокируется. Единственное разрешенное в такой ситуации действие – запуск модуля автоматического обновления с целью регистрации и получения ключевого файла (только для варианта **Dr.Web для рабочих станций**).



Начиная с антивируса версии 4.33, ключевые файлы для приложений **Dr.Web для рабочих станций** и **Dr.Web для серверов** различаются. При использовании ключевого файла от другого варианта антивируса некоторые компоненты, в частности, сторож **SpIDer Guard для Windows NT/2000/XP/2003/Vista**, работать не будут.



Глава 2. Установка Dr.Web для Windows

Перед установкой комплекса настоятельно рекомендуется:

- установить все критические обновления, выпущенные компанией Microsoft для вашей версии ОС (их можно загрузить и установить с сайта обновлений компании <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.

Установочный комплект поставляется в виде фирменного диска или отдельного исполняемого файла размером около 50 МБ.

Чтобы запустить установку, воспользуйтесь одним из следующих методов:

- в случае поставки в виде единого исполняемого файла запустите на исполнение этот файл;
- в случае поставки на фирменном диске, если для привода включен режим автозапуска диска, процедура установки запустится автоматически. Если режим автозапуска отключен, запустите на выполнение файл `autorun.exe`, расположенный на диске с дистрибутивом. Откроется окно, содержащее меню автозапуска. Нажмите на кнопку **Установить**.

Следуйте указаниям программы установки, основные действия которой описываются ниже. Чтобы вернуться к предыдущему шагу программы установки, на любом этапе установки (до начала



копирования файлов на компьютер) нажмите кнопку **Назад**. Для перехода на следующий шаг программы нажмите кнопку **Далее**. Для того чтобы прервать установку, нажмите кнопку **Отмена**.

Процедура установки и состав устанавливаемых компонентов **Dr. Web для Windows** различается в зависимости от операционной системы, установленной на вашем компьютере.

Установка **Dr.Web** на компьютер, работающий под управлением Microsoft® Windows® 2000(SP4)/XP/2003/Vista/2008, рассматриваются в следующих разделах:

[Первая установка Dr.Web для Windows](#)

[Обновление текущей версии Антивируса до версии 5.0](#)

[Повторная установка и удаление Dr.Web](#)

Установка на компьютер, работающий под управлением Microsoft® Windows® 95/98/NT(SP6a)/Me рассматривается в следующих разделах:

[Первая установка Dr.Web для Windows](#)

[Повторная установка и удаление Dr.Web](#)



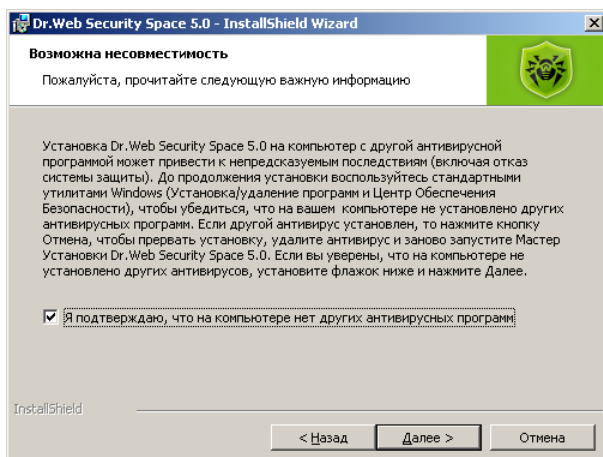
Установка на ПК под управлением Microsoft® Windows® 2000(SP4)/XP/2003/Vista/2008

Первая установка Dr.Web для Windows



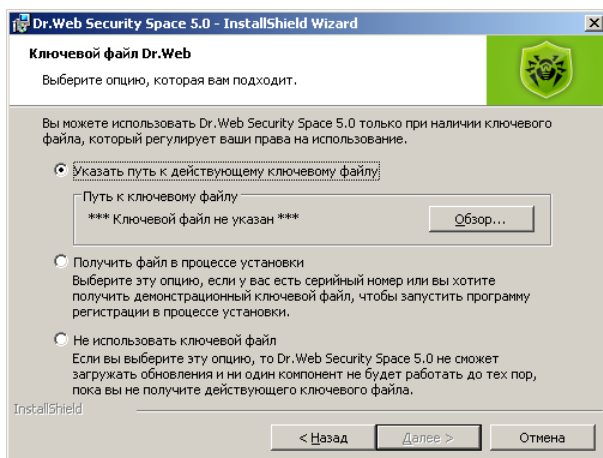
Для установки **Dr.Web для Windows** необходимы права Администратора.

1. Выберите язык установки (этот выбор не влияет на набор языков, который будет поддерживать установленный программный комплекс).
2. На следующем шаге вам будет предложено ознакомиться с лицензионным соглашением. Для продолжения установки его необходимо принять.
3. Программа установки предупредит вас о возможной несовместимости **Dr.Web для Windows** и иных антивирусов, установленных на вашем компьютере, и предложит удалить их с ПК. Если на вашем компьютере установлены другие антивирусы, рекомендуется нажать на кнопку **Отмена** и прервать установку, удалить или деактивировать эти антивирусы и после этого начать установку заново.



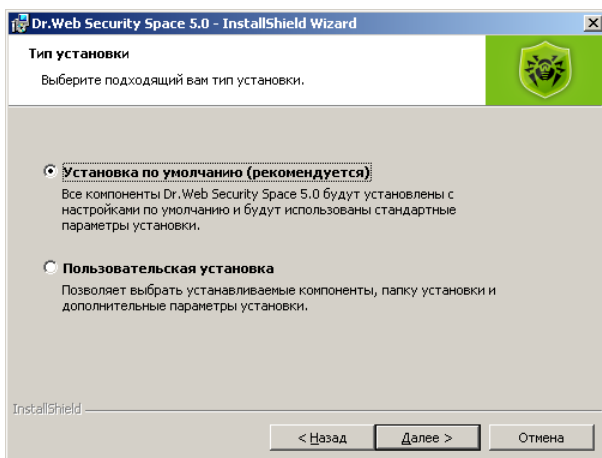
Для продолжения установите флажок **Я подтверждаю, что на компьютере нет других антивирусных программ** и нажмите на кнопку **Далее**.

4. На следующем шаге программа установки откроет окно с предупреждением о том, что для работы программы необходим ключевой файл (лицензионный или демонстрационный). Если у вас есть ключевой файл и он находится на жестком диске или сменном носителе, нажмите на кнопку **Обзор** и выберите этот файл в стандартном окне открытия файла. Если ключевого файла нет, но вы готовы его получить в процессе установки, выберите **Получить файл в процессе установки**. В противном случае выберите **Не использовать ключевой файл** и нажмите кнопку **Далее**.



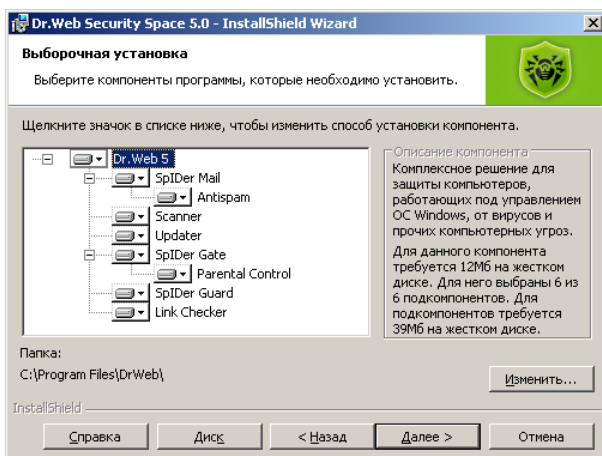
Используйте только ключевой файл варианта **Dr.Web для рабочих станций**. Ключевой файл должен иметь расширение .key. Если файл находится в архиве, необходимо извлечь его соответствующим архиватором.

5. Программа предложит вам выбрать вид установки.
Установка по умолчанию предполагает установку всех компонентов, английского и русского языков интерфейса, а также всех вспомогательных программ, причем этапы установки до шага 10 будут проведены автоматически.
Пользовательская установка предназначена для опытных пользователей. В процессе пользовательской установки вам будет предложено самостоятельно выбрать устанавливаемые компоненты, настройки прокси-сервера и некоторые дополнительные параметры установки.



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

6. Если вы выбрали режим установки по умолчанию, то перейдите к описанию шага 10. При **Пользовательской установке** откроется окно выбора устанавливаемых компонентов. Сделайте свой выбор и нажмите кнопку **Далее**.

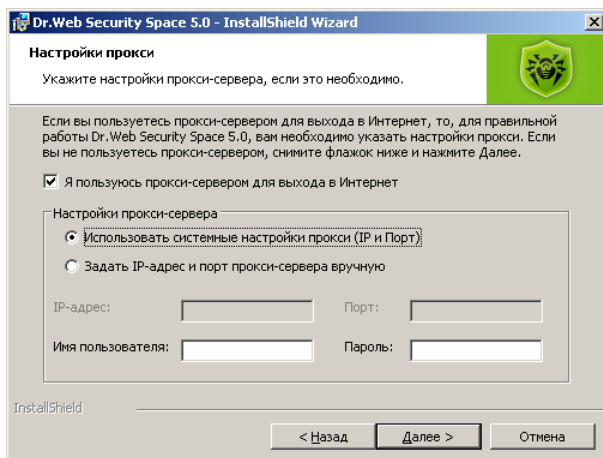


7. Откроется окно создания ярлыков для запуска **Dr.Web** для

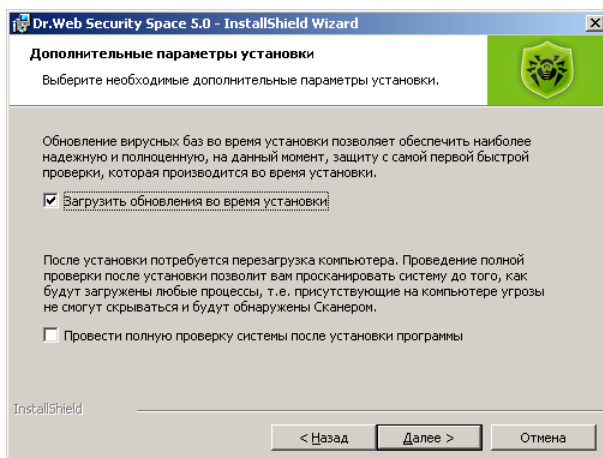


Windows. Укажите необходимые пункты и нажмите кнопку **Далее**.

- Откроется окно настроек прокси-сервера. Если для выхода в Интернет вы используете прокси-сервер, выберите необходимые настройки в группе **Настройки прокси-сервера**. Если прокси-сервер не используется, снимите флажок **Я пользуюсь прокси-сервером для выхода в Интернет**. Нажмите кнопку **Далее**.



- На следующем шаге вам будет предложено выбрать дополнительные параметры установки. Установите флажок **Загрузить обновления во время установки** чтобы в процессе установки были загружены актуальные вирусные базы.



Установите флажок **Провести проверку системы после установки программы** для проведения полной проверки файловой системы компьютера после установки **Dr.Web для Windows**.

10. Откроется информационное окно с сообщением о готовности к установке. Нажмите кнопку **Установить**, чтобы запустить процесс копирования файлов или кнопку **Назад**, чтобы изменить параметры установки **Dr.Web для Windows**.
11. Если на шаге 4 вы выбрали **Получить** ключевой файл в процессе установки, то модуль автоматического обновления запустит [процедуру регистрации пользователя](#). Для получения ключевого файла необходимо наличие подключения компьютера к сети Интернет.
12. После получения ключевого файла, если на шаге 9 был установлен флажок **Загрузить обновления во время установки**, будет выполнен процесс обновления вирусных баз, не требующий вмешательства пользователя.
13. По завершении установки, если в состав компонентов входит GUI-версия **Сканера**, программа установки запустит **Сканер**, который произведет сканирование оперативной памяти компьютера и файлов автозапуска. 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 drweb32.exe в список исключаемых программ.

14. Выполните перезагрузку компьютера, необходимую для завершения процесса установки.

Обновление Dr.Web для Windows

Обновление уже установленных компонентов программного комплекса Dr.Web для Windows версии 5.0 производится средствами [модуля автоматического обновления](#).

С помощью программы установки производится [изменение состава](#) установленных компонентов, а также обновление программного комплекса до текущей версии.



Обязательно сохраните действующий ключевой файл вне папки с установленным **Антивирусом Dr.Web**, перед проведением процедуры обновления до версии 5.0.

1. Для того чтобы обновить ранее установленный **Антивирус Dr.Web для Windows** версии 4.44 до версии 5.0 запустите программу установки.
2. Следуйте указаниям программы, описанным в [предыдущем разделе](#).
3. На шаге 4 укажите путь к ранее сохраненному ключевому файлу.

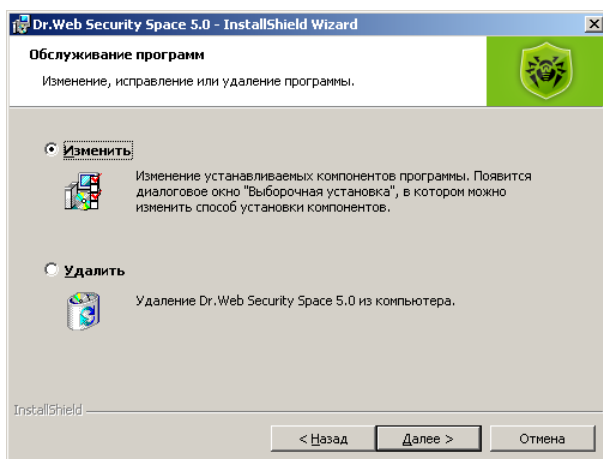


4. Завершите установку программы следуя [дальнейшим указаниям](#).

Повторная установка и удаление программного комплекса

Для того чтобы изменить, исправить или удалить ранее установленную программу **Dr.Web для Windows** запустите процедуру установки [Dr.Web для Windows](#).

После выбора языка работы программы установки, откроется следующее диалоговое окно:



а

В этом окне:

- чтобы изменить состав устанавливаемых компонентов, выберите вариант **Изменить** и в окне [Выбор компонентов](#) задайте нужный набор модулей. Дальнейший ход установки полностью аналогичен обычной установке приложения, начиная с данного окна.



- чтобы удалить все установленные компоненты, выберите пункт **Удалить**. В процессе удаления **Dr.Web для Windows** потребуется отключить модуль самозащиты. Введите код, изображенный на картинке в открывшемся окне, чтобы отключить защиту файлов программного комплекса. Для завершения процедуры удаления перезагрузите компьютер по просьбе программы.

Запустить процедуру изменения или удаления программного комплекса можно также воспользовавшись средствами утилиты **Установка и удаление программ** операционной системы Windows.



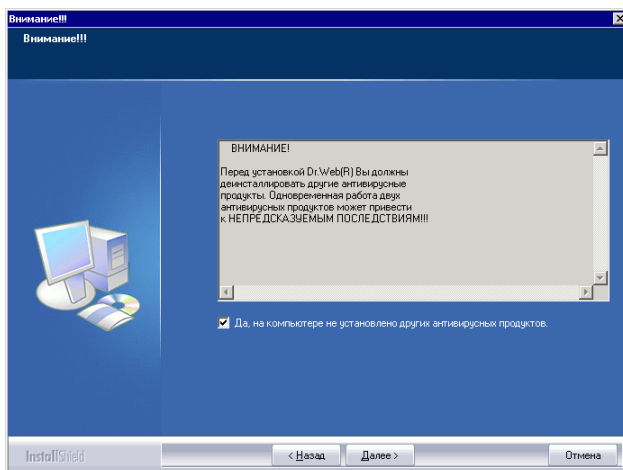
Установка на ПК под управлением Microsoft® Windows® 95/98/NT(SP6a)/Me

Первая установка Dr.Web для Windows



Для установки антивируса на ПК, работающий под управлением Microsoft® Windows® NT, необходимы права Администратора.

1. Выберите язык установки (этот выбор не влияет на набор языков, который будет поддерживать установленный программный комплекс).
2. При необходимости, программа установки предупредит вас о возможной несовместимости **Dr.Web для Windows** и иных антивирусов, установленных на вашем компьютере, и предложит удалить их с ПК.

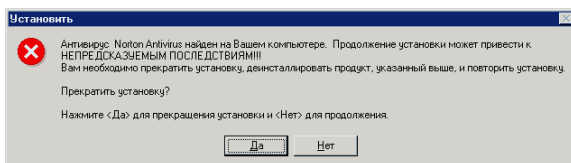


Если на вашем компьютере установлены другие антивирусы, рекомендуется нажать на кнопку **Отмена** и прервать



установку, удалить или деактивировать эти антивирусы и после этого продолжить установку. Для продолжения установки установите флаг **Да, на компьютере не установлено других антивирусных программ** и нажмите на кнопку **Далее**.

3. Программа установки проверяет ваш компьютер и в случае обнаружения известных ей антивирусов выдает также дополнительное предупреждение.



Чтобы прекратить установку, нажмите кнопку **Да**. Вы сможете повторить установку после удаления или деактивации обнаруженного антивируса. Чтобы продолжить без деактивации стороннего антивируса, нажмите кнопку **Нет**.



