Dr.WEB®
Security Space

Защити созданное

Руководство пользователя

Dr.Web Security Space
Версия 8.0
Руководство пользователя
02.11.2012

«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 8
1.1. О чем эта документация 10
1.2. Используемые обозначения и сокращения 11
1.3. Системные требования 12
1.4. Лицензирование 14
1.4.1. Ключевой файл 14
1.4.2. Получение ключевого файла 16
1.4.3. Продление лицензии 18
1.5. Методы обнаружения 20
1.6. Проверка антивируса 22
2. Установка программы 23
2.1. Первая установка 24
2.2. Повторная установка и удаление 34
2.3. Процедура получения ключевого файла 36
3. Приступая к работе 39
3.1. Модуль управления SpIDer Agent 43
3.2. Основные настройки 46
Раздел Уведомления 46
Раздел Обновление 51
Раздел Антивирусная сеть 54
Раздел Превентивная защита 55
Раздел Dr.Web Cloud 58
Раздел Отчет 59

Раздел Карантин 62
Раздел Прокси-сервер 65
Раздел Язык 67
Раздел Самозащита 68
Раздел Восстановление 69
3.3. Менеджер лицензий 70
3.4. Менеджер Карантина 72
3.5. Антивирусная сеть 74
4. Сканер Dr.Web 77
4.1. Проверка компьютера 78
4.2. Действия при обнаружении вирусов 82
4.3. Настройка Сканера 84
4.4. Запуск Сканера из командной строки 89
4.5. Консольный сканер 90
4.6 Запуск проверки по расписанию 91
5. SpIDer Guard 92
5.1. Управление SpIDer Guard 93
5.2. Настройка SpIDer Guard 95
6. SpIDer Mail 101
6.1. Управление SpIDer Mail 105
6.2. Настройка SpIDer Mail 106
7. Dr.Web для Outlook 116
7.1. Настройка Dr.Web для Outlook 116
7.2. Обнаружение угроз 118
7.2.1. Вредоносные объекты 118
7.2.2. Действия 119

7.3. Проверка на спам 122
7.3.1. Настройка спам-фильтра 123
7.3.2. Черный и белый списки 124
7.4. Регистрация событий 128
7.4.1. Журнал операционной системы 128
7.4.2. Текстовый журнал отладки 129
7.5. Статистика проверки 131
8. SpIDer Gate 133
8.1. Управление SpIDer Gate 133
8.2. Настройка SpIDer Gate 135
9. Родительский контроль 140
9.1. Управление Родительским контролем 141
9.2. Настройка Родительского контроля 143
10. Брандмауэр Dr.Web 151
10.1. Обучение Брандмауэра 151
10.2. Управление Брандмауэром 158
10.3. Настройка Брандмауэра 161
10.3.1. Раздел Приложения 163
10.3.2. Раздел Родительские процессы 170
10.3.3. Раздел Интерфейсы 171
10.3.4. Раздел Дополнительно 181
10.4. Регистрация событий 184
10.4.1. Активные приложения 185
10.4.2. Журнал приложений 187
10.4.3. Журнал пакетного фильтра 189
11. Автоматическое обновление 191

11.1. Запуск обновления **191**

Приложения **194**

Приложение А. Дополнительные параметры командной строки **194**

Параметры для Консольного сканера **194**

Параметры для Модуля обновления **201**

Коды возврата **207**

Приложение Б. Угрозы и способы их обезвреживания **208**

Классификация угроз **209**

Действия для обезвреживания угроз **215**

Приложение В. Принципы именования угроз **217**

Приложение Г. Техническая поддержка **223**

1. Введение

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

Важной особенностью программы **Dr.Web Security Space** является модульная архитектура. **Dr.Web Security Space** использует программное ядро и вирусные базы, общие для всех компонентов и различных сред. В настоящее время наряду с программой **Dr.Web Security Space** 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®).

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

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

Dr.Web Security Space 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 Dr.Web®**);
- **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, работающих на компьютере, 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. Почтовый сторож также может осуществлять проверку корреспонденции на спам с помощью компонента **Антиспам Dr.Web**;
- **Dr.Web для Outlook** – подключаемый модуль, который проверяет почтовые ящики Microsoft Outlook на вирусы и спам;
- **SpIDer Gate™** – веб-антивирус, который автоматически проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы (при настройках по умолчанию);
- **Родительский контроль** – компонент, с помощью которого осуществляется ограничение доступа пользователя к ресурсам, содержащимся как локально, на самом компьютере, так и в сети;
- **Dr.Web® Брандмауэр** – 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 **Dr.Web Security Space**.

1.1. О чем эта документация

Настоящее руководство содержит необходимые сведения по установке и эффективному использованию **Dr.Web Security Space**.

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 **Dr.Web Security Space** (настройки по умолчанию).

В Приложениях содержится подробная справочная информация по настройке **Dr.Web Security Space**, 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 **Dr.Web Security Space** 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 **Dr.Web Security Space** возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
Операционная система	Для 32-разрядных операционных систем: • Windows® XP с пакетом обновлений SP2; • Windows® XP с пакетом обновлений SP3; • Windows Vista®; • Microsoft® Windows® 7; • Microsoft® Windows® 8. Для 64-разрядных операционных систем: • Windows Vista®; • Microsoft® Windows® 7; • Microsoft® Windows® 8. Возможно, потребуется загрузить с сайта Microsoft и установить обновления ряда системных компонентов. **Dr.Web Security Space** сообщит вам, при необходимости, их наименования и URL.
Место на жестком диске	450 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 **Dr.Web Security Space**.

1.4. Лицензирование

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

Для работы **Dr.Web Security Space** 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 **Dr.Web Security Space** 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 (при получении демонстрационного ключа по акции — 3 месяца);

Демонстрационный ключ выдается на одну и ту же машину не чаще чем 1 раз в 4 месяца. При получении ключевого файла по акции — только раз в год.

- *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 **Dr.Web Security Space**, 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 **Dr.Web Security Space** 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;
- 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 Dr.Web Security Space

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 **Dr.Web Security Space** 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 **Dr.Web Security Space**. В таком случае вам потребуется заменить уже существующий и зарегистрированный в системе лицензионный ключевой файл. **Dr.Web Security Space** поддерживает обновление лицензии «на лету», при котором не требуется переустанавливать антивирус или прерывать его работу.

Замена ключевого файла

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

- в фоновом режиме;
- в обычном режиме.

Установка с параметрами командной строки

Для запуска установки **Dr.Web Security Space** с параметрами командной строки, в командной строке введите имя исполняемого файла с необходимыми параметрами (параметры влияют на установку в фоновом режиме, язык установки, перезагрузку после окончания установки и установку **Брандмауэра**):

Параметр	Значение
reboot	Автоматическая перезагрузка компьютера после завершения установки.
installFirewall	Будет установлен **Брандмауэр Dr.Web**.
lang	Язык продукта. Значение параметра – код языка в формате ISO 639-1.
silent	Установка в фоновом режиме.

Например, при запуске следующей команды будет проведена установка **Dr.Web Security Space** в фоновом режиме и проведена перезагрузка после установки:

```
C:\Documents and Settings\drweb-800-win-space.exe /silent yes /reboot yes
```

Установка в обычном режиме

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

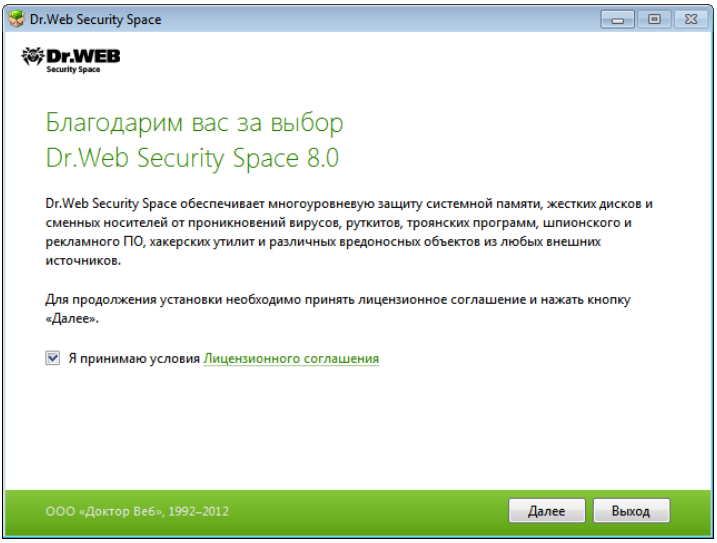
- в случае поставки установочного комплекта в виде единого исполняемого файла запустите на исполнение этот файл;
- в случае поставки установочного комплекта на фирменном диске вставьте диск в привод. Если для привода включен режим автозапуска диска, процедура установки запустится автоматически. Если 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:

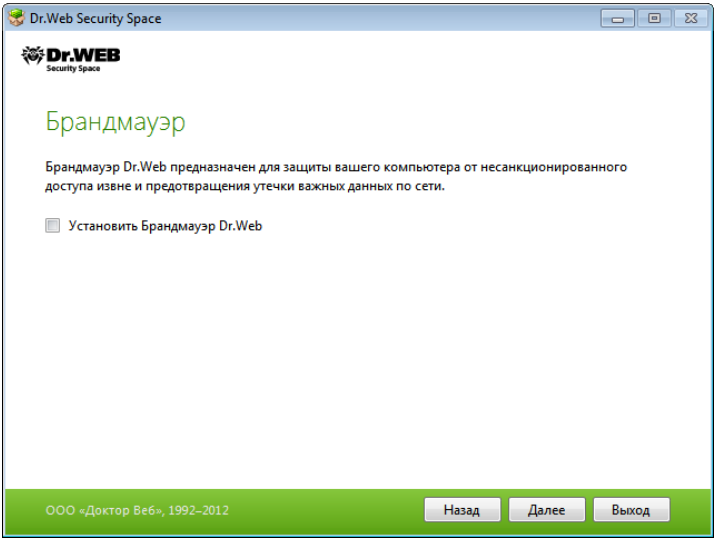
- чтобы вернуться к предыдущему шагу программы установки, нажмите кнопку **Назад**;
- чтобы перейти на следующий шаг программы, нажмите кнопку **Далее**;
- чтобы прервать установку, нажмите кнопку **Отмена**.

Процедура установки:

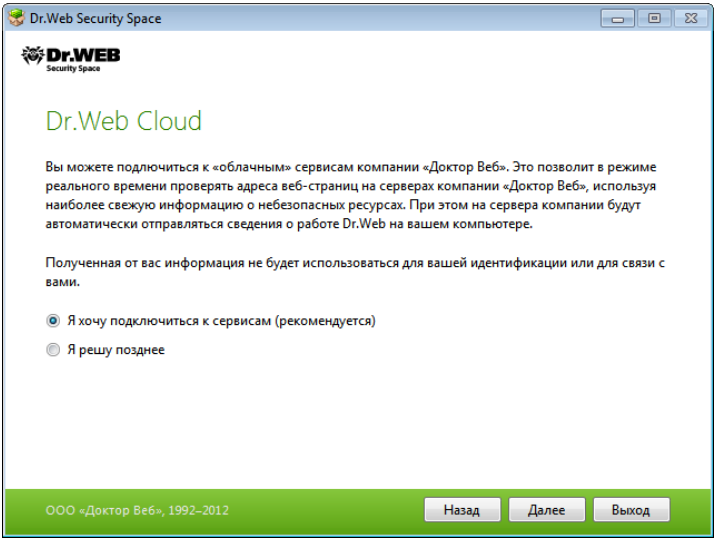
1. На первом шаге ознакомьтесь с лицензионным соглашением. Для продолжения установки его необходимо принять.



2. Если на вашем компьютере уже установлен другой антивирус, то на следующем шаге программа установки предупредит вас о несовместимости **Dr.Web Security Space** и иных антивирусных решений, и предложит удалить их.
3. На следующем шаге вам будет предложено установить **Брандмауэр Dr.Web**.

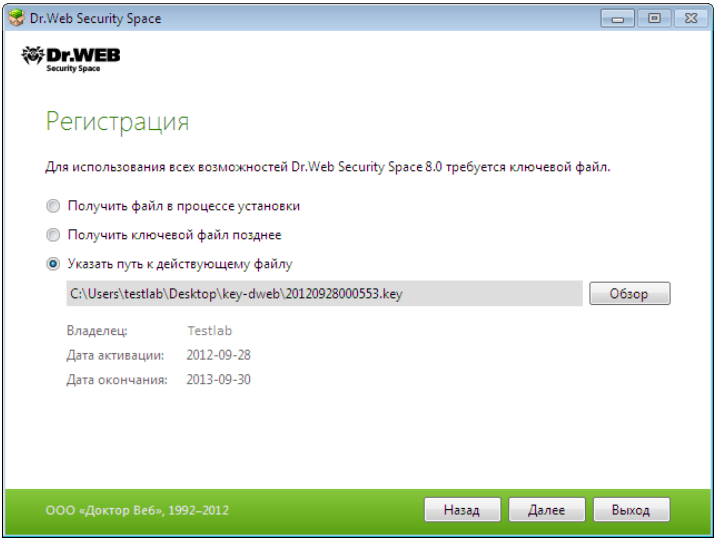


4. Далее вам будет предложено подключиться к «облачным» сервисам **Dr.Web**, которые позволят вам использовать наиболее свежую информацию для проверки веб-ресурсов.



5. На шаге **Ключевой файл Dr.Web** программа установки предупредит вас о том, что для работы **Dr.Web Security Space** 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.

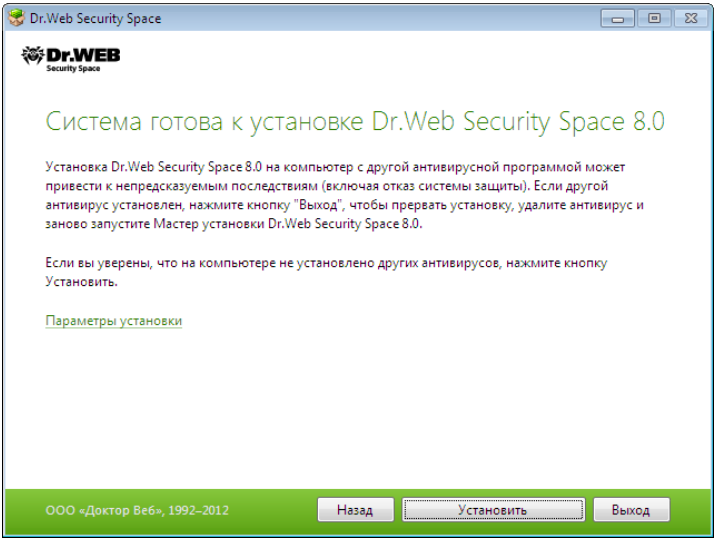
   Нажмите кнопку **Далее**.



