Dr.WEB®

Антивирус
для Windows

Защити созданное

Руководство пользователя

Антивирус Dr.Web для Windows
Версия 7.0
Руководство пользователя
27.04.2012

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

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

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение 7

1.1. О чем эта документация 9

1.2. Используемые обозначения и сокращения 10

1.3. Системные требования 11

1.4. Лицензирование 13

1.4.1. Ключевой файл 13

1.4.2. Получение ключевого файла 15

1.4.3. Продление лицензии 17

1.5. Методы обнаружения 19

1.6. Проверка антивируса 21

2. Установка программы 22

2.1. Первая установка 22

2.2. Повторная установка и удаление 35

2.3. Процедура получения ключевого файла 37

3. Приступая к работе 40

3.1. Модуль управления SpIDer Agent 43

3.2. Общие настройки 45

3.3. Менеджер лицензий 50

3.4. Менеджер Карантина 52

3.5. Антивирусная сеть 56

4. Сканер Dr.Web 57

4.1. Проверка компьютера 58

4.2. Действия при обнаружении вирусов 62

4.3. Настройка Сканера 64
4.4. Запуск Сканера из командной строки 68
4.5. Консольный сканер 69
5. SpIDer Guard 71
5.1. Управление SpIDer Guard 72
5.2. Настройка SpIDer Guard 74
6. SpIDer Mail 80
6.1. Управление SpIDer Mail 83
6.2. Настройка SpIDer Mail 84
7. Dr.Web для Outlook 92
7.1. Настройка Dr.Web для Outlook 92
7.2. Обнаружение угроз 94
7.2.1. Вредоносные объекты 94
7.2.2. Действия 95
7.4. Регистрация событий 97
7.4.1. Журнал операционной системы 98
7.4.2. Текстовый журнал отладки 99
7.5. Статистика проверки 100
8. Брандмауэр Dr.Web 102
8.1. Обучение Брандмауэра 102
8.2. Управление Брандмауэром 109
8.3. Настройка Брандмауэра 111
8.3.1. Фильтр приложений 112
8.3.2. Родительские процессы 119
8.3.3. Интерфейсы 120
8.3.4. Дополнительные настройки 130

8.3.5. Восстановление исходных настроек 134
8.4. Регистрация событий 135
8.4.1. Активные приложения 136
8.4.2. Журнал приложений 138
8.4.3. Журнал пакетного фильтра 140
9. Автоматическое обновление 142
9.1. Запуск обновления 142
Приложения 145
Приложение А. Дополнительные параметры командной строки 145
Параметры для Консольного сканера 145
Параметры для Модуля обновления 152
Коды возврата 158
Приложение Б. Угрозы и способы их обезвреживания 159
Классификация угроз 160
Действия для обезвреживания угроз 166
Приложение В. Принципы именования угроз 168
Приложение Г. Централизованная антивирусная защита 174
Приложение Д. Техническая поддержка 176

1. Введение

Антивирус Dr.Web для Windows обеспечивает многоуровневую защиту системной памяти, жестких дисков и сменных носителей от проникновений вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и различных вредоносных объектов из любых внешних источников.

Важной особенностью программы **Антивирус Dr.Web** является модульная архитектура. **Антивирус Dr.Web** использует программное ядро и вирусные базы, общие для всех компонентов и различных сред. В настоящее время наряду с программой **Антивирус Dr.Web** поставляются версии антивируса для IBM® OS/2®, Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Andorid®, Symbian®, а также ряда систем семейства Unix® (например, Linux®, FreeBSD® и Solaris®).

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

Антивирус 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 **Антивирус Dr.Web**.

Антивирус Dr.Web может включать в себя следующие компоненты:

- **Сканер Dr.Web** – антивирусный сканер с графическим интерфейсом, который запускается по запросу пользователя или по расписанию и проводит антивирусную проверку компьютера. Существует также версия программы с интерфейсом командной строки (**Консольный сканер для Windows**);
- **SpIDer Guard®** – антивирусный сторож, который

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

- **SpIDer Mail®** – почтовый антивирусный сторож, который 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;
- **Dr.Web для Outlook** – подключаемый модуль, который проверяет почтовые ящики Microsoft Outlook на вирусы;
- **Брандмауэр Dr.Web** – персональный межсетевой экран, предназначенный для защиты компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети;
- **Модуль обновления Dr.Web** – компонент, который позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов **Dr.Web**, а также производит их автоматическую установку;
- **SpIDer Agent** – модуль управления, с помощью которого осуществляется запуск и настройка компонентов программы **Антивирус Dr.Web**.

1.1. О чем эта документация

Настоящее руководство содержит необходимые сведения по установке и эффективному использованию программы **Антивирус Dr.Web**.

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

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

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

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

1.2. Используемые обозначения и сокращения

В данном руководстве используются обозначения, приведенные в таблице 1.

Таблица 1. Обозначения

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

1.3. Системные требования

Перед установкой программы **Антивирус Dr.Web** следует:

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

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

Компонент	Требование
Операционная система	Одна из следующих: • Microsoft® Windows® 2000 Workstation с пакетом обновлений SP4 и Update Rollup 1; • Windows® XP с пакетом обновлений SP2; • Windows® Vista; • Microsoft® Windows® 7. Поддерживаются 32- и 64-битные версии операционных систем. Возможно, потребуется загрузить с сайта Microsoft и установить обновления ряда системных компонентов. **Антивирус Dr.Web** сообщит вам, при необходимости, их наименования и URL.
Место на жестком диске	330 МБ для размещения компонентов продукта. Файлы, создаваемые в ходе установки, потребуют дополнительного места.
Процессор	Полная поддержка системы команд i686.

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

1.4. Лицензирование

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

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

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

1.4.1. Ключевой файл

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

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

Существует три типа ключевых файлов:

- *лицензионный ключевой файл*, который приобретается вместе с программой **Антивирус Dr.Web** и позволяет как пользоваться продуктом, так и получать техническую поддержку. Параметры этого ключевого файла, регулирующие права пользователя, установлены в соответствии с пользовательским договором. В такой файл также заносится информация о пользователе и продавце продукта;
- *демонстрационный ключевой файл*, который используется для ознакомления с продуктом. Такой ключевой файл обеспечивает полную функциональность основных

компонентов, но имеет ограниченный срок действия — 30 дней;

Демонстрационный ключ выдается на одну и ту же машину не чаще чем 1 раз в 4 месяца.

- *временный ключевой файл*, который используется в том случае, если при установке вы не указываете лицензионный или демонстрационный ключевой файл. Такой ключевой файл обеспечивает полную функциональность компонентов программы **Антивирус Dr.Web**, однако обновления не будут загружаться до тех пор, пока вы не установите лицензионный или демонстрационный ключевой файл. Также в меню SpIDer Agent будут отсутствовать пункты **Мой Dr.Web** и **Обновление**.

Ключевой файл **Dr.Web** является *действительным* при одновременном выполнении следующих условий:

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

При нарушении любого из условий ключевой файл становится *недействительным*, при этом **Антивирус Dr.Web** перестает обнаруживать и обезвреживать вредоносные программы.

1.4.2. Получение ключевого файла

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

Вы можете получить ключевой лицензионный файл одним из следующих способов:

- в процессе регистрации продукта на официальном сайте **«Доктор Веб»**;
- в процессе установки продукта или его первого обновления;
- вместе с дистрибутивом продукта, если лицензионный файл был включен в комплект поставки;
- на отдельном носителе.

Ключевые файлы, полученные в процессе установки или в комплекте дистрибутива, устанавливаются автоматически. Ключевые файлы, полученные другим путем, необходимо установить.

Получение ключевого файла в процессе регистрации на сайте

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

Для получения лицензионного ключевого файла необходим регистрационный серийный номер продукта. Во время данной процедуры получение демонстрационного файла невозможно.

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.
2. Заполните форму со сведениями о покупателе.
3. Введите регистрационный серийный номер (находится на регистрационной карточке).

4. Сформированный ключевой файл высылается по электронной почте в виде ZIP-архива, содержащего файл с расширением .key. Также вы можете загрузить архив со страницы регистрации.
5. После получения ключевого файла установите его на вашем компьютере.

Получение ключевого файла в процессе установки программы Антивирус Dr.Web

Регистрация на сайте и загрузка ключевого файла осуществляется по сети Интернет. Перед началом установки убедитесь, что ваш компьютер имеет действующее интернет-соединение. Во время данной процедуры возможно получение демонстрационного файла.

1. Запустите установку продукта (см. раздел Первая установка).
2. На шаге **Ключевой файл Dr.Web** выберите **Получить файл в процессе установки**.
3. Выполните остальные шаги установки в обычном режиме. На завершающей стадии установки запустится процедура получения ключевого файла. По завершении процедуры **Антивирус Dr.Web** автоматически загрузит и установит ключевой лицензионный файл.

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

Демонстрационный ключ может использоваться только на том компьютере, на котором вы проходили регистрацию.

Повторная регистрация

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

В случае использования демонстрационного ключа выдается тот же ключевой файл, который был выдан ранее.

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.

1.4.3. Продление лицензии

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

Замена ключевого файла

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

1.5. Методы обнаружения

Все антивирусы **Dr.Web** одновременно используют несколько методов обнаружения вредоносных объектов, что позволяет максимально тщательно проверить подозрительные файлы.

1. В первую очередь применяется *сигнатурный* анализ. Он выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов (*сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для опознания вируса). При этом сравнение проводится по контрольным суммам сигнатур, что позволяет значительно снизить размер записей в вирусных базах данных, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения и лечения зараженных файлов. **Вирусные базы Dr.Web** составлены таким образом, что благодаря одной записи можно обнаруживать целые классы угроз.
2. После завершения сигнатурного анализа применяется уникальная технология **Origins Tracing**, которая позволяет определить новые или модифицированные вирусы, использующие известные механизмы заражения файлов. Так, например, эта технология защищает пользователей антивирусных решений **Dr.Web** от таких вирусов, как вирус-шантажист Trojan.Encoder.18 (также известный под названием gpcode). Кроме того, именно введение **Origins Tracing™** позволяет значительно снизить количество ложных срабатываний эвристического анализатора.
3. Работа эвристического анализатора основывается на неких знаниях (*эвристиках*) о характерных признаках вирусного и, наоборот, безопасного кода. Каждый признак имеет определенный вес (число, показывающее серьезность и достоверность данного признака). На основании суммарного веса, характеризующего каждый конкретный файл, эвристический анализатор вычисляет вероятность заражения файла неизвестным вирусом. Как и любая система проверки гипотез в условиях неопределенности,

эвристический анализатор может допускать ошибки как первого (пропуск неизвестных вирусов), так и второго рода (ложная тревога).

Во время любой из проверок компоненты антивирусов **Dr.Web** используют самую свежую информацию о всех известных вредоносных программах. Сигнатуры вирусов, информация об их признаках и моделях поведения обновляется сразу же, как только специалисты **Антивирусной лаборатории «Доктор Веб»** обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейший вирус проникает на компьютер, минуя резидентные средства защиты, после обновления вирусных баз он будет обнаружен в списке процессов и нейтрализован.

1.6. Проверка антивируса

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

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

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

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

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

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

При работе в оптимальном режиме **SpIDer Guard** не прерывает запуск тестового файла EICAR и не определяет данную операцию как опасную, так как данный файл не представляет угрозы для компьютера. Однако при копировании или создании такого файла на компьютере **SpIDer Guard** автоматически обрабатывает файл как вредоносную программу и по умолчанию перемещает его в **Карантин**.

2. Установка программы

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

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

Перед установкой следует также удалить с компьютера другие антивирусные пакеты и межсетевые экраны для предотвращения возможной несовместимости их резидентных компонентов.

2.1. Первая установка

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

Установка программы **Антивирус Dr.Web** возможна в любом из следующих режимов:

- в фоновом режиме;
- в обычном режиме.

Установка в фоновом режиме

Для запуска установки программы **Антивирус Dr.Web** в фоновом режиме, в командной строке введите имя исполняемого файла с

необходимыми параметрами (параметры влияют на ведение отчета, перезагрузку после окончания установки и установку **Брандмауэра**):

Установка	Параметры
Без перезагрузки и без ведения отчета	/S /V/qn
С перезагрузкой и без ведения отчета	/S /V"/qn REBOOT=Force" или /S /V"/qn REBOOT=F"
Без перезагрузки и с ведением отчета	/S /V"/qn /lv* \"<*путь*>\drweb-setup.log\""
С перезагрузкой и с ведением отчета	/S /V"/qn /lv* \"<*путь*>\drweb-setup.log\" REBOOT=F" или /S /V"/qn /lv* \"<*путь*>\drweb-setup.log\" REBOOT=Force"
С установкой **Брандмауэра** и с перезагрузкой	/S /V"/qn INSTALL_FIREWALL=1 REBOOT=F" или /S /V"/qn INSTALL_FIREWALL=1 REBOOT=Force"

Например, при запуске следующей команды будет проведена установка программы **Антивирус Dr.Web**, создан файл отчета и проведена перезагрузка после установки:

```
C:\Documents and Settings\drweb-700-win.exe /S /V"/qn /lv* \"%temp%\drweb-setup.log\"REBOOT=F"
```

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

/L<*код_языка*>

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

Список языков:

Код	Язык
1033	английский
1026	болгарский
1038	венгерский
1032	греческий
1034	испанский
1040	итальянский
1028	китайский (традиционный)
2052	китайский (упрощенный)
1062	латышский
1063	литовский
1031	немецкий
1045	польский
2070	португальский
1049	русский
1051	словацкий
1055	турецкий
1058	украинский
1036	французский
1061	эстонский
1041	японский

Независимо от выбранного языка будет дополнительно установлен английский язык.

Установка в обычном режиме

Чтобы запустить установку в обычном режиме, воспользуйтесь одним из следующих методов:

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

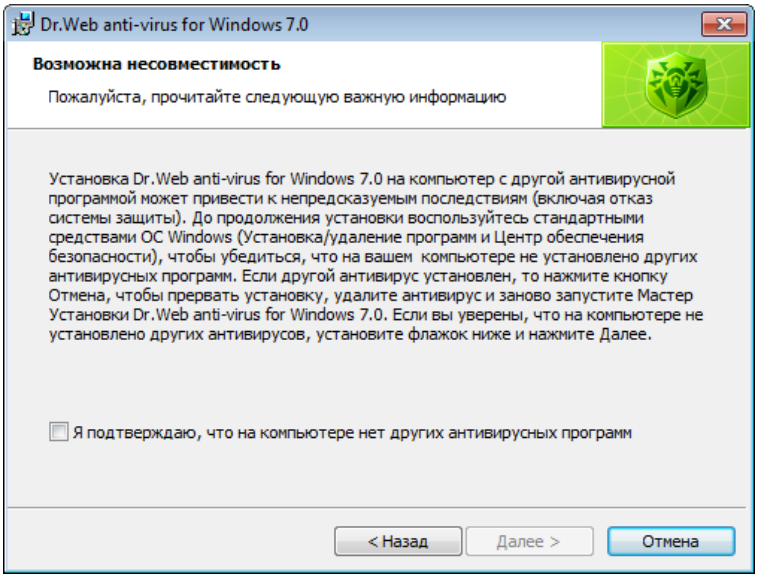
Следуйте указаниям программы установки. На любом шаге до начала копирования файлов на компьютер вы можете выполнить следующее:

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

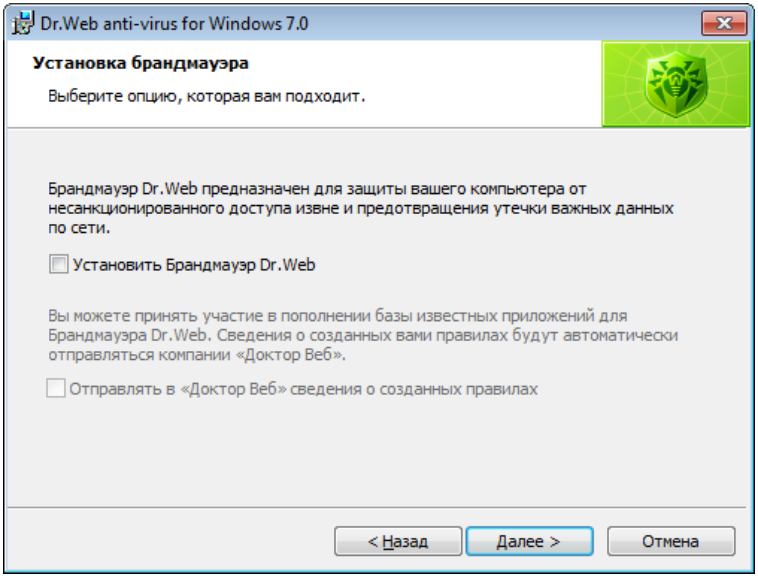
Процедура установки:

1. На первом шаге выберите язык установки, который будет использоваться в интерфейсе. Независимо от вашего выбора дополнительно будет установлен английский язык.
2. На следующем шаге ознакомьтесь с лицензионным соглашением. Для продолжения установки его необходимо принять.
3. На следующем шаге программа установки предупредит вас о возможной несовместимости **Антивируса Dr.Web** и иных антивирусов, установленных на вашем компьютере, и предложит удалить их. Выполните одно из следующих действий:

- если на вашем компьютере установлены другие антивирусы, то рекомендуется нажать кнопку **Отмена** и прервать установку, удалить или дезактивировать эти антивирусы и после этого начать установку заново;
- если на вашем компьютере не установлены другие антивирусы, для продолжения установите флажок **Я подтверждаю, что на компьютере нет других антивирусных программ** и нажмите кнопку **Далее**.



4. На следующем шаге вам будет предложено установить **Брандмауэр**.



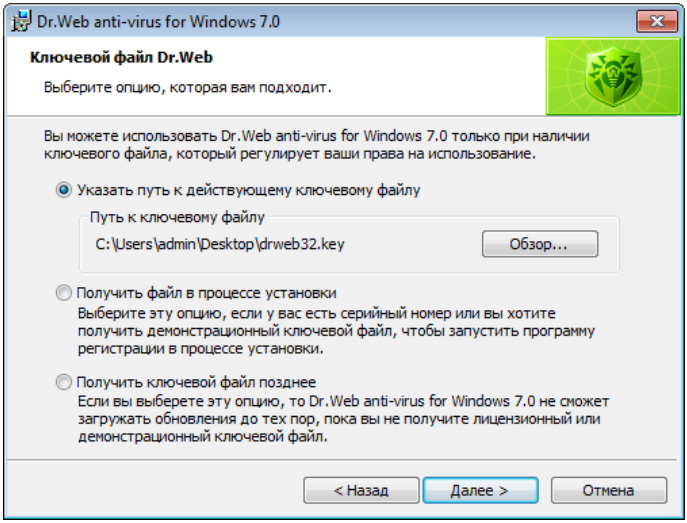
Также вы можете принять участие в пополнении базы известных приложений для **Брандмауэра**. Установите флажок **Отправлять в «Доктор Веб» сведения о созданных правилах**, чтобы разрешить **Брандмауэру** автоматически отправлять сведения о созданных вами правилах.

5. Если на предыдущем шаге вы установили флаг **Установить Dr.Web Брандмауэр**, то программа установки предупредит вас о возможной несовместимости программы **Антивирус Dr.Web** и других межсетевых экранов, установленных на вашем компьютере, и предложит удалить их. Выполните одно из следующих действий:
   - если на вашем компьютере установлен другой межсетевой экран, то рекомендуется нажать кнопку **Отмена** и прервать установку, удалить или дезактивировать межсетевой экран и после этого начать установку заново;

- если на вашем компьютере не установлены другие межсетевые экраны, для продолжения установите флажок **Я подтверждаю, что на компьютере нет других межсетевых экранов** и нажмите кнопку **Далее**.

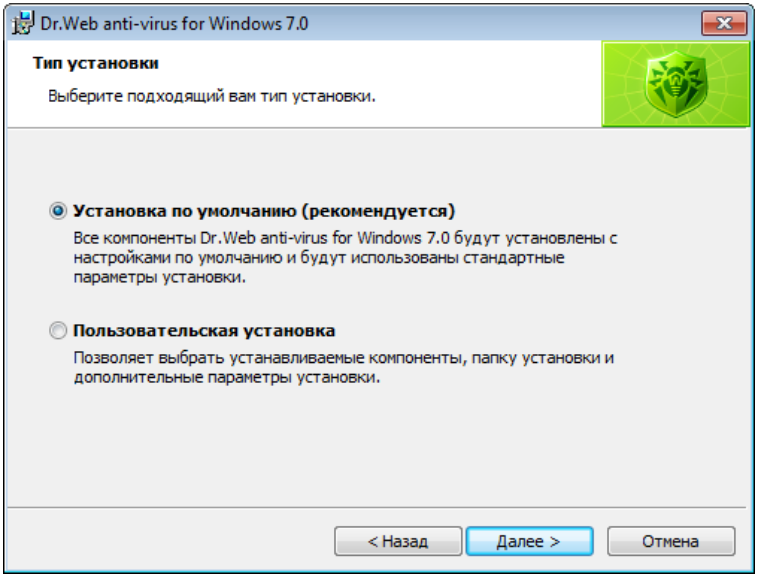
6. На шаге **Ключевой файл Dr.Web** программа установки предупредит вас о том, что для работы программы **Антивирус Dr.Web** необходим ключевой файл (лицензионный или демонстрационный). Выполните одно из следующих действий:
   - если у вас есть ключевой файл и он находится на жестком диске или сменном носителе, нажмите кнопку **Обзор** и выберите ключевой файл в стандартном окне открытия файла;
   - если у вас нет ключевого файла, но вы готовы его получить в процессе установки, выберите **Получить файл в процессе установки**;
   - для продолжения установки с временным ключевым файлом выберите **Получить ключевой файл позднее**. Обновления не будут загружаться до тех пор, пока вы не укажете лицензионный или демонстрационный ключевой файл.

   Нажмите кнопку **Далее**.