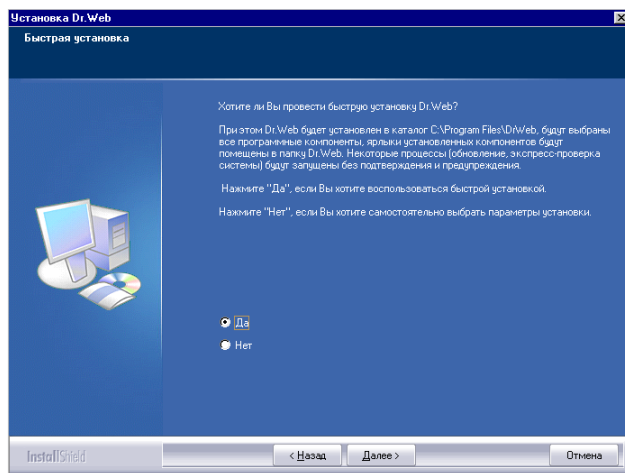
Далеко не все антивирусы могут быть обнаружены программой установки. Продолжать установку при наличии на компьютере иных антивирусов можно, только если в их составе отсутствуют активные резидентные модули (сторожи) и программы обработки почтового трафика.

4. На следующем шаге вам будет предложено ознакомиться с лицензионным соглашением. Для продолжения установки его необходимо принять.
5. На следующем шаге программа установки откроет окно с предупреждением о том, что для работы программы необходим ключевой файл (лицензионный или демонстрационный). Если у вас есть ключевой файл и он находится на жестком диске или сменном носителе, нажмите на кнопку **Обзор** и выберите этот файл в стандартном окне открытия файла. Если ключевого файла нет, нажмите кнопку **Далее**. Ключевой файл можно будет получить позднее в процессе установки.



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

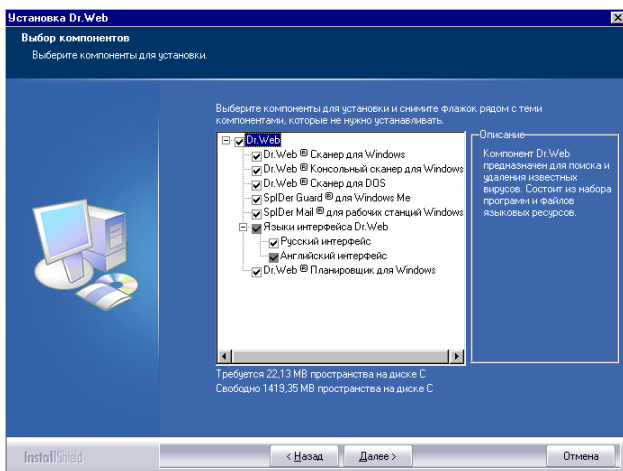
6. Программа предложит вам выбрать вид установки. Быстрый вариант установки предполагает установку всех антивирусных компонентов, английского и русского языков интерфейса, а также всех вспомогательных программ, причем этапы установки до шага 12 будут проведены автоматически. Во время быстрой установки также некоторые процессы (обновление, экспресс-проверка системы) будут запущены без подтверждения и предупреждения. Выберите **Да**, если хотите продолжить быструю установку, или **Нет**, если хотите самостоятельно выбрать параметры установки. Нажмите кнопку **Далее**.



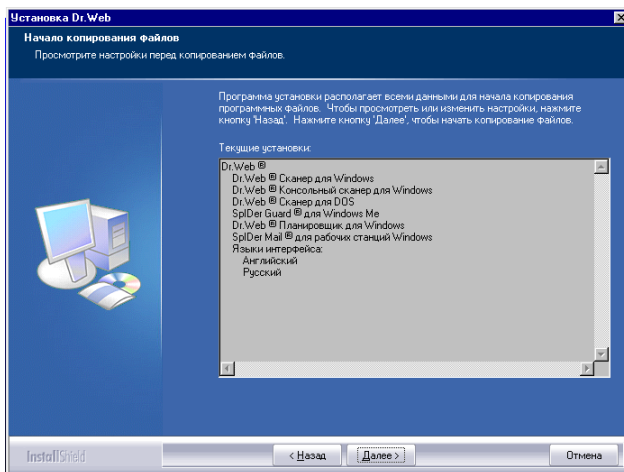
7. Если вы выбрали режим быстрой установки, то перейдите к шагу 11. Если вы отказались от быстрой установки, то в открывшемся окне выберите каталог установки программного комплекса и нажмите на кнопку **Далее**.
8. На следующем шаге откроется окно **Выбор компонентов**. Установите флажки напротив тех компонентов, которые вы



хотите установить, и снимите флажки у компонентов, которые вы устанавливать не хотите. Сделав выбор, нажмите кнопку **Далее**.



9. На следующем шаге вам будет предложено выбрать папку в подменю **Программы** главного меню операционной системы Windows (вызывается по нажатию кнопки **Пуск**). В данную папку будут помещены ярлыки установленных компонентов, файлов справки, файлов отчета по компонентам, а также ярлык **UnInstall Dr.Web**, позволяющий запустить процесс удаления **Dr.Web для Windows** с вашего компьютера. По умолчанию программа установки создает папку **Dr.Web**. Рекомендуется использовать этот вариант.
10. На следующем шаге откроется информационное окно **Начало копирования файлов**. Ознакомьтесь со списком компонентов для установки и, если он вас устраивает, нажмите кнопку **Далее**.



11. Далее откроется окно **Настройки прокси-сервера**. Если вы используете прокси-сервер для выхода в Интернет, заполните поля **Адрес**, **Имя** и **Пароль** и нажмите кнопку **Да**. Если прокси-сервер не используется, нажмите кнопку **Нет**.
12. Далее, если у вас имеется ключевой файл и вы указали его на шаге 6, откроется окно обновления вирусных баз. Подробнее о вирусных базах и их обновлении смотрите в главе [Автоматическое обновление](#). Чтобы произвести обновление вирусных баз, нажмите кнопку **Да**. Запустится модуль автоматического обновления.

Если ключевой файл отсутствует, модуль автоматического обновления оповестит вас об этом и попытается получить его через Интернет при помощи [процедуры регистрации пользователя](#).

После получения ключевого файла будет выполнен процесс обновления вирусных баз, не требующий вмешательства пользователя.
13. По завершении установки, если в состав компонентов входит GUI-версия **Сканера**, программа произведет сканирование оперативной памяти компьютера и файлов автозапуска и предложит вам произвести более подробное



сканирование компьютера.



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 drweb32.exe в список исключаемых программ.

14. Если вы установили антивирусный сторож **SpIDer Guard** или **SpIDer Mail**, программа предложит выполнить перезагрузку компьютера, необходимую для завершения процесса установки этих компонентов.

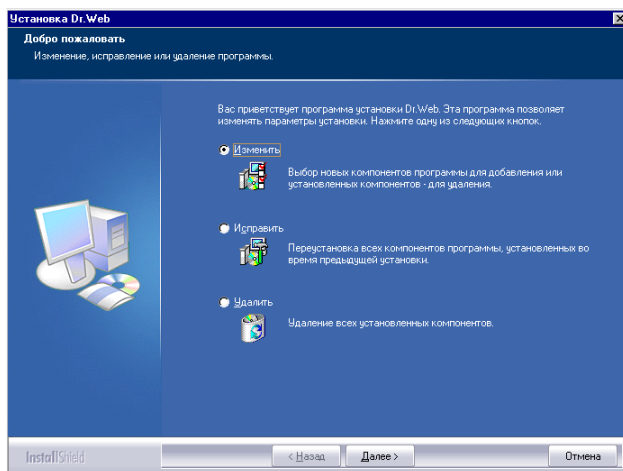


Программа установки по умолчанию не только устанавливает компонент **Планировщик для Windows**, но и создает для него расписание, включающее ежечасный автоматический запуск обновления программного комплекса и задание на антивирусное сканирование (отключенное).

Повторная установка и удаление программного комплекса

Для того чтобы изменить, исправить или удалить ранее установленную программу **Dr.Web для Windows** запустите процедуру [установки Dr.Web](#).

Откроется диалоговое окно, позволяющее выбрать режим работы программы установки.



В этом окне:

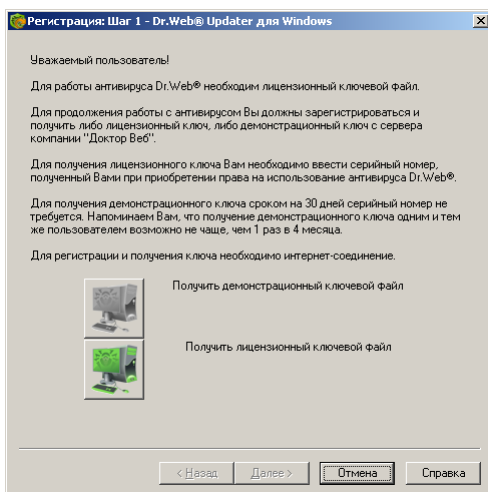
- чтобы изменить состав устанавливаемых компонентов, выберите вариант **Изменить** и в окне **Выбор компонентов** задайте нужный набор модулей. Дальнейший ход установки полностью аналогичен обычной установке приложения, начиная с данного окна.
- чтобы заново установить те же компоненты, которые были выбраны ранее (например, при необходимости исправления дефектных файлов), выберите вариант **Исправить**. Дальнейшая установка не требует вмешательства пользователя.
- чтобы удалить все установленные компоненты, выберите пункт **Удалить**.

Вышеописанное окно может быть вызвано также средствами утилиты **Установка и удаление программ**, доступной из **Панели управления** операционной системы Windows.

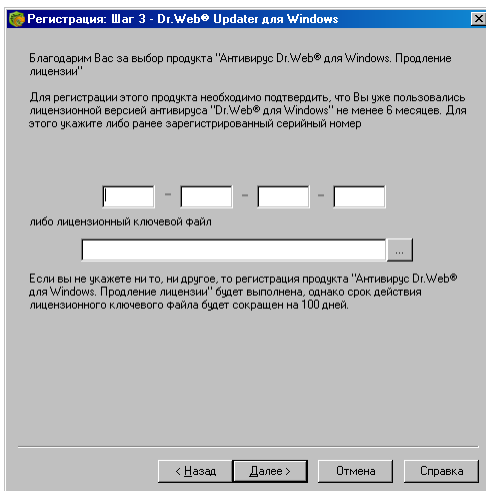


Получение ключевого файла

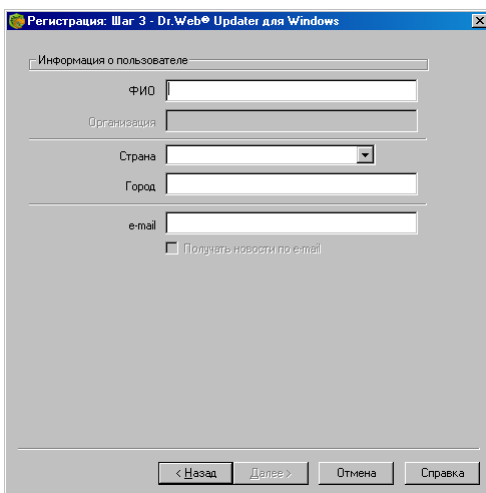
1. На первом шаге процедуры получения ключевого файла вам будет предложено выбрать: получить демонстрационный или лицензионный ключевой файл (подробно о ключевом файле см. [Лицензионный ключевой файл](#)). Если у вас имеется регистрационный серийный номер, выданный вам при приобретении антивируса, выберите вариант **Получить лицензионный ключевой файл**. Если вы устанавливаете программу с ознакомительными целями, выберите **Получить демонстрационный ключевой файл** и перейдите к шагу 4.



2. В открывшемся окне введите серийный номер и нажмите кнопку **Далее**.
3. Если на предыдущем шаге вы ввели серийный номер продления, то откроется окно для ввода данных предыдущих регистраций. Укажите в полях окна серийный номер либо лицензионный ключ предыдущей регистрации. Нажмите кнопку **Далее**.



4. В окне ввода персональных данных, необходимых для получения ключевого файла, заполните все поля и нажмите кнопку **Далее**.



5. В окне **Подтверждение регистрационных данных** проверьте правильность ввода. Если все данные введены верно, нажмите кнопку **Далее**.



6. Запускается процедура загрузки и установки ключевого файла. Протокол ее работы отображается в информационном окне. Если получение ключевого файла завершилось успешно, в информационном окне выводится соответствующее сообщения и указывается путь размещения полученного ключевого файла. В противном случае выводится сообщение об ошибке.



Глава 3. Приступая к работе

Состав и функции установленных компонентов

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

- при установке программного комплекса для рабочих станций, в зависимости от типа лицензии - **Сканер** для среды Windows (с GUI-интерфейсом и консольную версию) и для среды DOS, сторож **SpIDer Guard**, почтовый сторож **SpIDer Mail**, антивирусный HTTP-сторож **SpIDer Gate**, модуль **Родительского контроля** а также модуль управления **SpIDer Agent**. На компьютеры, работающие под управлением Microsoft® Windows® 95/98/Me также устанавливается **Планировщик**;
- при установке программного комплекса для серверов - **Сканер** для среды Windows (с GUI-интерфейсом и консольную версию), сторож **SpIDer Guard**, а также модуль управления компонентами **SpIDer Agent**.

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



На компьютеры, работающие под управлением Microsoft® Windows® 95/98/NT4(SP6a)/Me установка SpIDer Gate, модуля Родительского контроля, а также SpIDer Agent не производится.

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



взаимодополняющих стратегий защиты ПК.

Так, **Сканер для Windows** проверяет (по команде пользователя или команде, данной **Планировщиком**) 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.

Сканер для DOS может производить тщательную проверку дисков даже в случае отсутствия или неработоспособности операционной системы Windows. В сочетании с загрузкой ПК с защищенного от записи диска его использование позволяет обеспечить самый высокий уровень обнаружения вирусов в файлах.

Сторож SpIDer Guard постоянно находится в памяти ПК и перехватывает обращения к объектам файловой системы. Программа проверяет на наличие вирусов только открываемые файлы (при настройках по умолчанию – все открываемые файлы на сменных дисках и открываемые на запись файлы на жестких дисках). Благодаря менее детализированному способу проверки программа практически не создает помех другим процессам на ПК, однако, за счет некоторого (незначительного) снижения надежности обнаружения вирусов.

Достоинством программы является непрерывный, в течение всего времени работы ПК, контроль вирусной ситуации. Кроме того, некоторые вирусы могут быть обнаружены только сторожем по специфичным для них действиям.

Почтовый сторож SpIDer Mail также постоянно находится в памяти. Программа перехватывает все обращения почтовых клиентов вашего ПК к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP и проверяет входящую (и исходящую) почту до ее приема (или отправки) почтовым клиентом. **SpIDer Mail** ориентирован на проверку всего текущего почтового трафика, проходящего через компьютер, в результате чего проверка почтовых ящиков становится более эффективной и менее ресурсоемкой. В частности, могут отслеживаться попытки



массовой рассылки почтовыми червями своих копий по адресной книге пользователя с помощью собственных реализаций почтовых клиентов, которые могут быть встроены в функционал вирусов. Это также позволяет отключить проверку почтовых файлов в **SpIDer Guard**, что значительно снижает потребление ресурсов компьютера.

Антивирусный HTTP-сторож **SpIDer Gate** при настройках по умолчанию автоматически проверяет входящий и исходящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы. Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, т.е. работающие с сетью Интернет. При базовых настройках **SpIDer Gate** блокирует любую передачу объектов, содержащих вредоносные программ. Программа постоянно находится в оперативной памяти компьютера и автоматически перезапускается при загрузке Windows.

С помощью модуля **Родительского контроля** осуществляется ограничение доступа пользователя к ресурсам, содержащимся как локально, на самом ПК, так и в сети. Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность важных файлов и защитить их от заражения вирусами, а также сохранит необходимую конфиденциальность данных. Существует возможность защиты, как отдельных файлов, так и папок целиком, расположенных как на локальных дисках, так и на внешних носителях информации. Также можно наложить полный запрет на просмотр информации со всех внешних носителей. Контроль доступа к интернет-ресурсам позволяет, как оградить пользователя от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т.п.) так и разрешить пользователю доступ только к тем сайтам, которые определены настройками модуля **Родительского контроля**.

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

- произвести сканирование всей файловой системы ПК с предусмотренными по умолчанию (максимальными) настройками подробности сканирования;



- сохранить режим автоматического запуска и остальные настройки системного сторожа по умолчанию;
- осуществлять полную проверку почты при помощи почтового сторожа;
- осуществлять проверку всего HTTP-трафика при помощи **SpIDer Gate**;
- периодически, по мере обновления вирусных баз, повторять полное сканирование ПК (не реже раза в неделю);
- в случае временного отключения сторожа, если в за этот период ПК 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 комплекса (см. [Глава 4. Автоматическое обновление](#)).

Использование компонентов **Dr.Web** подробнее описано в следующих разделах.



Модуль управления SpIDer Agent

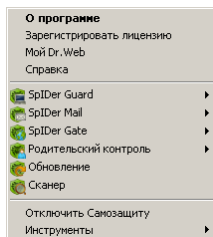


Данный компонент не устанавливается на ПК, работающий под управлением Microsoft® Windows® 95/98/Me.