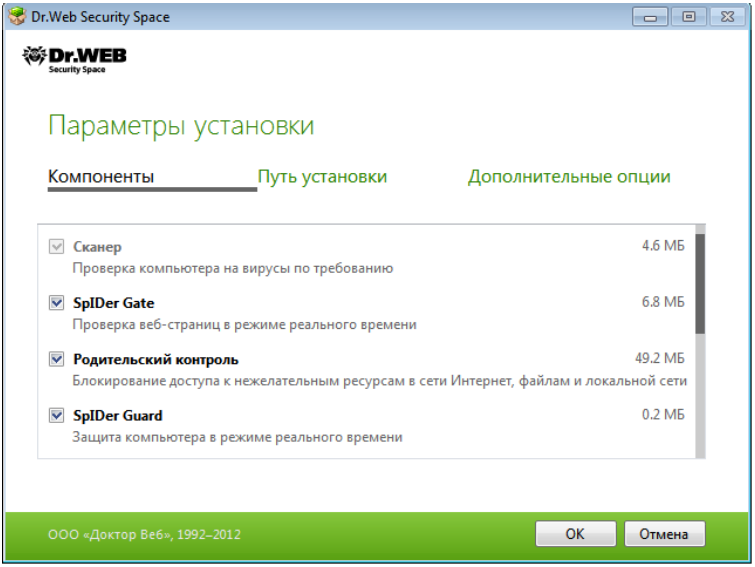
Используйте только ключевой файл варианта **Dr.Web Security Space**. Ключевой файл должен иметь расширение .key.

6. Откроется окно с сообщением о готовности к установке. Вы можете запустить процесс установки с параметрами по умолчанию, нажав кнопку **Установить**.

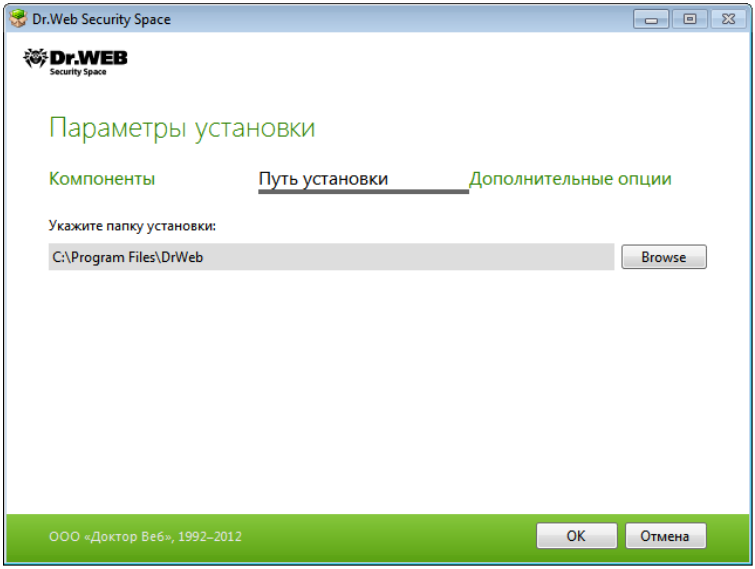
   Для того чтобы самостоятельно выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры установки, нажмите **Параметры установки**. Данная опция предназначена для опытных пользователей.



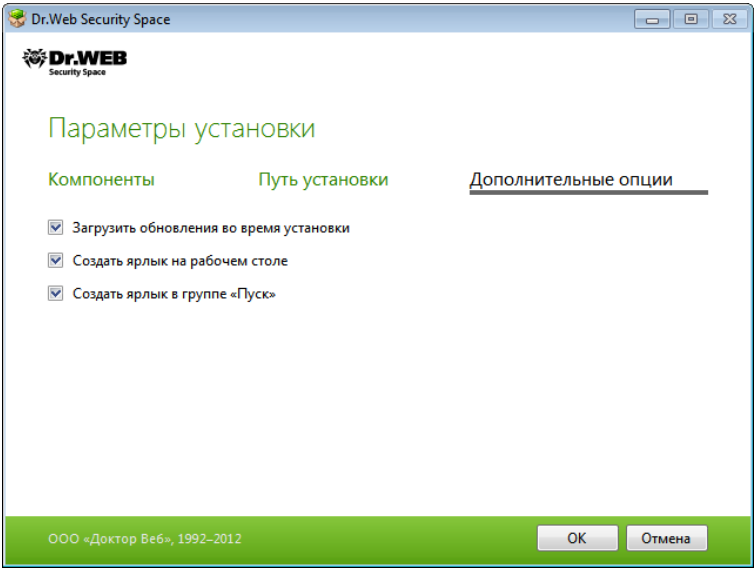
7. Если на предыдущем шаге вы нажали кнопку **Установить**, то перейдите к описанию шага 10. В противном случае откроется окно **Параметры установки**. На первой вкладке вы можете изменить состав устанавливаемых компонентов.



8. На следующей вкладке при необходимости вы можете изменить путь установки.



9. Если на шаге 5 вы указали действующий ключевой файл или выбрали пункт **Получить файл в процессе установки,** то на последней вкладке окна вы можете установить флажок **Загрузить обновления во время установки,** чтобы в процессе установки были загружены актуальные вирусные базы и другие модули антивируса. Также вам будет предложено настроить создание ярлыков для запуска **Dr.Web Security Space**.

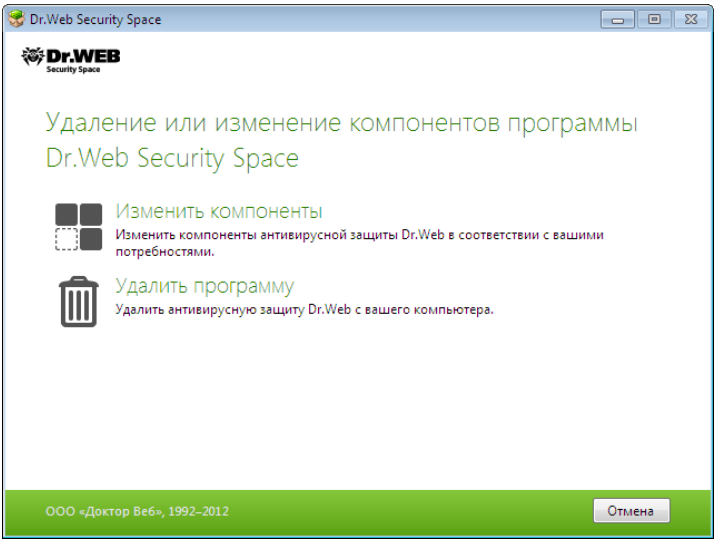


После того, как все необходимые изменения будут внесены, нажмите кнопку **ОК**.

10. Если на шаге 5 вы выбрали **Получить файл в процессе установки**, то на следующем шаге программа попытается получить ключевой файл через Интернет при помощи процедуры регистрации пользователя.
11. Если в процессе установки вы указали или получили действующий ключевой файл и на шаге 9 установили флажок **Загрузить обновления во время установки**, а также во время установки по умолчанию, будет выполнен процесс обновления вирусных баз и других компонентов **Dr.Web Security Space**. Обновление проводится автоматически и не требует дополнительных действий.
12. Если в состав устанавливаемых компонентов входит **Брандмауэр Dr.Web**, для завершения процесса установки выполните перезагрузку компьютера.

2.2. Повторная установка и удаление

1. 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 компоненты**;
   - чтобы удалить все установленные компоненты, выберите пункт **Удалить программу.**



3. Для удаления **Dr.Web Security Space** или изменения состава компонентов введите код подтверждения, изображенный в открывшемся окне.
4. 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.

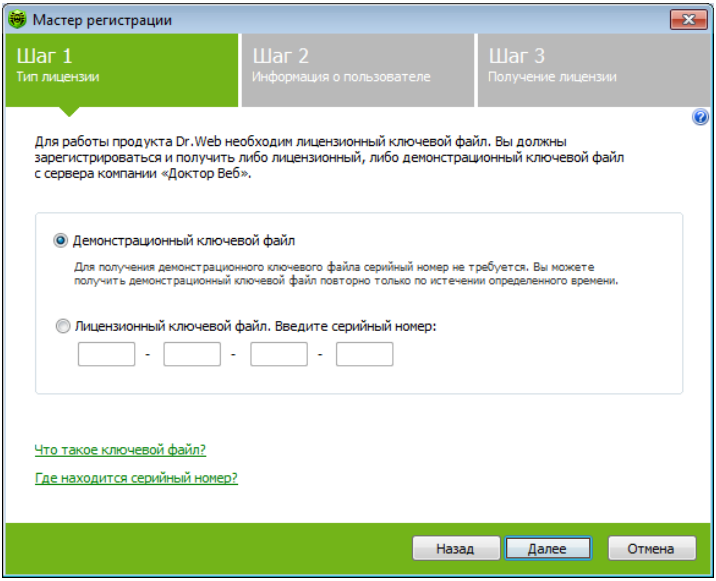
Получение ключевого файла

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

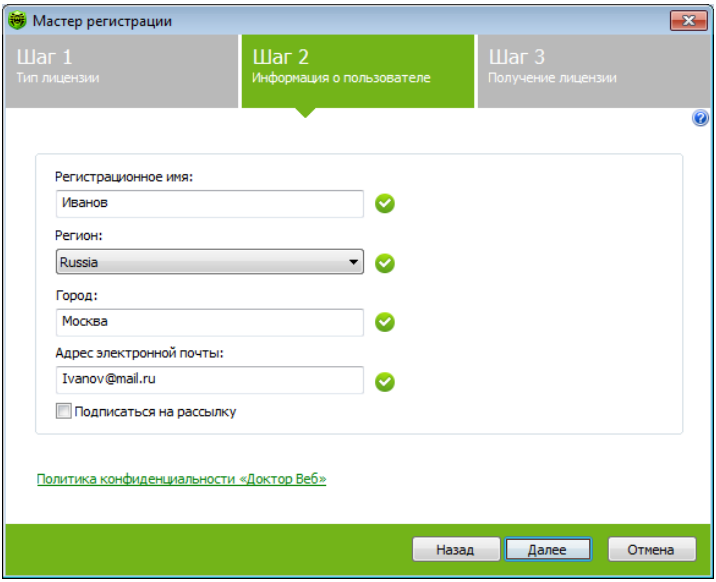
   Если у вас имеется регистрационный серийный номер, выданный вам при приобретении антивируса, выберите вариант **Лицензионный ключевой файл** и введите серийный номер. Если вы устанавливаете программу с ознакомительными целями, выберите пункт **Демонстрационный ключевой файл** и перейдите к шагу 2.

Если вы ранее уже являлись пользователем **Dr.Web Security Space**, 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**;
- веб-антивирус **SpIDer Gate**;
- модуль **Родительского контроля**;
- межсетевой экран **Брандмауэр Dr.Web**;
- компонент **Антиспам**;
- **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.

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

С помощью модуля **Родительского контроля** осуществляется ограничение доступа пользователя к ресурсам, содержащимся как локально, на самом компьютере, так и в сети. Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность важных файлов и защитить их от

заражения вирусами, а также сохранит необходимую конфиденциальность данных. Существует возможность защиты как отдельных файлов, так и папок целиком, расположенных как на локальных дисках, так и на внешних носителях информации. Также можно наложить полный запрет на просмотр информации со всех внешних носителей. Контроль доступа к интернет-ресурсам позволяет как оградить пользователя от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т.п.), так и разрешить пользователю доступ только к тем сайтам, которые определены настройками модуля **Родительского контроля**.

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 проверку всей файловой системы компьютера с предусмотренными по умолчанию (максимальными) настройками подробности проверки;
- сохранить настройки **SpIDer Guard** по умолчанию;
- осуществлять полную проверку почты при помощи **SpIDer Mail**;
- осуществлять проверку входящего HTTP-трафика при помощи **SpIDer Gate**;
- блокировать все неизвестные соединения с помощью **Брандмауэра Dr.Web**;
- периодически, по мере обновления вирусных баз, повторять полную проверку 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 полную проверку немедленно.

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

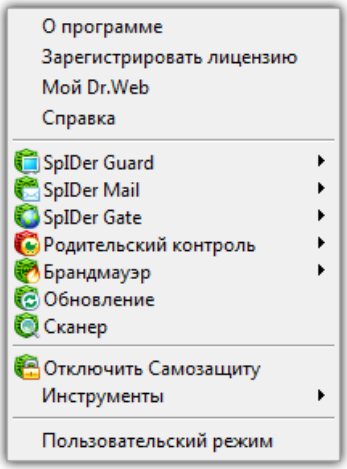
Использование компонентов **Dr.Web Security Space** подробнее описано в следующих разделах.

3.1. Модуль управления SpIDer Agent

После установки **Dr.Web Security Space** 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-настройками.

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



Пункт **О программе** открывает окно с информацией о версиях компонентов **Dr.Web Security Space**, 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 **Dr.Web Security Space**.

Пункт **Обновление** открывает окно **Модуля обновления**, в котором вы можете запустить обновление.

Пункты **SpIDer Guard**, **SpIDer Mail**, **SpIDer Gate**, **Родительский контроль**, **Брандмауэр**, **Обновление** открывают доступ к настройкам, статистике 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 возможно только в Административном режиме. Отключать самозащиту не рекомендуется.

Отключение самозащиты:

1. В меню **SpIDer Agent** выберите пункт **Отключить Самозащиту**.
2. Введите код подтверждения или пароль доступа к настройкам **Dr.Web Security Space**.
3. В меню **SpIDer Agent** пункт **Отключить Самозащиту** заменится на пункт **Включить Самозащиту**.

Для того чтобы произвести откат к точке восстановления системы, необходимо отключить модуль самозащиты.

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 **Dr.Web Security Space** (см. Основные настройки) и настройкам отдельных компонентов;
- к **Менеджеру Карантина** (см. Менеджер Карантина);
- к статистике компонентов;
- к Антивирусной сети;
- к созданию отчета.

  При обращении в службу технической поддержки компании **«Доктор Веб»** вы можете сформировать отчет о вашей операционной системе и работе программы **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 **Dr.Web Security Space**. В **Пользовательском режиме** действуют следующие ограничения: недоступны настройки компонентов и 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 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 **SpIder Agent** сразу предоставляет доступ ко всем функциям.

3.2. Основные настройки

Настройки **Dr.Web Security Space** недоступны в пользовательском режиме.

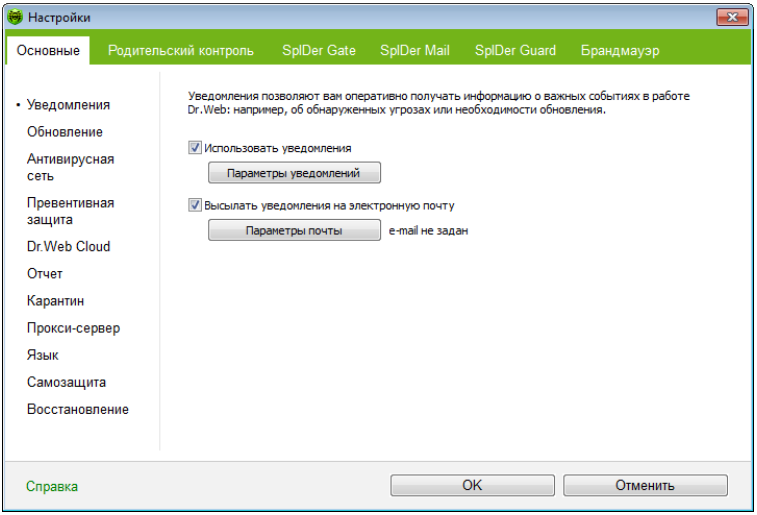
Единый центр управления настройками позволяет задать как общие параметры работы антивирусного комплекса, так и индивидуальные настройки всех компонентов **Dr.Web Security Space** за исключением **Сканера**.