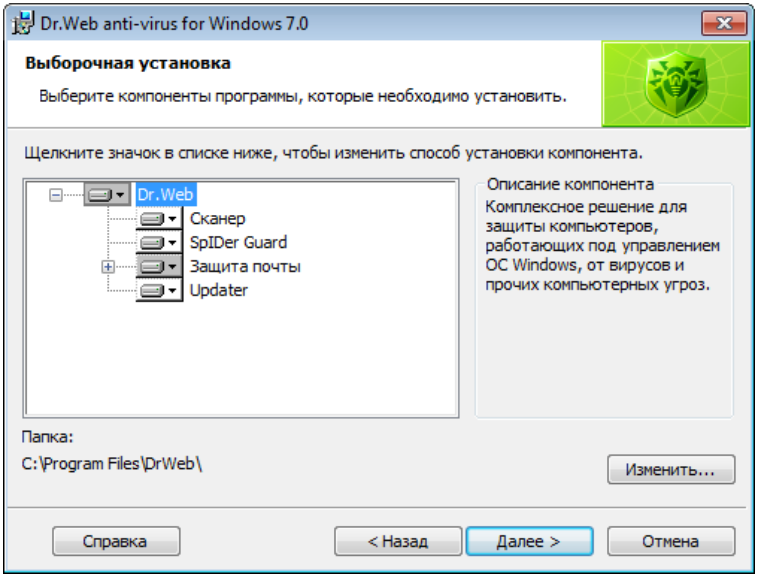
Используйте только ключевой файл варианта **Антивирус Dr.Web**. Ключевой файл должен иметь расширение .key. Если файл находится в архиве, необходимо извлечь его соответствующим архиватором.

7. На следующем шаге вам будет предложено выбрать тип установки:
   - **Установка по умолчанию** предполагает установку всех компонентов, а также всех вспомогательных программ, причем этапы установки до шага 12 будут проведены автоматически;
   - **Пользовательская установка** предназначена для опытных пользователей. В процессе пользовательской установки вам будет предложено самостоятельно выбрать устанавливаемые компоненты, указать настройки прокси-сервера и некоторые дополнительные параметры установки.



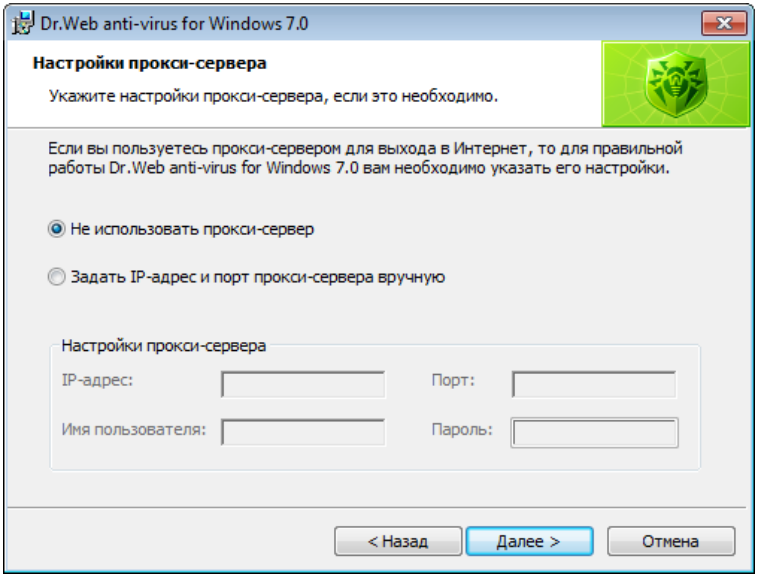
Выберите необходимый тип установки и нажмите кнопку **Далее**.

8. Если вы выбрали режим установки по умолчанию, то перейдите к описанию шага 12. Если вы выбрали режим **Пользовательской установки**, то в открывшемся окне выберите устанавливаемые компоненты, при необходимости измените каталог установки и нажмите кнопку **Далее**.



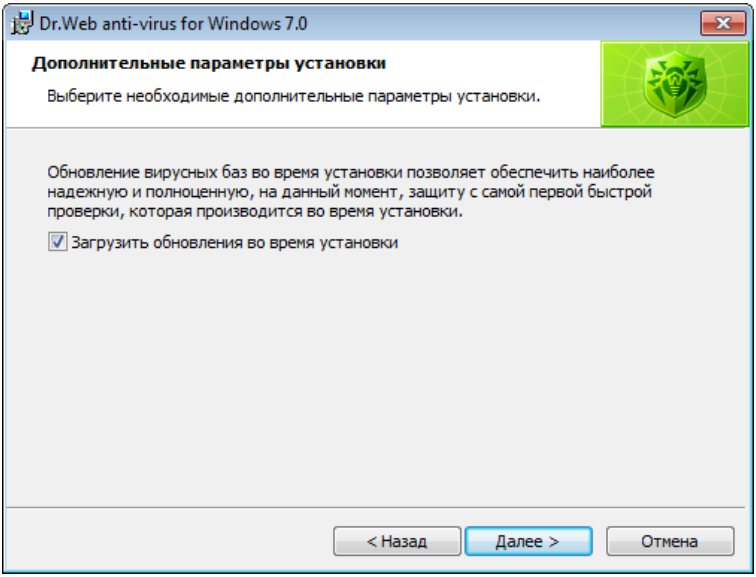
9. На следующем шаге вам будет предложено настроить создание ярлыков для запуска программы **Антивирус Dr.Web**. Укажите необходимые пункты и нажмите кнопку **Далее**.
10. На следующем шаге вам будет предложено указать настройки подключения к прокси-серверу. Выберите один из следующих вариантов:
    - если для выхода в Интернет прокси-сервер не используется, выберите **Не использовать прокси-сервер**;
    - если вы хотите задать настройки прокси-сервера, выберите пункт **Задать IP-адрес и порт прокси-сервера вручную** и укажите необходимые параметры.

    Нажмите кнопку **Далее**.



11. Если на шаге 6 вы указали действующий ключевой файл или выбрали пункт **Получить файл в процессе установки**, то на следующем шаге вы можете установить флажок **Загрузить обновления во время установки**, чтобы в процессе установки были загружены актуальные вирусные базы и другие модули антивируса.

    Нажмите кнопку **Далее**.



12. Откроется информационное окно с сообщением о готовности к установке. Вы можете выполнить одно из следующих действий:
    - чтобы запустить процесс копирования файлов, нажмите кнопку **Установить**;
    - чтобы изменить параметры установки, нажмите кнопку **Назад**.
13. Если на шаге 6 вы выбрали **Получить файл в процессе установки**, то на следующем шаге программа попытается получить ключевой файл через Интернет при помощи процедуры регистрации пользователя.
14. Если в процессе установки вы указали или получили действующий ключевой файл и на шаге 11 установили флажок **Загрузить обновления во время установки**, а также во время установки по умолчанию, будет выполнен процесс обновления вирусных баз и других компонентов программы **Антивирус Dr.Web**. Обновление проводится автоматически и не требует дополнительных действий.

15. По завершении установки запустится **Сканер**, который проведет быструю проверку. В случае обнаружения инфицированных файлов выберите необходимые действия для этих объектов. После завершения проверки закройте **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 программы **Антивирус Dr.Web** в настройках программы WindowBlinds, добавив файл dwscanner.exe в список исключаемых программ.

16. Для завершения процесса установки выполните перезагрузку компьютера.

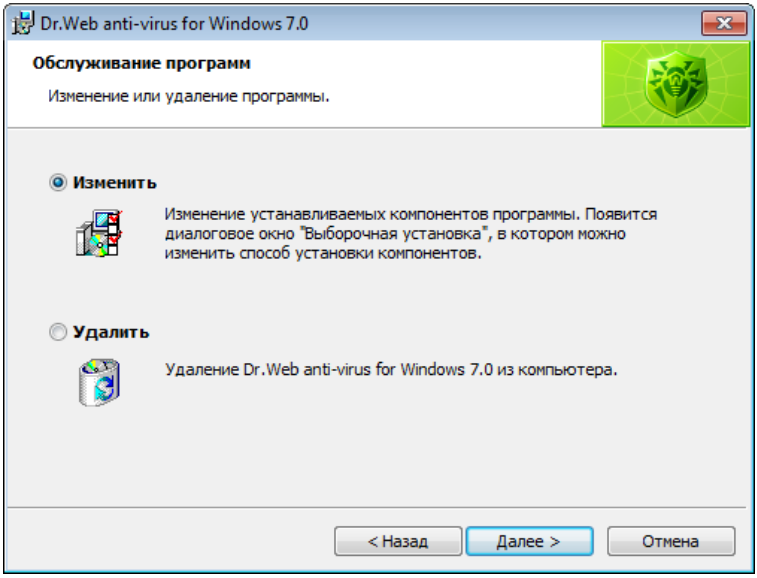
2.2. Повторная установка и удаление

С помощью программы установки вы также можете:

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

Изменение и удаление программы

1. Чтобы запустить установку, воспользуйтесь одним из следующих методов:
   - в случае поставки установочного комплекта в виде единого исполняемого файла запустите на исполнение этот файл;
   - в случае поставки установочного комплекта на фирменном диске вставьте диск в привод. 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 кнопку **Установить**;
   - запустите программу установки при помощи утилиты установки и удаления программ операционной системы Windows.
2. В открывшемся окне выберите режим работы программы установки:
   - чтобы изменить состав устанавливаемых компонентов, выберите вариант **Изменить**;
   - чтобы удалить все установленные компоненты, выберите пункт **Удалить**.



4. Для удаления программы **Антивирус Dr.Web** или изменения состава компонентов программе установки потребуется отключить самозащиту. Для этого введите код подтверждения, изображенный в открывшемся окне, или пароль (если на вкладке **Дополнительно** настроек SpIDer Agent вы установили флажок **Защищать паролем настройки Dr.Web**).
5. При необходимости по просьбе программы перезагрузите компьютер для завершения процедуры удаления или изменения состава компонентов.

2.3. Процедура получения ключевого файла

Процедура получения ключевого файла запускается автоматически в процессе установки или из меню **SpIDer Agent** после завершения установки и помогает подключиться к **официальному сайту «Доктор Веб»** и зарегистрировать продукт.

Получение ключевого файла

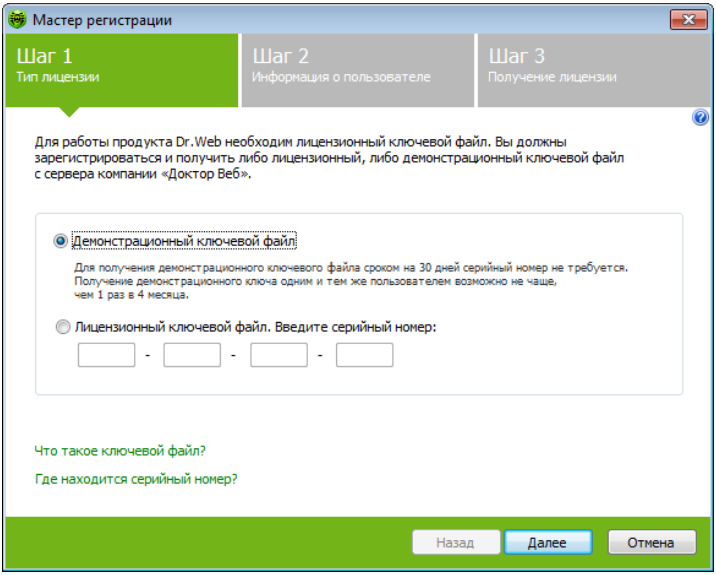
1. На первом шаге вам будет предложено выбрать: получить демонстрационный или лицензионный ключевой файл (подробно о ключевом файле см. Ключевой файл).

   Если у вас имеется регистрационный серийный номер, выданный вам при приобретении антивируса, выберите вариант **Лицензионный ключевой файл** и введите серийный номер. Если вы устанавливаете программу с ознакомительными целями, выберите пункт **Демонстрационный ключевой файл** и перейдите к шагу 2.

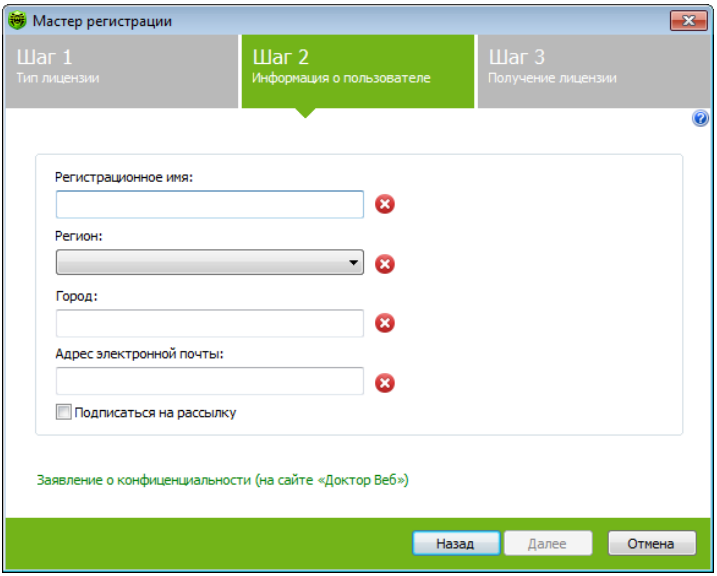
   

   Если вы ранее уже являлись пользователем программы **Антивирус Dr.Web**, то вы можете продлить действие приобретенной лицензии на 150 дополнительных дней. Для этого укажите серийный номер либо лицензионный ключевой файл предыдущей регистрации.

   Нажмите кнопку **Далее**. Откроется окно ввода регистрационных данных.



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



3. Запускается процедура загрузки и установки ключевого файла. Если получение ключевого файла завершилось успешно, выводится соответствующее сообщение и указывается срок действия лицензии. В противном случае выводится сообщение об ошибке.

3. Приступая к работе

Программа установки позволяет установить на компьютер следующие компоненты антивирусной защиты:

- **Сканер Dr.Web** для Windows (с GUI-интерфейсом и консольную версию);
- сторож **SpIDer Guard**;
- почтовый сторож **SpIDer Mail**;
- подключаемый модуль **Dr.Web для Outlook**;
- межсетевой экран **Брандмауэр Dr.Web**;
- **Модуль автоматического обновления Dr.Web**;
- модуль управления **SpIDer Agent**.

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

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

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

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

Почтовый сторож **SpIDer Mail** также постоянно находится в памяти. Программа перехватывает все обращения почтовых клиентов вашего компьютера 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 функциональность вирусов. Это также позволяет отключить проверку почтовых файлов в **SpIDer Guard**, что значительно снижает потребление ресурсов компьютера.

Персональный межсетевой экран **Брандмауэр Dr.Web** предназначен для защиты вашего компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети. **Брандмауэр** позволяет вам контролировать подключение и передачу данных по сети Интернет и блокировать подозрительные соединения на уровне пакетов и приложений.

Организация антивирусной защиты

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

- при помощи **Сканера Dr.Web** произвести сканирование всей файловой системы компьютера с предусмотренными по умолчанию (максимальными) настройками подробности сканирования;
- сохранить настройки **SpIDer Guard** по умолчанию;

- осуществлять полную проверку почты при помощи **SpIDer Mail**;
- блокировать все неизвестные соединения с помощью **Брандмауэра Dr.Web**;
- периодически, по мере обновления вирусных баз, повторять полное сканирование компьютера (не реже раза в неделю);
- в случае временного отключения **SpIDer Guard**, если в этот период компьютер подключался к сети Интернет или производилась загрузка файлов со сменного носителя, провести полное сканирование немедленно.

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

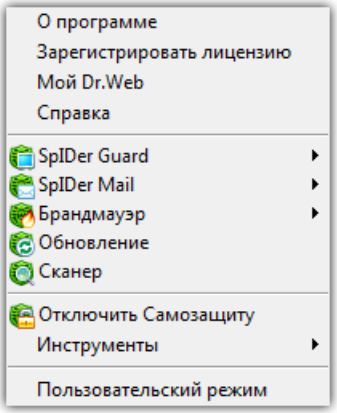
Использование компонентов программы **Антивирус Dr.Web** подробнее описано в следующих разделах.

3.1. Модуль управления SpIDer Agent

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

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

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



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

Пункт **Зарегистрировать лицензию** запускает процедуру регистрации пользователя для получения ключевого файла с сервера компании **«Доктор Веб»**.

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

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

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

Пункт **Сканер** запускает **Сканер Dr.Web**.

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

Отключение самозащиты:

1. В меню **SpIDer Agent** выберите пункт **Отключить Самозащиту**.
2. Введите код подтверждения.
3. В меню **SpIDer Agent** пункт **Отключить Самозащиту** заменится на пункт **Включить Самозащиту**.

Отключение самозащиты возможно только в Административном режиме. Отключать самозащиту не рекомендуется.

В случае возникновения проблем при использовании программ дефрагментации рекомендуется временно отключить модуль самозащиты.

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

- к **Менеджеру лицензий** (см. раздел Менеджер лицензий);
- к настройкам общих параметров работы программы **Антивирус Dr.Web** (см. Общие настройки);

- к **Менеджеру Карантина** (см. Менеджер Карантина);
- к созданию отчета.

  При обращении в службу технической поддержки компании **«Доктор Веб»** вы можете сформировать отчет о вашей операционной системе и работе программы **Антивирус Dr. Web**. Для настройки параметров в открывшемся окне нажмите **Параметры отчета**. Отчет будет сохранен в виде архива в каталоге Doctor Web, расположенном в папке профиля пользователя `%USERPROFILE%`.

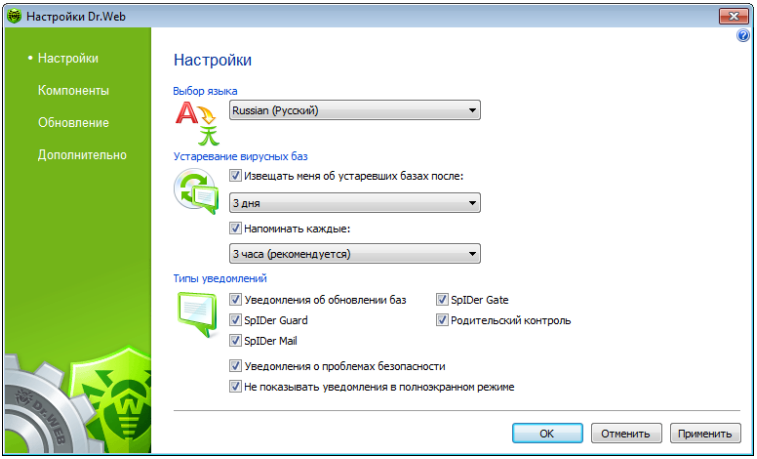
Пункт **Административный/Пользовательский режим** позволяет переключаться между полнофункциональным **Административным режимом** и ограниченным **Пользовательским режимом** работы с программой **Антивирус Dr.Web**. В **Пользовательском режиме** действуют следующие ограничения: недоступны настройки компонентов, пункт **Менеджер лицензий**, а также функции отключения всех компонентов и самозащиты. Для переключения в **Административный режим** вам необходимы права администратора.

Данный пункт отображается только при отсутствии административных привилегий. Например, при работе в среде операционных систем Microsoft Windows 2000 или Windows XP в пользовательском режиме, или в среде Windows Vista или Microsoft Windows 7 при включенной системе контроля учетной записи UAC. В противном случае данный пункт недоступен и **Антивирус Dr.Web** постоянно работает в полнофункциональном режиме.

3.2. Общие настройки

Настройка общих параметров работы программы **Антивирус Dr. Web** осуществляется в разделах окна **Настройки Dr.Web**. Чтобы открыть данное окно, щелкните значок **SpIDer Agent** в области уведомлений Windows и в подменю **Инструменты** выберите пункт **Настройки**.

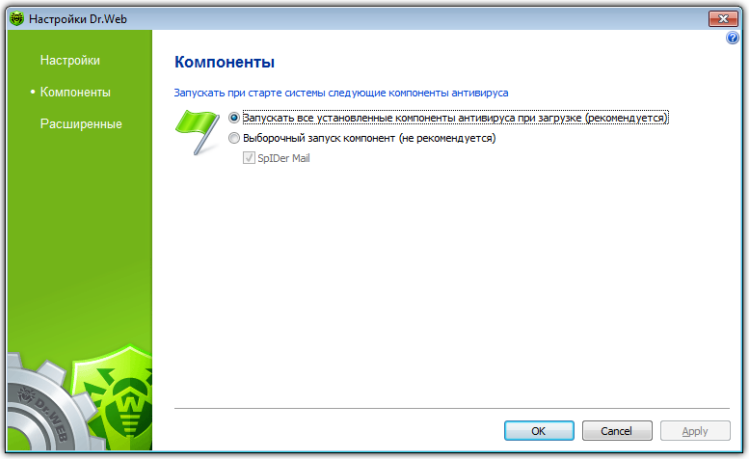
Раздел Настройки



В данном разделе производится выбор языка интерфейса программы **Антивирус Dr.Web**. Если в выпадающем списке вы выберете язык, который не был установлен, то вам будет предложено его установить.

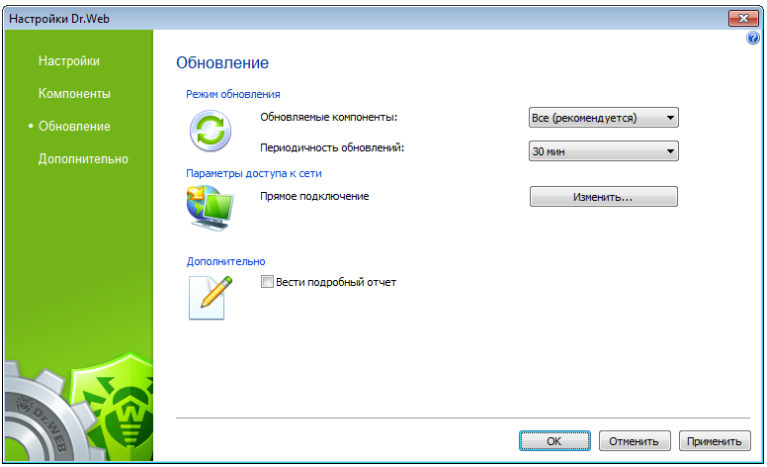
Также в этом разделе производится настройка типов подсказок-уведомлений, появляющиеся в виде всплывающего окна над значком **SpIDer Agent** в области уведомлений Windows. Компоненты, перечисленные в данной группе, посылают уведомления в случае срабатывания соответствующей защиты. Также уведомление может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

Раздел Компоненты



В данном разделе вы можете выбрать режим автоматической загрузки компонентов программы **Антивирус Dr.Web** при старте операционной системы.