После установки программного комплекса 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 (см. ниже) *see below*, над значком **SpIDer Agent** могут появляться различные подсказки-уведомления.

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



Пункт **О программе** открывает окно с информацией о версии Антивируса.

Пункт **Зарегистрировать лицензию** запускает [процедуру регистрации пользователя](#) для получения ключевого файла с сервера компании **ООО "Доктор Веб"**.



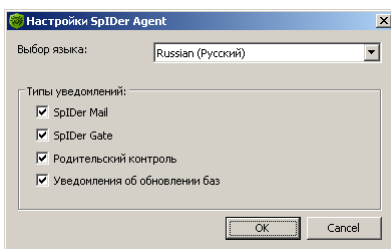
Пункт **Мой Dr.Web** открывает вашу персональную страницу на сайте компании **ООО "Доктор Веб"**. На данной странице вы сможете получить информацию о вашей лицензии (срок действия, серийный номер), продлить срок ее действия, задать вопрос службе поддержки и многое другое.

Пункт **Справка** открывает файл справки Антивируса.

Пункты **SpIDer Guard**, **SpIDer Mail**, **SpIDer Gate**, **Родительский контроль**, **Обновление** и **Сканер** открывают доступ к настройкам и управлению соответствующих компонентов.

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

Пункт **Инструменты** открывает меню, содержащее доступ к **Менеджеру лицензий** (см. [Менеджер лицензий](#)) а также настройкам самого **SpIDer Agent**.



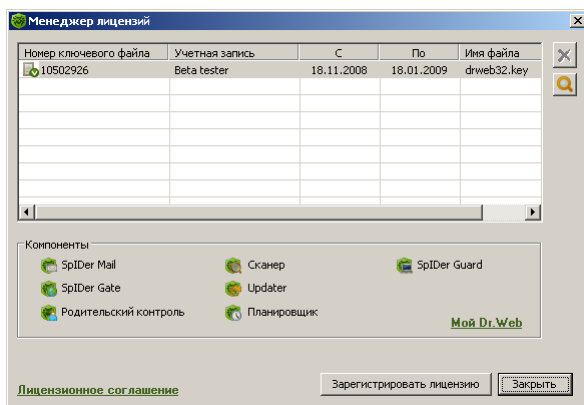
В окне настроек **SpIDer Agent** производится выбор языка интерфейса **Dr.Web для Windows**.


Также в этом окне 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.




Менеджер лицензий

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



Для того чтобы добавить в список ключевой файл нажмите на кнопку .

Для того чтобы удалить ключевой файл из списка нажмите на кнопку .

В группе **Компоненты** выделены те компоненты, с которыми согласно лицензии работает Антивирус.

Пункт **Лицензионное соглашение** открывает файл с текстом лицензии.

Кнопка **Зарегистрировать лицензию** запускает процедуру регистрации пользователя для получения ключевого файла с сервера компании **ООО "Доктор Веб"**.

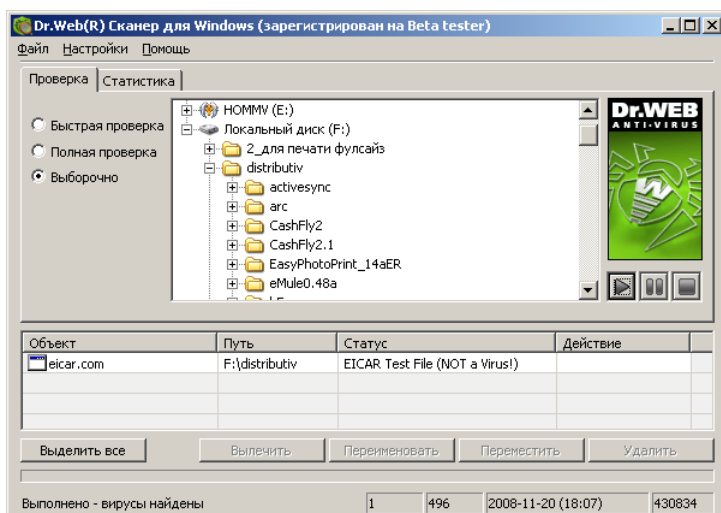


Сканер для Windows

Общие сведения

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 (ZIP, ARJ, LHA, RAR и многих других), файловых контейнерах (PowerPoint, RTF и других), а также файлы в составе писем в почтовых ящиках почтовых программ (формат писем должен соответствовать RFC822).

Версия **Dr.Web для рабочих станций** 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 (рис. 16). **Dr.Web для серверов** по умолчанию предпринимает автоматические действия по предотвращению вирусной угрозы, см. [Настраиваемые параметры программы](#).



Запуск Сканера

Сканер устанавливается как обычное приложение Windows и запускается по команде пользователя (или по команде **Планировщика**, см. [Планировщик для Windows](#)).

Запуск Сканера



При работе под управлением Microsoft® Windows® Vista® 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;

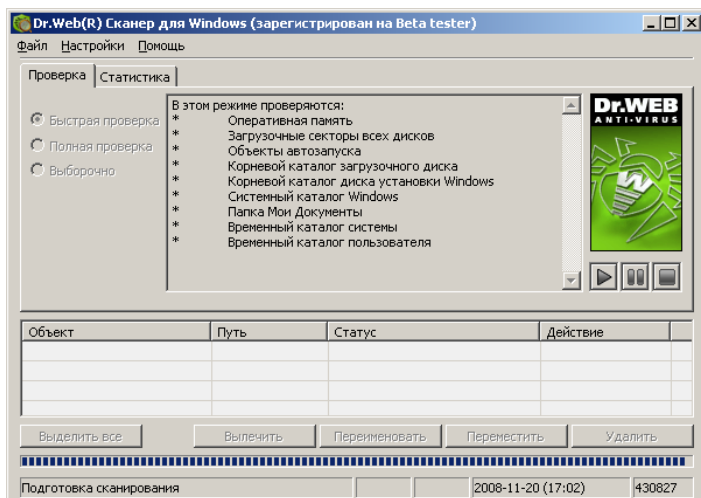


- пункт **Сканер** контекстного меню значка **SpIDer Agent** (см. [Модуль управления SpIDer Agent](#));
- пункт меню **Сканер Dr.Web** в папке **Dr.Web Главного меню** ОС Windows (открывается по кнопке **Пуск**);
- специальную команду операционной системы Windows (подробнее см. п. [Сканирование в режиме 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 запустили **Сканер** на проверку файла или каталога, то после этого начинается сканирование выбранного объекта начнется немедленно. В противном случае, при настройках по умолчанию, немедленно после



запуска программы производится антивирусное сканирование оперативной памяти и файлов автозапуска Windows. 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 система, представленная в виде иерархического дерева (в случае выборочной проверки).

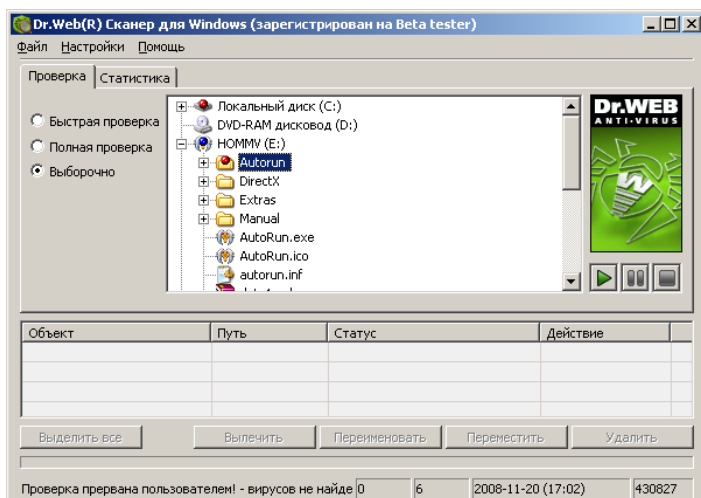
Во время *быстрой проверки* проверяются:

- 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 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 выбран для сканирования весь логический диск С и одна из папок на диске Е.



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.

5. Для того чтобы приступить к сканированию, нажмите на





кнопку **Пуск** 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 чтобы приостановить проверку, нажмите кнопку

Пауза . Для того чтобы возобновить проверку

после паузы, снова нажмите кнопку **Старт** .

- Чтобы полностью остановить проверку, нажмите кнопку

Стоп .

Действия при обнаружении вирусов

По умолчанию **Dr.Web для рабочих станций** 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 ликвидировать исходящую от него угрозу (*удалить* объект).

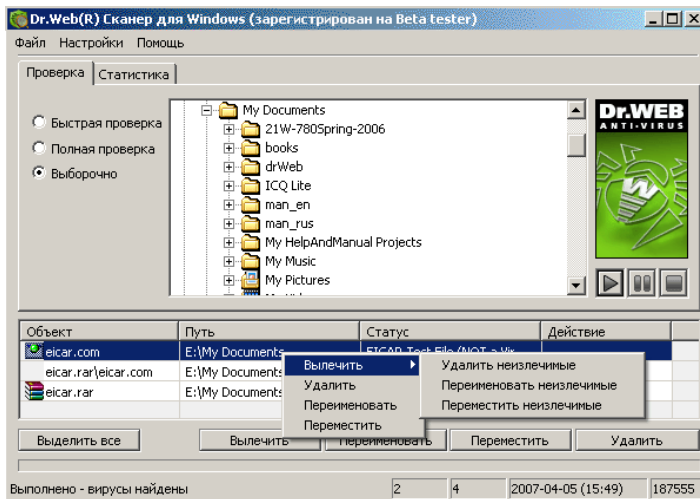
1. Выберите один или несколько зараженных объектов. Вы можете указать действие сразу для всех или нескольких объектов в списке отчета. Чтобы выделить все объекты, нажмите на кнопку **Выделить все**.

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

- INSERT – выделить объект с перемещением курсора на следующую позицию;
 - CTRL+A – выделить все;
 - клавиша умножения (*) на цифровой клавиатуре – отменить 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.!!!`.

Существуют следующие ограничения на возможные действия:

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



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



Подозрительные файлы, перемещенные в карантин, рекомендуется передавать для дальнейшего анализа в антивирусную лабораторию **ООО "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.

- 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** и т. п. 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 ОС для завершения лечения (см. [Настраиваемые параметры программы](#)).

Подробный отчет о работе программы сохраняется в виде файла отчета. По умолчанию он размещается в следующих папках:

- в операционных системах Microsoft Windows 95, Microsoft Windows 98 и Microsoft Windows Me - в папке установки программы;



- в операционных системах Microsoft Windows NT, Microsoft Windows 2000, Windows XP, Microsoft Windows Server 2003 и Windows Vista - в подпапке DoctorWeb, расположенной в папке профиля пользователя %USERPROFILE% и именуется drweb32w.log.

Просмотр отчетов

Чтобы просмотреть отчеты компонентов антивирусного комплекса, выберите подпапку **Отчеты** в папке **Dr.Web**, расположенной в подменю **Программы** главного меню операционной системы Windows (доступно по нажатию кнопки **Пуск**).

Настройка параметров программы



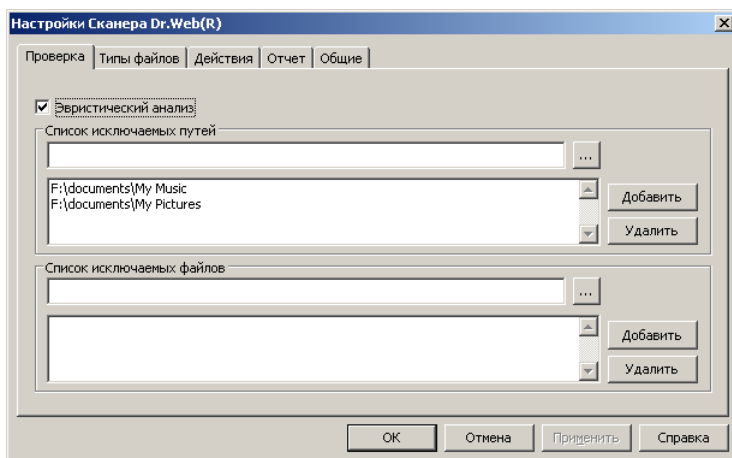
При работе под управлением Microsoft® Windows® Vista® рекомендуется запускать сканер от имени пользователя, обладающим правами администратора. В противном случае пользовательские настройки не будут сохранены при выходе из системы.



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

Для того чтобы изменить настройки программы:

1. Выберите в главном меню программы пункт **Настройки**, после чего в открывшемся подменю выберите пункт **Изменить настройки**. Откроется окно настроек, содержащее несколько вкладок.



2. Внесите необходимые изменения. При необходимости нажимайте на кнопку **Применить** перед переходом на другую вкладку.
3. Для более подробной информации о настройках, задаваемых на каждой вкладке, воспользуйтесь кнопкой **Справка**. Для большинства настроек, задаваемых на вкладках окна, имеется также отдельная подсказка, вызываемая при помощи щелчка правой клавишей мыши по соответствующему элементу интерфейса.
4. По окончании редактирования настроек нажмите на кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отмена** для отказа от них.

Ниже описываются часто используемые случаи изменения настроек по умолчанию.

Настройки по умолчанию **Dr.Web для рабочих станций** 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 назначать действия программы по отношению к ним. Исключением являются объекты, содержащие программы-шутки, потенциально опасные программы



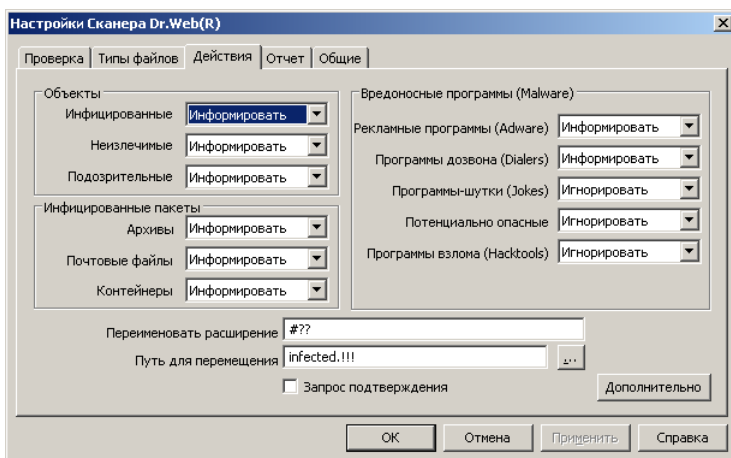
и программы взлома: по умолчанию они игнорируются.

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

Dr.Web для серверов по умолчанию автоматически предпринимает действия по предотвращению вирусной угрозы.

Для того чтобы настроить реакцию 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.



Оптимальным для автоматического режима является значение **Вылечить**. Именно это значение установлено по умолчанию в версии **Dr.Web для серверов**.

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.



В большинстве случаев оптимальным является вариант **Переместить**. Именно это значение установлено по умолчанию в версии **Dr.Web для серверов**.

4. Выберите в выпадающем списке **Подозрительные объекты** реакцию программы на обнаружение подозрительного объекта (полностью аналогично предыдущему пункту).



При использовании **Dr.Web для рабочих станций** рекомендуется сохранить настройку **Информировать**. При использовании **Dr.Web для серверов** рекомендуется сохранить используемое по умолчанию значение **Переместить**.

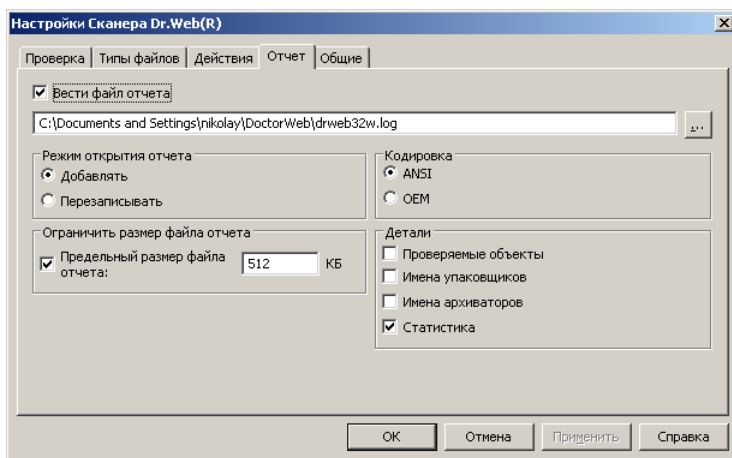
5. Аналогично настраивается реакция программы на обнаружение объектов, содержащих рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.
6. Аналогично настраиваются автоматические действия программы при обнаружении вирусов или подозрительного кода в файловых архивах, контейнерах и почтовых ящиках. Действия по отношению к вышеуказанным объектам выполняются над всем объектом, а не только над зараженной его частью. В **Dr.Web для рабочих станций** по умолчанию во всех этих случаях предусмотрено информирование. В **Dr.Web для серверов** по умолчанию во всех этих случаях предусмотрено перемещение.
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 на кнопку **Дополнительно**, расположенную в правом нижнем углу вкладки.

На вкладке **Отчет** 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.