Общая настройка Dr.Web Security Space

1. Щелкните значок **SpIDer Agent** в области уведомлений Windows.
2. В группе **Инструменты** выберите пункт **Настройки.** Откроется раздел **Основные** общего окна настроек.
3. Внесите необходимые изменения. Для получения информации о настройках, расположенных в разделе, нажмите на ссылку **Справка.**

Раздел Уведомления

В данном разделе вы можете задать типы подсказок-уведомлений, отправляемых по почте и появляющихся в виде всплывающего окна над значком **SpIDer Agent** в области уведомлений Windows.



Настройка уведомлений

1. Чтобы включить режим нотификации о событиях, установите флажок **Использовать уведомления**.
2. Нажмите кнопку **Параметры уведомлений**. Откроется окно со списком возможных уведомлений.
3. Выберите уведомления, которые вы хотите получать, и установите соответствующие флажки. Чтобы отображать экранные уведомления, устанавливайте флажок в столбце **Экран**. Чтобы получать оповещения по почте, устанавливайте флажок в столбце **Почта**.
4. При необходимости задайте дополнительные параметры отображения экранных оповещений:

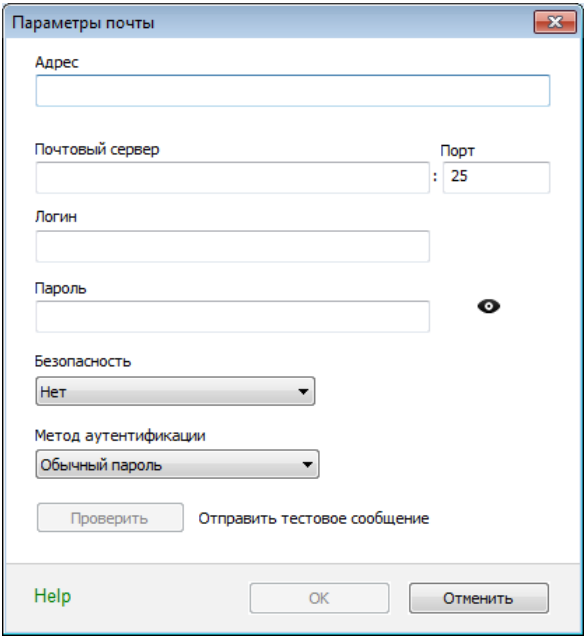
Флажок	Описание
Не показывать уведомления в полноэкранном режиме	Установите этот флажок, чтобы не получать уведомления при работе с приложениями в полноэкранном режиме (просмотр фильмов, графики и т.д.). Снимите этот флажок, чтобы получать уведомления всегда.

Отображать уведомления Брандмауэра на отдельном экране в полноэкранном режиме	Установите этот флажок, чтобы уведомления от **Брандмауэра** 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.

5. Если вы выбрали одно или несколько почтовых уведомлений, настройте отправку почты с вашего компьютера.
6. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Настройка почтовых уведомлений

1. Чтобы включить режим нотификации о событиях по почте, убедитесь, что флажок **Использовать уведомления** установлен и в окне **Параметры уведомлений** выбраны нужные типы оповещений.
2. Установите флажок **Высылать уведомления на электронную почту**.
3. Нажмите кнопку **Параметры почты**. Откроется окно настройки параметров.



4. В окне **Параметры почты** укажите следующую информацию:

Настройка	Описание
Адрес	Укажите почтовый адрес, на который вы хотите получать оповещения выбранных типов.
Почтовый сервер	Укажите адрес почтового сервера, который должен использовать **Dr.Web Security Space** для отправки почтовых оповещений.
Порт	Укажите порт почтового сервера, к которому должен подключаться **Dr.Web Security Space** для отправки почтовых оповещений.

Логин	Укажите имя учетной записи для подключения к почтовому серверу.
Пароль	Укажите пароль учетной записи для подключения к почтовому серверу.
Безопасность	Выберите параметры безопасности при подключении к почтовому серверу.
Метод аутентификации	Выберите метод аутентификации, используемый для подключения к почтовому серверу.

5. Нажмите кнопку **Проверить**, чтобы отправить тестовое сообщение на указанный адрес через заданный почтовый сервер. Если в течение некоторого времени вы не получите данное сообщение, проверьте настройки почтовых параметров.
6. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

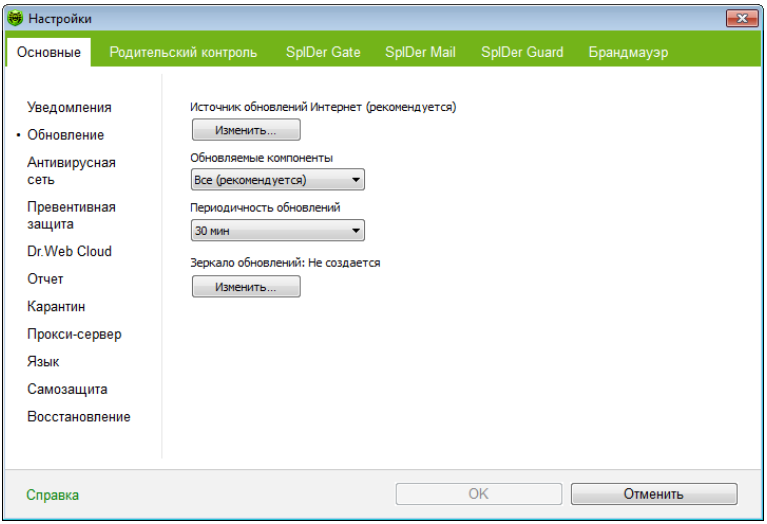
Временное отключение уведомлений

Чтобы временно отключить отправку почтовых оповещений, снимите флажок **Высылать уведомления на электронную почту**.

Чтобы временно отключить уведомления всех типов, снимите флажок **Использовать уведомления**.

Раздел Обновление

В данном разделе вы можете настроить параметры обновления **Dr.Web Security Space**. Вы можете указать источник обновлений, какие компоненты необходимо обновлять, периодичность, с которой будут происходить обновления, а также настроить зеркало обновлений.



Настройка	Описание
Источник обновлений	Вы можете указать удобный для вас источник обновлений.
Обновляемые компоненты	Вы можете выбрать один из вариантов загрузки обновлений:

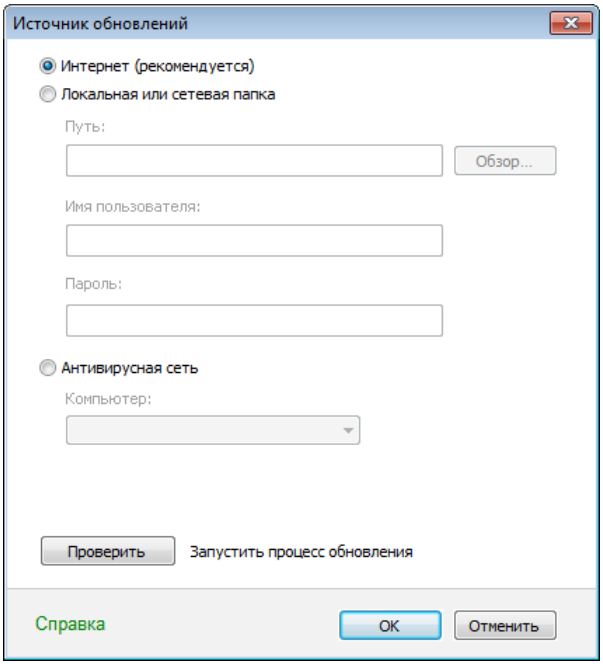
Настройка	Описание
	• **Все (рекомендуется)**, при котором загружаются обновления как для **вирусных баз Dr.Web**, так и для антивирусного ядра и других программных компонентов **Dr.Web Security Space**; • **Только базы**, при котором загружаются только обновления **вирусных баз Dr.Web** и антивирусного ядра; другие компоненты **Dr.Web Security Space** не обновляются.
Периодичность обновлений	Вы можете выбрать периодичность, с которой хотите получать обновления.
Зеркало обновлений	Вы можете создать зеркало обновлений, которое смогут использовать другие компьютеры в локальной сети, на которых установлен продукт **Dr.Web**.

Источник обновлений

Для того чтобы выбрать источник обновлений, нажмите кнопку **Изменить**. В открывшемся окне укажите удобный для вас источник обновлений:

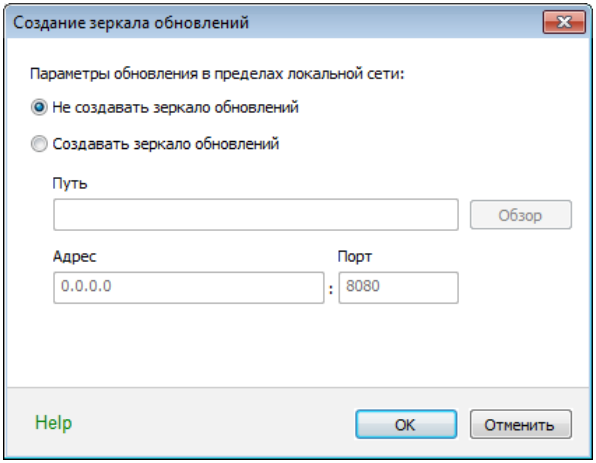
- **Интернет (рекомендуется)** – обновление с серверов компании **«Доктор Веб»**. Этот источник указан по умолчанию.
- **Локальная или сетевая папка** – обновление из локальной или сетевой папки, в которую скопированы обновления. Укажите путь к папке (для этого нажмите кнопку **Обзор** и выберите нужный каталог, или введите путь вручную), а также имя пользователя и пароль, если требуется.
- **Антивирусная сеть** – обновление через локальную сеть с

компьютера, на котором установлен продукт **Dr.Web** и создано зеркало обновлений.



Создание зеркала обновлений

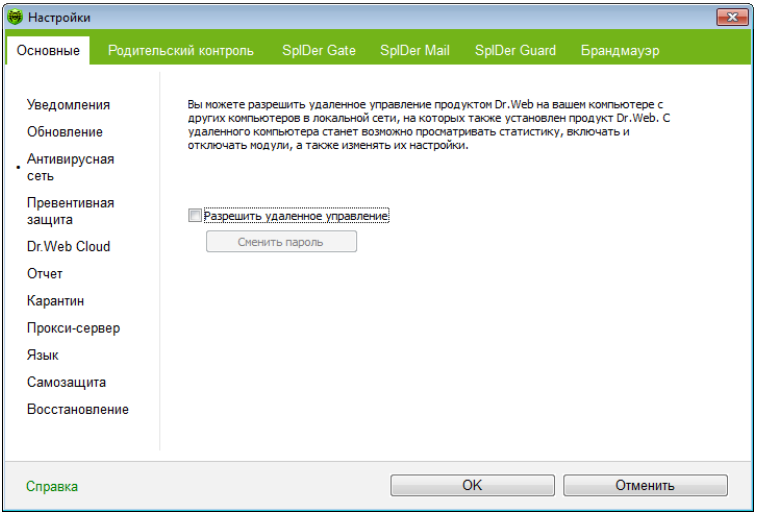
Чтобы ваш компьютер могли использовать как источник обновлений другие компьютеры в локальной сети, на которых установлен продукт **Dr.Web**, нажмите кнопку **Изменить** в пункте **Зеркало обновлений** и в открывшемся окне выберите Создавать зеркало обновлений. Укажите путь к папке, в которую будут копироваться обновления. Если ваш компьютер входит в несколько подсетей, вы можете указать адрес, который будет доступен только для одной из подсетей. Также вы можете указать порт, на котором сервер HTTP будет принимать запросы на соединение.



Раздел Антивирусная сеть

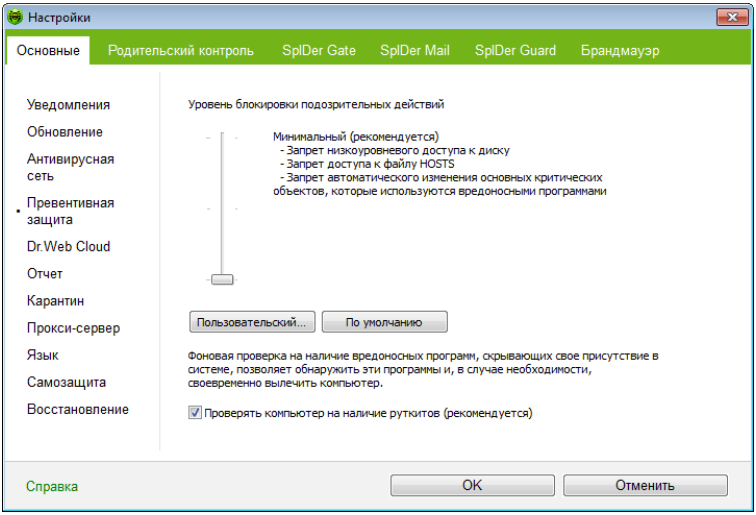
В данном разделе вы можете разрешить удаленное управление вашим антивирусом с других компьютеров локальной сети при помощи компонента Антивирусная сеть. Вхождение в состав антивирусной сети позволяет создавать на вашем компьютере зеркала обновлений, а также удаленно контролировать состояние антивирусной защиты (просматривать статистику, включать и отключать компоненты **Dr.Web Security Space**, а также изменять их настройки).

Для предотвращения несанкционированного доступа к настройкам **Dr.Web Security Space** на вашем компьютере необходимо задать пароль для удаленного управления.



Раздел Превентивная защита

В данном разделе вы можете настроить реакцию **Dr.Web Security Space** на действия сторонних приложений, которые могут привести к заражению вашего компьютера. Также в данном разделе включается фоновое сканирование операционной системы на заражение руткитами (вредоносными программами, предназначенными для сокрытия изменений в операционной системе, таких как работа определенных процессов, модификация ключей реестра, папок или файлов).



Уровень превентивной защиты

В режиме работы **Минимальный**, установленном по умолчанию, **Dr.Web Security Space** запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствует о попытке вредоносного воздействия на операционную систему. Также запрещается низкоуровневый доступ к диску и модификация файла HOSTS.

При повышенной опасности заражения вы можете поднять уровень защиты до **Среднего**. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.

В данном режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.

При необходимости полного контроля за доступом к критическим объектам Windows вы можете поднять уровень защиты до

Параноидального. В данном случае вам также будет доступен интерактивный контроль за загрузкой драйверов, автоматическим запуском программ и работой системных служб.

Пользовательский режим

Данный режим позволяет гибко настроить реакцию **Dr.Web Security Space** на определенные действия, которые могут привести к заражению 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.

Фоновая проверка на заражение

Входящий в состав **Dr.Web Security Space Антируткит** позволяет в фоновом режиме проводить проверку вашей операционной системы на наличие сложных угроз и при необходимости проводит лечение активного заражения.

При включении данной настройки **Антируткит Dr.Web** будет постоянно находиться в памяти. В отличие от проверки файлов «на лету», проводимой сторожем **SpIDer Guard**, поиск руткитов производится в таких критических областях Windows, как объекты автозагрузки, запущенные процессы и модули, оперативная память, MBR/VBR дисков, системный BIOS компьютера и других.