Раздел Обновление



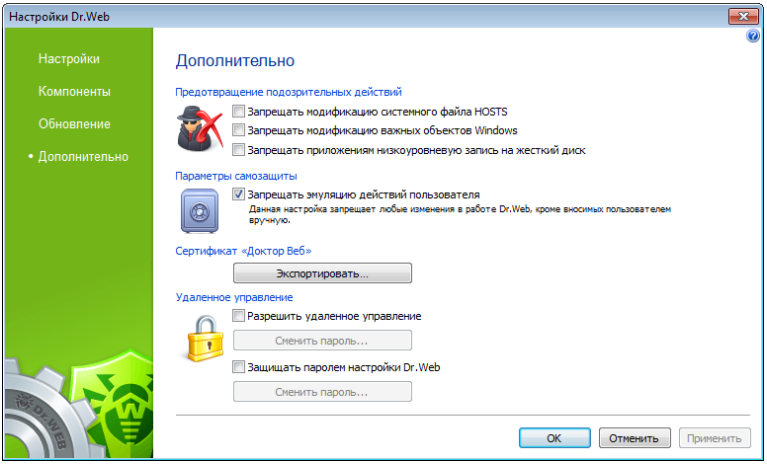
В данном разделе вы можете настроить параметры обновления программы **Антивирус Dr.Web**. Вы можете указать, какие компоненты необходимо обновлять, а также периодичность, с которой будут происходить обновления.

Вы можете настроить параметры доступа к сети. Для этого в группе **Параметры доступа к сети** нажмите кнопку **Изменить** и выберите один из следующих вариантов:

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

Также вы можете установить флаг **Вести подробный отчет**, для того чтобы об изменениях сохранялась детальная информация. Отчет записывается в файл dwupdater.log, который находится в каталоге %allusersprofile%\Application Data\Doctor Web\Logs\ (в Windows 7, %allusersprofile%\Doctor Web\Logs).

Раздел Дополнительно



В данном разделе вы можете настроить параметры самозащиты, а также запретить некоторые действия, которые могут поставить под угрозу безопасность вашего компьютера.

Если при установке важных обновлений от Microsoft или при установке и работе программ (в том числе программ дефрагментации) возникают проблемы, отключите соответствующие опции в этой группе настроек.

Сертификат «Доктор Веб»

Если вы хотите включить в проверку данные, передаваемые по криптографическому протоколу SSL (например, в **SpIDer Mail** вы можете настроить параметры проверки данных, передаваемых по протоколам POP3S, SMTPS, IMAPS), то для работы некоторых клиентов, которые передают и получают такие данные и при этом не обращаются к хранилищу сертификатов системы Windows, может потребоваться сертификат компании **«Доктор Веб»**. Нажмите кнопку **Экспортировать** и сохраните сертификат в удобный для вас каталог.

Защита паролем

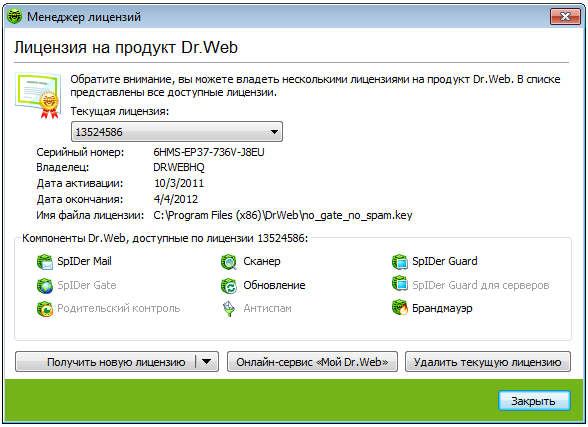
Вы также можете:

- разрешить удаленный доступ к **Антивирус Dr.Web** на вашем компьютере. Задайте пароль, который будет запрашиваться при удаленном подключении к вашему антивирусу;
- установить пароль для доступа к настройкам **Антивирус Dr. Web** на вашем компьютере. Задайте пароль, который будет запрашиваться при обращении к настройкам **Антивирус Dr. Web**.

3.3. Менеджер лицензий

Менеджер лицензий в доступном виде отображает информацию, содержащуюся в имеющихся у вас ключевых файлах программы **Антивирус Dr.Web**. Чтобы открыть **Менеджер лицензий**, щелкните значок **SpIDer Agent** в области уведомлений Windows и в подменю **Инструменты** выберите пункт **Менеджер лицензий**.

Пункт **Менеджер лицензий** доступен только в Административном режиме.



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

Получение ключевого файла

Для получения ключевого файла с сервера компании **«Доктор Веб»** нажмите кнопку **Получить новую лицензию** и в выпадающем списке выберите **через сеть Интернет**. Запустится процедура получения ключевого файла.

Для работы программы **Антивирус Dr.Web** требуется установить

в защищаемой системе ключевой файл.

Установка полученного ключевого файла

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

При получении ключевого файла в процессе установки или в комплекте дистрибутива установка ключевого файла производится автоматически и никаких дополнительных действий не требует.

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

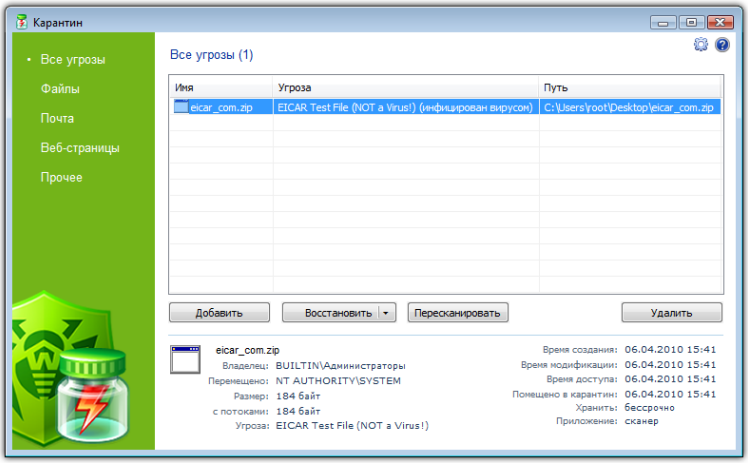
При работе программы ключевой файл по умолчанию должен находиться в каталоге установки. **Антивирус Dr.Web** регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа не модифицируйте ключевой файл.

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.

3.4. Менеджер Карантина

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

Чтобы открыть **Менеджер Карантина**, щелкните значок **SpIDer Agent** в области уведомлений Windows и в подменю **Инструменты** выберите пункт **Менеджер Карантина**.



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

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

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

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

Настройка отображения столбцов

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

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

объекты, не попадающие в данные категории.

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

В окне карантина доступны следующие кнопки управления:

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

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

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

- **Пересканировать** – сканировать файл из карантина повторно. Если при повторном сканировании файла обнаружится, что он не является зараженным, **Менеджер Карантина** предложит восстановить файл;
- **Удалить** – удалить файл из карантина и из системы.

В контекстном меню в таблице доступны следующие опции:

- **Отправить файл(ы) в лабораторию «Доктор Веб»** – отправить в **Антивирусную Лабораторию «Доктор Веб»** файл на проверку;
- **Копировать хэш в буфер обмена** – копировать хэш файла, полученный с помощью алгоритма MD5 или SHA256, в буфер обмена Windows.

Для работы одновременно с несколькими файлами выберите необходимые файлы, удерживая клавиши SHIFT или CTRL, затем

щелкните правой кнопкой мыши на любой строчке таблицы и выберите необходимое действие.

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

- в разделе **Задать размер карантина** вы можете управлять объемом дискового пространства, занимаемого папкой **Карантина**;
- в разделе **Вид** вы можете установить флаг **Показывать резервные копии**, чтобы отобразить в таблице объектов резервные копии файлов, находящихся в **Карантине**.

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

3.5. Антивирусная сеть

Компонент **Антивирусная сеть** не входит в состав продукта **Антивирус Dr.Web**. Однако вы можете разрешить доступ к **Антивирусу Dr.Web** на своем компьютере. Для этого на вкладке **Дополнительно** настроек модуля управления SpIDer Agent установите флажок **Разрешать удаленное управление** и задайте пароль, который необходимо будет ввести для удаленного управления вашим антивирусом.

Если вы используете ключ для **Dr.Web Security Space**, вы можете скачать соответствующую документацию на сайте компании http://download.drweb.com/doc, чтобы ознакомиться с работой компонента **Антивирусная сеть**.

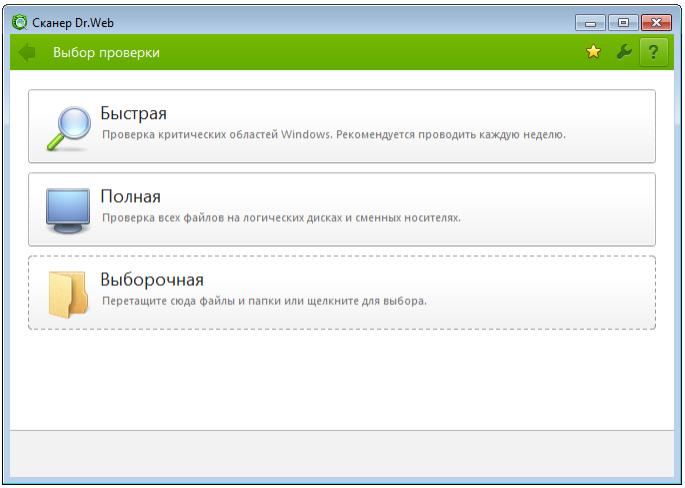
Пользователю антивируса, который получит удаленный доступ к **Антивирусу Dr.Web** на вашем компьютере, будут доступны следующие пункты:

- **О программе**
- **Зарегистрировать лицензию**
- **Мой Dr.Web**
- **Справка**
- SpIDer Guard
- SpIDer Mail
- **Инструменты**
- **Отключить/Включить Самозащиту**
- Менеджер лицензий
- Общие настройки
- **Создание отчета**

Удаленное управление позволяет просматривать статистику, включать и отключать модули, а также изменять их настройки. Компоненты **Карантин** и **Сканер** недоступны. Настройки и статистика **Брандмауэра Dr.Web** также недоступны, однако удаленно можно включить или отключить этот компонент.

4. Сканер Dr.Web

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



4.1. Проверка компьютера

Сканер устанавливается как обычное приложение Windows и запускается по команде пользователя.

Запуск Сканера

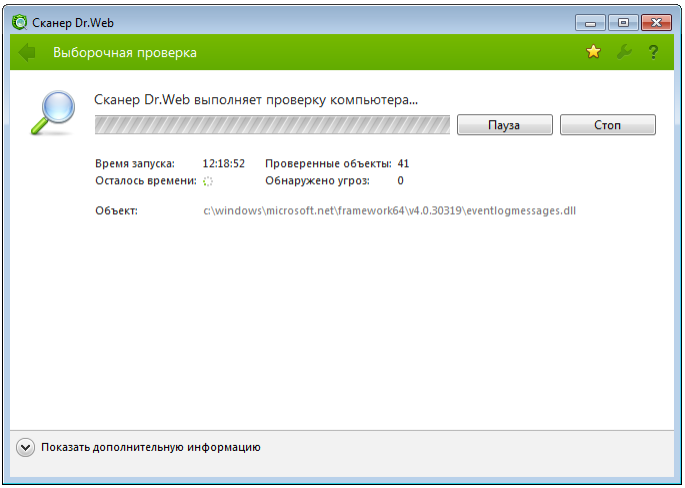
Рекомендуется запускать **Сканер** от имени пользователя, обладающего правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут подвергнуты проверке.

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

   Чтобы запустить **Сканер** с настройками по умолчанию для проверки конкретного 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 **Сканера** открывается его главное окно.

   Если вы запускаете **Сканер** на проверку файла или каталога, то после этого немедленно начинается сканирование заданного объекта.



3. На выбор предоставляется три возможных режима проверки: **Быстрая**, **Полная** и **Выборочная**.

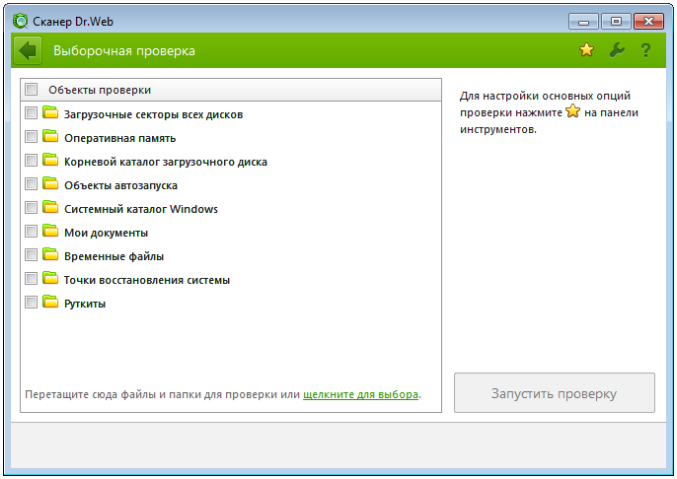
   Во время *быстрой проверки* проверяются:

   - 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;
   - наличие руткитов (если процесс проверки запущен от имени администратора).

   В режиме *полной проверки* производится полное сканирование оперативной памяти и всех жестких дисков (включая загрузочные секторы), а также осуществляется проверка на наличие руткитов.

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

4. При выборе выборочного режима в окне **Сканера Dr.Web** в таблице задаются объекты для проверки: любые файлы и папки, а также такие объекты, как оперативная память, объекты автозапуска, загрузочные секторы и т.п.). Для начала проверки выбранных объектов нажмите кнопку **Запустить проверку**. В случае полной или быстрой проверки выбирать объекты не требуется.



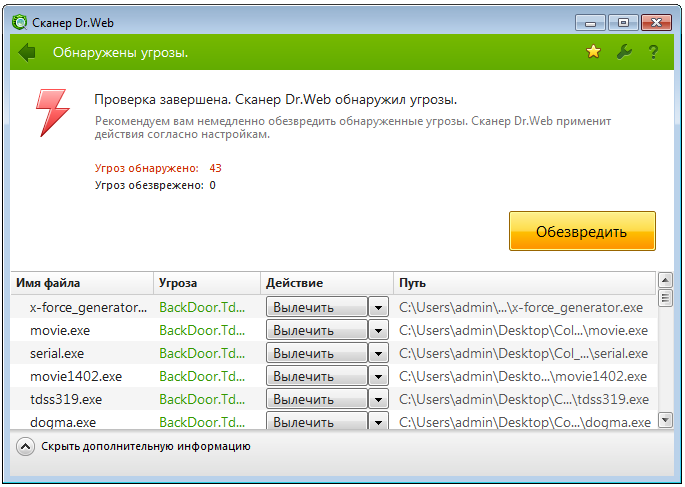
5. После начала сканирования в правой части окна становятся доступными кнопки **Пауза** и **Стоп**. На любом этапе проверки вы можете сделать следующее:
   - чтобы приостановить проверку, нажмите кнопку **Пауза**. Для того чтобы возобновить проверку после паузы, снова нажмите кнопку **Старт**;
   - чтобы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

Кнопка **Пауза** активна только при проверке файлов, объектов автозапуска, точек восстановления системы, а также при проверке на наличие руткитов. В остальных случаях кнопка **Пауза** недоступна.

4.2. Действия при обнаружении вирусов

По умолчанию **Сканер** лишь информирует пользователя обо всех зараженных и подозрительных объектах.

Вы можете обезвредить все обнаруженные угрозы одновременно. Для этого нажмите кнопку **Обезвредить** – **Сканер** применит оптимальные действия по умолчанию для всех обнаруженных угроз.



При необходимости вы можете применить действия для каждой угрозы в отдельности. Вы можете восстановить функциональность зараженного объекта (*вылечить* его), а при невозможности – устранить исходящую от него угрозу (*удалить* объект).

Выбор действия

1. В поле **Действие** в выпадающем списке выберите необходимое действие для каждого объекта (по умолчанию **Сканер Dr.Web** предлагает оптимальное значение).
2. Нажмите кнопку **Обезвредить**. **Сканер Dr.Web** обезвредит все обнаруженные угрозы одновременно.

Подозрительные файлы, перемещенные в **Карантин**, рекомендуется передавать для дальнейшего анализа в **антивирусную лабораторию «Доктор Веб»**, используя пункт **Отправить файл(ы) в лабораторию «Доктор Веб»** в контекстном меню **Карантина**.

Существуют следующие ограничения:

- лечение подозрительных объектов невозможно;
- перемещение или удаление объектов, не являющихся файлами (например, загрузочных секторов), невозможно;
- любые действия для отдельных файлов внутри архивов, инсталляционных пакетов или в составе писем невозможны – действие в таких случаях применяется только ко всему объекту целиком.

Подробный отчет о работе программы сохраняется в виде файла отчета dwscanner.log, который находится в каталоге %USERPROFILE%\Doctor Web.

4.3. Настройка Сканера

Изменение настроек программы

1. Чтобы вызвать **Настройки Сканера**, щелкните на панели инструментов иконку **Настройки**  .

   Откроется окно настроек, содержащее несколько вкладок.

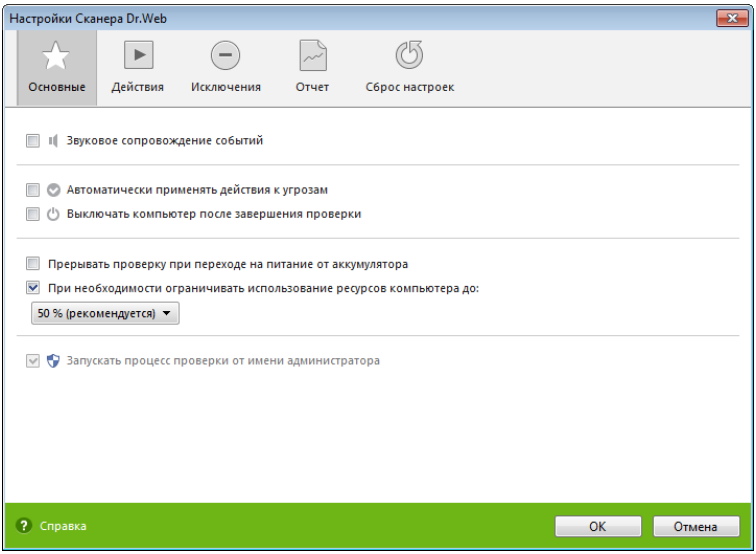
2. Внесите необходимые изменения.
3. Для более подробной информации о настройках, задаваемых на каждой вкладке, воспользуйтесь кнопкой **Справка**.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Вкладка Основные

На этой вкладке задаются основные параметры работы **Сканера Dr.Web**.

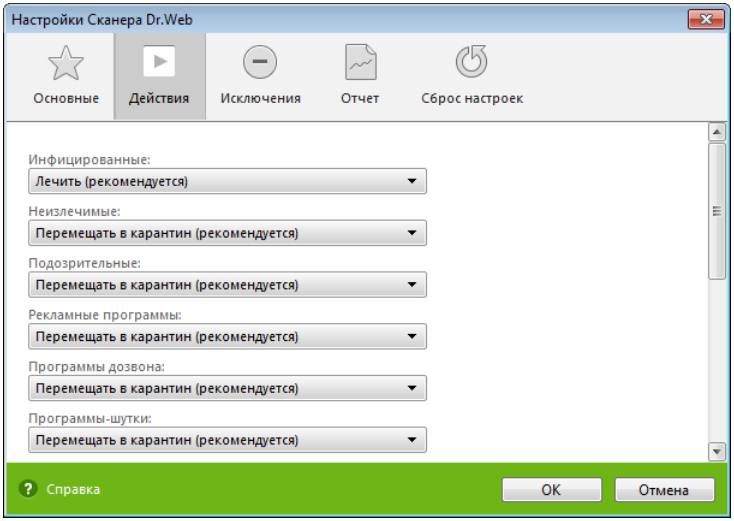
Вы можете включить звуковое сопровождение событий, а также указать **Сканеру Dr.Web** автоматически применять действия к угрозам и настроить взаимодействие программы с операционной системой.

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. Для этого установите флажок **Запускать процесс проверки от имени администратора**.



Настройка обезвреживания угроз

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



2. Выберите в выпадающем списке **Инфицированные** реакцию **Сканера** на обнаружение инфицированного объекта.

Оптимальным является значение **Лечить**.

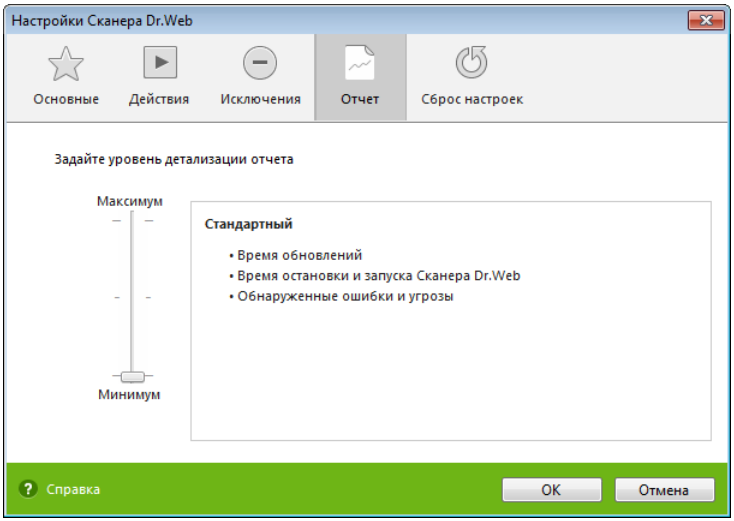
3. Выберите в выпадающем списке **Неизлечимые** реакцию **Сканера** на обнаружение неизлечимого объекта. Это действие аналогично рассмотренному в предыдущем пункте, с той разницей, что вариант **Лечить** отсутствует.

В большинстве случаев оптимальным является вариант **Перемещать в карантин**.

4. Выберите в выпадающем списке **Подозрительные** реакцию **Сканера** на обнаружение подозрительного объекта (полностью аналогично предыдущему пункту).
5. Аналогично настраивается реакция **Сканера** на обнаружение объектов, содержащих рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.
6. Аналогично настраиваются автоматические действия **Сканера** при обнаружении вирусов или подозрительного кода в файловых архивах, инсталляционных пакетах и почтовых ящиках. Действия по отношению к вышеуказанным объектам выполняются над всем объектом, а не только над зараженной его частью. По умолчанию во всех этих случаях предусмотрено информирование.
7. Для успешного завершения лечения некоторых зараженных (инфицированных) файлов требуется перезагрузка операционной системы. Вы можете выбрать один из вариантов:
   - **Перезагружать компьютер автоматически.** Этот режим может привести к потере несохраненных данных;
   - **Предлагать перезагрузку**.