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>]
```



Вместо программы **Dr.Web Сканер для Windows** может использоваться **Dr.Web Консольный сканер для Windows**. В этом случае вместо `drweb32w` необходимо набрать имя команды `drwebwcl`.



Аналогично вызывается **Dr.Web Сканер для DOS** (имя команды `drweb386`). При этом все имена файлов и пути должны задаваться в формате, принятом в этой ОС (в частности, допускаются только короткие имена файлов). Данный компонент не включается в состав **Dr.Web для серверов**.



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

Наиболее распространенные варианты указания объектов сканирования приведены ниже:

- * 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 В](#).

- /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).



Консольная версия сканера для Windows 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. Подробнее см. [Приложение С](#).



SpIDer Guard для Windows

Общие сведения

На компьютер устанавливается одна из двух версий сторожа, в зависимости от используемой ОС:

- **SpIDer Guard для Windows 95/98/Me** (далее кратко именуемый **SpIDer Guard Me**),
- **SpIDer Guard для Windows NT/2000/XP/2003/Vista/2008** (далее кратко именуемый **SpIDer Guard XP**).

По умолчанию сторож запускается автоматически при каждой загрузке операционной системы, при этом запущенный сторож **SpIDer Guard Me** не может быть выгружен в течение текущего сеанса работы операционной системы (о выгрузке **SpIDer Guard XP** см. п. [Настройка режима запуска SpIDer Guard](#)). При необходимости приостановить на некоторое время работу сторожа (например, при выполнении критически чувствительного к загрузке процессора задания в реальном масштабе времени) в случае использования **SpIDer Guard XP** выберите в меню **SpIDer Guard** контекстного меню модуля управления пункт **Отключить**. В случае использования **SpIDer Guard Me** следует отменить настройку автоматического запуска сторожа (это действие описывается ниже – см. п. [Настройка режима запуска SpIDer Guard](#)) и после этого перезагрузить компьютер.



При работе под управлением Microsoft® Windows® NT/2000/XP/2003/Vista®/2008 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 и сетевых дисках – все открываемые файлы, при этом каждый файл проверяет аналогично **Сканеру**, однако с более "мягкими" условиями проверки. Кроме того, сторож



постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при их обнаружении блокирует процессы с выводом соответствующего сообщения пользователю.

По умолчанию, сторож в пакете **Dr.Web для рабочих станций**, как и **Сканер**, только информирует пользователя об обнаружении зараженных объектов и предлагает ему принять решение о возможных действиях. **Dr.Web для серверов Windows** в случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом по умолчанию предпринимает автоматические действия по предотвращению вирусной угрозы.

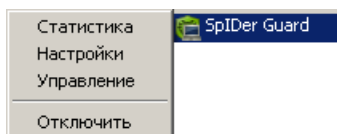


При работе под управлением Microsoft® Windows® Vista® доступ к **Панели управления** и вкладкам настроек **SpIDer Guard** возможен только для пользователя, обладающего правами администратора.

Соответствующим изменением настроек вы можете задать автоматическую реакцию программы на вирусные события; в этом случае работа сторожа будет происходить в автономном режиме. Пользователь сможет следить за ней с помощью окна статистики (об этом окне см. ниже) и файла отчета.

Управление сторожем SpIDer Guard

В меню **SpIDer Guard** контекстного меню значка модуля управления (только для **SpIDer Guard XP**) сосредоточены основные средства настройки и управления сторожем. (Аналогичное контекстное меню для **SpIDer Guard Me** появляется над значком самого сторожа, расположенным в области уведомлений Windows).



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](#)).



При работе под управлением ОС Windows® Vista® доступ к вкладкам настроек **SpIDer Guard** возможен только для пользователя, обладающего правами администратора.

Пункт **Управление** (только для **SpIDer Guard XP**) позволяет открыть окно **Панели управления SpIDer Guard XP** (доступно только пользователю, имеющему права администратора данного компьютера).

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

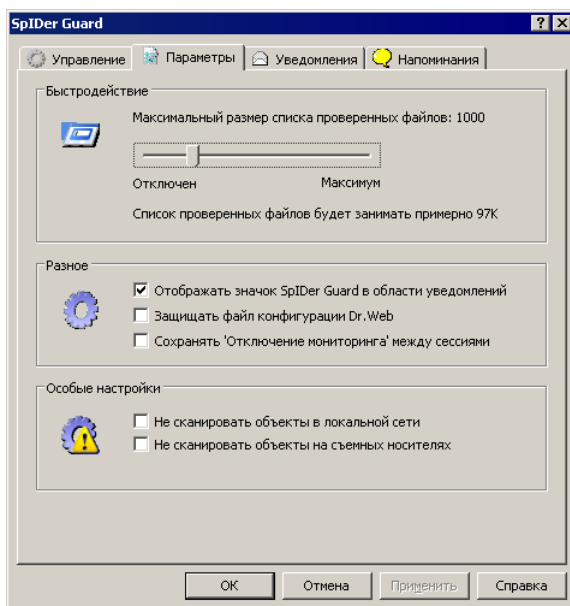
При установке **SpIDer Guard XP** на **Панели управления** ОС Windows создается элемент **Dr.Web Anti-virus**, в котором сосредоточены настройки, специфичные для программы в среде Microsoft® Windows®. Эти настройки доступны только пользователю, имеющему права администратора данного компьютера; в частности, он может разрешить отображение значка сторожа в области уведомлений ОС Windows.

В случае использования **SpIDer Guard XP** при наведении курсора мыши на значок появляется всплывающая подсказка со статистикой **SpIDer Guard**, информацией о версиях модулей **Антивируса**, датой последнего обновления антивируса и количеством записей в вирусных базах. Также над значком, с указанной в настройках периодичностью, может появляться всплывающая подсказка-предупреждение о произошедших событиях. Настройка всплывающих подсказок производится на вкладке настроек **Напоминания**.



Для того чтобы отображать значок SpIDer Guard XP в области уведомлений, администратору ПК следует выполнить следующие действия:

1. Воспользуйтесь одним из следующих способов, чтобы открыть окно элемента **SpIDer Guard XP** на **Панели управления** ОС Windows:
 - выберите в **Главном меню** ОС Windows (вызывается по кнопке **Пуск**) пункт **Панель управления** (в некоторых случаях он находится в подменю **Настройка**). В открывшемся окне **Панели управления** ОС Windows дважды щелкните по элементу **Dr.Web Anti-virus**;
 - или выберите пункт **Управление** в меню пункта **SpIDer Guard** контекстного меню **SpIDer Agent**.
2. В открывшемся окне перейдите на вкладку **Параметры** (рис. 24).
3. Для того чтобы разрешить отображение значка сторожа, установите флаг **Отображать значок SpIDer Guard в области уведомлений**; для того чтобы запретить отображение значка, снимите этот флаг.
4. Нажмите на кнопку **ОК**.



Настройка режима запуска SpIDer Guard

После установки **Dr.Web**, согласно стандартным настройкам, загрузка сторожа производится автоматически сразу после запуска операционной системы. Если необходимо, вы можете отменить режим автоматической загрузки **SpIDer Guard**.

Для того чтобы отменить режим автоматического запуска SpIDer Guard XP:

1. Перейдите на вкладку **Управление** окна элемента **Панели управления SpIDer Guard XP**.



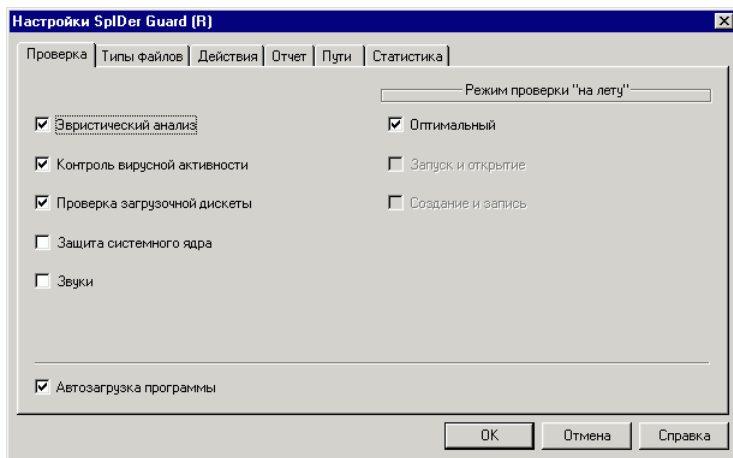
2. В группе кнопок выбора **Режим загрузки** выберите **Ручной режим**.
3. Нажмите на кнопку **ОК**.

При последующих запусках программа не будет запускаться автоматически. При необходимости ее можно будет запустить вручную, для чего следует нажать в вышеописанном окне на кнопку **Загрузить**. **SpIDer Guard XP** можно остановить нажатием на кнопку **Выгрузить**.

Версия сторожа **SpIDer Guard Me** всегда устанавливается в режиме автозапуска, однако этот режим также можно отменить.

Для этого:

1. В контекстном меню значка сторожа в **Панели задач** выберите пункт **Настройки**. Откроется окно настроек программы на вкладке **Проверка**.



2. Удалите флаг **Автозагрузка программы**.
3. Нажмите на кнопку **ОК**.

При последующей загрузке операционной системы сторож уже не будет запускаться автоматически.

Для того чтобы запустить сторож **SpIDer Guard Me** вручную, выберите в **Главном меню** ОС Windows (вызывается по кнопке **Пуск**) пункт **Программы**, далее выберите пункт **Dr.Web**, в открывшемся подменю выберите пункт **SpIDer Guard**. После запуска сторожа он автоматически переводится снова в автоматический режим запуска.

Основные настройки сторожа

Основные настраиваемые параметры обеих версий сторожа сосредоточены на вкладках окна **Настройки SpIDer Guard Me** (см. [ниже](#)) и **SpIDer Guard XP** (рис. [ниже](#)). Для того чтобы получить справку о параметрах, задаваемых на какой-либо вкладке, перейдите на эту вкладку и нажмите на кнопку **Справка**. Более детальные сведения о каком-либо параметре можно получить, щелкнув правой клавишей мыши по соответствующему элементу интерфейса.



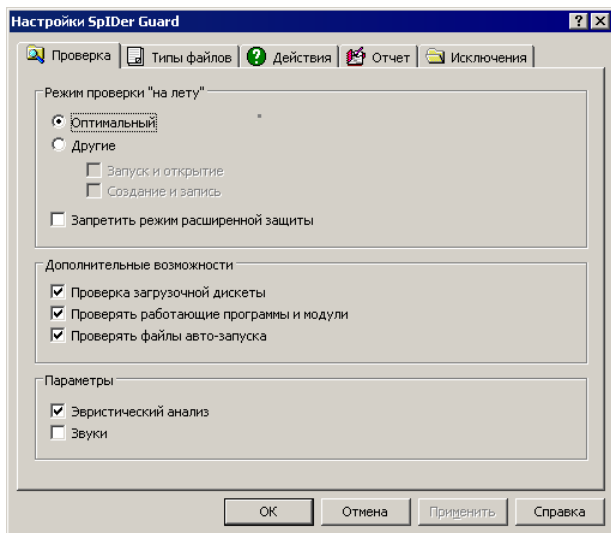
По окончании редактирования настроек нажмите на кнопку **ОК**, чтобы сохранить изменения, или на кнопку **Отмена**, чтобы отказаться от внесенных изменений.

Ниже описываются некоторые наиболее часто изменяемые настройки программы.

По умолчанию установлено сканирование на жестких дисках – только создаваемых или изменяемых файлов, на сменных носителях и сетевых дисках – всех открываемых файлов.

В режиме *расширенной защиты* (доступен только в **SpIDer Guard XP**) сторож проверяет все файлы, проверка которых предусмотрена настройками программы, немедленно, а остальные открываемые файлы помещает в очередь отложенной проверки (файлы, открываемые на чтение при режимах **Оптимальный** и **Создание и запись**). При наличии свободных ресурсов ПК эти файлы также будут проверены сторожем. Режим расширенной защиты по умолчанию выключен.

Вы можете включить данный режим. Для этого на вкладке **Проверка** окна **Настройки** снимите флаг **Запретить режим расширенной защиты**.



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**.

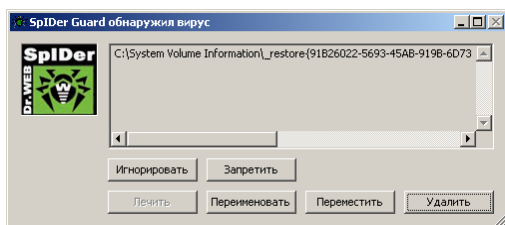


Отказ от проверки архивов в условиях постоянной работы сторожа не ведет к проникновению вирусов на ПК, а лишь откладывает момент их обнаружения. При распаковке зараженного архива (открытии зараженного письма) будет сделана попытка записать инфицированный объект на диск, при этом сторож неминуемо обнаружит.

При использовании **Dr.Web для рабочих станций** для предположительно излечимых вирусов, неизлечимых вирусов и подозрительных объектов по умолчанию предусмотрена реакция программы *информировать* пользователя, которому предлагается принять решение о дальнейших действиях. При этом сторож



открывает окно с запросом о дальнейших действиях.



Версия сторожа, включенная в состав **Dr.Web для серверов**, по умолчанию предпринимает действия по устранению обнаруженных вирусных угроз автоматически (подробнее см. ниже).

При обнаружении объекты, содержащие программы-шутки, потенциально опасные программы и программы взлома, по умолчанию *игнорируются*.

При обнаружении объектов, содержащих рекламные программы и программы дозвона, реакция сторожа по умолчанию предусмотрена разная: для серверов – *перемещение*, для рабочих станций – *информирование* пользователя.

Состав доступных реакций зависит от типа вирусного события.

Реакции **Лечить**, **Переименовать**, **Переместить** и **Удалить** аналогичны таким же реакциям **Сканера**.

При нажатии на кнопку **Запретить** зараженный файл помечается операционной системой как недоступный.

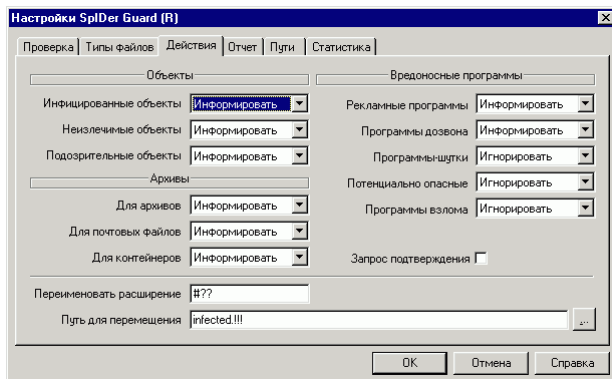
При нажатии на кнопку **Выключить** (только для **SpIDer Guard Me**) делается попытка корректного завершения работы операционной системы.

Вы можете изменить настройки сторожа, с тем чтобы он автоматически производил необходимые действия с зараженными объектами, не обращаясь к пользователю.



Чтобы изменить настройки сторожа в случае использования SpIDer Guard Me:

1. В окне **Настройки SpIDer Guard** перейдите на вкладку **Действия**.

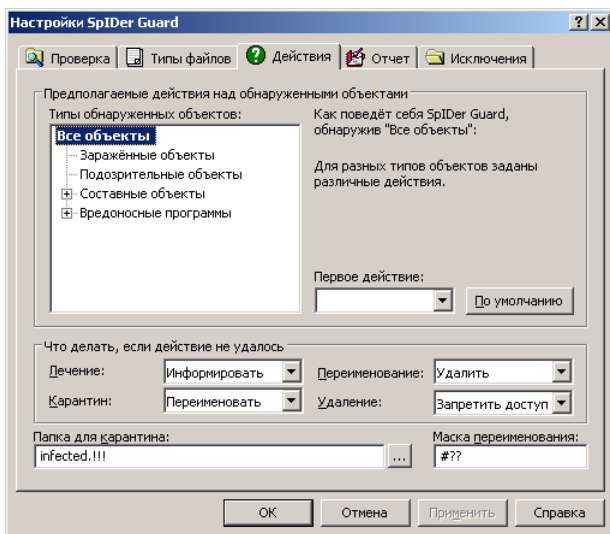


2. Выберите в выпадающем списке **Инфицированные объекты** реакцию программы на обнаружение инфицированного объекта (рекомендуется установить действие **Вылечить**).
3. Выберите в выпадающем списке **Неизлечимые объекты** реакцию программы на обнаружение неизлечимого объекта (рекомендуется установить действие **Переместить**). 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 **Переместить**.
5. Аналогично настраивается реакция программы на обнаружение объектов, содержащих рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.
6. Нажмите на кнопку **OK**.



Чтобы изменить настройки сторожа в случае использования SpIDer Guard XP:

1. В окне **Настройки SpIDer Guard** перейдите на вкладку **Действия**.



2. Выберите в иерархическом списке в левой части окна **Зараженные объекты**. В правой верхней части окна отобразится реакция программы на обнаружение объекта, зараженного известным вирусом. Указывается действие, предписанное текущими настройками, и альтернативное действие, которое будет предпринято, если предписанную реакцию осуществить не удалось. В следующем шаге описывается, как изменить настройки первого действия; настройки альтернативного действия описаны в шаге **5**.
3. Для того чтобы загрузить настройки действий при обнаружении данного типа объектов по умолчанию, нажмите на кнопку **По умолчанию**. В версии для рабочих станций, по умолчанию предусмотрено информирование для всех инфицированных, подозрительных и вредоносных объектов (кроме объектов, содержащих программы-шутки, потенциально опасные программы и программы взлома,



которые игнорируются). В версии для серверов предусмотрено лечение для инфицированных объектов, игнорирование – для объектов, содержащих программы-шутки, потенциально опасные программы и программы взлома, и перемещение – для объектов, содержащих рекламные программы и программы дозвона, а также для подозрительных объектов и инфицированных составных объектов.

4. Выберите в выпадающем списке **Первое действие** первичную реакцию программы на обнаружение инфицированного объекта. Нажмите на кнопку **Изменить**, чтобы предписать программе в дальнейшем использовать выбранную вами реакцию.
5. В области **Что делать, если действие не удалось** находятся настройки альтернативного действия, которое будет предпринято, если предписанную реакцию осуществить не удалось. Эти настройки задаются отдельно для следующих возможных вариантов первого действия: **лечение, перемещение в карантин, переименование, удаление**. Вы можете выбрать действие, которое будет предпринято при неудаче первого действия, в соответствующих выпадающих списках.
6. Аналогично настраивается реакция программы на обнаружение подозрительных объектов, зараженных файловых архивов, почтовых архивов и контейнеров, а также объектов, содержащих рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.
7. При необходимости задайте имя каталога для перемещаемых файлов и путь к нему в поле **Папка для карантина**.
8. При необходимости задайте маску для переименования расширения файла при выполнении операции переименования.
9. Нажмите на кнопку **ОК**.

На вкладке **Отчет** вы можете настроить параметры ведения файла отчета (аналогично одноименной настройке **Сканера**).



SpIDer Mail для рабочих станций Windows