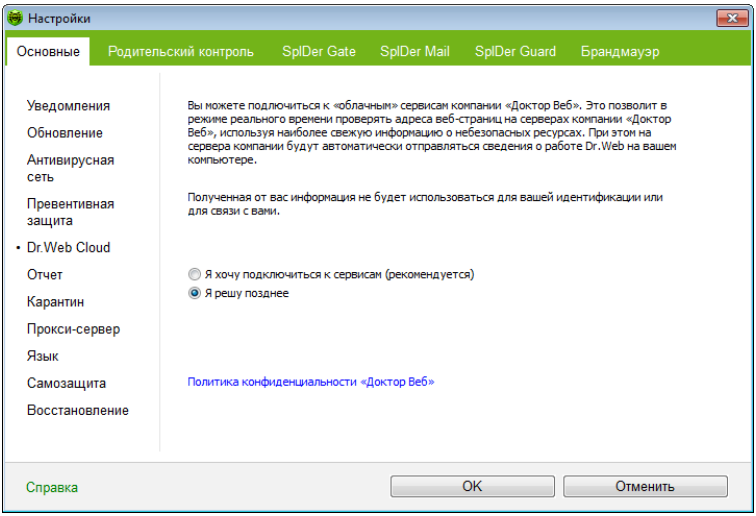
Одним из ключевых критериев работы **Антируткита Dr.Web** является бережное потребление ресурсов операционной системы (процессорного времени, свободной оперативной памяти и т.д.), а также учет мощности аппаратного обеспечения.

При обнаружении угроз **Антируткит Dr.Web** оповещает вас об угрозе и нейтрализует опасные воздействия.

Чтобы включить фоновую проверку, установите флажок **Проверять компьютер на наличие руткитов (рекомендуется).**

Раздел Dr.Web Cloud

В данном разделе вы можете подключиться к «облачным» сервисам компании **«Доктор Веб»** и программе улучшения качества работы продуктов **Dr.Web**.



«Облачные» сервисы

URL-фильтр **Dr.Web Cloud Checker** позволяет в режиме реального времени проверять адреса веб-страниц сети Интернет на серверах компании **«Доктор Веб»**.

В зависимости от настроек обновления информация о вредоносных сайтах и списки страниц различных категорий, используемые при работе компонентами **SpIDer Gate** и

Родительский контроль, могут устаревать. Использование « облачных» сервисов позволяет гарантированно оградить пользователей вашего компьютера от сайтов следующих типов:

- известные источники вирусов;
- сайты, нерекомендуемые к посещению специалистами компании **«Доктор Веб»**;
- сайты для взрослых;
- сайты о насилии;
- сайты об оружии;
- страницы азартных игр;
- сайты о наркотиках;
- сайты о терроризме;
- страницы с нецензурной лексикой;
- чаты;
- сайты электронной почты;
- сайты социальных сетей.

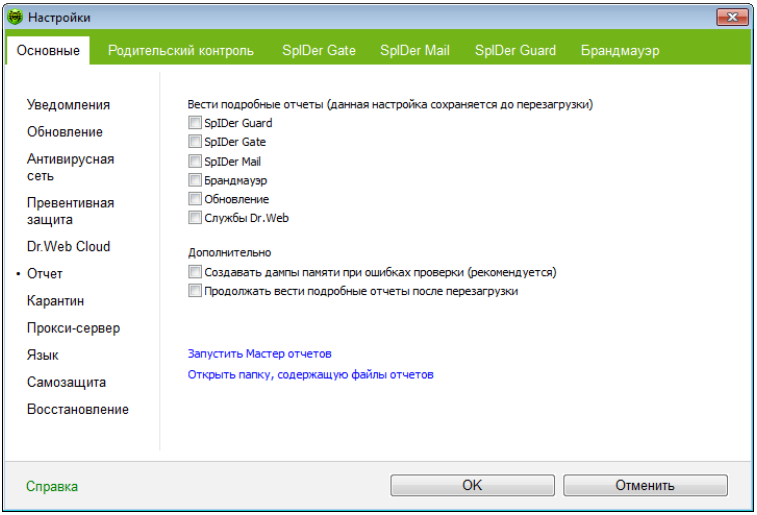
Программа улучшения качества ПО

При участии в программе на сервера компании **«Доктор Веб»** будут автоматически отправляться обезличенные сведения о работе **Dr.Web Security Space** на вашем компьютере, в частности, сведения о созданных вами правилах **Брандмауэра Dr.Web**. Полученная информация не будет использоваться для идентификации пользователя или связи с ним.

Нажмите на ссылку **Политика конфиденциальности «Доктор Веб»**, чтобы ознакомиться с политикой конфиденциальности на официальном сайте компании **«Доктор Веб»**.

Раздел Отчет

В данном разделе вы можете настроить параметры ведения файлов отчетов для компонентов **Dr.Web Security Space**.



По умолчанию для всех компонентов **Dr.Web Security Space** отчеты ведутся в стандартном режиме, фиксирующем следующую информацию:

Компонент	Информация
SpIDer Guard	Проведение обновлений, запуск и останов сторожа **SpIDer Guard**, вирусные события, данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых составных объектов (архивов, файлов электронной почты или файловых контейнеров). Рекомендуется использовать этот режим для определения объектов, которые сторож **SpIDer Guard** проверяет наиболее часто. При необходимости вы можете добавить такие объекты в список исключений, что может снизить нагрузку на компьютер.
SpIDer Mail	Проведение обновлений, запуск и останов почтового сторожа **SpIDer Mail**, вирусные события, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов.

Компонент	Информация
	Рекомендуется использовать этот режим для проверки настроек перехвата соединений с почтовыми серверами.
SpIder Gate	Проведение обновлений, запуск и останов веб-антивируса **SpIDer Gate**, вирусные события, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов. Рекомендуется использовать этот режим для получения более детальной информации о проверенных объектах и работе веб-антивируса.
Брандмауэр	В стандартном режиме **Брандмауэр** не ведет файл отчета. При включении режима ведения подробного отчета собираются данные о сетевых пакетах (pcap-логи).
Модуль обновления	Список обновленных файлов **Dr.Web Security Space** и статусы их загрузки, информация о работе вспомогательных скриптов, дата и время проведения обновления, информация о перезапуске компонентов **Dr.Web Security Space** после обновления.

Просмотр файлов отчетов

Чтобы просмотреть отчеты, нажмите на ссылку **Открыть папку, содержащую файлы отчетов**.

Включение подробных отчетов

При ведении подробных отчетов фиксируется максимальное количество информации о работе компонентов **Dr.Web Security Space**, что может привести к значительному увеличению файлов отчетов и снизить производительность работы операционной системы. Рекомендуется использовать этот режим только при возникновении проблем в работе компонентов или по просьбе технической поддержки компании **«Доктор Веб»**.

1. Чтобы включить режим ведения подробного отчета для одного из компонентов **Dr.Web Security Space**, установите соответствующий флажок.
2. По умолчанию подробный отчет ведется до первой перезагрузки операционной системы. Если необходимо зафиксировать поведение компонента в период до и после перезагрузки, установите флажок **Продолжать вести подробные отчеты после перезагрузки**.
3. Сохраните изменения.

Дополнительные настройки

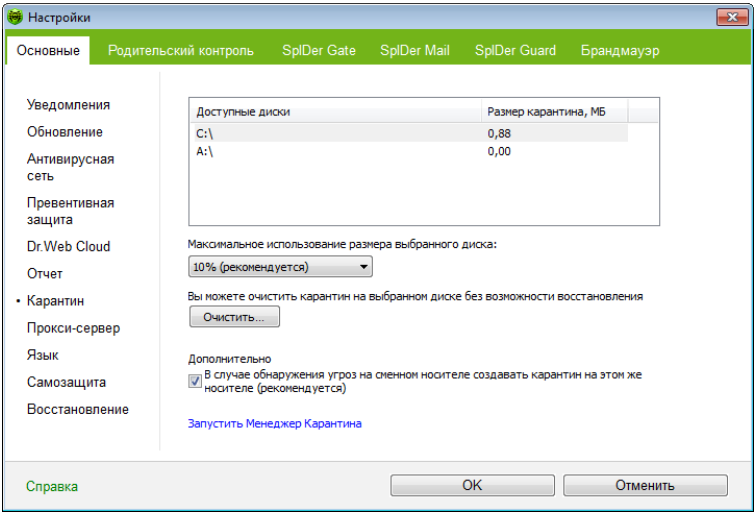
Настройка **Создавать дампы памяти при ошибках проверки (рекомендуется)** позволяет сохранять максимум полезной информации о причинах некорректной работы компонентов **Dr.Web Security Space**, что позволит специалистам компании **«Доктор Веб»** в дальнейшем провести более полный анализ проблемы и предложить ее решение. Рекомендуется включать данную настройку при возникновении ошибок в работе **Dr.Web Security Space**.

В данном разделе вы также можете собрать данные о вашей операционной системе и работе **Dr.Web Security Space** для обращения в службу технической поддержки компании **«Доктор Веб»**. Для этого нажмите на ссылку **Запустить Мастер отчетов**.

Раздел Карантин

В данном разделе вы можете настроить параметры работы Карантина Dr.Web Security Space, оценить его размер, а также удалить все изолированные файлы с конкретного диска.

Каталог **Карантина** создается отдельно на каждом логическом диске, где были обнаружены подозрительные файлы.



Ограничение размера Карантина

1. Чтобы задать максимальный размер папки **Карантина** на определенном диске, выберите этот диск в списке.
2. В списке **Максимальное использование размера выбранного диска** выберите необходимое ограничение.

   Максимально допустимый размер **Карантина** определяется в процентном соотношении относительно общего размера диска (при наличии нескольких логических дисков, данный размер будет рассчитан отдельно для каждого диска, на котором располагаются папки **Карантина**). При выборе значения **Не ограничено** папка **Карантина** может занимать все доступное дисковое пространство.

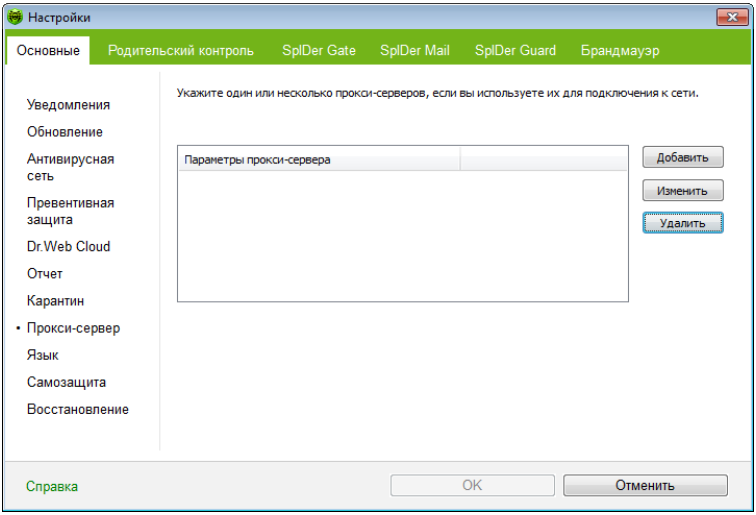
Очистка Карантина

1. Чтобы удалить все файлы, помещенные в каталог **Карантина** на определенном диске, выберите этот диск в списке.
2. Нажмите кнопку **Удалить** и подтвердите запрос на удаление.

В группе **Дополнительно** вы можете задать режим изоляции зараженных объектов, обнаруженных на съемных носителях. По умолчанию подобные угрозы помещаются в каталог на том же носителе и не шифруются. При этом папка **Карантина** создается только в том случае, если возможна запись на носитель. Использование отдельных каталогов и отказ от шифрования на съемных носителях позволяет предотвратить возможную потерю данных.

Раздел Прокси-сервер

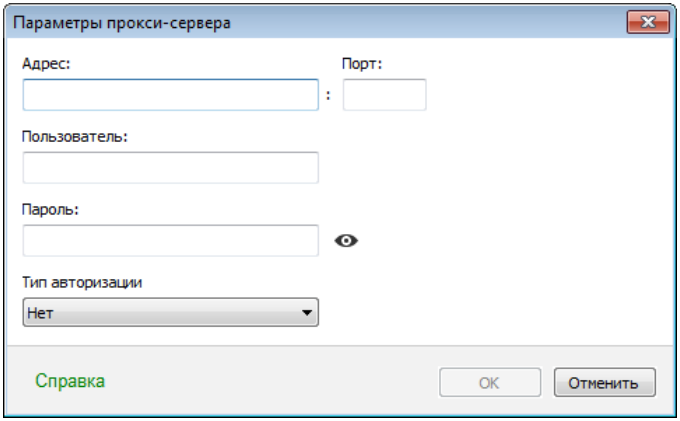
В данном разделе вы можете настроить параметры доступа к сети для **Модуля обновления**.



По умолчанию используется режим прямого подключения. При необходимости вы можете добавить настройки подключения к одному или нескольким прокси-серверам.

Формирование списка прокси-серверов

1. В Основных настройках **Dr.Web Security Space** выберите раздел **Прокси-сервер**.
2. Чтобы добавить новый прокси-сервер, нажмите кнопку **Добавить**. Откроется окно настройки подключения.



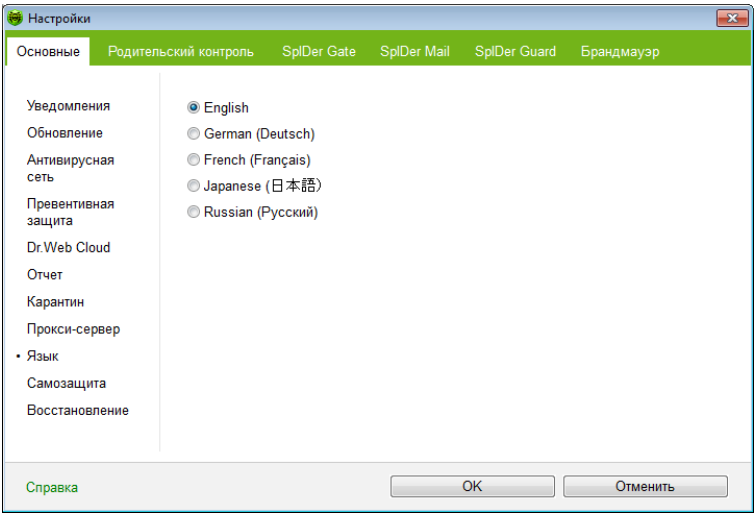
3. Укажите настройки подключения к прокси-серверу:

Настройка	Описание
Адрес	Укажите адрес прокси-сервера.
Порт	Укажите порт прокси-сервера.
Пользователь	Укажите имя учетной записи для подключения к прокси-серверу.
Пароль	Укажите пароль учетной записи, используемой для подключения к прокси-серверу.
Тип авторизации	Выберите тип авторизации, требуемый для подключения к прокси-серверу.