Вкладка Отчет

На этой вкладке вы можете настроить параметры ведения файла отчета.



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

4.4. Запуск Сканера из командной строки

Вы можете запускать **Сканер Dr.Web** в режиме командной строки. Такой способ позволяет задать настройки текущего сеанса сканирования и перечень сканируемых объектов в качестве параметров вызова.

Запуск Сканера из командной строки

Чтобы запустить **Сканер** с дополнительными параметрами командной строки, воспользуйтесь следующей командой:

[<*путь_к_программе*>]**dwscanner** [<*объекты*>] [<*ключи*>], где

- <*объекты*> – список объектов для проверки;
- <*ключи*> – это параметры командной строки, которые задают настройки работы **Сканера**. При их отсутствии проверка выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их).

Список объектов для проверки может быть пуст или содержать несколько элементов, разделенных пробелами. Наиболее распространенными являются следующие объекты проверки:

- `/LITE` – произвести стартовую проверку системы, при которой проверяются оперативная память, загрузочные секторы всех дисков и объекты автозапуска, а также провести проверку на наличие руткитов.
- `/FAST` – произвести быструю проверку системы;
- `/FULL` – произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы).

4.5. Консольный сканер

Также в состав программы **Антивирус Dr.Web** входит **Консольный сканер**, который позволяет проводить проверку в режиме командной строки, а также предоставляет большие возможности настройки.

Файлы, подозрительные на наличие вредоносных объектов, **Консольный сканер** помещает в **Карантин**.

Запуск Консольного сканера

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

[<*путь_к_программе*>]**dwscancl** [<*ключи*>][<*объекты*>], где

- <*объекты*> – список объектов для проверки;
- <*ключи*> – список параметров командной строки, которые задают настройки работы **Консольного сканера**.

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

Все ключи командной строки начинается с символа «/» и разделяются пробелами. Список ключей **Консольного сканера** содержится в Приложении А.

После выполнения **Консольный сканер** возвращает один из следующих кодов:

0 – сканирование успешно завершено, инфицированные объекты не найдены;

1 – сканирование успешно завершено, найдены инфицированные объекты;

10 – указаны некорректные ключи;

11 – ключевой файл не найден либо не поддерживает **Консольный сканер**;

12 – не запущен **Scanning Engine**;
255 – сканирование прервано пользователем.

5. SpIDer Guard

SpIDer Guard – это антивирусный сторож, который постоянно находится в оперативной памяти, осуществляя проверку файлов и памяти «на лету», а также обнаруживая проявления вирусной активности.

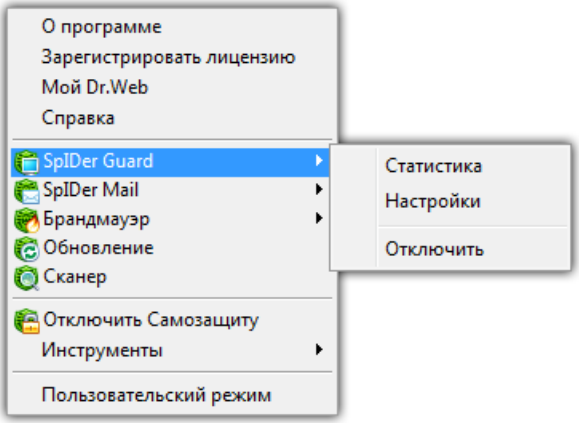
При настройках по умолчанию сторож «на лету» проверяет на жестком диске – только создаваемые или изменяемые файлы, на сменных носителях – все открываемые файлы. Кроме того, сторож постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при их обнаружении блокирует эти процессы. При обнаружении зараженных объектов сторож **SpIDer Guard** применяет к ним действия согласно установленным настройкам.

Соответствующим изменением настроек вы можете задать автоматическую реакцию сторожа **SpIDer Guard** на вирусные события. Вы сможете следить за ней с помощью окна статистики и файла отчета.

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

5.1. Управление SpIDer Guard

Основные средства настройки и управления сторожем **SpIDer Guard** находятся в подменю **SpIDer Guard**, которое открывается по щелчку на значке **SpIDer Agent** в области уведомлений Windows.



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

При выборе пункта пункта **Настройки** открывается окно настроек сторожа (см. Настройка SpIDer Guard).

Пункт **Отключить**/**Включить** позволяет приостановить/включить **SpIDer Guard** (доступно только пользователю, имеющему права администратора данного компьютера).

При отключении **SpIDer Guard** запрашивается код подтверждения.

Пункты **Настройки, Отключить/Запустить** доступны только в Административном режиме.

5.2. Настройка SpIDer Guard

Основные параметры работы сторожа **SpIDer Guard** сосредоточены в разделах окна **Настройки SpIDer Guard**.

Изменение настроек сторожа

1. Щелкните значок **SpIDer Agent** в области уведомлений Windows и выберите в подменю **SpIDer Guard** пункт **Настройки**.
2. Внесите необходимые изменения в разделах настроек.
3. Чтобы получить информацию о настройках, расположенных в разделе, нажмите кнопку **Справка** .
4. По окончании редактирования настроек:
   - чтобы сохранить изменения, нажмите кнопку **ОК**;
   - чтобы отказаться от внесенных изменений, нажмите кнопку **Отмена**.

Раздел Проверка

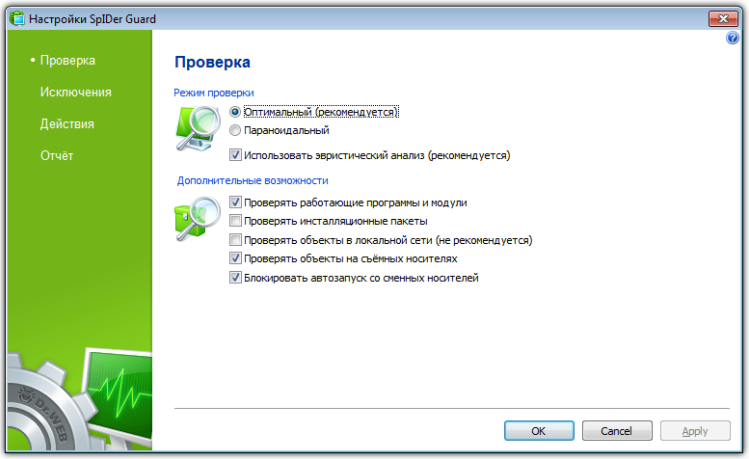
По умолчанию установлен режим проверки **Оптимальный**: сканирование на жестких дисках – только запускаемых, создаваемых или изменяемых файлов, на сменных носителях – всех открываемых файлов.

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

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

Флажок **Использовать эвристический анализ** включает режим эвристического анализатора (режим поиска неизвестных вирусов

на основании анализа структуры файла).



Группа настроек **Дополнительные возможности** позволяет задать параметры проверки «на лету», которые будут применяться вне зависимости от выбранного режима работы сторожа **SpIDer Guard**. Также вы можете запретить автоматический запуск активного содержимого внешних носителей данных (CD/DVD дисков, флеш-памяти и т.д.), установив флажок **Блокировать автозапуск со сменных носителей**. Использование этой настройки помогает предотвратить заражение вашего компьютера через внешние носители.

В случае возникновения проблем при установке программ, обращающихся к файлу autorun.inf, рекомендуется временно снять флажок **Блокировать автозапуск со сменных носителей**.

Здесь вы можете задать проверку:

- файлов запускаемых процессов вне зависимости от их расположения;
- установочных файлов;
- файлов на сетевых дисках;

- файлов и загрузочных секторов на съемных носителях.

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

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

Задание исключений

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

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

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

Вы можете формировать список исключений следующим образом:

- чтобы указать конкретный существующий каталог или файл, нажмите кнопку **Обзор** и выберите каталог или файл в стандартном окне открытия файла. Вы также можете вручную ввести полный путь к файлу или каталогу в поле ввода;
- чтобы исключить из проверки все файлы или каталоги с определенным именем, введите это имя в поле ввода.

Указывать путь к каталогу или файлу при этом не требуется;

- чтобы исключить из проверки файлы или каталоги определенного вида, введите определяющую их маску в поле ввода. Маска задает общую часть имени объекта. При этом:
  - символ «*» заменяет любую, возможно пустую последовательность символов;
  - символ «?» заменяет любой, но только один символ;
  - остальные символы маски ничего не заменяют и означают, что на данном месте в имени файла или каталога должен находиться именно этот символ.

  Пример:

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

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

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

Настройка действий

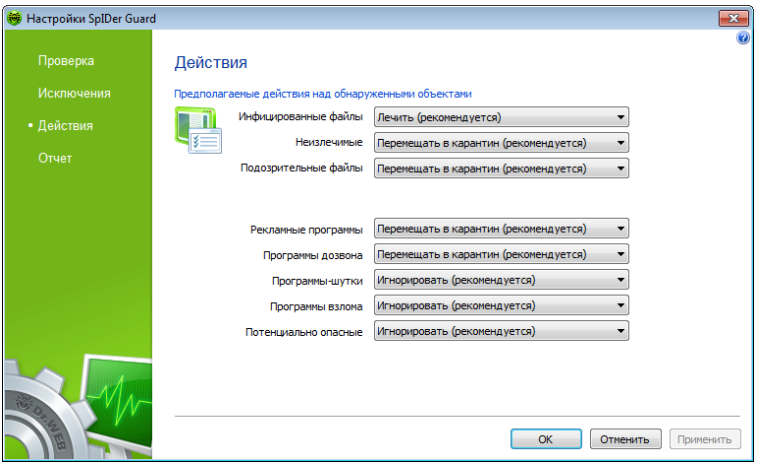
В разделе **Действия** вы можете настроить автоматические действия сторожа с зараженными объектами.

Состав доступных реакций зависит от типа вирусного события.

Реакции **Лечить**, **Перемещать в карантин, Игнорировать** и **Удалить** аналогичны таким же реакциям **Сканера**. Действия с обнаруженными угрозами рассмотрены в п. Действия при обнаружении вирусов.

Изменение настроек сторожа

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



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

в карантин.

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

Раздел Отчет

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

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

Отчет сторожа **SpIDer Guard** хранится в файле spiderg3.log, расположенном в каталоге %allusersprofile%\Application Data\Doctor Web\Logs\ (в Windows 7, %allusersprofile%\Doctor Web\Logs).

6. SpIDer Mail

Почтовый сторож **SpIDer Mail** 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.

При настройках по умолчанию **SpIDer Mail** 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.

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.

SpIDer Mail постоянно находится в оперативной памяти компьютера и по умолчанию запускается при загрузке операционной системы автоматически. Вы можете изменить режим автоматического запуска в общих настройках работы программы **Антивирус Dr.Web** или на некоторое время приостановить работу почтового сторожа.

Принцип работы почтового сторожа

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. Настройка SpIDer Mail):

- из зараженных писем удаляется вредоносная информация (лечение);
- письма с подозрительными объектами перемещаются в виде отдельных файлов в карантин, почтовой программе посылается сообщение об этом;
- 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, пользователь оповещается об отказе отправить письмо (как правило, почтовая программа при этом его сохранит).

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.

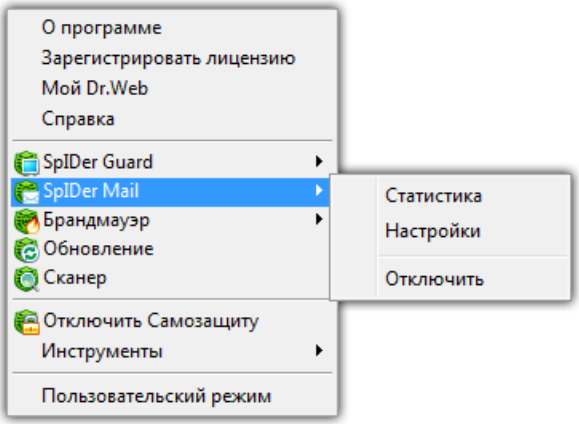
Сканер Dr.Web также может обнаруживать вирусы в почтовых ящиках некоторых форматов, однако почтовый сторож **SpIDer Mail** имеет перед **Сканером** ряд преимуществ:

- далеко не все форматы почтовых ящиков популярных программ поддерживаются **Сканером**; напротив, при использовании почтового сторожа зараженные письма даже не попадают в почтовые ящики;
- **Сканер** проверяет почтовые ящики, но только по запросу пользователя или по расписанию, а не в момент получения почты, причем данное действие является чрезвычайно ресурсоемким 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.

6.1. Управление SpIDer Mail

Основные средства настройки и управления почтовым сторожем **SpIDer Mail** находятся в подменю **SpIDer Mail**, которое открывается по щелчку на значке **SpIDer Agent** в области уведомлений Windows.



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

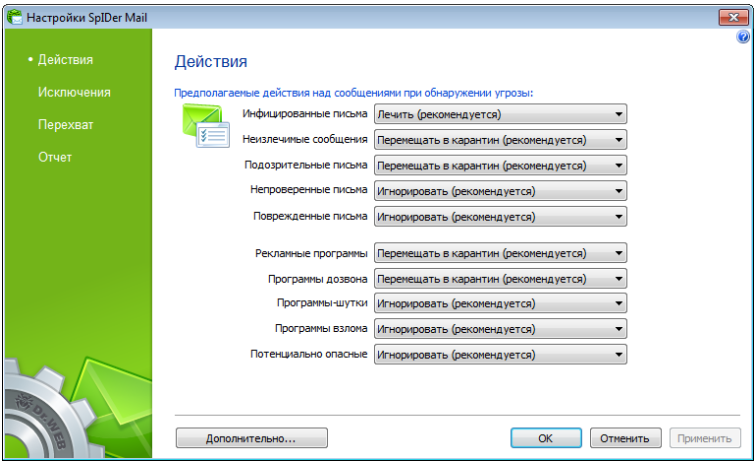
При выборе пункта **Настройки** открывается окно настроек почтового сторожа (см. Настройка SpIDer Mail).

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

Пункт **Настройки** доступен только в Административном режиме.

6.2. Настройка SpIDer Mail

Основные параметры работы почтового сторожа **SpIDer Mail** сосредоточены в разделах окна **Настройки SpIDer Mail** (см. ниже). 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.



Изменение настроек сторожа

1. Щелкните значок **SpIDer Agent** в области уведомлений Windows и выберите в подменю **SpIDer Mail** пункт **Настройки**.
2. Внесите необходимые изменения в разделах настроек.
3. Чтобы получить информацию о настройках, расположенных в разделе, нажмите кнопку **Справка** .
4. По окончании редактирования настроек:
   - чтобы сохранить изменения, нажмите кнопку **ОК**;

- чтобы отказаться от внесенных изменений, нажмите кнопку **Отмена**.

Настройка действий над сообщениями при обнаружении угрозы

Вы можете настроить реакцию программы в разделе **Действия**.

Реакция программы для каждого типа угрозы выбирается в выпадающих списках. Рекомендуется установить следующие действия:

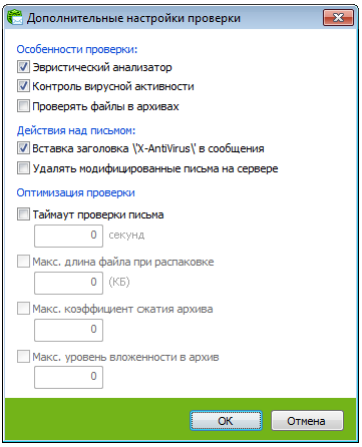
- для **Инфицированных писем** – действие **Лечить**;
- для **Неизлечимых сообщений** и **Подозрительных** – действие **Перемещать в карантин**;
- для **Непроверенных** и **Поврежденных писем –** действие **Игнорировать**;
- для рекламных программ и программ дозвона – действие **Перемещать в карантин**;
- для программ-шуток, программ взлома и потенциально опасных программ – действие **Игнорировать**.

Защиту от подозрительных писем можно отключать только в том случае, когда компьютер 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 **Перемещать в карантин**. Файлы с перемещенными письмами в этом случае рекомендуется проверить **Сканером**.

Также вы можете перейти в режим, в котором удаленные или перемещенные программой письма также немедленно удаляются на POP3/IMAP4-сервере. Для этого установите флаг **Удалять модифицированные письма на сервере** в дополнительных настройках.

Для доступа к дополнительным настройкам сканирования нажмите кнопку **Дополнительно**.



В открывшемся диалоговом окне вы можете настроить особенности проверки, действия над письмом, а также оптимизацию сканирования:

- **Таймаут проверки письма** - максимальное время, в течение которого письмо проверяется. По истечении указанного времени проверка письма прекращается;
- **Максимальную длину файла при распаковке**. Если программа определяет, что после распаковки архив будет больше указанной длины, проверка и распаковка производиться не будет;
- **Максимальный коэффициент сжатия архива**. Если программа определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка производиться не будут;
- **Максимальный уровень вложенности в архив**. Если уровень вложенности в архив превышает указанный, проверка будет производиться только до указанного уровня вложенности.

Раздел Исключения

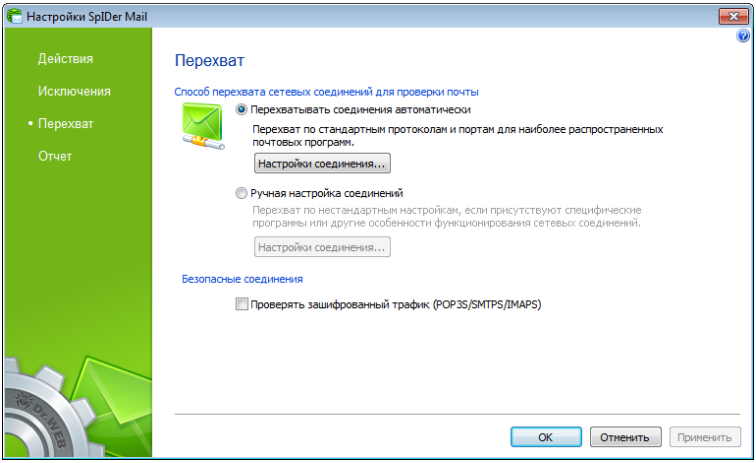
По умолчанию почтовый сторож **SpIDer Mail** автоматически перехватывает почтовый трафик всех пользовательских

приложений на вашем компьютере. В этом разделе задается список приложений, почтовый трафик которых не будет перехватываться и, соответственно, анализироваться почтовым сторожем.

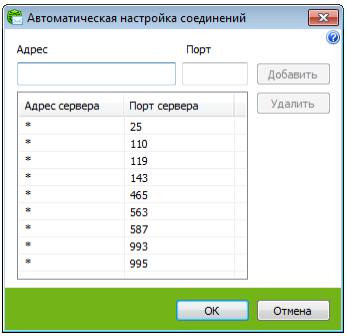
Чтобы добавить файл, папку или маску в список исключений, укажите необходимое имя в поле ввода и нажмите кнопку **Добавить**. Чтобы указать конкретный существующий каталог или файл, нажмите кнопку **Обзор** и выберите каталог или файл в стандартном окне открытия файла. Кнопка **Удалить** позволяет удалить из списка выбранное исключение.

Раздел Перехват

Управление перехватом соединений с почтовыми серверами сосредоточено в разделе **Перехват**.



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



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

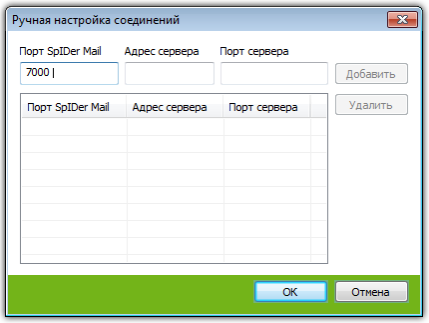
Для того чтобы удалить какой-либо элемент из списка, выберите его в списке и нажмите кнопку **Удалить**.

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 кнопку **Добавить**.

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

Настройка перехвата вручную

1. В приведенном выше окне выбора способа перехвата (см. выше) выберите вариант **Ручная настройка соединений** и нажмите кнопку **Настройки соединения**. 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 кнопку **Добавить**.
4. Повторите эти действия для каждого ресурса.
5. Нажмите кнопку **ОК**.

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.

Безопасные соединения

Вы можете включить в проверку данные, передаваемые по безопасным протоколам POP3S, SMTPS, IMAPS. Для этого установите флажок **Проверять зашифрованный трафик (POP3S/SMTPS/IMAPS)** в разделе **Безопасные соединения**. Если клиент, который получает и передает такие данные, не обращается к хранилищу сертификатов системы Windows, то необходимо будет экспортировать сертификат.

Раздел Отчет

Вы можете задать одну из следующих степеней детальности ведения отчета:

- **Стандартный** – в данном режиме в отчете фиксируются только наиболее значимые события, такие как проведение обновлений, запуск и останов почтового сторожа **SpIDer Mail** и вирусные события. Данный режим ведения отчета подходит для большинства применений;
- **Расширенный** – в данном режиме в отчете помимо общих событий фиксируются параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов;
- **Отладочный** – в данном режиме в отчете фиксируется максимальное количество информации о работе сторожа **SpIDer Mail**, что может привести к значительному увеличению файла отчета и снизить производительность работы операционной системы.

Отчет почтового сторожа **SpIDer Mail** записывается в файл netfilter.log, который находится в каталоге %allusersprofile% \Application Data\Doctor Web\Logs\ (в Windows 7, %allusersprofile%

\Doctor Web\Logs\).

7. Dr.Web для Outlook

Основные функции компонента

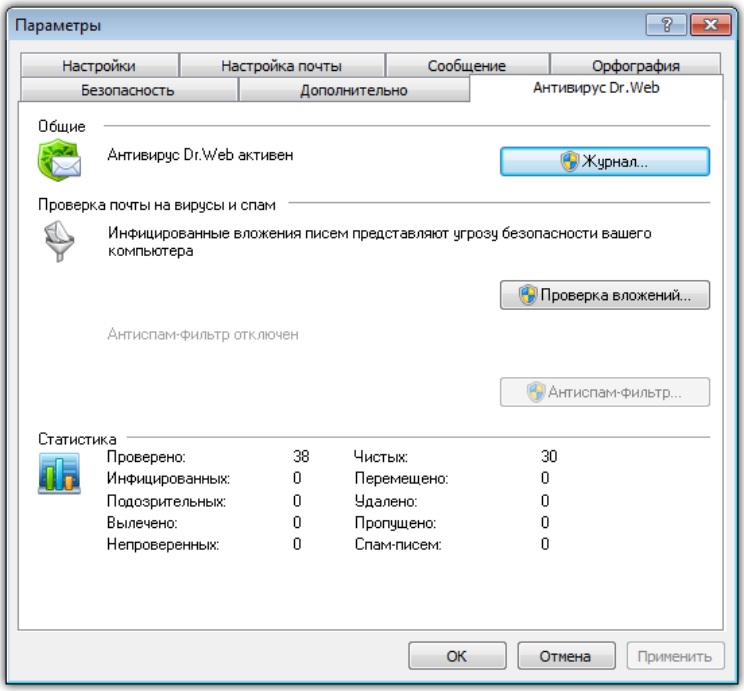
Подключаемый модуль **Dr.Web для Outlook** выполняет следующие функции:

- антивирусная проверка вложенных файлов почтовых сообщений;
- проверка почты, поступающей по зашифрованному соединению SSL;
- обнаружение и нейтрализация вредоносного программного обеспечения;
- использование эвристического анализатора для дополнительной защиты от неизвестных вирусов.