Данный компонент не включается в состав **Dr.Web для серверов**.

Общие сведения

Почтовый сторож **SpIDer Mail для рабочих станций Windows** по умолчанию включается в состав устанавливаемых компонентов, постоянно находится в памяти и автоматически запускается при загрузке ОС Windows.

По умолчанию программа автоматически перехватывает все обращения любых почтовых программ вашего компьютера к POP3-серверам по порту 110, к SMTP-серверам по 25, к IMAP4-серверам по порту 143 и к NNTP-серверам по порту 119.

Антивирусный почтовый сторож получает все входящие письма вместо почтового клиента и подвергает их антивирусному сканированию с максимальной степенью подробности. При отсутствии вирусов или подозрительных объектов письма передаются почтовой программе "прозрачным" образом – так, как если бы они поступили непосредственно с сервера. Аналогично проверяются исходящие письма до отправки на сервер.

Реакция программы на инфицированные и подозрительные входящие письма, а также письма, не прошедшие проверку (например, с чрезмерно сложной структурой), по умолчанию следующая (об изменении этих настроек см. п. [Основные настройки почтового сторожа](#)):

- зараженные вирусом письма не доставляются, почтовой программе передается сообщение об уничтожении письма, серверу – сообщение о приеме письма (это действие называется *удалением* письма);



- письма с подозрительными объектами перемещаются в виде отдельных файлов в специальный каталог карантина, почтовой программе посылается сообщение об этом (это действие называется *перемещением* письма);
- письма, не прошедшие проверку, пропускаются, как и незараженные;
- все удаленные или перемещенные письма также удаляются с POP3- или IMAP4-сервера.

Инфицированные или подозрительные исходящие письма не передаются на сервер, пользователя оповещают об отказе отправить письмо (как правило, почтовая программа при этом его сохраняет).

При наличии на компьютере неизвестного вируса, распространяющегося через электронную почту, программа может определять признаки типичного для таких вирусов "поведения" (массовые рассылки). По умолчанию эта возможность включена.

Почтовый сторож предоставляет возможность проверки входящих писем на спам с помощью спам-фильтра **Vade Retro**. По умолчанию эта возможность включена. (О настройках работы спам-фильтра см. п. [Основные настройки почтового сторожа](#)).



Функция проверки писем на спам доступна только в том случае, если система **Dr.Web** работает с лицензией на программный пакет "**Dr.Web Security Space 5.0**".

Настройки программы по умолчанию являются оптимальными для начинающего пользователя, обеспечивая максимальный уровень защиты при наименьшем вмешательстве пользователя. При этом, однако, блокируется ряд возможностей почтовых программ (например, направление письма по многим адресам может быть воспринято как рассылка, полученный спам не распознается), а также утрачивается возможность получения полезной информации из автоматически уничтоженных писем (из незараженной текстовой части). Более опытные пользователи могут изменить параметры сканирования почты и настройки



реакции программы на события.

В ряде случаев автоматический перехват POP3-, SMTP-, IMAP4- и NNTP-соединений невозможен; в таком случае программа предоставляет возможность настроить перехват соединений вручную.

Сторож **SpIDer Guard** и **Сканер** также могут обнаруживать вирусы в почтовых ящиках некоторых форматов, однако почтовый сторож **SpIDer Mail** имеет перед этими программами ряд преимуществ:

- далеко не все форматы почтовых ящиков популярных программ поддерживаются сторожем и **Сканером**; напротив, при использовании почтового сторожа зараженные письма даже не попадают в почтовые ящики;
- **SpIDer Guard** по умолчанию не проверяет почтовые ящики, при включении этой возможности производительность системы значительно снижается;
- **Сканер** проверяет почтовые ящики, но только по запросу пользователя или по расписанию, а не в момент получения почты, причем данное действие является чрезвычайно трудоемким и занимает значительное время.

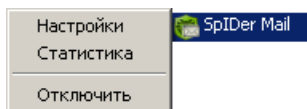
Таким образом, при настройках всех компонентов по умолчанию почтовый сторож **SpIDer Mail** первым обнаруживает и не допускает на компьютер вирусы и подозрительные объекты, распространяющиеся по электронной почте. Его работа является весьма экономичной с точки зрения расхода вычислительных ресурсов; остальные компоненты могут не использоваться для проверки почтовых файлов.

Управление почтовым сторожем SpIDer Mail

Управление компонентом **SpIDer Mail** осуществляется при помощи меню пункта **SpIDer Mail**, расположенного в контекстном меню значка модуля управления SpIDer Agent (см. [Модуль управления SpIDer Agent](#)). (Аналогичное контекстное меню для SpIDer Mail, установленный на ПК под управлением Microsoft®



Windows® 95/98/Me появляется над значком самого сторожа, расположенным в области уведомлений Windows).



При выборе пункта **Настройки** открывается окно настроек компонента (см. п. [Основные настройки почтового сторожа](#)).



При работе под управлением Microsoft® Windows® Vista® изменение настроек и языка интерфейса **SpIDer Mail** доступно только для пользователя, обладающего правами администратора.

При выборе пункта **Статистика** открывается окно с информацией о работе программы в текущем сеансе (количество проверенных, зараженных, подозрительных объектов и предпринятые действия).

Выберите **Отключить** чтобы остановить работу сторожа. Для того чтобы запустить **SpIDer Mail** выберите пункт **Включить**.

Основные настройки почтового сторожа

При необходимости вы можете изменить настройки почтового сторожа. Для этого откройте окно настроек, как было указано выше (см. п. [Управление почтовым сторожем SpIDer Mail](#)).

При редактировании настроек пользуйтесь системой помощи программы (общая справка по каждой вкладке вызывается при нажатии на кнопку **Справка**; имеется также контекстная подсказка для отдельных элементов интерфейса).

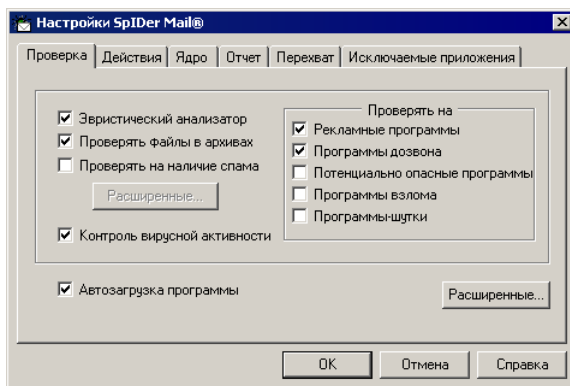
По окончании редактирования настроек нажмите на кнопку **ОК**.

Большинство настроек по умолчанию являются оптимальными в большинстве случаев. Ниже описываются параметры, для которых чаще всего возникает необходимость в настройках, отличных от



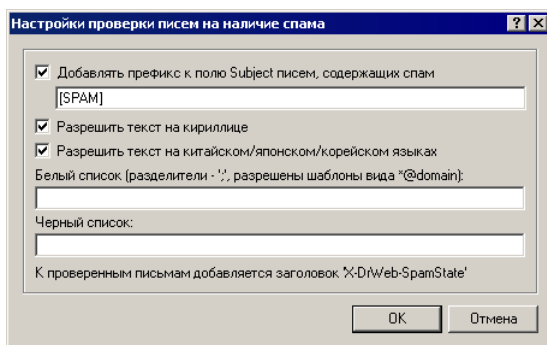
заданных по умолчанию.

Почтовый сторож по умолчанию не осуществляет проверку входящих писем на спам. Для того чтобы входящая корреспонденция проверялась спам-фильтром, на вкладке **Проверка** установите флаг в поле **Проверять на наличие спама**.



Функция проверки писем на спам доступна только в том случае, если система **Dr.Web** работает с лицензией на программный пакет "**Dr.Web Security Space 5.0**".

Изменение настроек спам-фильтра осуществляется в окне **Настройки проверки писем на наличие спама SpIDer Mail®**.



Для того чтобы открыть это окно нажмите кнопку **Расширенные**, расположенную на вкладке **Проверка** непосредственно под полем **Проверять на наличие спама**.

Ко всем проверенным письмам будут добавляться заголовки:

- X-DrWeb-SpamState: Yes/No. Значение Yes показывает, что письму присвоен статус спам, No — письмо, по мнению **SpIDer Mail**, спамом не является.
- X-DrWeb-SpamVersion: version.version – версия библиотеки спам-фильтра **Vade Retro**.

Установка флага в поле **Добавлять префикс к полю Subject писем, содержащих спам** указывает почтовому сторожу **SpIDer Mail** добавлять специальный префикс к темам писем, распознаваемых как спам. Этот префикс задается в поле, расположенном под флагом. Добавление префикса поможет вам создать правила для фильтрации почтовых сообщений, помеченных как спам, в тех почтовых клиентах (например MS Outlook Express), в которых невозможно настроить фильтры по заголовкам писем.



Если для получения почтовых сообщений вы используете протоколы IMAP/NNTP – настройте вашу почтовую программу таким образом, чтобы письма загружались с почтового сервера сразу целиком, без предварительного просмотра заголовков. Это необходимо для корректной работы спам-фильтра.

Флаг, установленный в поле **Разрешать текст на кириллице** указывает спам-фильтру не причислять письма, написанные с установленной кириллической кодировкой, к спаму без предварительного анализа. Если флаг снят, то такие письма с большой вероятностью будут отмечены фильтром как спам.

Установка и снятие флага **Разрешать текст на китайском/ японском/ корейском языках** работает аналогично.

Поля **Белый список** и **Черный список** содержат "черные" и "белые" списки адресов отправителей почтовых сообщений.

- Если адрес отправителя добавлен в "белый" список, письмо не подвергается анализу на содержание спама. Однако если доменное имя адресов получателя и отправителя письма совпадают, и это доменное имя занесено в белый список с использованием знака "*", то письмо подвергается проверке на спам.
- Если адрес отправителя добавлен в "черный" список, письму без дополнительного анализа присваивается статус спама.

Данные поля следует заполнять последовательно, разделяя разные почтовые адреса с помощью знака "; ". Допускается использование знака "*" вместо части адреса. (Например, запись вида *@domain.org означает все адреса с доменным именем domain.org).



Если какие-либо письма неправильно распознаются спам-фильтром, следует отправлять их на специальные почтовые адреса, для анализа и повышения качества работы фильтра. Письма, ошибочно оцененные как спам, отправляйте на адрес vrnospam@drweb.com, а спам, не распознанный системой - на адрес vrspam@drweb.com. Все сообщения следует пересылать только в виде вложения (а не в теле письма).

По умолчанию почтовый сторож обнаруживает, наряду с письмами, содержащими инфицированные файлы, письма, содержащие другие разновидности нежелательных программ:

- рекламные программы,
- программы дозвона.

Почтовый сторож также может обнаруживать следующие виды нежелательных программ:

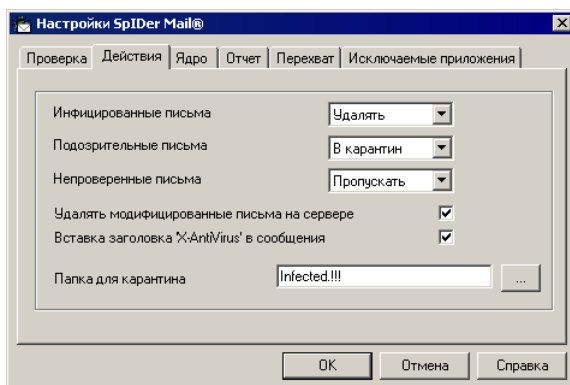
- потенциально опасные программы,
- программы взлома,
- программы-шутки.

Для того чтобы изменить состав обнаруживаемых нежелательных программ, на вкладке **Проверка** (см. [выше](#)) в поле **Проверить на** установите флаги у наименований типов нежелательных программ, которые необходимо обнаруживать, и удалите флаги у наименований типов программ, которые не надо обнаруживать.



Реакция почтового сторожа на обнаружение нежелательных программ совпадает с реакцией на обнаружение инфицированных писем (см. ниже).

Настройки реакции программы на обнаружение вирусных объектов во входящей почте сосредоточены на вкладке **Действия**.



По умолчанию для инфицированных писем (содержащих известный программе вирусный код) предусмотрено удаление, т. е. отказ от получения письма (как правило, письмо также уничтожается на POP3/IMAP4-сервере). Опытные пользователи могут выбрать в списке **Инфицированные письма** реакцию **В карантин**. В этом случае письма будут помещаться в специальный каталог (карантин) для дальнейшего исследования.

Пользователи, убежденные в том, что "подозрительные" письма, получаемые ими, на самом деле не содержат вирусов, могут выбрать в списке **Подозрительные письма** реакцию **Пропускать**.



Защиту от подозрительных писем можно отключать только в том случае, когда ПК дополнительно защищен постоянно загруженным сторожем **SpIDer Guard**.

Вы можете увеличить надежность антивирусной защиты по сравнению с уровнем, предусмотренным по умолчанию, выбрав в списке **Непроверенные письма** пункт **В карантин**. Файлы с перемещенными письмами в этом случае рекомендуется проверить **Сканером**.

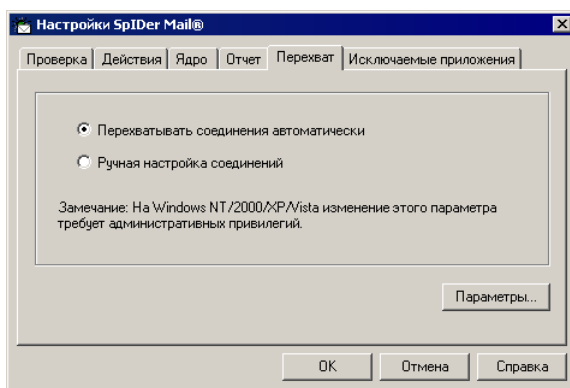
Опытные пользователи могут также отказаться от режима, в котором удаленные или перемещенные программой письма также



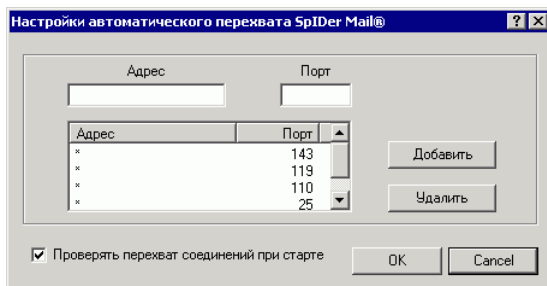
немедленно удаляются на POP3/IMAP4-сервере, удаляя такие письма вручную или с использованием более гибких настроек почтовой программы. Для этого снимите флаг **Удалять модифицированные письма на сервере**.

По умолчанию сторож автоматически перехватывает почтовый трафик всех пользовательских приложений на вашем компьютере. Отключить проверку почтового трафика некоторых программ вы можете на вкладке **Исключаемые приложения**. Для этого добавьте необходимое приложение в список исключений.

Управление перехватом соединений с почтовыми серверами сосредоточено на вкладке **Перехват**.



По умолчанию, перехват производится автоматически. Список перехватываемых адресов находится в дополнительном окне, для открытия которого нажмите на кнопку **Параметры**.



По умолчанию, список автоматически перехватываемых обращений включает все IP-адреса (задано при помощи символа *) и портов 143 (стандартный для IMAP4-протокола), 119 (стандартный для NNTP-протокола), 110 (стандартный для POP3-протокола) и 25 (стандартный для SMTP-протокола).

Для того чтобы удалить какой-либо элемент из списка, выберите его в списке и нажмите на кнопку **Удалить**.

Для того чтобы добавить какой-либо сервер или группу серверов в список, введите его адрес (доменное имя или IP-адрес) в поле **Адрес**, а номер порта, к которому происходит обращение, в поле **Порт**, и нажмите на кнопку **Добавить**.

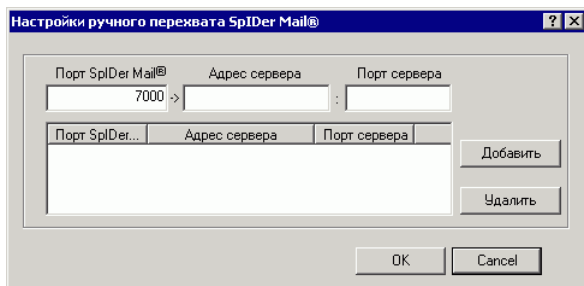


Адрес `localhost` не перехватывается при указании символа *. Данный адрес при необходимости следует указывать в списке перехвата в явном виде.

Если автоматический перехват невозможен (программа сообщает об этом, если флаг **Проверять перехват соединений при старте** установлен), требуется задавать перехват вручную.

Для того, чтобы настроить перехват вручную:

1. В приведенном выше окне выбора способа перехвата (см. [выше](#)) выберите вариант **Ручная настройка соединений** и нажмите на кнопку **Параметры**. Откроется окно настройки соединений в ручном режиме.



2. Составьте список ресурсов (POP3/SMTP/IMAP4/NNTP-серверов), обращения к которым предполагается перехватывать. Перенумеруйте их без пропусков, начиная с числа 7000. Эти номера далее будут именоваться портами **SpIDer Mail**.
3. Для каждого из ресурсов введите в поле **Порт SpIDer Mail** присвоенный ему номер, в поле **Адрес сервера** – доменное имя сервера, либо его IP-адрес, в поле **Порт сервера** – номер порта, к которому происходит обращение, и нажмите на кнопку **Добавить**.
4. Повторите эти действия для каждого ресурса.
5. Нажмите на кнопку **OK**.



В настройках почтового клиента вместо адреса и порта POP3/SMTP/IMAP4/NNTP-сервера укажите адрес `localhost: <порт_SpIDer_Mail>`, где `<порт_SpIDer_Mail>` – порт, назначенный соответствующему POP3/SMTP/IMAP4/NNTP-серверу.