4. При необходимости повторите шаги 2 и 3 для добавления других прокси-серверов. Чтобы отредактировать настройки подключения к прокси-серверу, выберите его в списке и нажмите кнопку **Изменить**. Чтобы удалить прокси-сервер из списка, выберите его в списке и нажмите кнопку **Удалить**.
5. По окончании редактирования списка нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

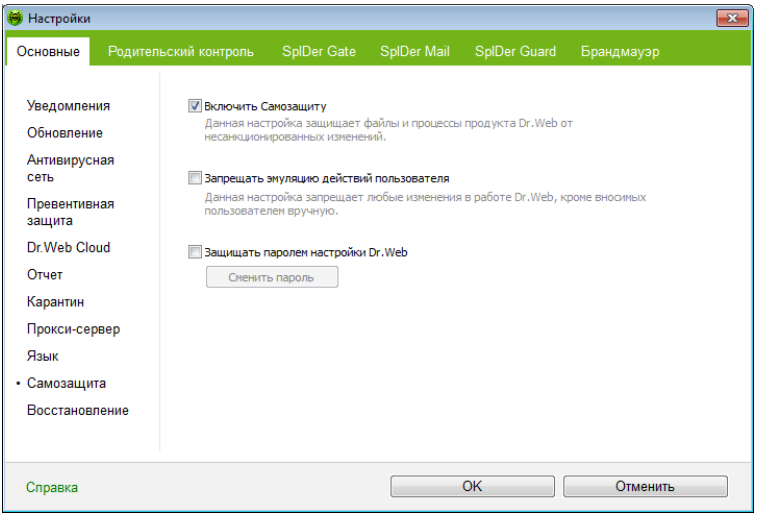
Раздел Язык

В данном разделе вы можете выбрать язык программы. Список языков пополняется автоматически и содержит все доступные на текущий момент локализации графического интерфейса **Dr.Web Security Space**.



Раздел Самозащита

В данном разделе вы можете настроить параметры защиты самого **Dr.Web Security Space** от несанкционированного воздействия, например, анти-антивирусных программ, а также от случайного повреждения.



Настройка **Включить самозащиту** позволяет защитить файлы и процессы **Dr.Web Security Space** от несанкционированного доступа. Отключать самозащиту не рекомендуется.

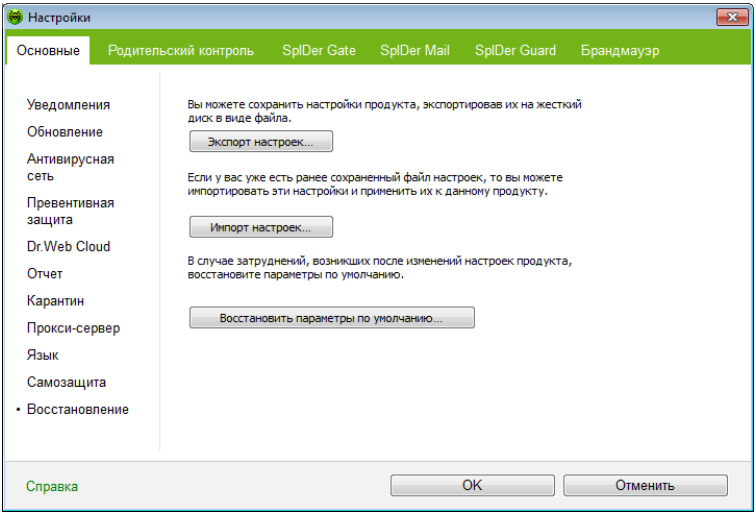
Настройка **Запрещать эмуляцию действий пользователя** позволяет предотвратить любые изменения в работе **Dr.Web Security Space**, производимые автоматизированно. В том числе будет запрещено исполнение скриптов, эмулирующих работу пользователя с программой **Dr.Web Security Space**, запущенных самим пользователем.

Настройка **Защищать паролем настройки Dr.Web** позволяет установить пароль для доступа к настройкам **Dr.Web Security Space** на вашем компьютере. Задайте пароль, который будет

запрашиваться при обращении к настройкам **Dr.Web Security Space**.

Раздел Восстановление

В данном разделе вы можете восстановить настройки **Dr.Web Security Space** по умолчанию, а также экспортировать или импортировать их.



3.3. Менеджер лицензий

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

Для доступа к этому окну в группе **Инструменты** контекстного меню **SpIDer Agent**  выберите пункт **Менеджер лицензий.**

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 **Dr.Web Security Space** 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. **Dr.Web Security Space** 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.

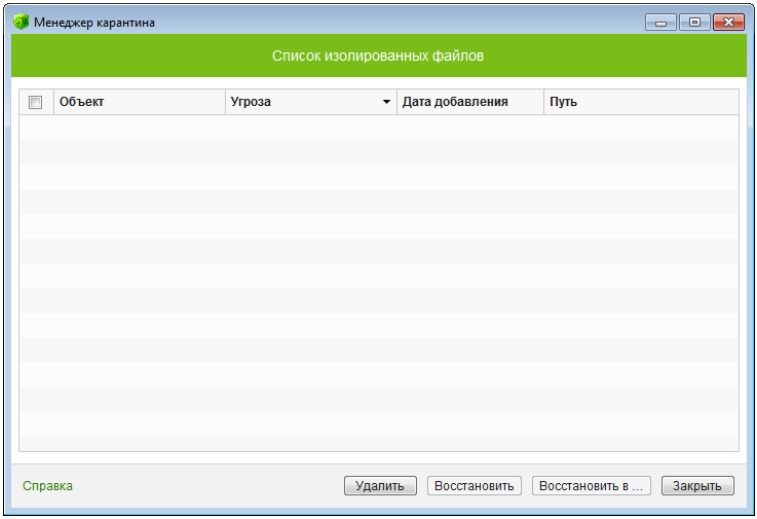
При работе программы ключевой файл по умолчанию должен находиться в каталоге установки. **Dr.Web Security Space** регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа не модифицируйте ключевой файл.

При отсутствии действительного ключевого файла (лицензионного или демонстрационного) активность всех компонентов блокируется. Чтобы получить действительный ключевой файл, выберите пункт **Зарегистрировать лицензию** в контекстном меню значка **SpIDer Agent**.

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.

Для доступа к этому окну в группе **Инструменты** контекстного меню **SpIDer Agent** выберите пункт **Менеджер Карантина.**



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

- **Объект** – список имен объектов, находящихся в карантине;
- **Угроза** – классификация вредоносной программы, определяемая **Dr.Web Security Space** при автоматическом

перемещении объекта в карантин;

- **Дата добавления** – дата, когда объект был перемещен в **Карантин**;
- **Путь** – полный путь, по которому находился объект до перемещения в карантин.

В окне **Карантина** файлы могут видеть только те пользователи, которые имеют к ним доступ.

Чтобы отобразить скрытые объекты, запустите под административной учетной записью либо файл dwqrui.exe, расположенный в каталоге установки, либо собственно **Dr.Web Security Space**.

В окне карантина доступны следующие кнопки управления:

- **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);
- **Восстановить в** – переместить файл под заданным именем в нужную папку;

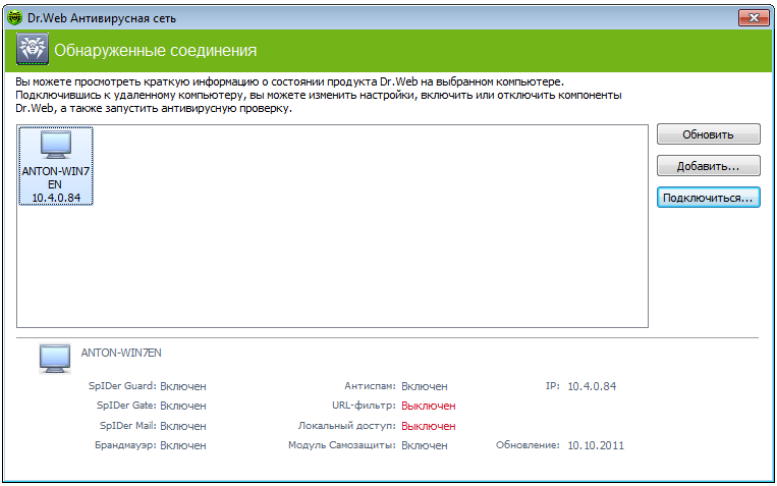
Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

- **Удалить** – удалить файл из карантина и из системы.

Для одновременной работы с несколькими файлами установите флажки рядом с названиями объектов, а затем выберите необходимое действие.

3.5. Антивирусная сеть

Этот компонент позволяет управлять программами **Антивирус Dr.Web**, **Антивирус Dr.Web для серверов** и **Dr.Web Security Space** версии 8.0 на других компьютерах в пределах одной локальной сети. Для удаленной работы с **продуктами Dr.Web** щелкните значок **SpIDer Agent** в области уведомлений Windows и в подменю **Инструменты** выберите пункт **Антивирусная сеть**.



Для доступа к удаленному антивирусу, выберите компьютер в списке и нажмите кнопку **Подключиться**. Введите пароль, заданный в настройках удаленного антивируса. В области уведомлений Windows появится значок удаленного **SpIDer Agent**. Пользователь антивируса, к которому вы подключились, получит уведомление в виде всплывающей подсказки. При работе с удаленным антивирусом вам доступны следующие пункты (набор компонентов варьируется в зависимости от того, к какому продукту **Dr.Web** установлено подключение):

- **О программе**

- Зарегистрировать лицензию
- **Мой Dr.Web**
- **Справка**
- SpIDer Guard
- SpIDer Mail
- SpIDer Gate
- Родительский контроль
- Брандмауэр
- Обновление
- **Инструменты**
- **Отключить/Включить Самозащиту**

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

- к Менеджеру лицензий;
- к настройкам общих параметров работы **Dr.Web** (см. Основные настройки).
- к созданию отчета.

Вы можете просматривать статистику, включать и отключать модули, а также изменять их настройки.

Компоненты **Антивирусная сеть**, **Карантин** и **Сканер** недоступны. Настройки и статистика **Брандмауэра Dr.Web** также недоступны, однако вы можете включить или отключить этот компонент. Также вам доступен пункт **Отсоединиться**, при выборе которого завершается установленное соединение с удаленным антивирусом.

Если необходимый компьютер не отображается в сети, попробуйте добавить его вручную. Для этого нажмите кнопку **Добавить** и введите IP-адрес.

Вы можете установить только одно соединение с удаленным **продуктом Dr.Web**. При наличии установленного соединения кнопка **Подключиться** недоступна.

Компьютеры в локальной сети отображаются в списке только в том случае, если в установленном на них продукте **Dr.Web**

разрешено удаленное управление. Вы можете разрешить подключение к **Dr.Web Security Space** на вашем компьютере в разделе **Антивирусная сеть** Основных настроек.

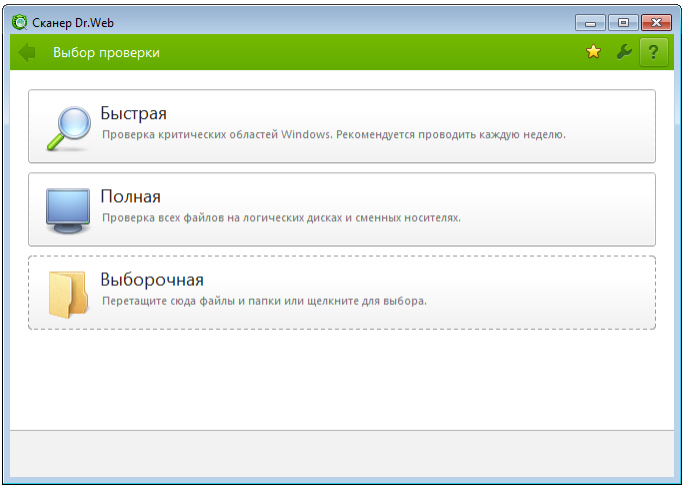
Пункт **Антивирусная сеть** доступен только в Административном режиме.

4. Сканер Dr.Web

По умолчанию **Сканер Dr.Web** производит антивирусную проверку 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).

В случае обнаружения вредоносного объекта **Сканер Dr.Web** только предупреждает вас об угрозе. Отчет о результатах проверки приводится в таблице, где вы можете выбрать необходимое действие для обработки обнаруженного вредоносного или подозрительного объекта. Вы можете как применить действия по умолчанию ко всем обнаруженным угрозам, так и выбрать необходимый метод обработки для отдельных объектов.

Действия по умолчанию являются оптимальными для большинства применений, но при необходимости вы можете изменить их в окне настройки параметров работы **Сканера Dr.Web**. Если действие для отдельного объекта вы можете выбрать по окончании проверки, то общие настройки по обезвреживанию конкретных типов угроз необходимо задавать до начала проверки.



4.1. Проверка компьютера

Сканер устанавливается как обычное приложение Windows и запускается по команде пользователя (или по расписанию, см. Запуск проверки по расписанию).

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**);

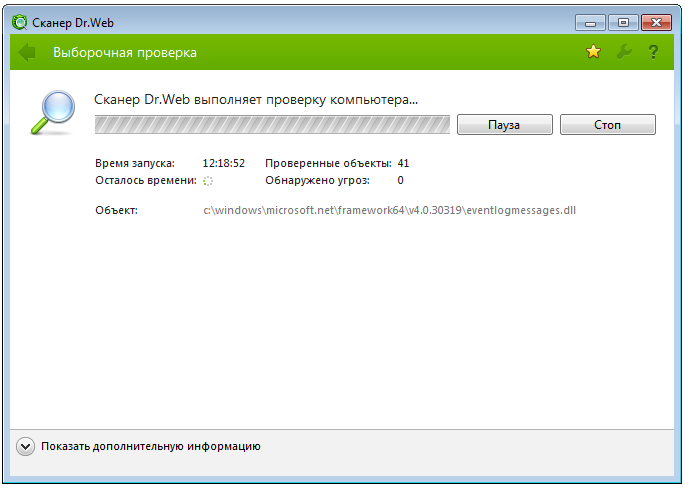
- специальную команду операционной системы Windows (подробнее см. п. Запуск Сканера из командной строки).

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 проверка заданного объекта.



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

   Во время *быстрой проверки* проверяются:

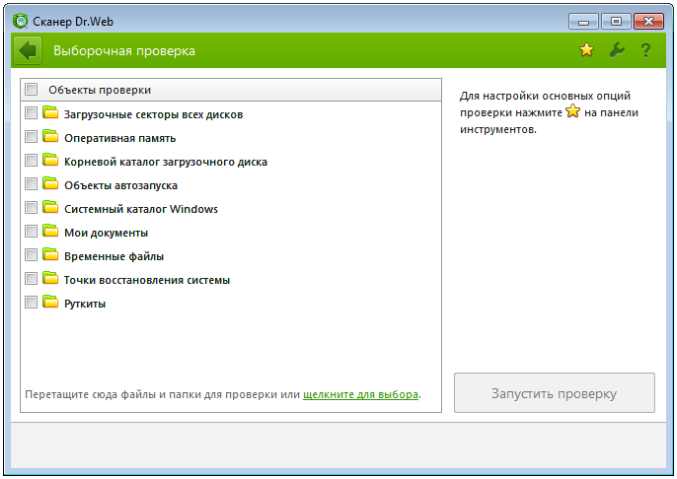
   - оперативная память;
   - загрузочные секторы всех дисков;

- 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 запуске 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.