7.1. Настройка Dr.Web для Outlook

Настройка параметров и просмотр статистики работы программы осуществляется в почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web** (для Microsoft Outlook 2010 в разделе **Файл** → **Параметры** → **Надстройки** необходимо выбрать модуль **Dr.Web для Outlook** и нажать кнопку **Параметры надстройки**).

Вкладка **Антивирус Dr.Web** в настройках приложения Microsoft Outlook доступна только при наличии у пользователя прав, позволяющих изменять данные настройки.



На вкладке **Антивирус Dr.Web** отображается текущее состояние защиты (включена/выключена). Кроме того, она предоставляет доступ к следующим функциям программы:

- Журнал – позволяет настроить регистрацию событий программы;
- Проверка вложений – позволяет настроить проверку электронной почты и определить действия программы для обнаруженных вредоносных объектов;
- Статистика – показывает данные об объектах, проверенных и обработанных программой.

7.2. Обнаружение угроз

Dr.Web для Outlook использует различные методы обнаружения вирусов и других угроз безопасности компьютера. К найденным вредоносным объектам применяются определяемые пользователем действия: лечение инфицированных объектов, удаление или перемещение в Карантин для их изоляции и безопасного хранения.

7.2.1. Вредоносные объекты

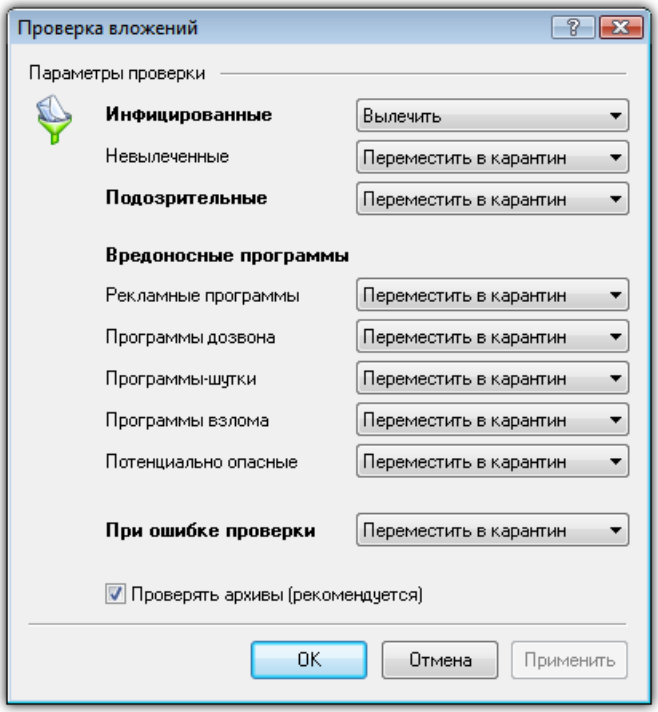
Dr.Web для Outlook обнаруживает следующие вредоносные объекты:

- инфицированные объекты;
- файлы-бомбы или архивы-бомбы;
- рекламные программы;
- программы взлома;
- программы дозвона;
- программы-шутки;
- потенциально опасные программы;
- шпионские программы;
- троянские программы;
- компьютерные черви и вирусы.

7.2.2. Действия

Dr.Web для Outlook позволяет задать реакцию программы на обнаружение зараженных или подозрительных файлов и вредоносных программ при проверке вложений электронной почты.

Чтобы настроить проверку вложений и определить действия программы для обнаруженных вредоносных объектов, в почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web** нажмите кнопку **Проверка вложений** (для Microsoft Outlook 2010 в разделе **Файл** → **Параметры** → **Надстройки** необходимо выбрать модуль **Dr.Web для Outlook** и нажать кнопку **Параметры надстройки**).



Окно **Проверка вложений** доступно только при наличии у пользователя прав администратора системы.

Для ОС Windows Vista и старше при нажатии кнопки **Проверка вложений**:

- При включенном UAC: администратору будет выдан запрос на подтверждение действий программы, пользователю без административных прав будет выдан запрос на ввод учетных данных администратора системы;
- При выключенном UAC: администратор сможет изменять настройки программы, пользователь не сможет получить доступ к изменению настроек.

В окне **Проверка вложений** вы можете задать действия программы для различных категорий проверяемых объектов, а также для случая, когда при проверке возникли ошибки. Кроме того, вы можете включить или выключить проверку архивов.

Для задания действий над обнаруженными вредоносными объектами служат следующие настройки:

- Выпадающий список **Инфицированные** задает реакцию на обнаружение объектов, зараженных известными и (предположительно) излечимыми вирусами;
- Выпадающий список **Невылеченные** задает реакцию на обнаружение объектов, зараженных известным неизлечимым вирусом, а также когда предпринятая попытка излечения не принесла успеха.
- Выпадающий список **Подозрительные** задает реакцию на обнаружение объектов, предположительно зараженных вирусом (срабатывание эвристического анализатора).
- Раздел **Вредоносные программы** задает реакцию на обнаружение следующего нежелательного ПО:
    - рекламные программы;
    - программы дозвона;
    - программы шутки;

  - программы взлома;
  - потенциально опасные.
- Выпадающий список **При ошибке проверки** позволяет настроить действия программы в случае, если проверка вложения невозможна, например, если оно представляет собой поврежденный или защищенный паролем файл.
- Флаг **Проверка архивов** позволяет включить или отключить проверку вложенных файлов, представляющих собой архивы. Установите данный флаг для включения проверки, снимите - для отключения.

Состав доступных реакций зависит от типа вирусного события.

Предусмотрены следующие действия над обнаруженными объектами:

- **Вылечить** (действие доступно только для инфицированных объектов) – означает, что программа предпримет попытку вылечить инфицированный объект;
- **Как для невылеченных** (действие доступно только для инфицированных объектов) – означает, что к инфицированному вложению будет применено действие, выбранное для невылеченных объектов;
- **Удалить** – означает, что объект будет удален;
- **Переместить в карантин** – означает, что объект будет изолирован в каталоге Карантина;
- **Пропустить** – означает, что объект будет пропущен без изменений.

7.4. Регистрация событий

Dr.Web для Outlook регистрирует ошибки и происходящие события в следующих журналах регистрации:

- журнал регистрации событий операционной системы (Event Log);
- текстовый журнал отладки.

7.4.1. Журнал операционной системы

В журнал регистрации событий операционной системы (Event Log) заносится следующая информация:

- сообщения о запуске и остановке программы;
- параметры лицензионного ключевого файла: действительность или недействительность лицензии, срок действия лицензии (информация заносится при запуске программы, в процессе ее работы и при замене лицензионного ключевого файла);
- параметры модулей программы: сканера, ядра, вирусных баз (информация заносится при запуске программы и при обновлении модулей);
- сообщение о недействительности лицензии: отсутствие ключевого файла, отсутствие в ключевом файле разрешения на использование модулей программы, лицензия заблокирована, нарушение целостности ключевого файла (информация заносится при запуске программы и в процессе ее работы);
- сообщения об обнаружении вирусов;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).

Просмотр журнала регистрации событий операционной системы

1. Откройте **Панель управления** операционной системы.
2. Выберите раздел **Администрирование** → **Просмотр Событий**.
3. В левой части окна **Просмотр Событий** выберите пункт **Приложение**. Откроется список событий, зарегистрированных в журнале пользовательскими приложениями. Источником сообщений **Dr.Web для Outlook** является приложение **Dr.Web for Outlook**.

7.4.2. Текстовый журнал отладки

В текстовый журнал отладки заносится следующая информация:

- сообщения о действительности или недействительности лицензии;
- сообщения об обнаружении вирусов;
- сообщения об ошибках записи или чтения файлов, ошибках анализа архивов или файлов, защищенных паролем;
- параметры модулей программы: сканера, ядра, вирусных баз;
- сообщения об экстренных остановках ядра программы;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).

Ведение текстового журнала программы приводит к снижению быстродействия системы, поэтому рекомендуется включать регистрацию событий только в случае возникновения ошибок работы **Dr.Web для Outlook**.

Настройка регистрации событий

1. На вкладке **Антивирус Dr.Web** нажмите кнопку **Журнал**. Откроется окно настроек журнала.
2. Выберите уровень детализации (от 0 до 5) для записи событий:
   - уровень 0 означает, что регистрация событий в текстовом журнале отладки не ведется;
   - уровень 5 соответствует максимальной детализации регистрируемых событий.

   По умолчанию регистрация событий отключена.
3. Задайте максимальный размер (в килобайтах) файла журнала.
4. Нажмите кнопку **ОК** для сохранения изменений.

Окно **Журнал** доступно только при наличии у пользователя прав администратора системы.

Просмотр журнала событий

Для просмотра текстового журнала событий программы нажмите кнопку **Показать в папке**. Откроется каталог, в котором хранится журнал.

7.5. Статистика проверки

В почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web** (для Microsoft Outlook 2010 в разделе **Файл** → **Параметры** → **Надстройки** необходимо выбрать модуль **Dr.Web для Outlook** и нажать кнопку **Параметры надстройки**) содержится статистическая информация об общем количестве объектов, проверенных и обработанных программой.

Объекты разделяются на следующие категории:

- **Проверено** – общее количество проверенных писем;
- **Инфицированных** – количество писем, содержащие вирусы;
- **Подозрительных** – количество писем, предположительно зараженных вирусом (срабатывание эвристического анализатора);
- **Вылечено** – количество объектов, успешно вылеченных программой;
- **Непроверенных** – количество объектов, проверка которых невозможна или при проверке которых возникли ошибки;
- **Чистых** – количество писем, не содержащих вредоносных объектов.

Затем указывается количество объектов, к которым были применены действия:

- **Перемещено** – количество объектов, перемещенных в Карантин;
- **Удалено** – количество объектов, удаленных из системы;
- **Пропущено** – количество объектов, пропущенных без изменений.

По умолчанию статистика сохраняется в файле `drwebforoutlook.stat`, который находится в каталоге %USERPROFILE%\DoctorWeb (в Windows 7, C:\Users\<*имя пользователя*>\DoctorWeb).

Файл статистики drwebforoutlook.stat ведется отдельно для каждого пользователя системы.

8. Брандмауэр Dr.Web

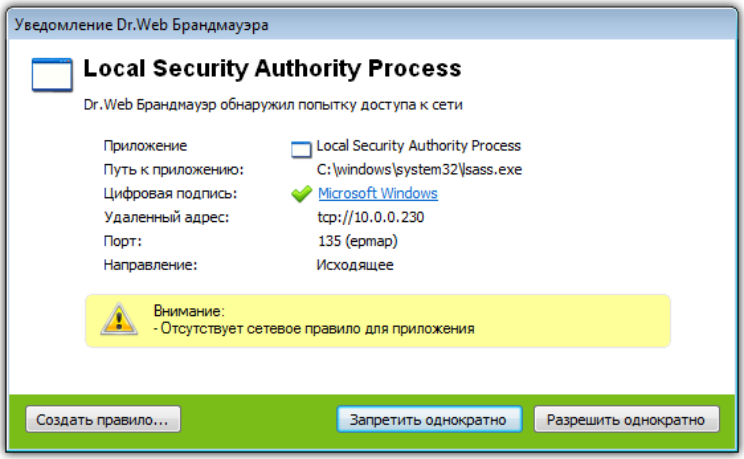
Dr.Web® Брандмауэр предназначен для защиты вашего компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети. Этот компонент позволяет вам контролировать подключение и передачу данных по сети Интернет и блокировать подозрительные соединения на уровне пакетов и приложений.

Брандмауэр предоставляет вам следующие преимущества:

- контроль и фильтрация всего входящего и исходящего трафика;
- контроль подключения на уровне приложений;
- фильтрация пакетов на сетевом уровне;
- быстрое переключение между наборами правил;
- регистрация событий.

8.1. Обучение Брандмауэра

После установки **Брандмауэра** некоторое время в процессе вашей работы за компьютером производится обучение программы. При обнаружении попытки со стороны операционной системы или пользовательских приложений подключиться к сети **Брандмауэр** проверяет, заданы ли для этих программ правила фильтрации, и, если правила отсутствуют, выводит соответствующее предупреждение:



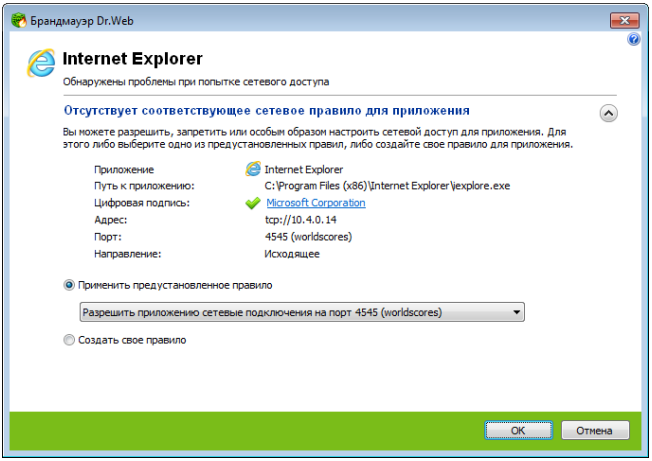
При работе под ограниченной учетной записью (Гость) **Брандмауэр Dr.Web** не выдает пользователю предупреждения о попытках доступа к сети. Предупреждения будут выдаваться под учетной записью с правами администратора, если такая сессия активна одновременно с гостевой.

Обработка сообщений

1. При обнаружении попытки подключения к сети со стороны приложения, ознакомьтесь со следующей информацией:

Поле	Описание
Приложение	Наименование программы. Удостоверьтесь, что путь к нему, указанный в поле **Путь к приложению**, соответствует правильному расположению программы.
Путь к приложению	Полный путь к исполняемому файлу приложения и его имя.
Цифровая подпись	Цифровая подпись приложения.
Целевой адрес	Протокол и адрес хоста, к которому совершается попытка подключения.
Порт	Порт, по которому совершается попытка подключения.
Направление	Тип соединения.

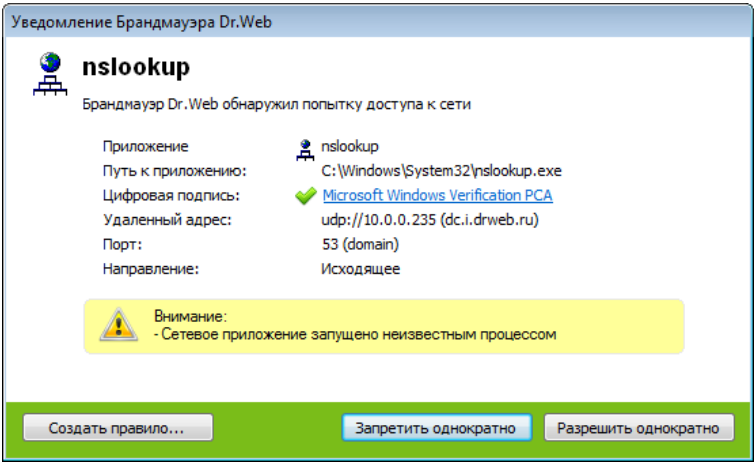
2. Примите решение о подходящей для данного случая операции и выберите соответствующее действие в нижней части окна:
   - чтобы однократно блокировать данное подключение, выберите действие **Запретить однократно**;
   - чтобы однократно позволить приложению данное подключение, выберите действие **Разрешить однократно**;
   - чтобы перейти к форме создания правила фильтрации, выберите действие **Создать правило**. Откроется окно, в котором вы можете либо выбрать предустановленное правило, либо вручную создать правило для приложений.



3. Нажмите кнопку **OK**. **Брандмауэр** выполнит указанную вами операцию, и окно оповещения будет закрыто.

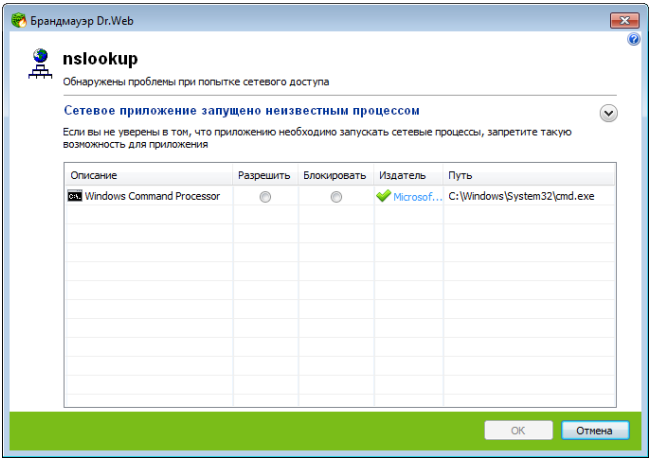
Для создания правил необходимы права администратора.

В случаях, когда программа, осуществляющая попытку подключения, уже известна **Брандмауэру** (то есть для нее заданы правила фильтрации), но запускается другим неизвестным приложением (родительским процессом), **Брандмауэр** выводит соответствующее предупреждение:



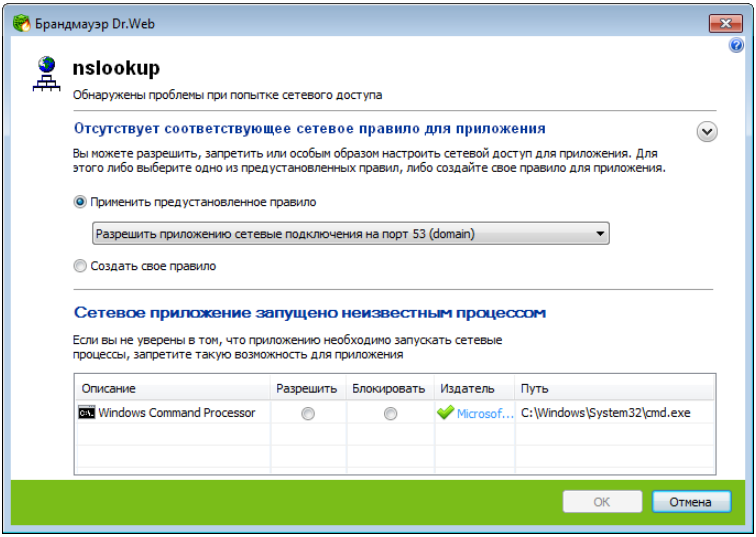
Правила для родительских процессов

1. При обнаружении попытки подключения к сети со стороны приложения, запущенного неизвестной для **Брандмауэра** программой, ознакомьтесь с информацией об исполняемом файле родительской программы.
2. Когда вы примете решение о подходящей для данного случая операции, выполните одно из следующий действий:
   - чтобы однократно блокировать подключение приложения к сети, нажмите кнопку **Запретить**;
   - чтобы однократно позволить приложению подключиться к сети, нажмите кнопку **Разрешить**;
   - чтобы создать правило, нажмите **Создать правило** и в открывшемся окне задайте необходимые настройки для родительского процесса.



3. **Брандмауэр** выполнит указанную вами операцию, и окно оповещения будет закрыто.

Также возможна ситуация, при которой неизвестное приложение запускается другим неизвестным приложением, в таком случае в предупреждении будет выведена соответствующая информация и при выборе **Создать правило** откроется окно, в котором вы можете настроить правила и для приложений, и для родительских процессов:

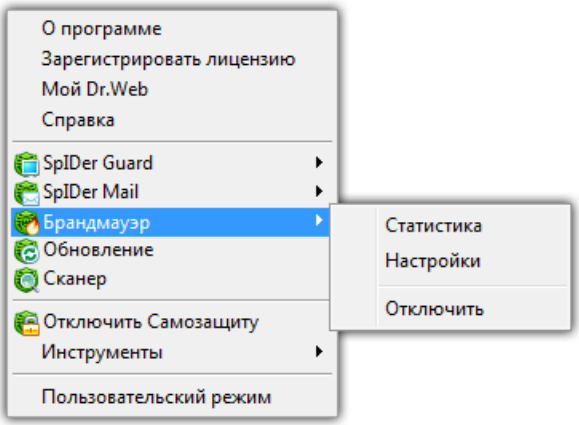

Брандмауэр Dr.Web
nslookup
Обнаружены проблемы при попытке сетевого доступа
Отсутствует соответствующее сетевое правило для приложения
Вы можете разрешить, запретить или особым образом настроить сетевой доступ для приложения. Для этого либо выберите одно из предустановленных правил, либо создайте свое правило для приложения.
Применить предустановленное правило
Разрешить приложению сетевые подключения на порт 53 (domain)
Создать свое правило
Сетевое приложение запущено неизвестным процессом
Если вы не уверены в том, что приложению необходимо запускать сетевые процессы, запретите такую возможность для приложения
Описание
Разрешить
Блокировать
Издатель
Путь
Windows Command Processor
Microsof...
C:\Windows\System32\cmd.exe
OK
Отмена

8.2. Управление Брандмауэром

Брандмауэр устанавливается как компонент сетевого подключения и запускается автоматически при загрузке операционной системы. При необходимости вы можете временно приостановить работу **Брандмауэра**, просмотреть статистику фильтрации и изменить настройки программы.

После открытия сессии под ограниченной учетной записью (Гость) **Брандмауэр** выдаст сообщение об ошибке доступа. При этом в **SpIDer Agent** состояние **Брандмауэра** отображается как неактивное. Однако **Брандмауэр** включен и работает в соответствии с настройками по умолчанию или с настройками, заданными ранее в административном режиме.