SpIDer Gate Dr.Web



Данный компонент не устанавливается на ПК, работающий под управлением Microsoft® Windows® 95/98/Me.

Данный компонент не включается в состав **Dr.Web для Windows Server**.

SpIDer Gate - антивирусный HTTP-сторож. При настройках по умолчанию **SpIDer Gate** автоматически проверяет входящий и исходящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы. Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, т.е. работающие с сетью Интернет.

С помощью изменения настроек **SpIDer Gate** (см. [Настройка SpIDer Gate](#)) вы можете отключить проверку исходящего или входящего трафика, а также сформировать список тех приложений, HTTP-трафик которых будет проверяться в любом случае и в полном объеме. Также существует возможность исключения из проверки трафика отдельных приложений.

При базовых настройках **SpIDer Gate** блокирует любую передачу объектов, содержащих вредоносные программ.

Программа постоянно находится в оперативной памяти компьютера и автоматически перезапускается при загрузке Windows. Вы можете изменить режим автоматического запуска программы, сняв соответствующий флажок.



Общие сведения



Данный компонент не устанавливается на ПК, работающий под управлением Microsoft® Windows® 95/98/Me.

Данный компонент не включается в состав **Dr.Web для Windows Server**.

SpIDer Gate - антивирусный HTTP-сторож. При настройках по умолчанию **SpIDer Gate** автоматически проверяет входящий и исходящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы. Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, т.е. работающие с сетью Интернет.

С помощью изменения настроек **SpIDer Gate** (см. [Настройка SpIDer Gate](#)) вы можете отключить проверку исходящего или входящего трафика, а также сформировать список тех приложений, HTTP-трафик которых будет проверяться в любом случае и в полном объеме. Также существует возможность исключения из проверки трафика отдельных приложений.

При базовых настройках **SpIDer Gate** блокирует любую передачу объектов, содержащих вредоносные программ.

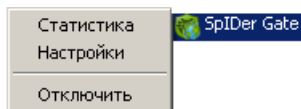
Программа постоянно находится в оперативной памяти компьютера и автоматически перезапускается при загрузке Windows. Вы можете изменить режим автоматического запуска программы, сняв соответствующий флажок.

Управление SpIDer Gate

Управление компонентом **SpIDer Gate** осуществляется при помощи меню пункта **SpIDer Gate**, расположенного в контекстном меню значка модуля управления SpIDer Agent (см.



[Модуль управления SpIDer Agent](#)).



При выборе пункта **Настройки** откроется окно настроек программы (см. [Настройка SpIDer Gate](#)).



Доступ к изменению настроек модуля защищен [паролем](#).


При выборе пункта **Статистика** откроется окно с информацией о работе программы в текущем сеансе.

Пункт **Отключить/Включить** позволяет запустить/остановить работу **SpIDer Gate**.


Настройка SpIDer Gate

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

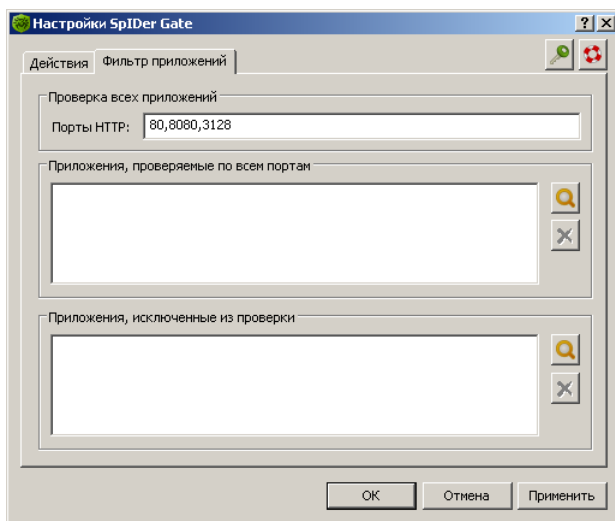
При необходимости вы можете изменить настройки HTTP-сторожа:

1. Выберите в меню **SpIDer Gate** (см. п. [Управление SpIDer Gate](#)) пункт **Настройки**. Откроется окно задания пароля
2. Введите ранее сохраненный пароль. Задание пароля производится при вызове окна настроек модуля в первый раз. Для того чтобы изменить пароль нажмите на кнопку , расположенную в окне настроек.
3. Внесите необходимые изменения на вкладках настроек.
4. Для того чтобы получить информацию о настройках,



- расположенных на вкладке, нажмите на кнопку .
5. Нажмите на кнопку **Применить** для немедленного сохранения внесенных изменений.
 6. По окончании редактирования настроек нажмите на кнопку **ОК**.

По умолчанию **SpIDer Gate** проверяет трафик обоих направлений, входящий и исходящий. На вкладке **Фильтр приложений** производится настройка параметров проверки HTTP-трафика.




SpIDer Gate производит проверку того HTTP-трафика, который проходит через порты указанные в верхней части вкладки. По умолчанию проверяются 80, 8080 и 3128 HTTP порты; данные порты чаще всего используются приложениями для передачи информации по протоколу HTTP. Если вы знаете, что какое-либо приложение, установленное на вашем компьютере, использует иной порт для HTTP-трафика, то добавьте данный порт в список **Порты HTTP**.


Добавьте в список **Приложения, проверяемые по всем портам** те программы, сетевую активность которых следует проверять с особенной тщательностью. Такими программами



могут считаться веб-обозреватели, менеджеры загрузок, а также новые установленные программы.

Добавьте в список **Приложения, исключенные из проверки** те программы, сетевую активность которых **SpIDer Gate** контролировать не должен. Исключать из проверки следует только те приложения, действиям и защищенности которых вы полностью доверяете.

Для того чтобы добавить приложение в список, нажмите на кнопку  и выберите приложение в стандартном окне операционной системы.

Для того чтобы удалить приложение из списка, выберите его в этом списке и нажмите на кнопку .

Для того чтобы подробнее ознакомиться с какой-либо настройкой, задаваемой на этой вкладке, щелкните по соответствующему фрагменту окна на рисунке.



Модуль Родительского контроля

Общие сведения



Данный компонент не устанавливается на ПК, работающий под управлением Microsoft® Windows® 95/98/Me.

Данный компонент не включается в состав **Dr.Web для Windows Server**.

С помощью модуля **Родительского контроля** осуществляется ограничение доступа пользователя к ресурсам, содержащимся как локально, на самом ПК, так и в сети.

Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность важных файлов и защитить их от заражения вирусами, а также сохранит необходимую конфиденциальность данных. Существует возможность защиты, как отдельных файлов, так и папок целиком, расположенных как на локальных дисках, так и на внешних носителях информации. Также можно наложить полный запрет на просмотр информации со всех внешних носителей.

Контроль доступа к интернет-ресурсам позволяет, как оградить пользователя от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т.п.) так и разрешить пользователю доступ только к тем сайтам, которые определены настройками модуля **Родительского контроля**.



Доступ к изменению настроек модуля Родительского контроля защищен паролем.





Настройка параметров модуля

На вкладке **Фильтр URL** осуществляется настройка ограничения доступа к ресурсам сети Интернет. Настройки вкладки **Локальный доступ** позволяют ограничить доступ как к ресурсам файловой системы самого компьютера, так и ресурсам внешних носителей.

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

Для того чтобы изменить настройки программы:

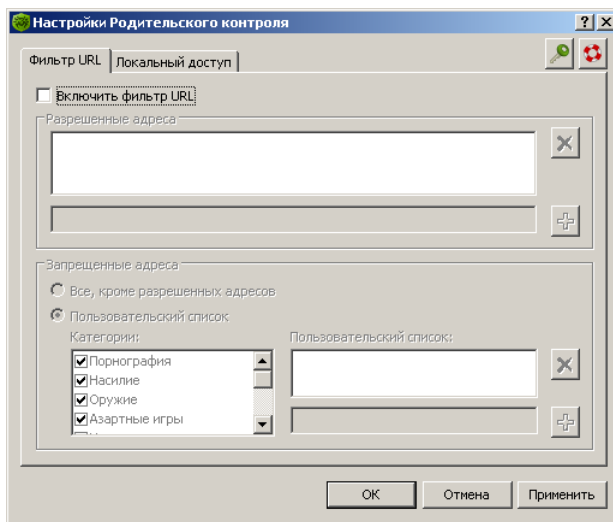
1. Выберите в контекстном меню модуля пункт **Настройки**. Откроется окно задания пароля.
2. Введите ранее сохраненный пароль. Задание пароля производится при вызове настроек параметров модуля в первый раз. Для того чтобы изменить пароль нажмите на кнопку , расположенную в окне настроек.
3. Внесите необходимые изменения на вкладках настроек.
4. Для того чтобы получить информацию о настройках, расположенных на вкладке, нажмите на кнопку .
5. Нажмите на кнопку **Применить** для немедленного сохранения внесенных изменений.
6. По окончании редактирования настроек нажмите на кнопку **ОК**.



Для того чтобы полностью ограничить доступ к сети Интернет установите флажок **Локальная сеть** на вкладке настроек **Локальный доступ**.

Для того чтобы включить контроль доступа к веб-ресурсам:

1. Установите флажок **Включить фильтр URL** на вкладке

настроек **Фильтр URL**.

2. Внесите в список (см. [ниже](#)) **Разрешенные адреса** доменные адреса, доступ к которым разрешен всегда.
3. В группе **Запрещенные адреса** выберите группу адресов, доступ к которым будет заблокирован.
4. Для того чтобы ограничить доступ ко всем веб-ресурсам, кроме тех, что есть в списке **Разрешенные адреса**, выберите **Все, кроме разрешенных адресов**. Для того чтобы включить фильтрацию веб-адресов на основе тематических категорий или/и пользовательского списка выберите **Пользовательский список**.
5. В списке **Категории** выберите категории блокируемых веб-сайтов.
6. В **Пользовательский список** (см. [ниже](#)) добавьте доменные адреса, доступ к которым будет заблокирован.



Списки адресов веб-сайтов, относящихся ко всем тематическим категориям, регулярно обновляются модулем автоматического обновления вместе с обновлением вирусных баз.


Для того чтобы создать список доменных адресов:

- Введите в поле ввода доменное имя (часть доменного имени).


Если вы хотите добавить в список определенный сайт, введите его полный адрес (прим.: www.example.com). Доступ ко всем ресурсам, расположенным на этом сайте будет разрешен/запрещен.

Если вы хотите разрешить/запретить доступ к тем веб-сайтам, в адресе которых содержится определенный текст, введите в поле этот текст. (Прим.: **example**. Доступ к адресам **example.com**, **example.test.com**, **test.com/example**, **test.example222.ru** и т.п. будет заблокирован/разрешен).

В том случае, когда введенная строка содержит символ ".", данная строка будет рассматриваться как имя домена. Тогда все ресурсы, находящиеся на этом домене будут отфильтрованы. Если данная строка содержит и символ "/" (прим.: **example.com/test**), то та часть, что стоит слева от символа, будет считаться доменным именем, а части справа от символа - частью разрешенного/блокируемого на данном домене адреса (т.о. будут отфильтрованы такие адреса как **example.com/test11**, **template.example.com/test22** и т.п.).

- Нажмите на кнопку , расположенную справа. Адрес (часть адреса) будет добавлен в список, расположенный выше.

Введенная строка при добавлении в список может быть преобразована модулем к универсальному виду. (Прим.: <http://www.example.com> будет преобразована в www.example.com).

Для того чтобы удалить какой-либо ресурс из списка, выберите его в этом списке и нажмите на кнопку .



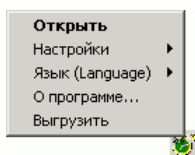
Планировщик для Windows



Данный компонент устанавливается на ПК, работающий под управлением Microsoft® Windows® 95/98/Me. Для управления автоматическим запуском заданий на остальных операционных системах рекомендуется использовать **Планировщик заданий** (штатный планировщик ОС), в котором при установке **Dr.Web** автоматически создаются задания на сканирование ПК и обновление программного комплекса.

В состав **Dr.Web для Windows** по умолчанию включается утилита управления автоматическим запуском заданий – **Планировщик для Windows**. Эта программа является дополнительной, ее функции могут быть исполнены и другими планировщиками заданий, привычными для вас. Однако рассматриваемая программа предназначена для управления именно заданиями на сканирование и обновление антивирусного программного комплекса и предоставляет дополнительные удобства пользователю.

В контекстном меню значка сосредоточены основные средства настройки и управления программы.



При выборе пункта **Открыть** открывается главное окно **Планировщика** (подробнее см. ниже).

Пункт **Язык (Language)** позволяет выбрать один из установленных языков интерфейса программы.

Пункт **Настройки** повторяет одноименный пункт меню главного окна и позволяет выполнить следующие действия:



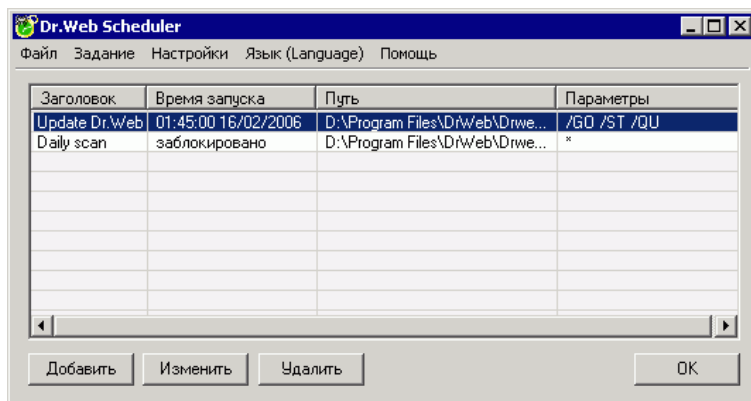
- отменить (восстановить) автозагрузку программы;
- скрыть (показать) значок **Планировщика** в **Панели задач**;
- отменить (разрешить) ведение отчета.

По умолчанию программа постоянно загружена в память и активна. Вы можете выгрузить ее из памяти, выбрав пункт меню **Выгрузить**.

Для того чтобы запустить Планировщик вручную:

1. Выберите в **Главном меню** ОС Windows (меню кнопки **Пуск**) пункт **Программы**.
2. В открывшемся меню выберите папку **Dr.Web**.
3. В открывшемся подменю выберите **Планировщик**.

Функции управления программой сосредоточены в ее главном окне. Для того чтобы открыть главное окно, дважды щелкните по значку программы в **Панели задач** или выберите в контекстном меню значка пункт **Открыть**.



Для того чтобы выгрузить программу из памяти, выберите в меню **Файл** пункт **Выгрузить**.

Для того чтобы отменить (восстановить) автозагрузку программы, в меню **Настройки** удалите (установите) пункт **Автозагрузка**



программы.

Для того чтобы скрыть (показать) значок **Планировщика** в панели задач, снимите (установите) флаг у пункта **Показывать значок Планировщика в области уведомлений** в меню **Настройки**.

Для того чтобы отменить (разрешить) ведение отчета, снимите (установите) флаг у пункта **Вести файл отчета** в меню **Настройки**.

Основные средства работы со списком заданий сосредоточены в меню **Задание**. Они полностью дублируются контекстным меню списка заданий и кнопками в нижней части окна.

По умолчанию программа устанавливается со списком из двух заданий:

- ежечасное получение обновлений из Интернета, в режиме "критично" (подробнее см. ниже),
- ежедневное, в 3 часа, сканирование с параметрами по умолчанию всех жестких дисков.

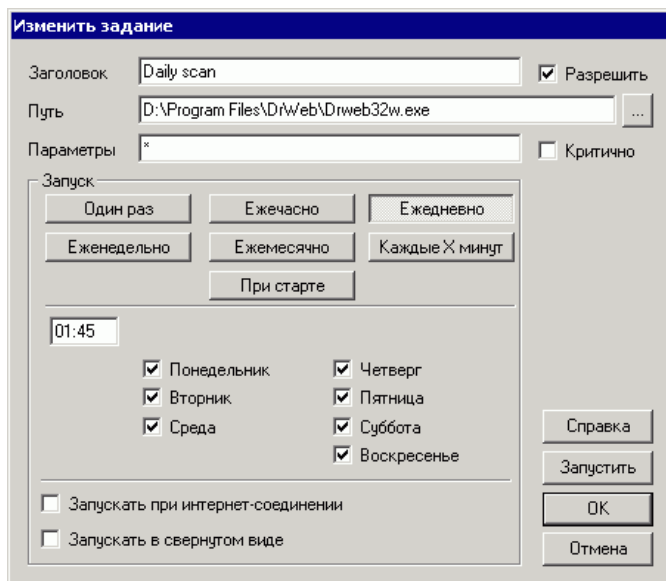
Второе задание имеет статус "заблокировано", запрещающий его фактическое выполнение.

Вы можете разблокировать задание, открыв его для редактирования, как описано ниже.

Для того чтобы просмотреть и при необходимости отредактировать задание:

1. Выполните одно из следующих действий:
 - дважды щелкните по строке задания;
 - выделив задание в списке, выберите в контекстном меню или в меню **Задание** пункт **Изменить**;
 - выделив задание в списке, нажмите на кнопку **Изменить** в нижней части окна.

Откроется окно редактирования задания.



2. Если задание заблокировано, вы можете разблокировать его. Для этого установите флаг **Разрешить**. Параметры задания станут доступными для редактирования.

Если вы не хотите, чтобы задание фактически выполнялось, но не хотите удалять его (например, планируете использовать его позднее), вы аналогично можете заблокировать активное задание.

3. При необходимости отредактируйте расписание запуска (при нажатии различных кнопок в поле **Запуск** вид окна будет меняться).
4. Если хотите, чтобы задание выполнялось только при условии наличия доступа в Интернет, установите флаг **Запускать при интернет-соединении**.
5. Если хотите, чтобы задание, время выполнения которого пропущено, было все же выполнено при первой возможности, установите флаг **Критично**.
6. Если хотите, чтобы приложение по заданию **Планировщика** запускалось в свернутом виде, установите флаг **Запускать в свернутом виде**.



7. Нажмите на кнопку **ОК**.