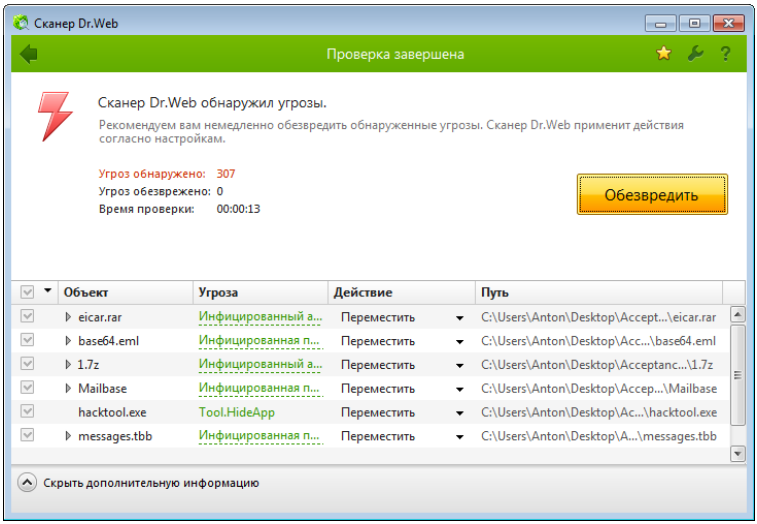


5. После начала проверки в правой части окна становятся доступными кнопки **Пауза** и **Стоп**. На любом этапе проверки вы можете сделать следующее:
   - чтобы приостановить проверку, нажмите кнопку **Пауза**. Для того чтобы возобновить проверку после паузы, нажмите кнопку **Продолжить**;
   - чтобы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

Кнопка **Пауза** недоступна во время проверки оперативной памяти и процессов.

4.2. Действия при обнаружении вирусов

По окончании проверки **Сканер Dr.Web** лишь информирует об обнаруженных угрозах и предлагает применить к ним наиболее оптимальные действия по обезвреживанию. Вы можете обезвредить все обнаруженные угрозы одновременно. Для этого после завершения проверки нажмите кнопку **Обезвредить**, и **Сканер Dr.Web** применит оптимальные действия по умолчанию для всех обнаруженных угроз. Также вы можете применить действие для каждой угрозы по отдельности.



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 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, которы находится в каталоге %USERPROFILE%\Doctor Web.

4.3. Настройка Сканера

Изменение настроек программы

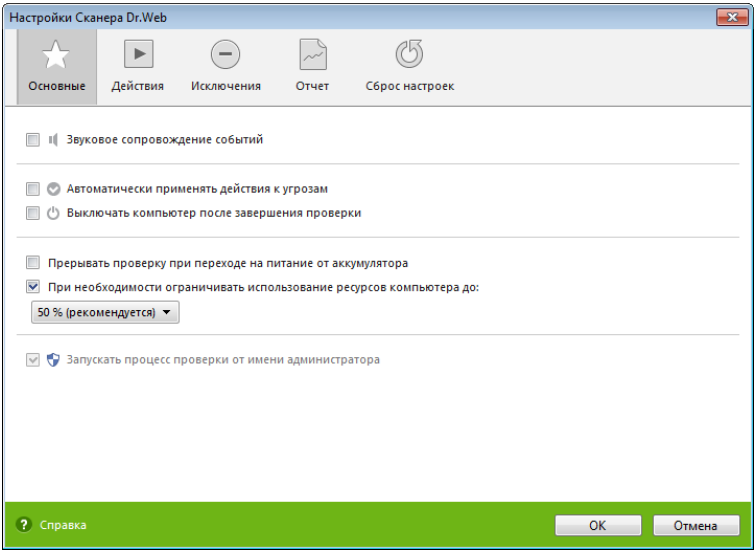
1. Чтобы вызвать **Настройки Сканера**, щелкните на панели инструментов иконку **Настройки**  .

   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**.

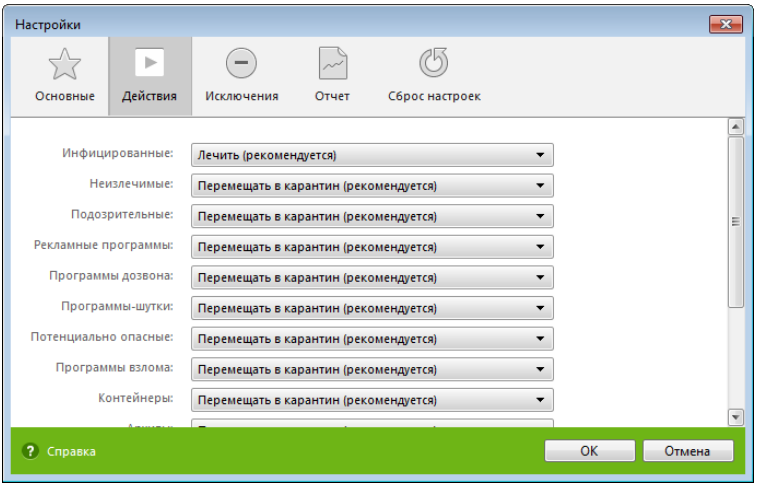


Вы можете включить звуковое сопровождение событий, а также указать **Сканеру Dr.Web** автоматически применять действия к угрозам и настроить взаимодействие программы с операционной системой.

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

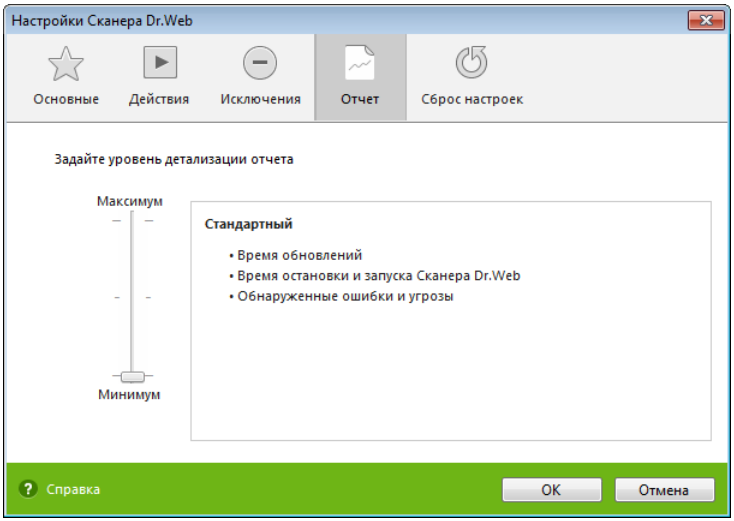
Сканера при обнаружении вирусов или подозрительного кода в файловых архивах, инсталляционных пакетах и почтовых ящиках. Действия по отношению к вышеуказанным объектам выполняются над всем объектом, а не только над зараженной его частью. По умолчанию во всех этих случаях предусмотрено информирование.

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 проверки и перечень проверяемых объектов в качестве параметров вызова. Именно в таком режиме возможен автоматический вызов **Сканера** по расписанию.

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 **Dr.Web Security Space** 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 – проверка успешно завершена, инфицированные объекты не найдены;

1 – проверка успешно завершена, найдены инфицированные объекты;

10 – указаны некорректные ключи;

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

12 – не запущен **Scanning Engine**;
255 – проверка прервана пользователем.

4.6 Запуск проверки по расписанию

При установке **Dr.Web** в стандартном **Планировщике** заданий Windows автоматически создается задание на проведение антивирусной проверки (оно по умолчанию выключено).

Для запуска **Планировщика** заданий откройте **Панель управления** (расширенный вид) → **Администрирование** → **Планировщик заданий**.

В списке заданий выберите задание на антивирусную проверку. Вы можете активировать задание, а также настроить время запуска проверки и задать необходимые параметры.

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

Вы также можете создавать собственные задания на антивирусную проверку. Подробнее о работе с системным расписанием см. справочную систему и документацию операционной системы Windows.

Если в состав устанавленных компонентов входит **Брандмауэр**, то после установки **Dr.Web Security Space** и первой перезагрузки служба системного расписания будет заблокирована **Брандмауэром**. Компонент **Назначенные задания** будет функционировать только после повторной перезагрузки, т. к. необходимое правило уже будет создано к этому моменту.

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.

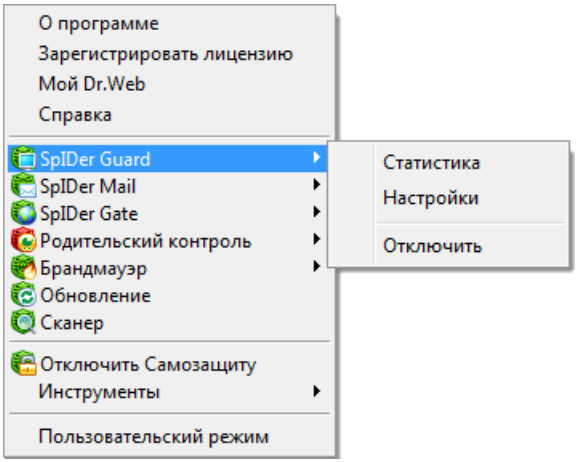
При настройках по умолчанию сторож «на лету» проверяет на жестком диске – только создаваемые или изменяемые файлы, на сменных носителях – все открываемые файлы. Кроме того, сторож постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при их обнаружении блокирует эти процессы.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

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 временно отключить или заново запустить **SpIDer Guard** (доступно только пользователю, имеющему права администратора данного компьютера).

При отключении **SpIDer Guard** запрашивается код подтверждения или пароль (если в разделе **Самозащита** Основных настроек **Dr.Web Security Space** вы установили флажок **Защищать паролем настройки Dr.Web**).

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

Восстановить параметры работы программы, используемые по умолчанию, а также экспортировать или импортировать настройки вы можете в разделе **Восстановление** Основных настроек **Dr.Web Security Space**.

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 на ссылку **Справка**.
4. По окончании редактирования настроек:
   - чтобы сохранить изменения, нажмите кнопку **ОК**;
   - чтобы отказаться от внесенных изменений, нажмите кнопку **Отмена**.

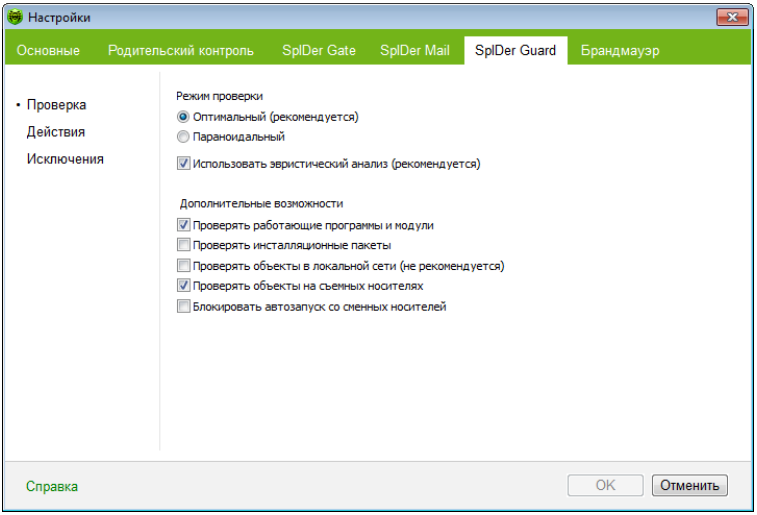
Раздел Проверка

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

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**.

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.

Настройка действий

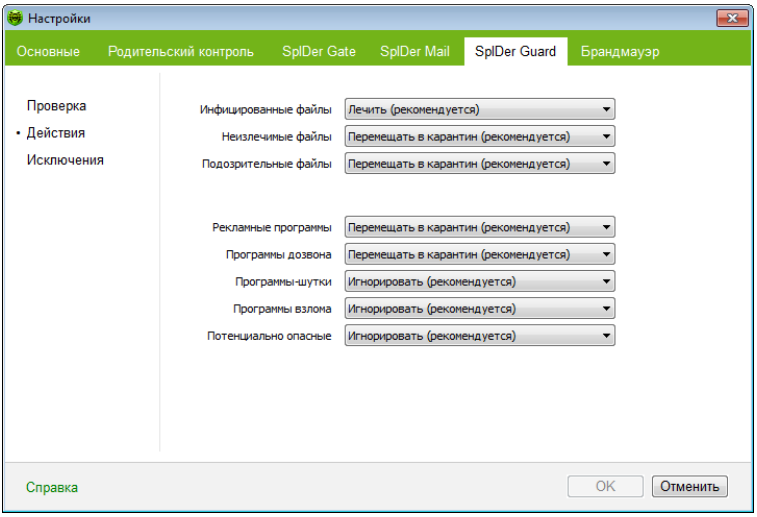
В разделе **Действия** вы можете настроить автоматические действия сторожа с зараженными объектами.

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**.

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 можете вручную ввести полный путь к файлу или каталогу в поле ввода, а также отредактировать запись в поле ввода перед добавлением ее в список;
- 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.

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. Почтовый сторож также может осуществлять проверку корреспонденции на спам с помощью компонента **Антиспам Dr.Web**.

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 проверки 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 на некоторое время приостановить работу почтового сторожа.

Принцип работы почтового сторожа

Антивирусный почтовый сторож получает все входящие письма вместо почтового клиента и подвергает их антивирусной проверке 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 остаются на POP3- или IMAP4-сервере.

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.

Почтовый сторож предоставляет возможность проверки входящих писем на спам с помощью компонента Антиспам Dr.Web. По умолчанию эта возможность включена. (О настройках работы

Антиспама Dr.Web см. п. Настройка SpIDer Mail).

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.

Антиспам Dr.Web

Технологии **Антиспама Dr.Web** состоят из нескольких тысяч правил, которые условно можно разбить на несколько групп:

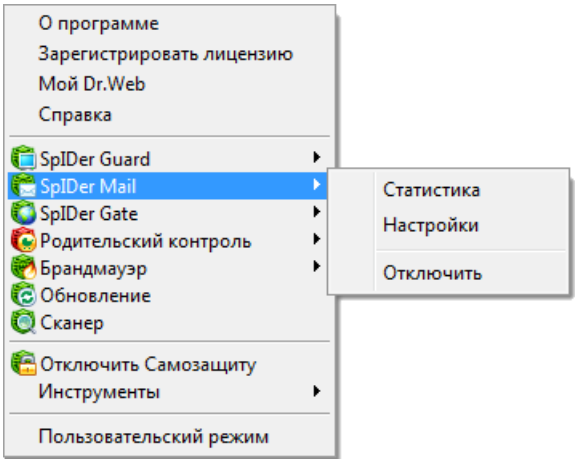
- **эвристический анализ** – чрезвычайно сложная, высокоинтеллектуальная технология эмпирического разбора всех частей письма: поля заголовка, тела, содержания вложения;
- **фильтрация противодействия** – состоит в распознавании уловок, используемых спамерами для обхода антиспам-фильтров;
- **анализ на основе HTML-сигнатур** – сообщения, в состав которых входит HTML-код, сравниваются с образцами библиотеки HTML-сигнатур антиспама;
- **семантический анализ** – сравнение слов и выражений сообщения со словами и идиомами, типичными для спама,

производится по специальному словарю. Анализу подвергаются как видимые, так и визуально скрытые специальными техническими уловками слова, выражения и символы;

- **анти-скамминг технология** – к числу скамминг- и фарминг-сообщений относятся т.н. «нигерийские письма», сообщения о выигрышах в лотерею, казино, поддельные письма банков. Для их фильтрации применяется специальный модуль;
- **фильтрация технического спама** – так называемые bounce-сообщения возникают как реакция на вирусы, или как проявление вирусной активности. Специальный модуль антиспама определяет такие сообщения как нежелательные.