Управление **Брандмауэром** осуществляется с помощью компонента **SpIDer Agent**:



Управление Брандмауэром

1. Щелкните значок **SpIDer Agent** в области уведомлений Windows и выберите пункт **Брандмауэр**.
2. В открывшемся меню выберите необходимый пункт:

Пункт	Описание
Статистика	Выберите этот пункт, чтобы открыть окно со сведениями об обработанных **Брандмауэром** событиях.
Настройки	Выберите этот пункт, чтобы получить доступ к основной части настраиваемых параметров программы. На странице **Сброс настроек** окна настройки **Брандмауэра** вы можете восстановить параметры работы программы, используемые по умолчанию.
Отключить	Выберите этот пункт, чтобы временно отключить межсетевой экран. Временное отключение доступно только пользователю, обладающему правами администратора. Прибегайте к этой возможности с осторожностью.
Запустить	Выберите этот пункт, чтобы запустить отключенный межсетевой экран. Этот пункт появляется в меню в том случае, когда работа **Брандмауэра** была временно приостановлена.

При отключении **Брандмауэра** запрашивается код подтверждения.

Пункты **Настройки, Отключить/Запустить** доступны только в Административном режиме.

8.3. Настройка Брандмауэра

Настройки **Брандмауэра** недоступны в пользовательском режиме.

Для начала работы с **Брандмауэром** необходимо:

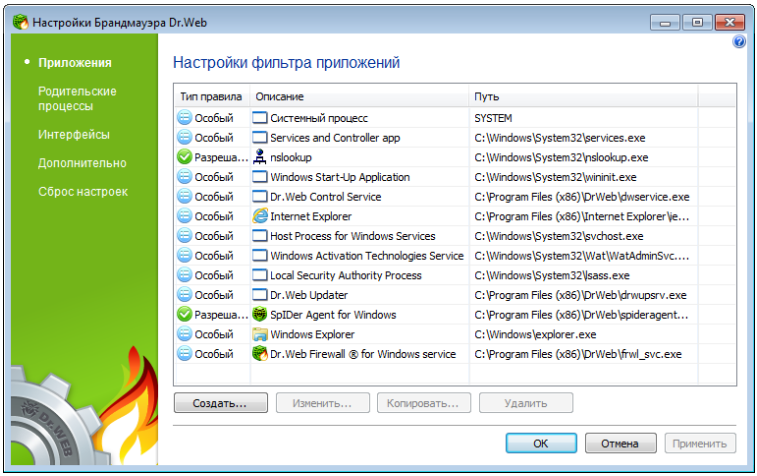
- выбрать режим работы программы;
- настроить список авторизованных приложений.

После перезагрузки операционной системы, если не выбрано иное, **Брандмауэр** начнет работу в режиме обучения. Вне зависимости от режима работы автоматически начнется регистрация событий.

В случае возникновения проблем с общим доступом к подключению Интернета (т.е. блокируется доступ в Интернет с компьютеров, подключенных к узловому), настройте на узловом компьютере правило для пакетного фильтра, разрешающее все пакеты из подсети, согласно вашим локальным настройкам.

8.3.1. Фильтр приложений

Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам. Вы можете задавать правила как для пользовательских, так и для системных приложений.



На странице **Настройки фильтра приложений** (раздел **Приложения**) вы можете формировать наборы правил фильтрации, создавая новые, редактируя существующие или удаляя ненужные правила. Приложение однозначно идентифицируется полным путем к исполняемому файлу. Для указания ядра операционной системы Microsoft Windows (процесс system, для которого нет соответствующего исполняемого файла) используется имя SYSTEM.

Если файл приложения, для которого было создано правило, изменился (например, было установлено обновление), то **Брандмауэр** предложит подтвердить, что приложение может обращаться к сетевым ресурсам.

Формирование набора правил

Для формирования набора правил выполните одно из следующий действий:

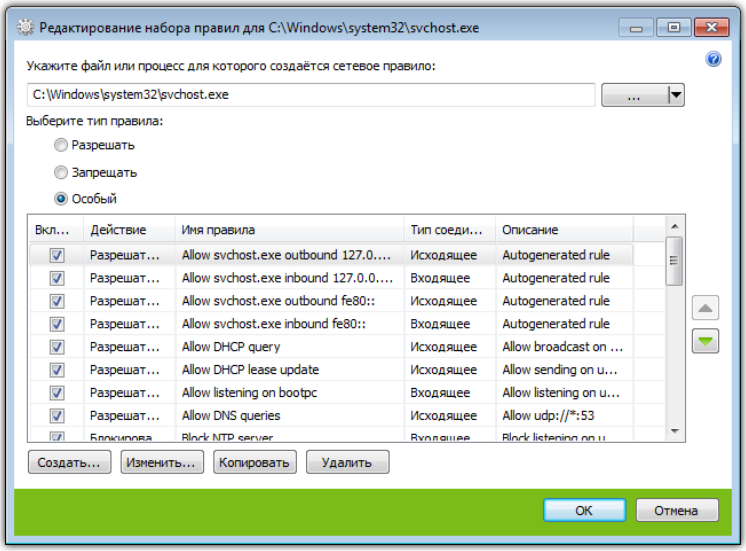
- чтобы создать набор правил для новой программы, нажмите кнопку **Создать**;
- чтобы отредактировать существующий набор правил, выберите его в списке и нажмите кнопку **Изменить**;
- чтобы добавить копию существующего набора правил, нажмите кнопку **Копировать**. Копия добавляется под выбранным набором;
- чтобы удалить все правила для программы, выберите соответствующий набор в списке и нажмите кнопку **Удалить**.

Для каждой программы может быть не более одного набора правил фильтрации.

Правила для приложений

В окне **Создание нового набора правил** (или **Редактирование набора правил**) отображается тип правила для конкретного приложения или процесса, а также список правил, если выбран тип правила **Особый**. Вы можете изменять тип правила, формировать список, добавляя новые или редактируя существующие правила фильтрации, а также изменяя порядок их выполнения. Правила применяются последовательно, согласно очередности в списке.

Вы можете создать правило при помощи окна настроек **Брандмауэра**. При работе в режиме обучения вы можете инициировать создание правила непосредственно из окна оповещения о попытке несанкционированного подключения.

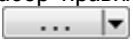
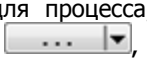


Для каждого правила в списке предоставляется следующая краткая информация:

Параметр	Описание
Включено	Состояние правила.
Действие	Указывает на действие, выполняемое **Брандмауэром** при попытке программы подключиться к сети Интернет: • **Блокировать пакеты** – блокировать попытку подключения; • **Разрешать пакеты** – разрешить подключение.
Имя правила	Название правила.
Тип соединения	Указывает на инициатора подключения: • **Входящее** – правило применяется, если инициируется подключение из сети к программе на вашем компьютере;

Параметр	Описание
	• **Исходящее** – правило применяется, если подключение инициирует программа на вашем компьютере; • **Любое** – правило применяется вне зависимости от того, кто является инициатором подключения.
Описание	Пользовательское описание правила.

Редактирование правил

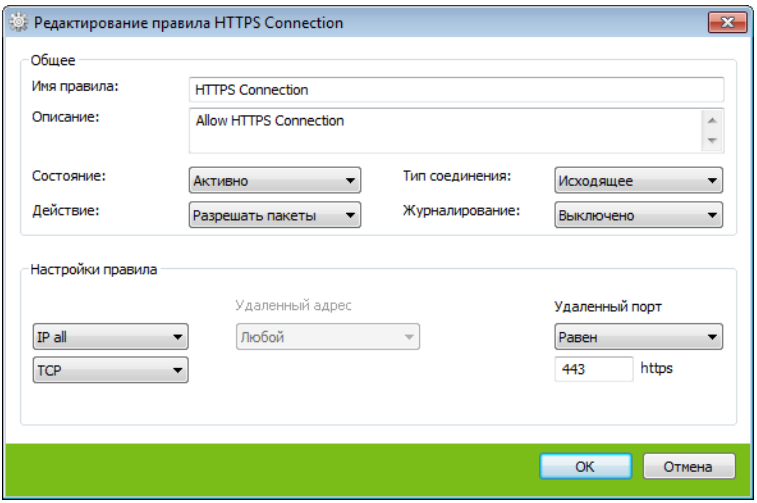
1. Если на странице **Настройки фильтра приложений** вы выбрали создание или редактирование набора правил, в открывшемся окне задайте программу или процесс, для которых будет применяться набор правил. Для этого выполните одно из следующих действий:
   - чтобы задать набор правил для программы, нажмите кнопку **Обзор**  и выберите исполняемый файл программы;
   - чтобы задать набор правил для процесса, нажмите стрелку на кнопке **Обзор**  , выберите **Запущенное приложение** и укажите процесс;
2. Выберите тип правила:
   - **Разрешать** – все соединения приложения будут разрешены;
   - **Запрещать** – все соединения приложения запрещены;
   - **Особый** – в этом режиме вы можете создать набор правил, разрешающих или запрещающих те или иные соединения приложения.
3. Если вы выбрали тип правила **Особый**, создайте набор правил для приложения используя следующие опции:
   - чтобы добавить новое правило, нажмите кнопку **Создать**. Правило добавляется в конец списка;
   - чтобы отредактировать выбранное правило, нажмите кнопку **Изменить**;

- чтобы добавить копию выбранного правила, нажмите кнопку **Копировать**. Копия добавляется после выбранного правила;
- чтобы удалить выбранное правило, нажмите кнопку **Удалить**.

4. Если вы выбрали создание нового или редактирование существующего правила, настройте его параметры в отобразившемся окне.
5. По окончании редактирования списка нажмите кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отмена** для отказа от изменений.

Настройка параметров правила

Правила фильтрации регулируют сетевое взаимодействие программы с конкретными хостами сети.



Создание правила

1. Задайте следующие параметры правила:

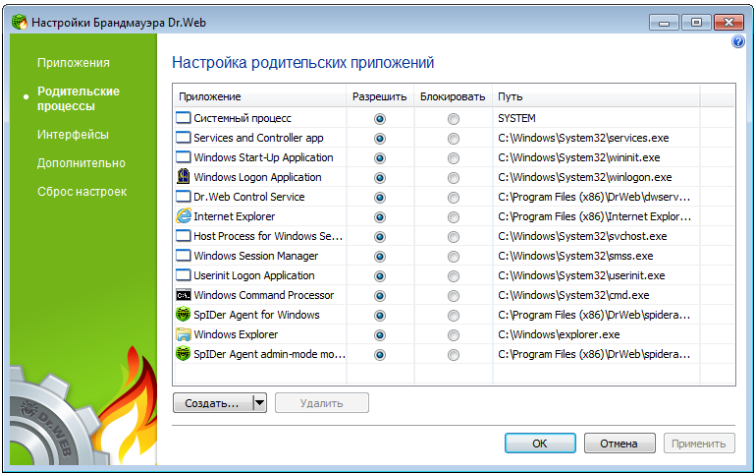
Параметр	Описание
Общее	
Имя правила	Имя создаваемого/редактируемого правила.
Описание	Краткое описание правила.
Состояние	Состояние правила: • **Активно** – правило применяется; • **Неактивно** – правило временно не применяется.
Тип соединения	Инициатор подключения: • **Входящее** – правило применяется, если инициируется подключение из сети к программе на вашем компьютере; • **Исходящее** – правило применяется, если подключение инициирует программа на вашем компьютере; • **Любое** – правило применяется вне зависимости от того, кто является инициатором подключения.
Действие	Указывает на действие, выполняемое **Брандмауэром** при попытке программы подключиться к сети Интернет: • **Блокировать пакеты** – блокировать попытку подключения; • **Разрешать пакеты** – разрешить подключение.
Настройки правила	
Протокол	Протоколы сетевого и транспортного уровня, по которым осуществляется подключение. Поддерживаются следующие протоколы сетевого уровня: • **IPv4**;

Параметр	Описание
	• **IPv6**; • **IP all** - протокол IP любой версии. Поддерживаются следующие протоколы транспортного уровня: • **TCP**; • **UDP**; • **TCP & UDP** - протокол TCP или UDP.
Входящий/ Исходящий адрес	IP-адрес удаленного хоста, участвующего в подключении. Вы можете указывать как конкретный адрес (**Равен**), так и диапазон адресов (**В диапазоне**), а также маску конкретной подсети (**Маска**) или маски всех подсетей, в которых ваш компьютер имеет сетевой адрес (**MY_NETWORK**). Чтобы задать правило для всех хостов, выберите вариант **Любой**.
Входящий/ Исходящий порт	Порт, по которому осуществляется подключение. Вы можете указывать как конкретный порт (**Равен**), так и диапазон портов (**В диапазоне**). Чтобы задать правило для всех портов, выберите вариант **Любой**.

2. По окончании редактирования нажмите кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отмена** для отказа от изменений.

8.3.2. Родительские процессы

Чтобы разрешить или запретить процессам и приложениям запускать другие приложения, в разделе **Родительские процессы** задайте необходимые правила.



Создание правил для родительских процессов

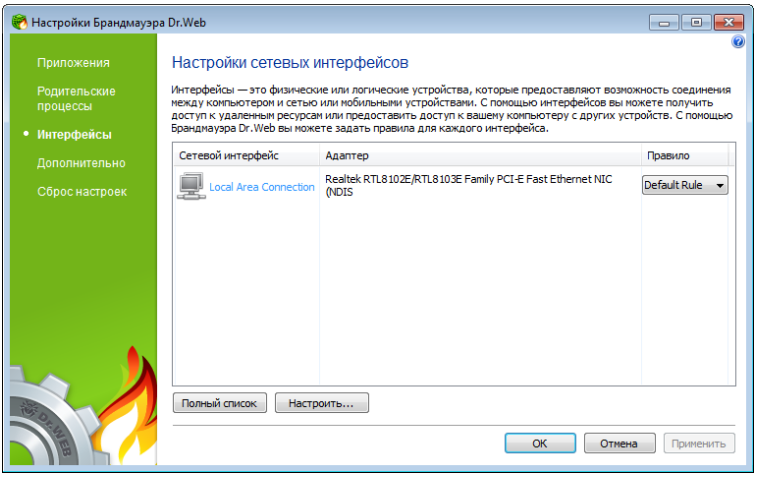
1. Выберите родительский процесс:
   - чтобы задать правило для программы, нажмите кнопку **Создать** и выберите исполняемый файл программы;
   - чтобы задать правило для процесса, нажмите стрелку на кнопке **Создать**, выберите **Запущенное приложение** и укажите процесс.
2. Установите необходимое действие:
   - **Блокировать**, чтобы запретить приложению запускать процессы;
   - **Разрешить**, чтобы разрешить приложению запускать процессы.

По умолчанию добавляемый родительский процесс блокируется.

Если файл родительского приложения, для которого было создано правило, изменился (например, было установлено обновление), то **Брандмауэр** предложит подтвердить, что приложение может запускать другие приложения.

8.3.3. Интерфейсы

На странице настроек сетевых интерфейсов (**Настройки сетевых интерфейсов**) вы можете указать, какой набор правил фильтрации применять для пакетов, передающихся через определенный сетевой интерфейс.



Набор правил для интерфейса

1. Чтобы задать набор правил фильтрации пакетов, передающихся через определенный интерфейс, в окне настроек **Брандмауэра** выберите раздел **Интерфейсы**.
2. Найдите в списке интересующий вас интерфейс и сопоставьте ему соответствующий набор правил. Если

подходящий набор правил отсутствует в списке, создайте его.

3. Чтобы сохранить настройки, нажмите кнопку **ОК**.

Для того чтобы увидеть все доступные интерфейсы, нажмите кнопку **Полный список**. В открывшемся окне вы можете указать, какие интерфейсы должны всегда отображаться в таблице. Активные интерфейсы будут отображаться в таблице автоматически.

Для того чтобы настроить правила для интерфейсов, нажмите кнопку **Настроить**.

Фильтр пакетов

Фильтрация на уровне пакетов позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение. Правила применяются ко всем сетевым пакетам определенного типа, которые передаются через один из сетевых интерфейсов вашего компьютера.

Данный вид фильтрации предоставляет вам общие механизмы контроля, в отличие от фильтра приложений.

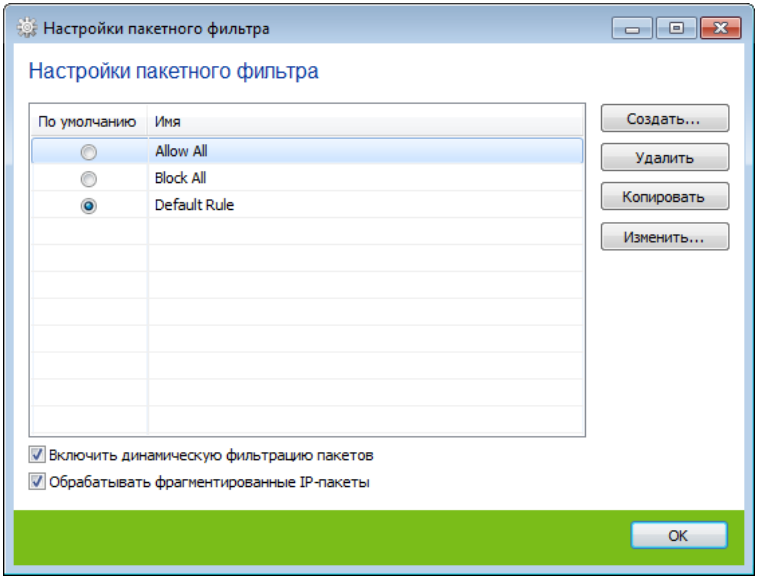
Брандмауэр поставляется со следующими предустановленными наборами правил:

- **Allow all** – все пакеты пропускаются;
- **Deny all** – все пакеты блокируются;
- **Default rule** – правила, описывающие наиболее часто встречающиеся конфигурации сети и распространенные атаки (используется по умолчанию для всех новых интерфейсов).

Для удобства использования и быстрого переключения между режимами фильтрации вы можете задать дополнительные наборы правил.

Набор правил для интерфейса

1. Чтобы задать параметры работы пакетного фильтра, в окне настроек **Брандмауэра** выберите раздел **Пакетный фильтр**.
2. На этой странице вы можете:
   - формировать наборы правил фильтрации, создавая новые, редактируя существующие или удаляя ненужные правила;
   - задать дополнительные параметры фильтрации.



Формирование набора правил

Для формирования набора правил выполните одно из следующий действий:

- чтобы создать набор правил для новой программы, нажмите кнопку **Создать**;

- чтобы отредактировать существующий набор правил, выберите его в списке и нажмите кнопку **Изменить**;
- чтобы добавить копию существующего набора правил, нажмите кнопку **Копировать**. Копия добавляется под выбранным набором;
- чтобы удалить выбранный набор правил, нажмите кнопку **Удалить**.

Дополнительные настройки

Чтобы задать общие настройки фильтрации пакетов, на странице **Настройки пакетного фильтра** установите следующие флажки:

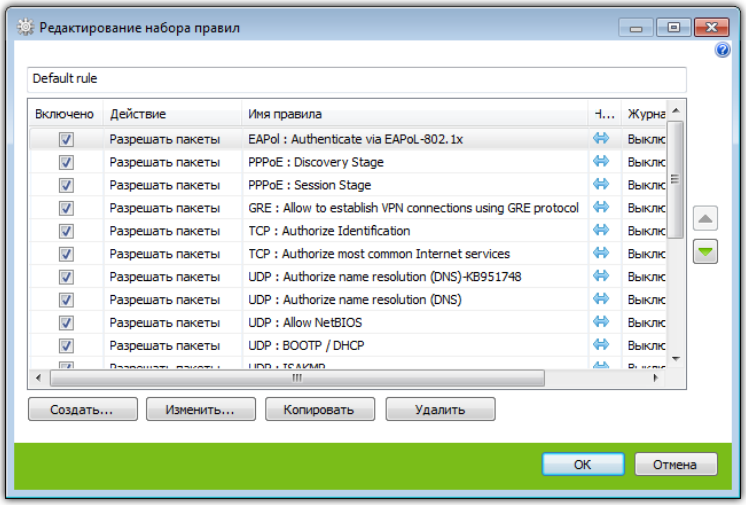
Флажок	Описание
Включить динамическую фильтрацию пакетов	Установите этот флажок, чтобы учитывать при фильтрации состояние TCP-соединения и пропускать только те пакеты, содержимое которых соответствует текущему состоянию. В таком случае все пакеты, передаваемые в рамках соединения, но не соответствующие спецификации протокола, блокируются. Этот механизм позволяет лучше защитить ваш компьютер от DoS-атак (отказ в обслуживании), сканирования ресурсов, внедрения данных и других злонамеренных операций. Также рекомендуется устанавливать этот флажок при использовании протоколов со сложными алгоритмами передачи данных (FTP, SIP и т.п.). Снимите этот флажок, чтобы фильтровать пакеты без учета TCP-соединений.

Флажок	Описание
Обрабатывать фрагментированные IP пакеты	Установите этот флажок, чтобы корректно обрабатывать передачу больших объемов данных. Размер максимального пакета (MTU – Maximum Transmission Unit) для разных сетей может варьироваться, поэтому часть IP-пакетов при передаче может быть разбита на несколько фрагментов. При использовании данной опции ко всем фрагментарным пакетам применяется одно и то же действие, предусмотренное правилами фильтрации для головного (первого) пакета. Снимите этот флажок, чтобы обрабатывать все пакеты по отдельности.

Набор правил

В окне **Редактирование набора правил** отображается список правил фильтрации пакетов, входящих в конкретный набор. Вы можете формировать список, добавляя новые или редактируя существующие правила фильтрации, а также изменяя порядок их выполнения. Правила применяются последовательно, согласно очередности в списке.

Вы можете формировать список, добавляя новые или редактируя существующие правила фильтрации, а также изменяя порядок их выполнения. Правила применяются последовательно, согласно очередности в списке.



Для каждого правила в списке предоставляется следующая краткая информация:

Параметр	Описание
Включено	Состояние правила.
Действие	Указывает на действие, выполняемое **Брандмауэром** при обработке пакета: • **Блокировать пакеты** – блокировать пакет; • **Разрешать пакеты** – передать пакет.
Имя правила	Имя правила.
Направление	Отправитель пакета: • – правило применяется, если принимается пакет из сети; • – правило применяется, если пакет отправляется с вашего компьютера; • – правило применяется вне зависимости от того, кто является отправителем пакета.
Журналирование	Режим регистрации событий. Указывает на то, какая информация должна быть занесена в отчет:

Параметр	Описание
	• **Только заголовки** – заносить в отчет только заголовки пакетов; • **Весь пакет** – заносить в отчет пакеты целиком; • **Выключено** – не сохранять информацию о пакете.
Описание	Краткое описание правила.