Для того чтобы запустить задание немедленно, нажмите на кнопку **Запустить**.

Опытные пользователи могут также редактировать параметры и путь запускаемого задания.

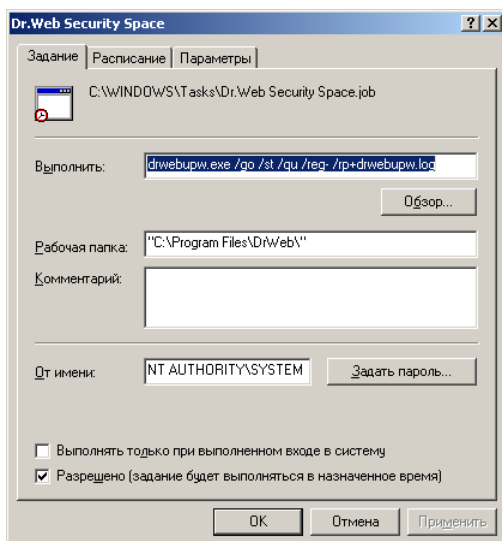
Для того чтобы сформировать новое задание, в контекстном меню или в меню **Задание** выберите пункт **Добавить** или нажмите на кнопку **Добавить** в нижней части главного окна. Откроется окно ввода параметров нового задания, аналогичное рассмотренному выше. Дальнейшие действия аналогичны действиям при редактировании задания.

Задания на сканирование и обновление

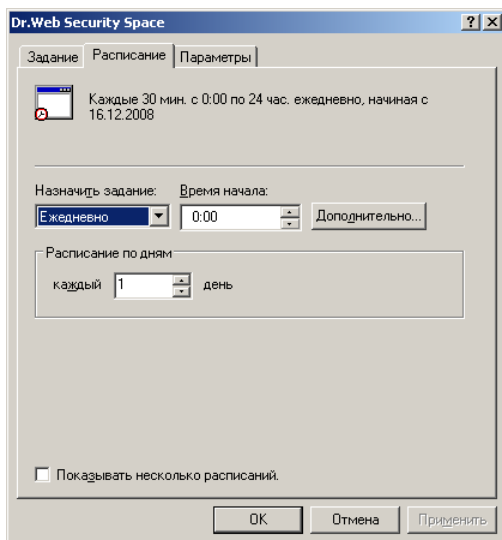
При установке **Dr.Web** на компьютер, работающий под управлением Microsoft® Windows® NT(SP6a)/2000(SP4)/XP/2003/Vista/2008 в системном расписании (папка **Назначенные задания**) автоматически создается задание на обновление вирусных баз и других файлов пакета.

Для того чтобы просмотреть параметры этого задания, укажите в меню **Программы** на пункт **Стандартные**, далее выберите **Служебные**, далее выберите **Назначенные задания**. Откроется папка **Назначенные задания**. В этой папке дважды щелкните по значку **Automatic update of DrWeb**. Откроется окно настройки задания.

На вкладке **Задание** указывается полное имя исполняемого файла и параметры командной строки задания. Флаг Разрешено предписывает выполнять настроенное задание (при снятом флаге задание сохраняется в папке, но не выполняется).

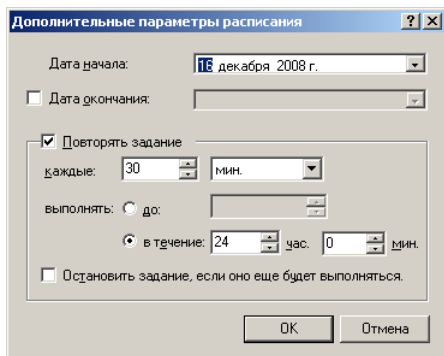


На вкладке **Расписание** задается расписание, в соответствии с которым задание будет автоматически запускаться.





Нажмите на кнопку **Дополнительно**. Откроется окно **Дополнительные параметры расписания**.



Вы также можете создавать собственные задания на обновление и антивирусное сканирование, а также удалять и редактировать задания. Подробнее о работе с системным расписанием см. справочную систему и документацию ОС 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 антивирусного комплекса непрерывно пополняют вирусные базы новыми вирусными записями. После установки таких дополнений антивирусный комплекс 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 комплекса. 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 комплекса в целом:

- в состав программного комплекса входит основная вирусная база (файл `drwebase.vdb`) и ее расширения (файлы `drw50000.vdb` и `drw50001.vdb`). Все вместе они содержат вирусные записи, известные в момент выпуска данной версии программного комплекса (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: `drwXXXXYY.vdb`, где `XXX` – номер текущей версии антивируса (без разделительной точки), а `YY` – порядковый номер еженедельного дополнения. Нумерация еженедельных дополнений начинается с номера 02, т.е. первое дополнение баз антивируса версии 5.0 названо `drw50002.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`. При получении очередного такого файла предыдущий файл уничтожается. При установке очередного еженедельного дополнения в него включаются, в частности, все вирусные записи из последнего файла горячего дополнения, файл горячего дополнения загружается с нулевым числом вирусных записей;
- в состав программного комплекса 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;
- также время от времени выпускаются файлы, содержащие обновленные списки веб-сайтов, блокируемых модулем Родительского контроля;
- 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, например, после установки версии с номером 5.0 и получения нескольких еженедельных обновлений структура вирусных баз будет следующей:

- основная вирусная база `drwebase.vdb`,
- расширения основной вирусной базы `drw50000.vdb` и `drw50001.vdb`,
- еженедельные дополнения (`drw50002.vdb`, `drw50003.vdb` и т. д.),
- горячее дополнение `drwtoday.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.

При работе с ОС Windows NT, ОС Windows 2000, ОС Windows XP, ОС Windows Vista обновление **Dr.Web** должно производиться при наличии у пользователя полномочий администратора.

Запуск модуля автоматического обновления

Модуль автоматического обновления можно запустить одним из следующих способов:

1. автоматически, по расписанию (см. п. [Автоматическое сканирование и обновление](#)),
2. в режиме командной строки вызовом исполняемого файла `drwebupw.exe` из каталога установки программы,
3. выбором пункта **Обновление** контекстного меню значка **SpIDer Agent**;
4. нажатием на кнопку **Обновить** раскрывающегося меню **Файл** в главном окне сканера;

При запуске модуля обновления программа проверяет наличие лицензионного ключевого файла в каталоге установки и при его отсутствии пытается получить его через Интернет на сервере www.drweb.com (это действие рассмотрено в конце п. [Получение ключевого файла](#)). При отсутствии ключевого файла автоматическое 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 программного комплекса могут быть заблокированы;



пользователю выдается соответствующее сообщение.

В случае блокировки вашего ключевого файла свяжитесь с дилером, у которого вы приобрели антивирус.

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



При обновлении исполняемых файлов и библиотек может потребоваться перезагрузка ПК, о чем пользователю сообщается в соответствующем информационном окне. Если изменения затрагивают сам модуль автоматического обновления, дополнительно может потребоваться еще одна перезагрузка в ходе обновления.

Сканер может использовать обновленные базы при следующем после обновления запуске. **Сторож** и **Почтовый сторож** периодически проверяют состояние баз и загружают обновленные базы автоматически.

При запуске модуля автоматического обновления **Планировщиком** или в режиме командной строки используются параметры командной строки (см. [Приложение В](#)).



Приложения

Приложение А. Различия между Dr.Web для Windows и Dr.Web для Windows Server

Состав компонентов и установка

В состав Dr.Web для серверов не включаются следующие компоненты:

- Сканер для DOS,
- почтовый сторож SpIDer Mail,
- Планировщик для Windows.

Программа установки **Dr.Web для серверов** при режиме установки с выбором компонентов (выборочная установка) не предлагает данные компоненты.

Настройки по умолчанию

Отличия настроек по умолчанию двух версий антивирусного комплекса связаны с предполагаемым режимом использования программы: версия для серверов должна работать в автоматическом режиме с периодическим контролем файлов отчета, версия для рабочих станций управляется пользователем. В табл. 2 сведены настройки по умолчанию, различающиеся для двух версий антивируса. В первой колонке приводится наименование параметра с указанием компонента и наименование параметра конфигурационного файла, во второй колонке – значение параметра по умолчанию при использовании антивируса для рабочих станций (словесное описание и значение параметра в конфигурационном файле), в третьей – те же сведения в случае использования антивируса для серверов.

**Таблица 2. Настройки по умолчанию двух версий антивирусного комплекса**

Параметр	Версия для рабочих станций	Версия для серверов
Сканер: действия с зараженными файлами InfectedFiles	Информировать Report	Лечить Cure
Сканер: действия с подозрительными файлами SuspiciousFiles	Информировать Report	Перемещать Move
Сканер: действия с неизлечимыми файлами IncurableFiles	Информировать Report	Перемещать Move
Сторож: действия с зараженными файлами InfectedFiles	Информировать Report	Лечить Cure
Сторож: действия с подозрительными файлами SuspiciousFiles	Информировать Report	Перемещать Move
Сторож: действия с неизлечимыми файлами IncurableFiles	Информировать Report	Перемещать Move
Сканер и сторож: действия с инфицированными архивами ActionInfectedArchive	Информировать Report	Перемещать Move
Сканер и сторож: действия с инфицированными почтовыми файлами ActionInfectedMail	Информировать Report	Перемещать Move
Сканер и сторож: записывать в отчет список просмотренных (неинфицированных) объектов LogScanned	Нет No	Да Yes
Размер файла отчета, Кбайт MaxLogSize	512	8192



Приложение В. 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 Сканеров

- /? – вывести на экран краткую справку о работе с программой.
- /@ <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, созданных архиваторами 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](#)).
- /FN – загружать русские буквы в знакогенератор видеоадаптера (только для **Dr.Web для DOS**).
- /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) ключ задает информирование пользователя в случае обнаружения зараженного или подозрительного объекта в почтовом архиве. Если ключ 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, ключ 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) ключ задает информирование пользователя. Если ключ 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 ОС Windows, только для **Сканеров для Windows**).
- /TS – выполнять поиск вирусов в файлах автозапуска (по папке Автозагрузка, системным .ini файлам, реестру ОС Windows). Используется только для **Сканеров для 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 3](#).

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 /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 командной строки для модуля автоматического обновления

При запуске модуля автоматического обновления из **Планировщика** 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 прокси-сервера.
- /PUSER: *<имя пользователя прокси>* – имя пользователя прокси-сервера.
- /PURL: *<адрес прокси>* – адрес прокси-сервера.
- /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).
- /REG – запуск модуля обновления в режиме регистрации и получения регистрационного ключа.
- /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.
- /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 прокси-сервера; 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; применяется в паре с ключом /REG: в режиме регистрации дополнительно запустить и собственно сеанс обновления.
- /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 3](#).

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:

- 0 – ОК, 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 С. Настраиваемые параметры компонентов Dr.Web

Настраиваемые параметры компонентов программного комплекса 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, сторожа, почтового сторожа**). Наиболее важные из таких настроек были приведены выше (см. пп. 3.2.3, 3.4.3 и 3.5.3);
- заданием параметров командной строки при вызове программ из режима командной строки или по расписанию (для **Сканера** различных версий). Подробнее об этой возможности см. [Приложение В](#).
- 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 антивирусного программного комплекса может снизить качество защиты и даже привести к полной неработоспособности некоторых программ.

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



Параметры Windows-версий Сканера, сторожа, Планировщика и модуля автоматического обновления

В колонках [таблицы 3](#) 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).

Следующие наименования компонентов, используемые в таблице, требуют пояснения:

- "**Сторож**" – обе версии **SpIDer Guard** ("**Сторож-XP**" и "**Сторож-Me**"),
- "**Сканер**" – 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**, **Планировщика** и модуля автоматического обновления выделены полужирным шрифтом, для сторожа – курсивом, для всех компонентов – полужирным курсивом.

Значения по умолчанию для Сканера и сторожа, включенных в состав **Dr.Web для серверов Windows**, в тех случаях, когда они отличаются от значений по умолчанию параметров антивируса



для рабочих станций, подчеркиваются.

Ключи командной строки, соответствующие данному параметру, описываются сокращенно, без большинства модификаторов. Более подробная информация о ключах приведена в [Приложении В](#).

Таблица 3. Настраиваемые параметры Windows-версий Сканера, сторожа и модуля автоматического обновления

Наименование параметра	КомпONENTЫ	Параметр конф. файла	Значения	Ключи
Режим проверки "на лету"	Сторож	GuardMode	Smart RunAnd Open CreateA ndWrite оба последн их	
Режим проверки	Сканер, Сторож	ScanFiles	All ByType ByMasks	/AL /EX
Быстрая проверка системы	Сканер			/FA ST
Полная проверка системы	Сканер			/FU LL
Приоритет выполнения сканирования, от 1 до 50	Сканер			/SC P
Эвристический анализ	Сканер, Сторож	HeuristicAnalysis	Yes / No	/HA
Контроль вирусной активности	Сторож-М е	VirusActivity Control	Yes / No	
Проверка загрузочной дискеты	Сторож	ScanBootOn ShutDown	Yes / No	
Защита системного ядра	Сторож-М е	DisableIDTh ook	Yes / No	



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Запретить работу с сетью	Сторож-Ме	DisableNetworkScan	Yes / No	
Не сканировать объекты в локальной сети	Сторож-XP		(Вкл./Выкл.)	
Не сканировать объекты на съемных носителях	Сторож-XP		(Вкл./Выкл.)	
Проверять память	Сканер, Сторож	TestMemory	Yes / No	/TM
Проверять файлы автозагрузки	Сканер, Сторож	TestStartup	Yes / No	/TS
Проверять загрузочные секторы	Сканер, Сторож-Ме	TestBootSectors	Yes / No	/TB
Проверять подкаталоги	Сканер	ScanSubDirectories	Yes / No	/SD
Проверка нескольких дискет	Сканер	PromptFloppy	Yes / No	/PF
Файлы в архивах	Сканер, Сторож	CheckArchives	Yes / No	/AR
Упакованные файлы	Сторож	CheckPackagedFiles	Yes / No	
Почтовые файлы	Сканер, Сторож	CheckEmailFiles	Yes / No	/ML
Макс. длина распакованного из архива файла, подлежащего проверке, Кбайт	Сторож-XP, Сканер-консольный	MaxFileSizeToExtract	(не задано)	
Макс. коэффициент сжатия файла в архиве	Сторож-XP, Сканер-консольный	MaxCompressionRatio	(не задано)	



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Нижний порог срабатывания параметра MaxCompressionRatio, Кбайт	Сторож-XP, Сканер-консольный	CompressionCheckThreshold	(не задано)	
Список расширений	Сканер, Сторож	FileTypes	(см. после табл.)	
Список масок	Сканер, Сторож	UserMasks	(см. после табл.)	
Список исключаемых путей	Сканер, Сторож	ExcludePaths	(пусто)	
Список исключаемых файлов	Сканер, Сторож-Me	ExcludeFiles	(пусто)	
Разрешить использование масок	Сторож-XP	AllowWildcards	Yes / No	
Разрешить исключение файлов без указания пути	Сторож-XP	AllowRelativeFileNames	Yes / No	
Проверять жесткие диски (при сканировании с параметром командной строки * и при нажатии на кнопку Выделить диски)	Сканер	ScanHDD	Yes / No	
Проверять дискеты (при сканировании с параметром командной строки * и при нажатии на кнопку Выделить диски)	Сканер	ScanFDD	Yes / No	
Проверять компакт-диски (при сканировании с параметром командной строки * и при нажатии на кнопку Выделить диски)	Сканер	ScanCD	Yes / No	