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).

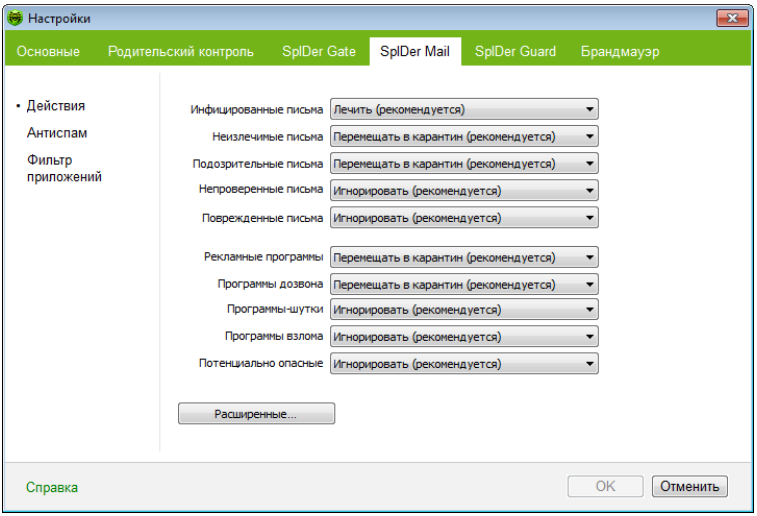
Пункт **Отключить**/**Включить** позволяет временно отключить или заново запустить работу **SpIDer Mail**.

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

Восстановить параметры работы программы, используемые по умолчанию, а также экспортировать или импортировать настройки вы можете в разделе **Восстановление** Основных настроек **Dr.Web Security Space**.

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 на ссылку **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**.

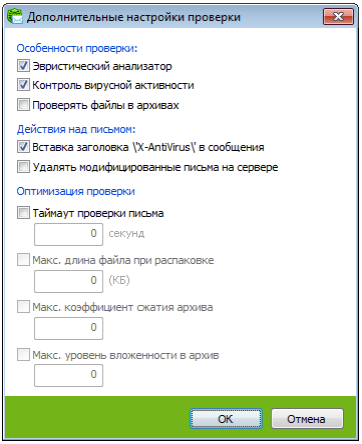
Защиту от подозрительных писем можно отключать только в том случае, когда компьютер дополнительно защищен постоянно загруженным сторожем **SpIDer Guard**.

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 проверки нажмите кнопку **Дополнительно**.



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

- **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

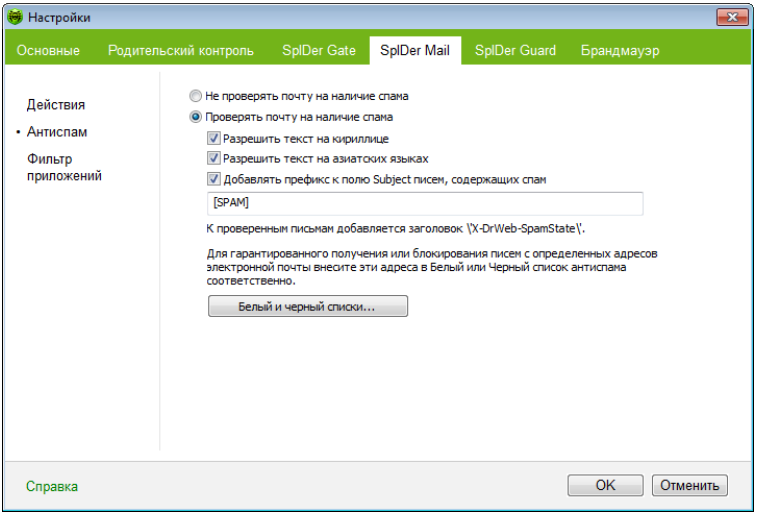
программа определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка производиться не будут;

- **Максимальный уровень вложенности в архив**. Если уровень вложенности в архив превышает указанный, проверка будет производиться только до указанного уровня вложенности.

Раздел Антиспам

Изменение настроек **Антиспама Dr.Web** осуществляется в разделе **Антиспам**.

Почтовый сторож по умолчанию осуществляет проверку входящих писем на спам. Для того чтобы входящая корреспонденция не проверялась **Антиспамом**, выберите режим **Не проверять почту на наличие спама**.



Ко всем проверенным письмам будут добавляться заголовки:

- `X-DrWeb-SpamState: Yes/No`. Значение `Yes` показывает, что письму присвоен статус спам, `No` — письмо, по мнению **SpIDer Mail**, спамом не является.
- `X-DrWeb-SpamVersion: version`. version – версия библиотеки **Антиспама Dr.Web**.
- `X-DrWeb-SpamReason: рейтинг спама`. Рейтинг спама включает в себя перечень оценок по различным критериям принадлежности к спаму.

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

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

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

Установка и снятие флага **Разрешать текст на азиатских языках** работает аналогично.

При нажатии кнопки **Белый и Черный списки** открывается окно, в котором содержатся «черные» и «белые» списки адресов отправителей почтовых сообщений.

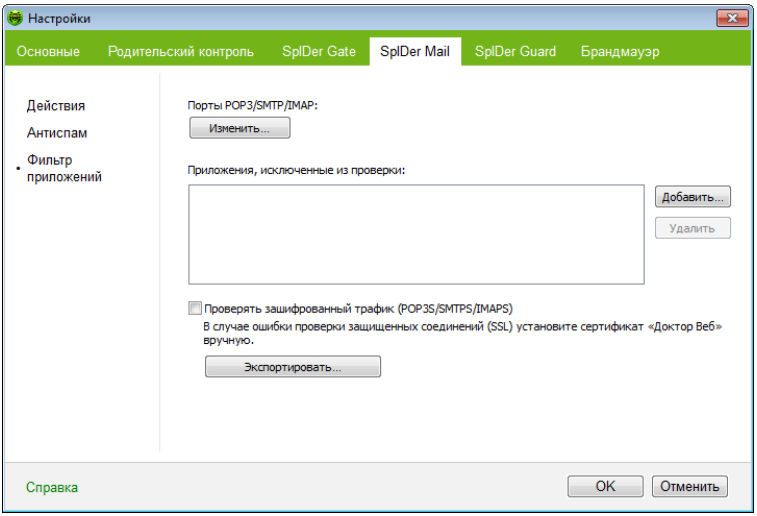
- Если адрес отправителя добавлен в «белый» список, письмо не подвергается анализу на содержание спама.
- Если адрес отправителя добавлен в «черный» список, письму без дополнительного анализа присваивается статус спама.

Чтобы добавить в список определенного отправителя, введите его полный почтовый адрес. Допускается использование знака «*» вместо части адреса. (Например, запись вида `*@domain.org` означает все адреса с доменным именем `domain.org`).

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

Раздел Фильтр приложений

По умолчанию почтовый сторож **SpIDer Mail** автоматически перехватывает почтовый трафик всех пользовательских приложений на вашем компьютере. В этом разделе задаются параметры перехвата соединений с почтовыми серверами, а также список приложений, почтовый трафик которых не будет перехватываться и, соответственно, анализироваться почтовым сторожем.

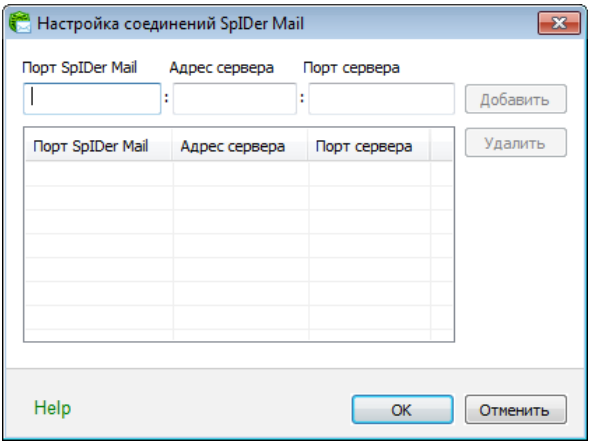


Чтобы добавить файл, папку или маску в список исключений,

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

Чтобы изменить настройки перехвата соединений, нажмите кнопку **Изменить.**

По умолчанию список включает все IP-адреса (задано при помощи символа *) и любые адреса с портами 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 сервера,** а номер порта, к которому происходит обращение, в поле **Порт сервера,** 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 настройках почтового сторожа **SpIDer Mail** выберите раздел **Фильтр приложений,** затем выберите ручной режим перехвата и нажмите соответствующую кнопку **Изменить.**
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 – порт SpIDer Mail**, выбранный для почтового сервера, 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)**. Если клиент, который получает и передает такие данные, не обращается к хранилищу сертификатов системы Windows, то необходимо будет экспортировать сертификат.

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.

7. Dr.Web для Outlook

Основные функции компонента

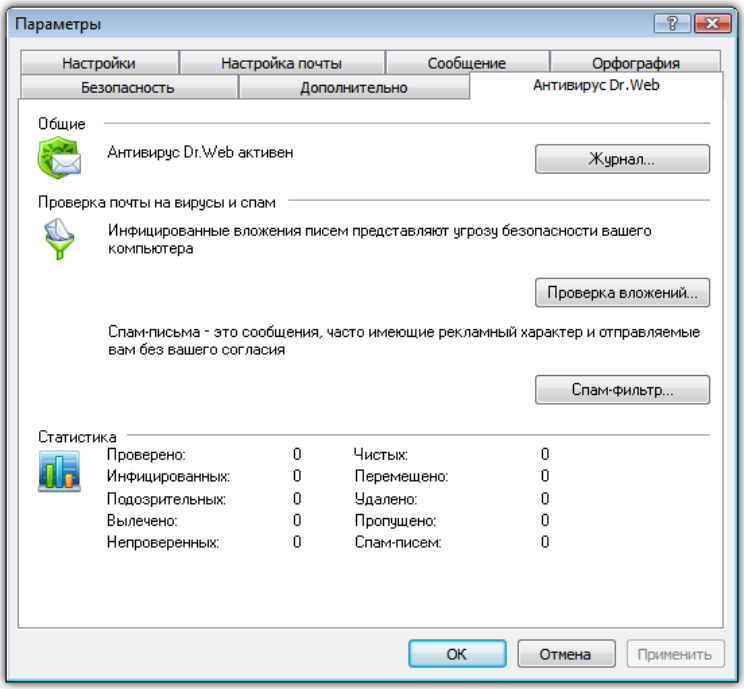
Подключаемый модуль **Dr.Web для Outlook** выполняет следующие функции:

- антивирусная проверка вложенных файлов почтовых сообщений;
- проверка почты, поступающей по зашифрованному соединению SSL;
- проверка почтовых сообщений на спам;
- 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;
- Спам-фильтр – позволяет определить действия программы для спам-сообщений, а также создать белый и черный списки электронных адресов;
- 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

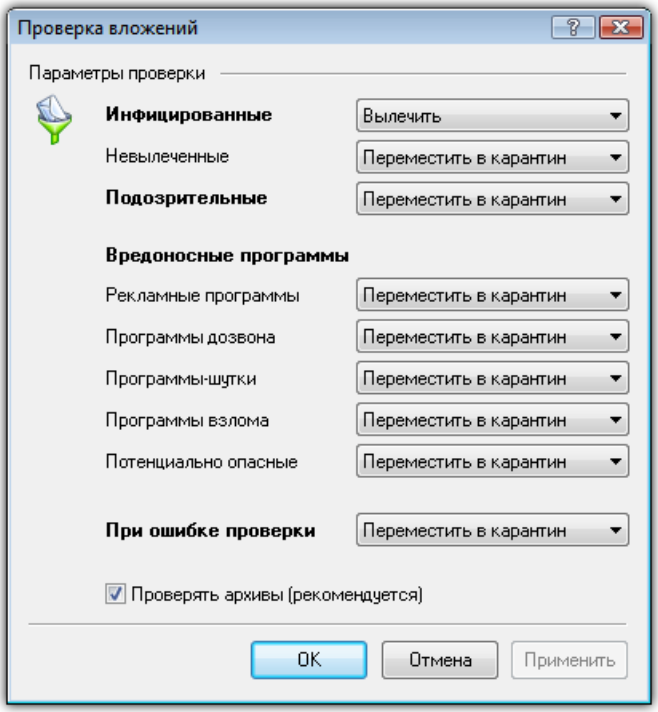
Dr.Web для Outlook обнаруживает следующие вредоносные объекты:

- 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.

7.3. Проверка на спам

Dr.Web для Outlook проверяет на спам все почтовые сообщения с помощью **Антиспама Dr.Web** и осуществляет фильтрацию сообщений в соответствии с настройками, задаваемыми пользователем.

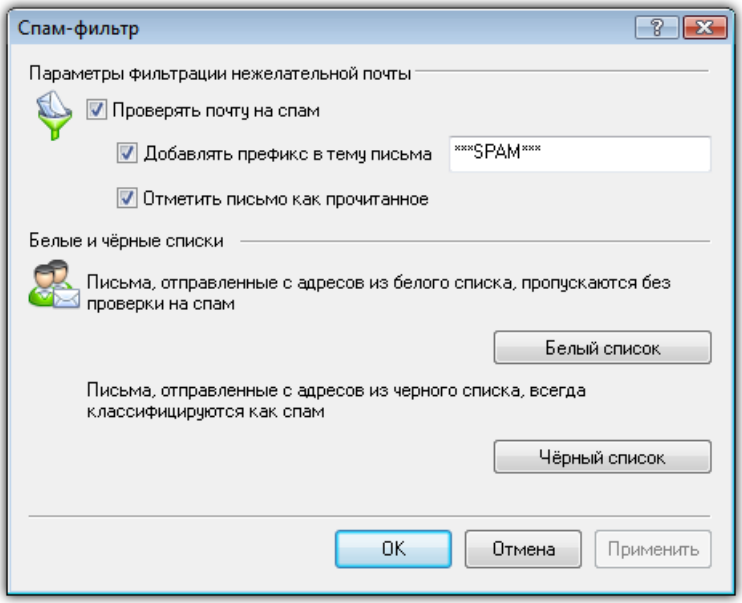
Чтобы настроить проверку сообщений на спам, в почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web** нажмите кнопку **Спам-фильтр** (для Microsoft Outlook 2010 в разделе **Файл** → **Параметры** → **Надстройки** необходимо выбрать модуль **Dr.Web для Outlook** и нажать кнопку **Параметры надстройки**). Откроется окно настроек Спам фильтра.

Окно **Спам-фильтр** доступно только при наличии у пользователя прав администратора системы.

Для ОС Windows Vista и старше при нажатии кнопки **Спам-фильтр**:

- 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.

7.3.1. Настройка спам-фильтра



Настройка спам-фильтра

Для настройки параметров фильтрации спама выполните любые из следующих действий:

- для активации спам-фильтра установите флажок **Проверять почту на спам**;
- если вы хотите добавлять специальный текст в заголовок сообщения, распознанного как спам, установите флажок **Добавлять префикс в тему письма**. Добавляемый текст можно ввести в текстовом поле справа от флага. По умолчанию добавляется префикс ***SPAM***;
- если вы хотите, чтобы проверенные сообщения отмечались как прочитанные в свойствах письма, установите флажок **Отметить письмо как прочитанное**. По умолчанию

флажок **Отметить как прочитанное** установлен;

- настройте белые и черные списки для фильтрации писем.