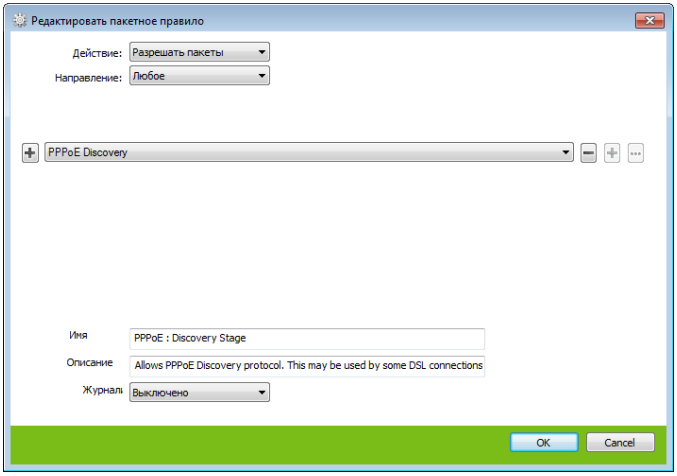
Редактирование набора правил

1. Если на странице **Настройки пакетного фильтра** вы выбрали создание или редактирование набора правил, в открывшемся окне задайте название набора правил.
2. Создайте правила фильтрации, используя следующие опции:
   - чтобы добавить новое правило, нажмите кнопку **Создать**. Правило добавляется в начало списка;
   - чтобы отредактировать выбранное правило, нажмите кнопку **Изменить**;
   - чтобы добавить копию выбранного правила, нажмите кнопку **Копировать**. Копия добавляется перед выбранным правилом;
   - чтобы удалить выбранное правило, нажмите кнопку **Удалить**.
3. Если вы выбрали создание нового или редактирование существующего правила, настройте его параметры.
4. Используйте стрелочки справа от списка, чтобы определить порядок выполнения правил. Правила выполняются последовательно, согласно очередности в списке.
5. По окончании редактирования списка нажмите кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отмена** для отказа от изменений.

Создание правил фильтрации

Добавление или редактирование правила фильтрации

1. В окне редактирования набора правил для пакетного фильтра нажмите кнопку **Создать** или кнопку **Изменить**. Откроется окно создания или редактирования правила пакетной фильтрации.



2. Задайте следующие параметры правила:

Параметр	Описание
Действие	Указывает на действие, выполняемое **Брандмауэром** при обработке пакета: • **Блокировать пакеты** – блокировать пакет; • **Разрешать пакеты** – передать пакет.
Направление	Отправитель пакета: • **Входящее** – правило применяется, если принимается пакет из сети;

Параметр	Описание
	• **Исходящее** – правило применяется, если пакет отправляется с вашего компьютера; • **Любое** – правило применяется вне зависимости от того, кто является отправителем пакета.
Заголовок пакета	Категория правила. Например, транспортный или сетевой протокол. Для некоторых заголовков доступны дополнительные поля.
Журналирование	Режим регистрации событий. Указывает на то, какая информация должна быть занесена в отчет: • **Только заголовки** – заносить в отчет только заголовки пакетов; • **Весь пакет** – заносить в отчет пакеты целиком; • **Выключено** – не сохранять информацию о пакете.
Имя правила	Имя создаваемого/редактируемого правила.
Описание	Краткое описание правила.

3. По окончании редактирования нажмите кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отмена** для отказа от изменений.

Настройка расширенных параметров фильтрации

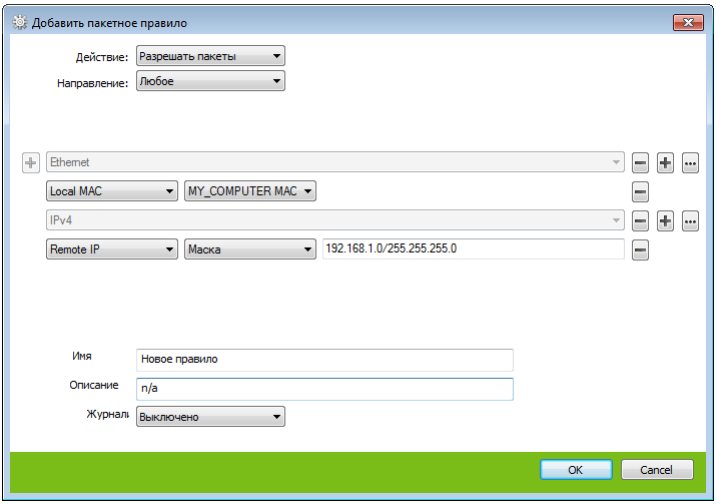
Для настройки расширенных параметров фильтрации вы можете использовать следующие возможности:

- чтобы добавить заголовок пакета выше или ниже используйте кнопки **Добавить**  слева и справа от заголовка пакета соответственно;

- чтобы настроить поля внутри заголовка, нажмите кнопку **Обзор** ;
- чтобы удалить заголовок или поля внутри заголовка используйте кнопку **Удалить** .

Кнопки **Добавить** и **Обзор** неактивны, если действие невозможно (например, когда для некоторого заголовка отсутствуют критерии фильтрации по полям внутри заголовка или невозможна фильтрация по заголовкам уровнем выше или ниже).

Пример правила для пакетного фильтра, которое разрешает передавать все пакеты из подсети:



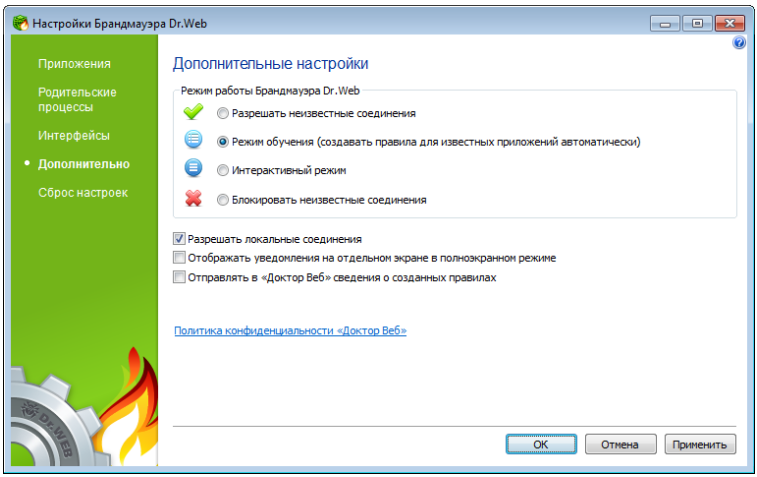
Если в данном правиле не указать поля внутри заголовка IPv4, правило сработает для любого пакета, содержащего заголовок IPv4 и отправленного с физического адреса локального

компьютера.

8.3.4. Дополнительные настройки

На странице **Дополнительные настройки** вы можете задать режим работы **Брандмауэра**, а также общие настройки фильтрации для всех приложений.

Режим работы задает реакцию **Брандмауэра** на сетевые подключения на уровне приложений.



Выбор режима работы

1. В окне настроек **Брандмауэра** выберите раздел **Дополнительно**.
2. Выберите один из следующих режимов работы:
   - **Разрешать неизвестные соединения** – режим, при котором всем неизвестным приложениям предоставляется доступ к сетевым ресурсам;

- **Режим обучения (создавать правила для известных приложений автоматически)** – режим обучения, при котором правила для известных приложений добавляются автоматически (используется по умолчанию);
- **Интерактивный режим** – режим обучения, при котором пользователю предоставляется полный контроль над реакцией **Брандмауэра**;
- **Блокировать неизвестные соединения** – режим, при котором все неизвестные подключения автоматически блокируются.

3. Нажмите кнопку **ОК**.

Режим обучения

В этом режиме правила для известных приложений добавляются автоматически. Для других приложений **Брандмауэр** предоставляет вам возможность вручную запрещать или разрешать неизвестное соединение, а также создавать для него правило.

При обнаружении попытки со стороны операционной системы или пользовательского приложения получить доступ к сетевым ресурсам **Брандмауэр** проверяет, заданы ли для этих программ правила фильтрации. Если правила отсутствуют, то выводится соответствующее предупреждение, где вам предлагается выбрать либо временное решение, либо создать правило, по которому в дальнейшем подобные подключения будут обрабатываться.

Этот режим используется по умолчанию.

Интерактивный режим

В этом режиме вам предоставляется полный контроль над реакцией **Брандмауэра** на обнаружение неизвестного подключения, и таким образом производится обучение программы в процессе вашей работы за компьютером.

При обнаружении попытки со стороны операционной системы или пользовательского приложения получить доступ к сетевым

ресурсам **Брандмауэр** проверяет, заданы ли для этих программ правила фильтрации. Если правила отсутствуют, то выводится соответствующее предупреждение, где вам предлагается выбрать либо временное решение, либо создать правило, по которому в дальнейшем подобные подключения будут обрабатываться.

Режим блокировки неизвестных подключений

В этом режиме все неизвестные подключения к сетевым ресурсам, включая Интернет, автоматически блокируются.

При обнаружении попытки со стороны операционной системы или пользовательского приложения получить доступ к сетевым ресурсам **Брандмауэр** проверяет, заданы ли для этих программ правила фильтрации. Если правила фильтрации отсутствуют, то **Брандмауэр** автоматически блокирует доступ к сети и не выводит никаких сообщений. Если правила фильтрации для данного подключения заданы, то выполняются указанные в них действия.

Режим разрешения неизвестных подключений

В этом режиме доступ к сетевым ресурсам, включая Интернет, предоставляется всем неизвестным приложениям, для которых не заданы правила фильтрации. При обнаружении попытки подключения **Брандмауэр** не выводит никаких сообщений.

Дополнительные настройки

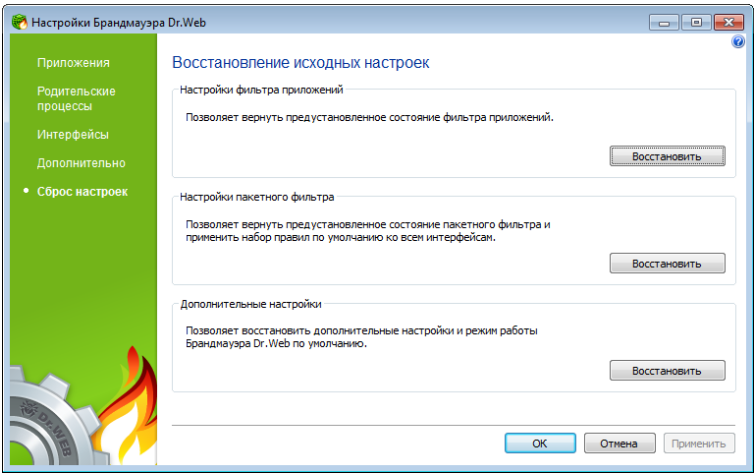
Чтобы задать общие настройки фильтрации для всех приложений, установите следующий флажок:

Флажок	Описание
Разрешать локальные соединения	Установите этот флажок, чтобы разрешить всем приложениям беспрепятственно устанавливать соединения на вашем компьютере. К таким подключениям правила применяться не будут.

	Снимите этот флажок, чтобы применять правила фильтрации вне зависимости от того, происходит ли соединение по сети или в рамках вашего компьютера.
Отображать уведомления на отдельном экране в полноэкранном режиме	Установите этот флажок, чтобы уведомления отображались на отдельном рабочем столе во время работы приложений в полноэкранном режиме (игры, видео). Снимите этот флажок, чтобы уведомления выводились на том же рабочем столе, на котором запущено приложение в полноэкранном режиме.
Отправлять в «Доктор Веб» сведения о созданных правилах	Установите этот флажок, чтобы разрешить **Брандмауэру** автоматически отправлять сведения о созданных вами правилах. Нажмите на ссылку **Политика конфиденциальности «Доктор Веб»**, чтобы ознакомиться с политикой конфиденциальности на официальном сайте компании **«Доктор Веб»**.

8.3.5. Восстановление исходных настроек

На странице **Восстановление исходных настроек** вы можете восстановить настройки работы вашего межсетевого экрана, рекомендуемые **Брандмауэром Dr.Web**.



Восстановление настроек

1. В окне настроек **Брандмауэра** выберите раздел **Сброс настроек**.
2. Выполните любое из следующих действий:
   - чтобы восстановить стандартные настройки фильтра приложений, в разделе **Настройки фильтра приложений** нажмите кнопку **Восстановить**;
   - чтобы восстановить стандартные настройки пакетного фильтра, в разделе **Настройки пакетного фильтра** нажмите кнопку **Восстановить**;
   - чтобы восстановить дополнительные настройки и стандартный режим работы **Брандмауэра**, в разделе **Дополнительные настройки** нажмите кнопку **Восстановить**.
3. Нажмите кнопку **ОК**.

8.4. Регистрация событий

Все события, обработанные **Брандмауэром**, регистрируются в следующих журналах:

- Журнал приложений, хранящий информацию о попытках подключения к сети со стороны приложений и примененных правилах фильтрации;
- Журнал пакетного фильтра, хранящий информацию об обработанных **Брандмауэром** пакетах, примененных правилах фильтрации и интерфейсах, через которые эти пакеты были переданы. Уровень детализации зависит от настроек конкретных правил пакетной фильтрации.

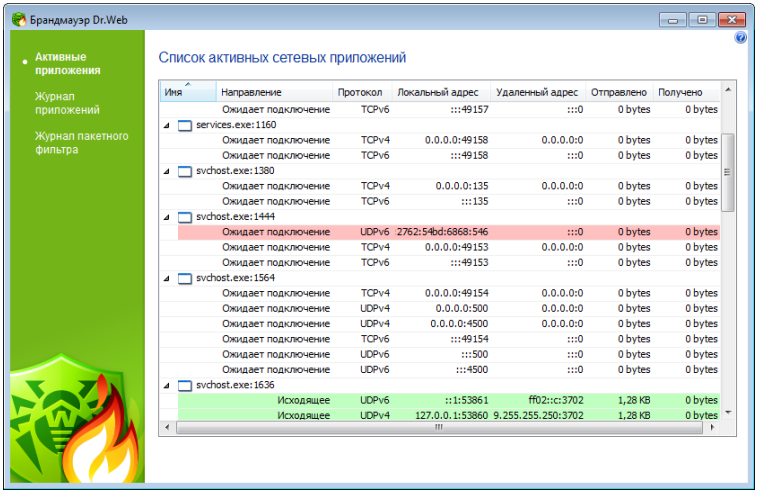
В окне **Активные приложения** также отображается список приложений, подключенных к сети в данный момент.

Просмотр журналов

1. Щелкните значок **SpIDer Agent** в области уведомлений Windows и выберите пункт **Брандмауэр**.
2. В открывшемся меню выберите пункт **Статистика**.

8.4.1. Активные приложения

Список активных приложений отображает информацию о приложениях, подключенных к сети в данный момент.



Для каждого приложения доступна следующая информация об активных соединениях:

Столбец	Описание
Имя	Название приложения.
Направление	Инициатор подключения: • **Входящее** – правило применяется, если инициируется подключение из сети к программе на вашем компьютере; • **Исходящее** – правило применяется, если подключение инициирует программа на вашем компьютере;

Столбец	Описание
	• **Ожидает подключение** – приложение на вашем компьютере ждет подключения из сети.
Протокол	Протокол, по которому осуществляется передача данных.
Локальный адрес	Протокол и адрес хоста, с которого совершается попытка подключения.
Удаленный адрес	Протокол и адрес хоста, к которому совершается попытка подключения.
Отправлено	Количество байт, отправленных через данное соединение.
Получено	Количество байт, полученных через данное соединение.

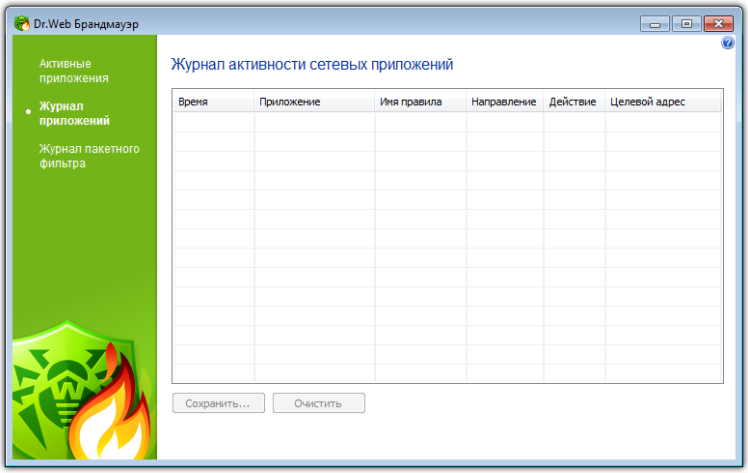
В окне статистики активных приложений вы можете завершить активный процесс. Для этого щелкните правой кнопкой мыши по процессу в таблице и выберите опцию **Завершить процесс**.

Для того чтобы завершить любой активный процесс, необходимы права администратора. В противном случае можно завершить только те процессы, которые запущены от имени пользователя.

Также с помощью контекстного меню вы можете заблокировать активное соединение или разрешить заблокированное (заблокированные соединения отмечены в таблице красным цветом).

8.4.2. Журнал приложений

Журнал приложений хранит информацию о попытках подключения к сети, совершенных установленными на вашем компьютере программами.



Столбец	Описание
Время	Дата и время попытки подключения.
Приложение	Полный путь к исполняемому файлу приложения, совершавшего попытку подключения, его имя и идентификатор процесса (PID).
Имя правила	Название правила, согласно которому попытка была обработана.
Направление	Инициатор подключения: • **Входящее** – правило применяется, если инициируется подключение из сети к программе на вашем компьютере; • **Исходящее** – правило применяется, если подключение инициирует программа на вашем компьютере;

Столбец	Описание
	• **Любое** – правило применяется вне зависимости от того, кто является инициатором подключения.
Результат	Указывает на действие, выполненное **Брандмауэром** при попытке подключения: • **Заблокирован** – попытка подключения была заблокирована; • **Разрешен** – подключение было разрешено.
Целевой адрес	Протокол, адрес удаленного хоста и порт, по которым осуществлялось подключение.

Вы можете сохранить информацию в отчете или очистить журнал.

Сохранение журнала

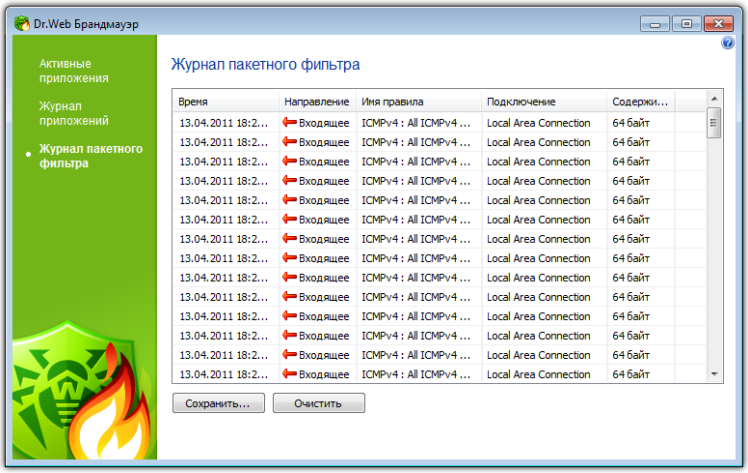
Чтобы сохранить информацию о попытках приложений подключиться к сети, нажмите кнопку **Сохранить** и укажите имя файла.

Очистка журнала

Чтобы удалить из журнала устаревшую информацию о попытках приложений подключиться к сети, нажмите кнопку **Очистить**.

8.4.3. Журнал пакетного фильтра

Журнал пакетного фильтра хранит информацию о пакетах, переданных через установленные на вашем компьютере сетевые интерфейсы, если для этих пакетов указан режим регистрации событий **Только заголовки** или **Весь пакет**. Если для пакета был выбран режим **Выключено**, информация о нем отражаться не будет.



Столбец	Описание
Время	Дата и время обработки пакета.
Направление	Отправитель пакета: • – пакет был принят из сети; • – пакет был отправлен с вашего компьютера; • – пакет, идущий из сети, был заблокирован; • – пакет, отправленный с вашего компьютера, был заблокирован.

Столбец	Описание
Имя правила	Название правила, согласно которому пакет был обработан.
Подключение	Сетевой интерфейс, через который был передан пакет.
Содержимое	Информация о содержимом пакета. Подробность детализации зависит от настроек правил пакетной фильтрации (параметр **Режим отчета**).

Вы можете сохранить информацию в отчете или очистить журнал.

Сохранение журнала

Чтобы сохранить информацию о пакетах, обработанных **Брандмауэром Dr.Web**, нажмите кнопку **Сохранить** и укажите имя файла.

Очистка журнала

Чтобы удалить из журнала устаревшую информацию о пакетах, обработанных **Брандмауэром**, нажмите кнопку **Очистить**.

9. Автоматическое обновление

Для обнаружения вредоносных объектов антивирусы компании **«Доктор Веб»** используют специальные **вирусные базы Dr. Web**, в которых содержится информация обо всех известных вредоносных программах. Так как каждый день появляются новые вирусные угрозы, то эти базы требуют периодического обновления. Такое обновление позволяет обнаруживать ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев – излечивать ранее неизлечимые зараженные файлы.

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

Для поддержания актуальности вирусных баз и программных алгоритмов компанией **«Доктор Веб»** реализована система распространения обновлений через сеть Интернет. **Модуль обновления Dr.Web** позволяет вам в течение срока действия лицензии загружать и устанавливать дополнения к вирусным базам и обновленные программные модули.

9.1. Запуск обновления

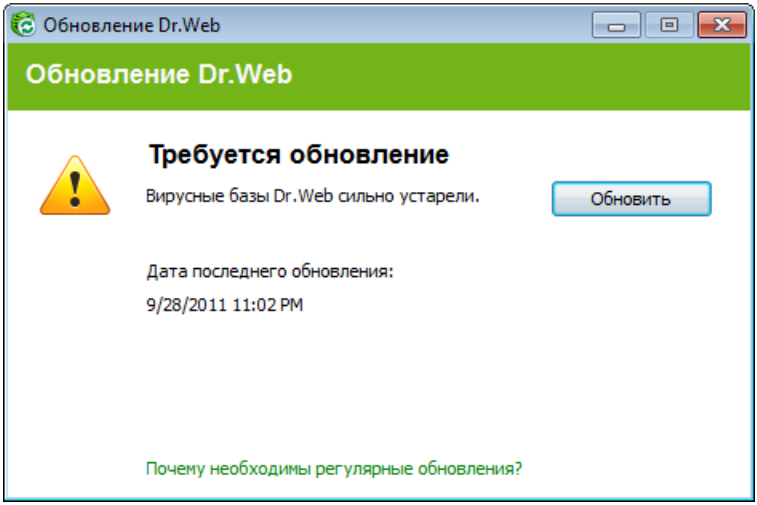
Для запуска **Модуля обновления** вы можете использовать одно из следующих средств:

- в режиме командной строки вызвать исполняемый файл drwupsrv.exe из каталога установки программы **Антивирус Dr.Web**;
- пункт **Обновление** контекстного меню значка **SpIDer Agent**  в области уведомлений Windows.