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Проверять сетевые диски (при сканировании с параметром командной строки * и при нажатии на кнопку Выделить диски)	Сканер	ScanNet	Yes / No	
Запрос подтверждения	Сканер, Сторож-М е	PromptOnAction	Yes / No	/PR
Переименовать расширение	Сканер, Сторож	RenameFilesTo	#??	
Имя каталога карантина	Сканер, Сторож	MoveFilesTo	infected.!!!	
Список путей к вирусным базам	Сканер, Сторож	VirusBase	*.vdb	
Флаг-файл для перезагрузки вирусных баз	Сторож	UpdateFlags	<i>drwtoday.vdb</i>	
Выдавать всплывающее окно-уведомление	Сторож-XP	Acknowledge	Yes / No	
Путь к каталогу временных файлов компонента	Сканер, Сторож	TempPath	%TMP %, %TEMP R%, каталог установки	
Разрешить отключение сторожа	Сторож	EnableSwitch	Yes / No	
Режим загрузки сторожа XP-версии	Сторож-XP		Ручной режим <i>Автоматич. режим</i>	



Наименование параметра	Компоне нты	Параметр конф. файла	Значен ия	Кл юч и
Сохранять состояние "Мониторинг отключен" после перезагрузки	Сторож-XP		(Вкл./ Выкл.)	
Защищать файл конфигурации Dr.Web	Сторож-XP		(Вкл./ Выкл.)	
Запретить режим расширенной защиты	Сторож-XP	DisableEnhancedProtection	Yes / No	
Размер списка проверенных файлов	Сторож-XP		100	
Действия со всеми видами нежелательных программ	Сканер		Информировать	/M W
Инфицированные объекты	Сканер, Сторож	InfectedFiles	Report Cure Delete Rename Move Lock (сторож) Shutdown (сторож)	/CU
Неизлечимые объекты	Сканер, Сторож	IncurableFiles	Report Delete Rename Move Lock (сторож) Shutdown (сторож)	/IC



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Подозрительные объекты	Сканер, Сторож	SuspiciousFiles	Report Delete Rename <u>Move</u> Lock (сторож) Ignore (сторож) Shutdown (сторож)	/SP
Инфицированные архивы	Сканер, Сторож	ActionInfectedArchive	Report Delete Rename <u>Move</u> Lock (сторож) Ignore (сторож) Shutdown (сторож)	/AR



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Инфицированные почтовые файлы	Сканер, Сторож	ActionInfectedMail	Report Delete Rename Move Lock (сторож)) Ignore (сторож)) Shutdown (сторож))	/ML
Рекламные программы	Сканер, Сторож	ActionAdware	Report Delete Rename Move Ignore Lock (сторож)) Shutdown (сторож))	/AD W
Программы дозвона	Сканер, Сторож	ActionDialers	Report Delete Rename Move Ignore Lock (сторож)) Shutdown (сторож))	/DL S



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Программы-шутки	Сканер, Сторож	ActionJokes	Report Delete Rename Move Ignore Lock (сторож)) Shutdown (сторож))	/JOK
Потенциально опасные программы	Сканер, Сторож	ActionRiskware	Report Delete Rename Move Ignore Lock (сторож)) Shutdown (сторож))	/RSK
Программы взлома	Сканер, Сторож	ActionHacksols	Report Delete Rename Move Ignore Lock (сторож)) Shutdown (сторож))	/HCK



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Что делать, если не удалось переименование	Сторож-XP	ActionIfRenameFailed	Report <i>Delete</i> Rename Move <i>Lock</i> Shutdown	
Что делать, если не удалось перемещение	Сторож-XP	ActionIfMoveFailed	Report Delete <i>Rename</i> Move Lock Shutdown	
Что делать, если не удалось удаление	Сторож-XP	ActionIfDeleteFailed	Report Delete Rename Move <i>Lock</i> Shutdown	
Что делать, если не удалось информирование	Сторож-XP	ActionIfReportFailed	Report Delete Rename Move <i>Lock</i> Shutdown	
Разрешить удаление архивов без запроса предупреждения	Сканер, Сторож	EnableDeleteArchiveAction	Yes / No	
Обнаружен инфицированный объект (посылать уведомление)	Сторож-XP		(Вкл./ <i>Выкл.</i>)	
Обнаружен неизлечимый объект (посылать уведомление)	Сторож-XP		(Вкл./ <i>Выкл.</i>)	



Наименование параметра	КомпONENTЫ	Параметр конф. файла	Значения	Ключи
Обнаружен подозрительный объект (посылать уведомление)	Сторож-XP		(Вкл./ <i>Выкл.</i>)	
Уведомления по E-mail о вирусных событиях	Сторож-XP		(Вкл./ <i>Выкл.</i>)	
Уведомления в сети о вирусных событиях	Сторож-XP		(Вкл./ <i>Выкл.</i>)	
Вести файл отчета	Сканер, Сторож, модуль обновления	LogToFile	Yes / No	/RP /NR
Вести файл отчета	Планировщик		(Вкл. ./ <i>Выкл.</i>)	
Имя файла отчета	Сканер Сторож-М е Сторож-XP	LogFileName	drweb3 2w.log <i>spider.log</i> <i>spidernt.log</i>	/RP
Имя файла отчета	Модуль обновления		drwebu pw.log	/RP
Имя файла отчета	Планировщик		drwebs cd.log	
Режим открытия отчета	Сканер, Сторож, модуль обновления	OverwriteLog	Yes / No	/RP
Кодировка отчета	Сканер, Сторож, модуль обновления	LogFormat	ANSI OEM	



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Проверяемые объекты в отчете	Сканер, Сторож	LogScanned	<u>Yes</u> / No	/OK
Имена упаковщиков в отчете	Сканер, Сторож	LogPacked	Yes / <u>No</u>	
Имена архиваторов в отчете	Сканер, Сторож	LogArchived	Yes / <u>No</u>	
Статистика в отчете	Сканер, Сторож	LogStatistics	<u>Yes</u> / No	
Предельный размер файла отчета	Сканер, Сторож, модуль обновления	LimitLog	Yes / <u>No</u>	
Предельный размер файла отчета, Кбайт	Сканер, Сторож, модуль обновления	MaxLogSize	512 <u>8192</u>	
Закрывать окно после сеанса	Сканер, модуль обновления		Yes / <u>No</u>	/QU
Ожидать нажатия на клавишу (после завершения сканирования в случае обнаружения вирусов)	Сканер-копировальный	WaitAfterScan	(Вкл./ Выкл.)	/WA
Исполнять в пакетном режиме	Сканер, модуль обновления		(Вкл./ Выкл.)	/GO
Запретить прерывание пользователем	Сканер		(Вкл./ Выкл.)	/NS
Проверять один раз в сутки	Сканер		(Вкл./ Выкл.)	/DA



Наименование параметра	КомпONENTЫ	Параметр конф. файла	Значения	Ключи
Проверять только явно заданные объекты	Сканер-G UI		(Вкл./ Выкл.)	/SHELL
Не открывать окон (режим stealth)	Сканер-G UI		(Вкл./ Выкл.)	/STEALTH
Использовать альтернативный конфиг. файл. Не использовать никакого конфиг. файла	Сканер, модуль обновления		(Вкл./ Выкл.)	/INI /NOINI
Использовать собственный файл подкачки	Сканер, Сторож	UseDiskForSwap	Yes / No	
Отображать индикатор работы (прогресс-индикатор)	Сканер	ShowProgressBar	Yes / No	
Звуки	Сканер, Сторож, модуль обновления	PlaySounds	Yes / No	/SOUNDS
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	
Конец проверки (звук)	Сканер	FinishWav	finish.wav	
Ошибка (звук)	Сканер, модуль обновления	ErrorWav	error.wav	



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Автосохранение настроек при выходе	Сканер	AutoSaveSettings	Yes / No	/SS
Запретить изменение настроек без перезагрузки	Сторож-Me	DisableHotReconfigure	Yes / <i>No</i>	
Отображать значок Spider Guard в области уведомлений	Сторож-XP		(Вкл /Выкл.)	
Показывать значок Планировщика в области уведомлений	Планировщик		(Вкл /Выкл.)	
Использовать настройки из реестра	Сканер-GUI		(Вкл /Выкл.)	
Приоритет проверки	Сканер	ScanPriority	25 50	
Язык (Language)	Сканер, Сторож, модуль обновления	LngFileName	ru-drw eb.dwl	/LNG
Режим прокси	Сканер-GUI (настроек и модуля обновления)	UpdateProxy Mode	direct ieproxu userproxu	/UPM
Обновлять только вирусные базы и ядро <i>drweb32.dll</i>	модуль обновления	UpdateVirus BasesOnly	Yes / No	/UVB
Загрузка всех файлов, заявленных в списке обновления	модуль обновления	UpdateAllFiles	Yes / No	/UA



Наименование параметра	Компоненты	Параметр конф. файла	Значения	Ключи
Режим перезагрузки при обновлении	модуль обновления	UpdateRebootMode	prompt noprompt force disable	/UR M
Вести подробный отчет	модуль обновления		(Вкл./ Выкл.)	/DB G

Список расширений файлов (значение параметра `FileTypes` 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").

Параметры SpIDer Mail для рабочих станций Windows

Параметры **SpIDer Mail для рабочих станций Windows** описываются в отдельной таблице 4. Таблица оформлена по принципам, аналогичным принципам оформления [таблицы 3](#). В списке допустимых значений параметра значения по умолчанию для почтового сторожа выделены курсивом.



Таблица 4. Настраиваемые параметры почтового сторожа

Наименование параметра	Параметр конф. файла	Значения	Ключ
Использовать альтернативный конфигурационный файл		(Вкл./Выкл.)	-ini:имя_файла
Использовать альтернативный файл пользовательского ключа		(Вкл./Выкл.)	-key:имя_файла
Язык (Language)	LngFileName	<i>ru-drweb.dwl</i>	-lng:имя_файла
Эвристический анализатор	HeuristicAnalysis	Yes / No	
Проверять файлы в архивах	CheckArchives	Yes / No	
Контроль вирусной активности	VirusActivityControl	Yes / No	
Таймаут проверки письма, с	ScanTimeout	250	
Макс. длина файла при распаковке, Кбайт	MaxFileSizeToExtract	30720	
Макс. коэффициент сжатия архива	MaxCompressionRatio	<i>Infinite</i>	
Макс. уровень вложенности в архив	MaxArchiveLevel	64	
Предупреждение о вирусах в исход. почте	ShowAlerts	Yes / No	
Инфицированные письма	ActionInfected	<i>Delete Move</i>	
Подозрительные письма	ActionSuspicious	<i>Delete Move Skip</i>	
Непроверенные письма	ActionNotChecked	<i>Delete Move Skip</i>	



Наименование параметра	Параметр конф. файла	Значения	Ключ
Удалять модифицированные письма на сервере	DeleteMessagesOnServer	Yes / No	
Вставка заголовка 'X-AntiVirus' в сообщения	InsertXAntiVirus	Yes / No	
Папка для карантина	PathForMovedFiles	<i>infected.!!!</i>	
Путь к поисковому модулю	EnginePath	<i>(пусто)</i>	
Путь к вирусным базам	VirusBasesPath	<i>(пусто)</i>	
Флаг-файл для обновлений	UpdateFlag	<i>drwtoday.vdb</i>	
Период проверки флаг-файла, с	UpdatePeriod	300	
Всего поисковых модулей	MaximumLoadEngines	10	
Поисковых модулей при старте	PreloadEngines	1	
Выгружать свободные модули через, с	UnusedEngineUnloadTimeout	420	
Вести отчет	EnableLog	Yes / No	
Отчет о проверяемых объектах	EnableLogScanInfo	Yes / No	
Файл отчета	LogFileName	spiderml.log	
Предельный размер файла отчета, Кбайт	MaximumLogSize	500	
Разрешить анимацию иконки	EnableIconAnimation	Yes / No	
Разрешить иконку в трее	HideIcon	Yes / No	



Наименование параметра	Параметр конф. файла	Значения	Ключ
Показывать уведомления	NoBalloons	Yes / No	
Переключатель Перехватывать соединения автоматически или Ручная настройка соединений	HookModeAuto	Yes / No	
Проверять перехват соединений при старте (авт. режим)	HookCheck	Yes / No	
Адрес-Порт (первый элемент списка, авт. Режим)	Hook1	*:143 адрес:порт	
Адрес-Порт (продолжение списка, авт. Режим)	Hook2 Hook3 ...	адрес:порт адрес:порт ...	
Порт SpIDerMail- Адрес сервера-Порт сервера (ручной режим, первый элемент списка)	HookManual1	7000->адрес POP3/SMTP/I MAP4/NNTP: порт	
Порт SpIDerMail- Адрес сервера-Порт сервера (ручной режим, продолжение списка)	HookManual2 HookManual3 ...	7001->адрес POP3/SMTP/I MAP4/NNTP: порт 7002->адрес POP3/SMTP/I MAP4/NNTP: порт ...	
Разрешить пункт меню Выключить	AllowDisable	Yes / No	
Разрешить пункт меню Выход	AllowExit	Yes / No	
Разрешить пункт меню Настройки	AllowSettings	Yes / No	
Разрешить пункт меню Переинициализация	AllowReinitialize	Yes / No	



Наименование параметра	Параметр конф. файла	Значения	Ключ
Максимальное количество одновременно обрабатываемых запросов на один лок. порт (ручной режим)	MaximumChild Connections	20	
Добавляемая в сообщение строка	Xbanner	<i>(пусто)</i>	
Путь к каталогу временных файлов компонента	TempPath	<i>%TMP%, %TEMP%, каталог установки</i>	
Переинициализация			-reinit
Выключить			-disable
Включить			-enable
Обновить			-update
Выход			-exit



Приложение D. 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 **ООО «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 измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишется 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 (тройанские 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 закладываются 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 интернет-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 отправке 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 производится 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 **ООО «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 **ООО «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 **ООО «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 Е. Принципы именования вирусов

При обнаружении вирусного кода компоненты антивирусного комплекса **Dr.Web** сообщают пользователю средствами интерфейса и заносят в файл отчета имя вируса, присвоенное ему специалистами **ООО "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://support.drweb.com/faq/>.

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 называвания 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,
- HLLQ – 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 Relay 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 именованя 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 F. Защита корпоративной сети с помощью **Dr.Web® Enterprise Suite**

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

Версии комплекса, предназначенные для рабочих станций и для серверов ОС 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 антивирусных комплексов, 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.

Специально для решения указанных задач разработан программный комплекс **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.

Программный комплекс **Dr.Web ES** имеет архитектуру "клиент-сервер". Его компоненты устанавливаются на компьютеры локальной сети и обмениваются информацией, используя сетевые протоколы (подробнее взаимодействие компонентов комплекса 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 ОС 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.* Этот компонент используется для удаленного управления антивирусной сетью путем редактирования настроек антивирусного сервера, а также настроек защищаемых компьютеров, хранящихся на антивирусном сервере.



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 программный комплекс **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 ОС Windows 2000, ОС Windows XP, ОС Windows 2003, ОС 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 антивирусных комплексов.

Программный комплекс **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 G. Dr.Web® AV-Desk для провайдеров интернет-услуг.

Программный комплекс **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 для Windows** 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 антивирусных комплексов, 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 комплекса 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.

Программный комплекс **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 ОС 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.
- *Антивирусная консоль.* Этот компонент используется для удаленного управления антивирусной сетью путем редактирования настроек антивирусного сервера, а также настроек защищаемых компьютеров, хранящихся на антивирусном сервере и на защищаемых компьютерах.
- *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 отправляет 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 антивирусных комплексов.

Программный комплекс **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.