После запуска **Модуля обновления** появится диалоговое окно, в котором отображается информация об актуальности вирусных баз

и компонентов, а также дата последнего обновления. При необходимости из этого окна вы можете запустить обновление. Настроить необходимые параметры вы можете на вкладке **Обновление** общих настроек работы программы **Антивирус Dr. Web**.

Отчёт записывается в файл dwupdater.log, который находится в каталоге %allusersprofile%\Application Data\Doctor Web\Logs\ (в Windows 7 в каталоге %allusersprofile%\Doctor Web\Logs\).



Запуск обновления

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

При наличии ключевого файла программа проверяет на серверах компании **«Доктор Веб»**, 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 программы **Антивирус Dr.Web** могут быть заблокированы; пользователю выдается соответствующее сообщение.

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

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

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

Сканер, **SpIDer Guard** и **SpIDer Mail** начинают использовать обновленные базы автоматически.

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

Приложения

Приложение А. Дополнительные параметры командной строки

Дополнительные параметры командной строки (*ключи*) используются для задания параметров программам, которые запускаются открытием на выполнение исполняемого файла. Это относится к **Сканеру Dr.Web**, **Консольному сканеру** и к **Модулю автоматического обновления**.

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

Параметры перечислены в алфавитном порядке.

Параметры для Консольного сканера

- `/AA` – автоматически применять действия к обнаруженным угрозам. (Только для **Сканера**).
- `/AR` – проверять архивы. По умолчанию – опция включена.
- `/AC` – проверять инсталляционные пакеты. По умолчанию – опция включена.
- `/AFS` – использовать прямой слеш при указании вложенности внутри архива. По умолчанию – опция отключена.
- `/ARC`: <*число*> – максимальный уровень сжатия. Если сканер определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка не производится. По умолчанию – без ограничений.
- `/ARL`: <*число*> – максимальный уровень вложенности проверяемого архива. По умолчанию – без ограничений.
- `/ARS`: <*число*> – максимальный размер проверяемого архива, в килобайтах. По умолчанию – без ограничений.

- /ART: *<число>* – порог проверки уровня сжатия (минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия), в килобайтах. По умолчанию – без ограничений.
- /ARX:*<число>* – максимальный размер проверяемых объектов в архивах, в килобайтах. По умолчанию – без ограничений.
- /BI – вывести информацию о вирусных базах. По умолчанию – опция включена.
- /DR – рекурсивно сканировать директории (проверять поддиректории). По умолчанию – опция включена.
- /E:*<число>* – использовать указанное количество движков.
- /FAST – произвести быструю проверку системы. (Только для **Сканера**).
- /FL:*<имя_файла>* – сканировать пути, указанные в файле.
- /FR:*<регулярное_выражение>* – сканировать файлы по регулярному выражению. По умолчанию – сканируются все файлы.
- /FULL – произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы). (Только для **Сканера**).
- /FM:*<маска>* – сканировать файлы по маске. По умолчанию – сканируются все файлы.
- /H или /? – вывести на экран краткую справку о работе с программой. (Только для **Консольного Сканера**).
- /HA – производить эвристический анализ файлов и поиск в них неизвестных вирусов. По умолчанию – опция включена.
- /KEY:*<ключевой_файл>* – указать путь к ключевому файлу. Параметр необходим в том случае, если ключевой файл находится не в той же директории, что и сканер. По умолчанию – используется drweb32.key или другой подходящий ключевой файл из директории c:\Program Files\DrWeb\.
- /LITE – произвести стартовую проверку системы, при которой проверяются оперативная память, загрузочные секторы всех дисков и объекты автозапуска, а также провести проверку на наличие руткитов. (Только для **Сканера**).

- /LN – сканировать файлы, на которые указывают ярлыки. По умолчанию – опция отключена.
- /LS – сканировать под учетной записью LocalSystem. По умолчанию – опция отключена.
- /MA – проверять почтовые файлы. По умолчанию – опция включена.
- /MC:<*число*> – установить максимальное число попыток вылечить файл. По умолчанию – без ограничений.
- /NB – не создавать резервные копии вылеченных/удаленных файлов. По умолчанию – опция отключена.
- /NI[:X] – уровень использования ресурсов системы, в процентах. Определяет количество памяти используемой для сканирования и системный приоритет задачи сканирования. По умолчанию – без ограничений.
- /NOREBOOT – отменяет перезагрузку и выключение после сканирования. (Только для **Сканера**).
- /NT – сканировать NTFS-потоки. По умолчанию – опция включена.
- /OK – выводить полный список сканируемых объектов, сопровождая незараженные пометкой **Ok**. По умолчанию – опция отключена.
- /P:<*приоритет*> – приоритет запущенной задачи сканирования в общей очереди задач на сканирование:
- 0 – низший.
- L – низкий.
- N – обычный. Приоритет по умолчанию.
- H – высший.
- M – максимальный.
- /PAL:<*число*> – уровень вложенности упаковщиков. По умолчанию – 1000.
- /RA:<*имя файла*> – дописать отчет о работе программы в указанный файл. По умолчанию отчет не создается.
- /RP:<*имя файла*> – записать отчет о работе программы в указанный файл. По умолчанию отчет не создается.
- /RPC:<*число*> – таймаут соединения с Scanning Engine, в секундах. По умолчанию – 30 секунд. (Только для

Консольного Сканера).

- /RPCD – использовать динамический идентификатор RPC. (Только для **Консольного Сканера**).
- /RPCE – использовать динамический целевой адрес RPC. (Только для **Консольного Сканера**).
- /RPCE:<*целевой_адрес*> – использовать указанный целевой адрес RPC. (Только для **Консольного Сканера**).
- /RPCH:<*имя_хоста*> – использовать указанное имя хоста для вызовов RPC. (Только для **Консольного Сканера**).
- /RPCP:<*протокол*> – использовать указанный протокол RPC. Возможно использование протоколов: lpc, np, tcp. (Только для **Консольного Сканера**).
- /QL – вывести список всех файлов, помещенных в карантин на всех дисках. (Только для **Консольного Сканера**).
- /QL:<*имя_логического_диска*> – вывести список всех файлов, помещенных в каранатин на указанном логическом диске. (Только для **Консольного Сканера**).
- /QR[:[d][:p]] – удалить файлы с указанного диска <*d*> *(имя_логического_диска)*, находящие в карантине дольше <*p*>*(количество)* дней. Если <*d*> и <*p*> не указаны, то будут удалены все файлы, находящиеся в карантине, со всех логических дисков. (Только для **Консольного Сканера**).
- /QNA – выводить пути в двойных кавычках.
- /QUIT – закрыть **Сканер** после проверки (вне зависимости от того, были ли применены действия к обнаруженным угрозам). (Только для **Сканера**).
- /REP – сканировать по символьным ссылкам. По умолчанию – опция отключена.
- /SCC – выводить содержимое составных объектов. По умолчанию – опция отключена.
- /SCN – выводить название инсталляционного пакета. По умолчанию – опция отключена.
- /SPN – выводить название упаковщика. По умолчанию – опция включена.
- /SLS – выводить логи на экран. По умолчанию – опция включена. (Только для **Консольного Сканера**).
- /SPS – отображать процесс проведения сканирования. По

умолчанию – опция включена. (Только для **Консольного Сканера**).

- `/SST` – выводить время сканирования файла. По умолчанию – опция отключена.
- `/TB` – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска. По умолчанию – опция отключена.
- `/TM` – выполнять поиск вирусов в оперативной памяти (включая системную область Windows). По умолчанию – опция отключена.
- `/TS` – выполнять поиск вирусов в файлах автозапуска (по папке Автозагрузка, системным ini-файлам, реестру Windows). По умолчанию – опция отключена.
- `/TR` – сканировать системные точки восстановления. По умолчанию – опция отключена.
- `/W:`*<число>* – максимальное время сканирования, в секундах. По умолчанию – без ограничений.
- `/WCL` – вывод, совместимый с drwebwcl. (Только для **Консольного Сканера**).
- `/X:S[:R]` – по окончании сканирования перевести машину в указанный режим: выключение/перезагрузка/ждущий режим/спящий режим.

Задание действий с различными объектами (C – вылечить, Q – переместить в карантин, D – удалить, I – игнорировать, R – информировать. Действие R возможно только для **Консольного Сканера**. По умолчанию для всех – информировать (также только для **Консольного Сканера**)):

- `/AAD:`*<действие>* – действия для рекламных программ (возможные действия: DQIR, по умолчанию – информирование)
- `/AAR:`*<действие>* – действия с инфицированными архивами (возможные действия: DQIR, по умолчанию – информирование)
- `/ACN:`*<действие>* – действия с инфицированными инсталляционными пакетами (возможные действия: DQIR, по умолчанию – информирование)
- `/ADL:`*<действие>* – действия с программами дозвона

(возможные действия: DQIR, по умолчанию – информирование)

- /AHT:<*действие*> – действия с программами взлома (возможные действия: DQIR, по умолчанию – информирование)
- /AIC:<*действие*> – действия с неизлечимыми файлами (возможные действия: DQR, по умолчанию – информирование)
- /AIN:<*действие*> – действия с инфицированными файлами (возможные действия: CDQR, по умолчанию – информирование)
- /AJK:<*действие*> – действия с программами-шутками (возможные действия: DQIR, по умолчанию – информирование)
- /AML:<*действие*> – действия с инфицированными почтовыми файлами (возможные действия: QIR, по умолчанию – информирование)
- /ARW:<*действие*> – действия с потенциально опасными файлами (возможные действия: DQIR, по умолчанию – информирование)
- /ASU:<*действие*> – действия с подозрительными файлами (возможные действия: DQIR, по умолчанию – информирование)

Некоторые ключи могут иметь модификаторы, с помощью которых режим явно включается либо отключается. Например:

/AC- режим явно отключается,
/AC, /AC+ режим явно включается.

Такая возможность может быть полезна в случае, если режим включен/отключен по умолчанию или по выполненным ранее установкам в конфигурационном файле. Список ключей, допускающих применение модификаторов: /AR /AC /AFS /BI /DR /HA /LN /LS /MA /NB /NT /OK /QNA /REP /SCC /SCN /SPN /SLS /SPS /SST /TB /TM /TS /TR /WCL.

Для ключа /FL модификатор "-" означает: сканировать пути,

перечисленные в указанном файле, и удалить этот файл.

Для ключей `/ARC /ARL /ARS /ART /ARX /NI[:X] /PAL /RPC /W`, принимающих в качестве значения параметра <*число*>, "`0`" означает, что параметр используется без ограничений.

Пример использования ключей при запуске **Консольного сканера**:

[<*путь_к_программе*>]`dwscancl /AR- /AIN:C /AIC:Q C:\`

просканировать все файлы, за исключением архивов, на диске `C`, инфицированные файлы лечить, неизлечимые поместить в карантин. Для аналогичного запуска **Сканера для Windows** необходимо набрать имя команды `dwscanner`.

Параметры для Модуля обновления

Общие параметры:

Параметр	Описание
-h [--help]	Вывести на экран краткую справку о работе с программой.
-v [--verbosity] arg	Уровень детализации отчета: error (стандартный), info (расширенный), debug (отладочный).
-d [--data-dir] arg	Каталог, в котором размещены репозиторий и настройки.
--log-dir arg	Каталог, в котором будет сохранен отчет.
--log-file arg (=dwupdater.log)	Имя файла отчета.
-r [--repo-dir] arg	Каталог репозитория, (по умолчанию <data_dir>/repo).
-t [--trace]	Включить трассировку.
-c [--command] arg (=update)	Выполняемая команда: getversions - получить версии, getcomponents - получить компоненты, init - инициализация, update - обновление, uninstall - удалить, exec - выполнить, keyupdate - обновить ключ.
-z [--zone] arg	Список зон, который будет использоваться вместо заданных в конфигурационном файле.

Параметры команды инициализации (init):

Параметр	Описание
-s [--version] arg	Номер версии.
-p [--product] arg	Название продукта.

Параметр	Описание
-a [--path] arg	Путь, по которому будет установлен продукт. Этот каталог будет использоваться по умолчанию в качестве каталога для всех компонентов, включенных в продукт. Модуль обновления будет проверять наличие ключевого файла именно в этом каталоге.
-n [--component] arg	Имя компонента и каталог установки в формате *<name>, <install path>*.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-g [--proxy] arg	Прокси-сервер для обновления в формате *<адрес>:<порт>*.
-e [--exclude] arg	Имя компонента, который будет исключен из продукта при установке.

Параметры команды обновления (update):

Параметр	Описание
-p [--product] arg	Название продукта. Если название указано, то будет произведено обновление только этого продукта. Если продукт не указан и не указаны конкретные компоненты, будет произведено обновление всех продуктов. Если указаны компоненты, будет произведено обновление указанных компонентов.
-n [--component] arg	Перечень компонентов, которые необходимо обновить до определенной модификации. Формат: *<name>* , *<target revision>*.
-x [--selfrestart] arg (=yes)	Перезапуск после обновления модуля обновления. По умолчанию значение `yes`. Если указано значение `no`, то выводится предупреждение о необходимости перезапуска.
--geo-update	Получить список IP-адресов update.drweb.com перед обновлением.

Параметр	Описание
--type arg (=normal)	Может быть одним из следующих: • reset-all – принудительное обновление всех компонентов; • reset-failed – сбросить все изменения для поврежденных компонентов; • normal-failed – попытаться обновить компоненты, включая поврежденные, до последней либо до указанной версии; • update-revision – обновить компоненты в пределах текущей ревизии; • normal – обновить все компоненты.
-g [--proxy] arg	Прокси-сервер для обновления в формате *<адрес>:<порт>*.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
--param arg	Передать дополнительные параметры в скрипт. Формат: *<имя>: <значение>*.
-l [--progress-to-console]	Вывести на консоль информацию о загрузке и выполнении скрипта.

Особые параметры команды исполнения (exec):

Параметр	Описание
-s [--script] arg	Выполнить указанный скрипт.
-f [--func] arg	Выполнить функцию скрипта.
-p [--param] arg	Передать дополнительные параметры в скрипт. Формат: *<имя>: <значение>*.
-l [--progress-to-console]	Вывести на консоль информацию о прогрессе выполнения скрипта.

Параметры команды получения компонентов (getcomponents):

Параметр	Описание
-s [--version] arg	Номер версии.
-p [--product] arg	Укажите имя продукта, чтобы увидеть, какие компоненты он включает. Если продукт не указан, будут выведены все компоненты этой версии.

Параметры команды получения изменений (getrevisions):

Параметр	Описание
-s [--version] arg	Номер версии.
-n [--component] arg	Имя компонента.

Параметры команды uninstall (удаления):

Параметр	Описание
-n [--component] arg	Имя компонента, который необходимо удалить.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.
--param arg	Передать дополнительные параметры в скрипт. Формат: *<имя>: <значение>*.
-e [--add-to-exclude]	Компоненты, которые будут удалены и их обновление производиться не будет.

Параметры команды автоматического обновления ключа (keyupdate):

Параметр	Описание
-m [--md5] arg	Контрольная сумма md5 старого ключевого файла.
-o [--output] arg	Имя файла.
-b [--backup]	Резервное копирование старого ключевого файла, если он существует.
-g [--proxy] arg	Прокси-сервер для обновления в формате *<адрес>:<порт>*.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-l [--progress-to-console]	Вывести на консоль информацию о загрузке ключевого файла.

Параметры команды скачивания (download):

Параметр	Описание
--zones arg	Файл, содержащий список зон.
--key-dir arg	Каталог, в котором находится ключевой файл.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.
-g [--proxy] arg	Прокси-сервер для обновления в формате *<адрес>:<порт>*.
-u [--user] arg	Имя пользователя прокси-сервера.

Параметр	Описание
-k [--password] arg	Пароль пользователя прокси-сервера.
-s [--version] arg	Имя версии
-p [--product] arg	Название продукта, который необходимо скачать.

Коды возврата

Возможные значения кода возврата и соответствующие им события следующие:

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

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

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

Приложение Б. Угрозы и способы их обезвреживания

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

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

В данной главе представлены описания всех основных и наиболее распространенных типов вредоносных программ, на борьбу с которыми в первую очередь и направлены разработки **«Доктор Веб»**.

Классификация 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 пишутся на ассемблере, высокоуровневых языках программирования, скриптовых языках и т.д.) и по поражаемым операционным системам.

Компьютерные черви

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

Черви не всегда целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-

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

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

Троянские программы (троянские кони, трояны)

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

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

Руткит

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

утилит, которые взломщик устанавливает в систему, к которой получил первоначальный доступ.

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

Программы взлома

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

Шпионские программы

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

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

компьютере – нестабильная работа браузера и замедление производительности системы.

Рекламные программы

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

Программы-шутки

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

Программы дозвона

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

Все вышеперечисленные типы программ считаются вредоносными, т.к. представляют угрозу либо данным пользователя, либо его правам на конфиденциальность информации. К вредоносным не принято причислять программы, не скрывающие своего внедрения в систему, программы для рассылки спама и анализаторы трафика,

хотя потенциально и они могут при определенных обстоятельствах нанести вред пользователю.

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

Ниже приведены некоторые виды хакерских атак и интернет-мошенничества:

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

производятся при помощи специальной невредоносной программы - пакетного сниффера, который осуществляет перехват всех сетевых пакетов домена, за которым идет наблюдение.

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

Действия для обезвреживания угроз

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

1. *Лечение* – действие, применяемое к вирусам, червям и троянам. Оно подразумевает удаление вредоносного кода из зараженных файлов либо удаление функциональных копий вредоносных программ, а также, по возможности, восстановление работоспособности пораженных объектов (т.е. возвращение структуры и функционала программы к состоянию, которое было до заражения). Далеко не все

вредоносные программы могут быть вылечены, однако именно продукты **«Доктор Веб»** предоставляют самые эффективные алгоритмы лечения и восстановления файлов, подвергшихся заражению.

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

Приложение B. Принципы именования угроз

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

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

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

Основные префиксы

Префиксы операционной системы

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

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

Windows 98, ОС Windows Me;

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

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

Вирусы, поражающие файлы MS Office

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

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

Префиксы языка разработки

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

указывающие на базовый алгоритм функционирования, в частности:

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

К группе префиксов языка разработки можно также отнести:

- Java – вирусы для среды виртуальной машины Java.

Троянские кони

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

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

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

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

Средство использования уязвимостей

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

Средства для сетевых атак

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

Скрипт-вирусы

Префиксы вирусов, написанных на различных языках сценариев:

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

Вредоносные программы

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

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

Разное

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

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

Суффиксы

Суффиксы используются для именования некоторых специфических вирусных объектов:

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

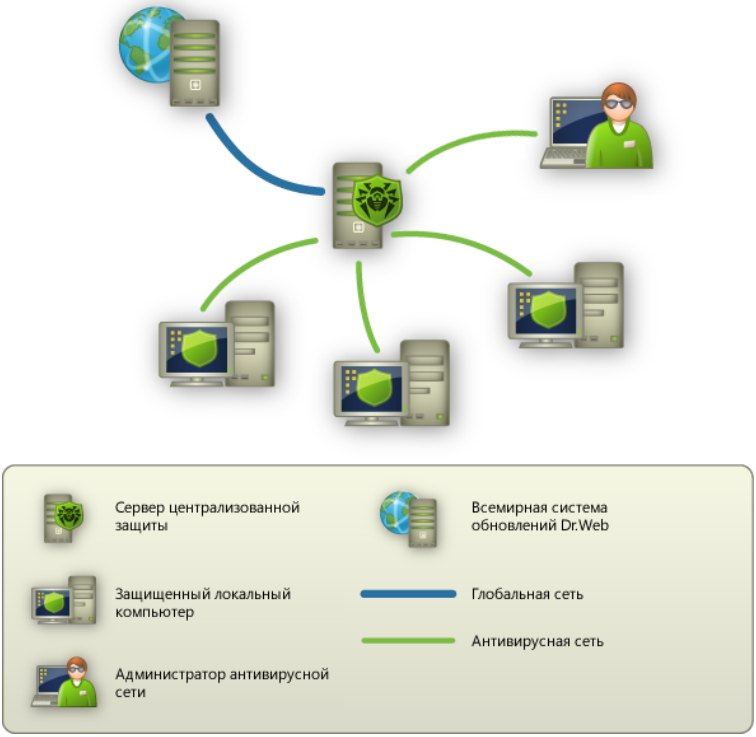
Приложение Г. Централизованная антивирусная защита

Решения компании **«Доктор Веб»** по организации централизованной антивирусной защиты позволяют автоматизировать и упростить настройку и управление информационной безопасностью компьютеров, объединенных в единую логическую структуру (например, компьютеры одной компании, расположенные как внутри локальной сети, так и вне ее). Защищаемые компьютеры объединяются в единую *антивирусную сеть*, безопасность которой контролируется и управляется администраторами с центрального сервера. Подключение к системам централизованной защиты позволяет получить гарантированно высокий уровень защиты компьютера при минимальных усилиях со стороны конечных пользователей.

Взаимодействие компонентов антивирусной сети

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

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



Обновление и конфигурация локальных компонентов производится через *центральный сервер*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и антивирусным сервером может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

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

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

Локальные антивирусные компоненты несовместимы с антивирусным программным обеспечением как других компаний, так и антивирусными решениями **Dr.Web**, не поддерживающими режим централизованной защиты (например, **Антивирусом Антивирус Dr.Web** версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Приложение Д. Техническая поддержка

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

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

- ознакомиться с последними версиями описаний и руководств по адресу http://download.drweb.com/doc
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com
- попытаться найти ответ в базе знаний **Dr.Web** по адресу http://wiki.drweb.com/

- посетить форумы **Dr.Web** по адресу http://forum.drweb.com/

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

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