Если некоторые письма были неправильно распознаны, следует отправить их на специальные почтовые адреса для анализа и повышения качества работы фильтра:

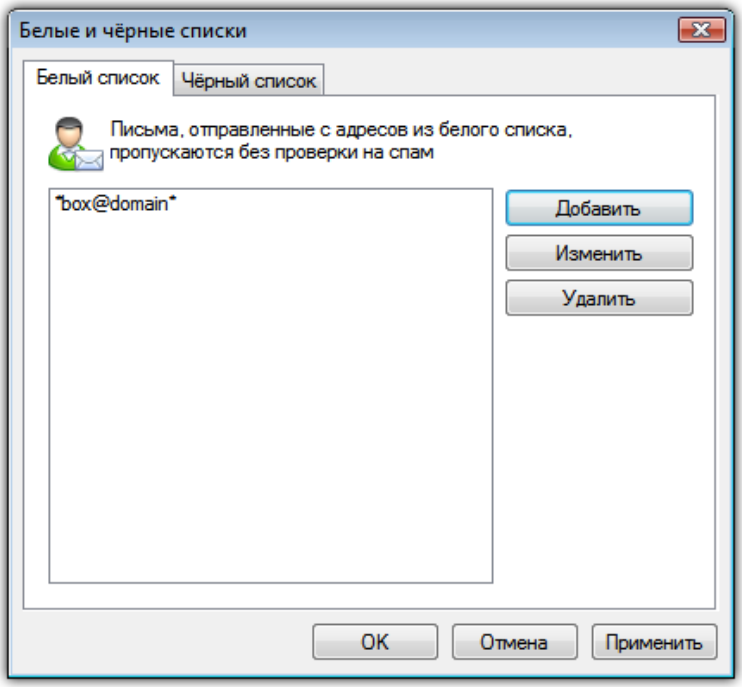
- Письма, ошибочно принятые за спам, следует отправлять на адрес vrnonspam@drweb.com;
- Нераспознанные и пропущенные спам-сообщения следует отправлять на адрес vrspam@drweb.com.

Все сообщения необходимо высылать только в виде вложения (а не в теле письма).

7.3.2. Черный и белый списки

Черный и белый списки электронных адресов служат для фильтрации сообщений.

Для просмотра и редактирования черного или белого списка, в настройках спам-фильтра, нажмите кнопку **Черный список** или **Белый список** соответственно.



Пополнение черного или белого списка

1. Нажмите кнопку **Добавить**.
2. Введите электронный адрес в соответствующее поле (см. методы заполнения белого и черного списков).
3. Нажмите кнопку **ОК** в окне **Редактировать список**.

Изменение адреса в списке

1. Выберите в списке адрес, который вы хотите изменить, и нажмите кнопку **Изменить**.
2. Отредактируйте необходимую информацию.
3. Нажмите **ОК** в окне **Редактировать список**.

Удаление адреса из списка

1. Выберите в списке адрес, который вы хотите удалить.
2. Нажмите кнопку **Удалить**.

В окне **Белые и черные списки** нажмите **ОК**, чтобы сохранить внесенные изменения.

Белый список

Если адрес отправителя добавлен в «белый» список, письмо не подвергается анализу на содержание спама. Однако, если доменное имя адресов получателя и отправителя письма совпадают, и это доменное имя занесено в белый список с использованием знака «*», то письмо подвергается проверке на спам. Методы ввода:

- чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, mail@example.net). Все письма, полученные с этого адреса, будут доставляться без проверки на спам;
- каждый элемент списка может содержать только один почтовый адрес или одну маску почтовых адресов;
- чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ *, который заменяет любую (в том числе пустую) последовательность любых символов.

  Например, допускаются следующие варианты:

  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

Знак * может ставиться только в начале или в конце адреса.

Символ @ обязателен.

- чтобы гарантированно получать письма с почтовых адресов в конкретном домене, используйте символ * вместо имени пользователя. Например, чтобы получать все письма от адресатов из домена example.net, введите *@example.net.
- чтобы гарантированно получать письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте символ * вместо имени домена. Например, чтобы получать все письма от адресатов с названием почтового ящика ivanov, введите ivanov@*.

Черный список

Если адрес отправителя добавлен в «черный» список, то письму без дополнительного анализа присваивается статус спам. Методы ввода:

- чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, spam@spam.ru). Все письма, полученные с этого адреса, будут автоматически распознаваться как спам;
- каждый элемент списка может содержать только один почтовый адрес или одну маску почтовых адресов;
- чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ *, который заменяет любую (в том числе пустую) последовательность любых символов.
- чтобы гарантированно помечать как спам письма с почтовых адресов в конкретном домене, используйте символ * вместо имени пользователя. Например, чтобы помечать как спам все письма от адресатов из домена `spam.ru`, введите `*@spam.ru`;
- чтобы гарантированно помечать как спам письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте символ * вместо имени домена. Например, чтобы помечать как спам все письма от адресатов

с названием почтового ящика `ivanov`, введите `ivanov@*`.

- адреса из домена получателя не обрабатываются. Например, если почтовый ящик получателя (ваш почтовый ящик) находится в домене `mail.ru`, то письма, отправленные с домена `mail.ru` обрабатываться спам-фильтром не будут.

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.

Для операционной системы Windows Vista и старше при нажатии кнопки **Журнал**:

- 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.

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;
- **Спам-писем** – количество писем, распознанных как спам.

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. SpIDer Gate

SpIDer Gate – это веб-антивирус, который автоматически проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы (при настройках по умолчанию). Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, то есть работающие с сетью Интернет.

При настройках по умолчанию **SpIDer Gate** блокирует получаемые по сети объекты, содержащие вредоносные программы.

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

При базовых настройках **SpIDer Gate** блокирует получаемые по сети объекты, содержащие вредоносные программы. Также по умолчанию включена URL-фильтрация нерекомендуемых сайтов и сайтов, известных как источники распространения вирусов.

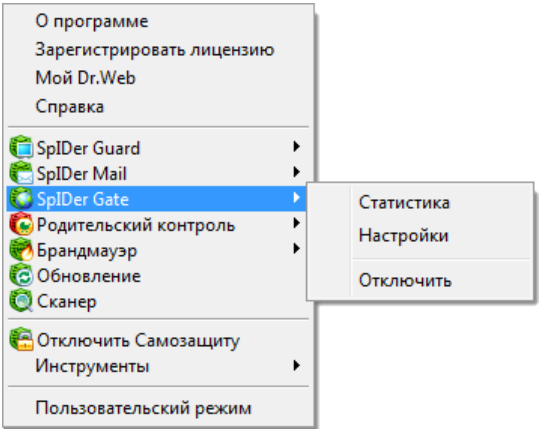
Вы можете подключиться к «облачным» сервисам компании **«Доктор Веб»** и проверять безопасность веб-страниц сети Интернет в режиме реального времени.

SpIDer Gate постоянно находится в оперативной памяти компьютера и по умолчанию запускается при загрузке операционной системы автоматически.

8.1. Управление SpIDer Gate

Основные средства настройки и управления веб-антивирусом

SpIDer Gate находятся в подменю **SpIDer Gate**, которое открывается по щелчку на значке **SpIDer Agent** в области уведомлений Windows.



При выборе пункта **Статистика** открывается окно с информацией о работе **SpIDer Gate** в текущем сеансе.

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

Пункт **Отключить/Включить** позволяет временно отключить или заново запустить работу **SpIDer Gate**.

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

Восстановить параметры работы программы, используемые по умолчанию, а также экспортировать или импортировать настройки вы можете в разделе **Восстановление** Основных настроек **Dr.Web Security Space**.

8.2. Настройка SpIDer Gate

Основные параметры работы веб-антивируса **SpIDer Gate** сосредоточены в разделах окна **Настройки SpIDer Gate** (см. ниже). Настройки **SpIDer Gate** по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

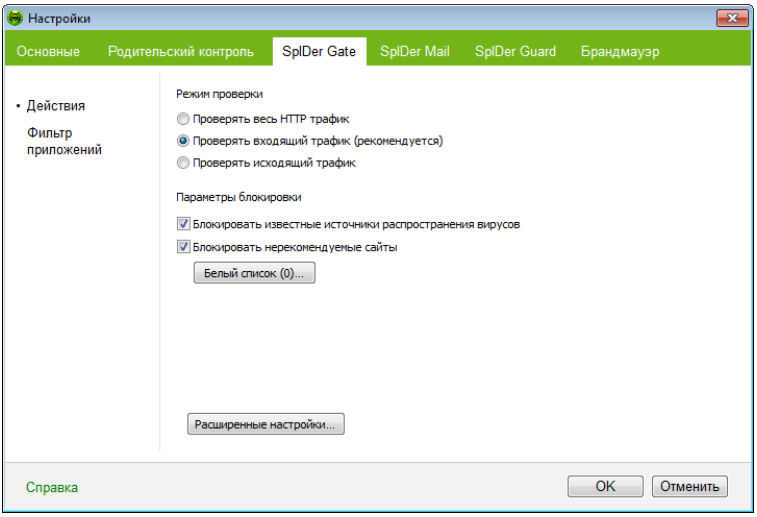
Изменение настроек веб-антивируса

1. Щелкните значок **SpIDer Agent** в области уведомлений Windows и выберете в подменю **SpIDer Gate** пункт **Настройки**.
2. Внесите необходимые изменения в разделах настроек.
3. Чтобы получить информацию о настройках, расположенных в разделе, нажмите на ссылку **Справка**.
4. Нажмите кнопку **Применить** для немедленного сохранения внесенных изменений.
5. По окончании редактирования настроек нажмите кнопку **ОК**.

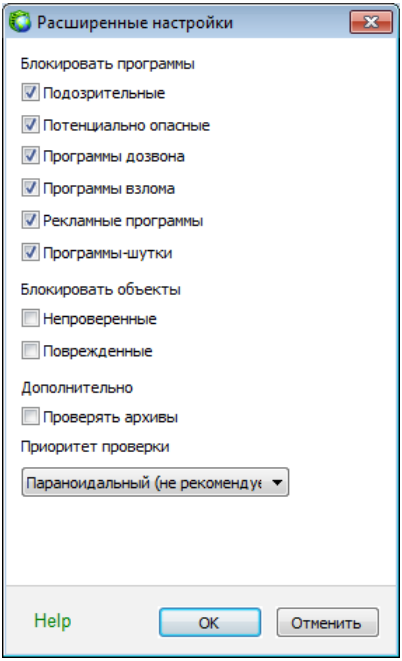
Раздел Действия

В группе **Режим проверки** предоставляется возможность выбора типа проверяемого HTTP-трафика. По умолчанию проверяется только входящий трафик, т.е. выбран режим **Проверять входящий HTTP-трафик (рекомендуется)**.

В группе **Параметры блокировки** вы можете установить автоматическую блокировку доступа к известным веб-сайтам, с которых распространяются вирусы или вредоносные программы других типов (для этого установите флажок **Блокировать известные источники распространения вирусов**), а также к нерекомендованным сайтам, известным как неблагонадежные (для этого установите флажок **Блокировать нерекомендуемые сайты**). Нажмите кнопку **Белый список**, чтобы указать сайты, доступ к которым должен быть разрешен несмотря на установленные ограничения.



Для настройки дополнительных опций в разделе **Действия** нажмите кнопку **Расширенные настройки**.



В появившемся окне вы можете настроить блокировку вредоносных программ и объектов, а также проверку архивов. По умолчанию блокируются все вредоносные программы и опция проверки архивов выключена.

В этом же окне вы можете настроить **Приоритет проверки** – распределение ресурсов в зависимости от приоритетности проверки трафика. При меньшем приоритете проверки скорость работы с сетью Интернет уменьшается, поскольку веб-антивирусу **SpIDer Gate** приходится дольше ждать загрузки данных и проверять больший объем информации. При увеличении приоритета проверка производится чаще, что позволяет веб-антивирусу отдавать данные быстрее, тем самым повышая скорость работы с сетью. Однако при более частых проверках повышается нагрузка на процессор. Вы можете подобрать наилучший баланс опытным путем.

Раздел Фильтр приложений

По умолчанию **SpIDer Gate** проверяет входящий трафик. В разделе **Фильтр приложений** производится настройка параметров проверки HTTP-трафика.

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

Добавьте в список **Приложения, проверяемые по всем портам** те программы, сетевую активность которых следует проверять с особенной тщательностью. Такими программами могут считаться веб-обозреватели, менеджеры загрузок, а также новые установленные программы.

В список **Приложения, проверяемые по всем портам** необходимо добавлять только те программы, которые используют протокол HTTP.

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

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

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

Также при необходимости вы можете настроить веб-антивирус для

проверки данных, передаваемых по протоколу HTTPS. Для этого установите флажок **Проверять зашифрованный трафик (HTTPS)**. Если клиент, который получает и передает такие данные, не обращается к хранилищу сертификатов системы Windows, то необходимо будет экспортировать сертификат.

Сертификат «Доктор Веб»

Если вы хотите включить в проверку данные, передаваемые по криптографическому протоколу SSL (например, в **SpIDer Gate** вы можете настроить параметры проверки данных, передаваемых по протоколу HTTPS), 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.

9. Родительский контроль

С помощью модуля **Родительского контроля** осуществляется ограничение доступа пользователей к аппаратному обеспечению компьютера и различным программным ресурсам, содержащимся как на самом компьютере, так и в сети, а также контролируется время работы в сети Интернет и за компьютером.

Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность и конфиденциальность важных данных и защитить файлы от заражения. Существует возможность защиты, как отдельных файлов, так и папок целиком, расположенных как на локальных дисках, так и на внешних носителях информации. Также для предотвращения несанкционированного доступа к данным или их кражи вы можете ограничить доступ к таким устройствам, как USB-порты, жесткие диски, дисководы и т. п.

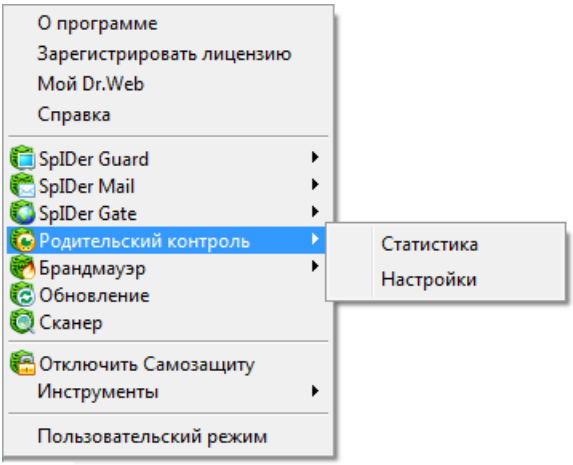
Контроль доступа к интернет-ресурсам позволяет, как оградить пользователя от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т. п.), так и разрешить пользователю доступ только к тем сайтам, которые определены настройками модуля **Родительского контроля**.

Вы можете подключиться к «облачным» сервисам компании **«Доктор Веб»**, чтобы проверять содержимое веб-страниц сети Интернет в режиме реального времени.

Родительский контроль постоянно находится в оперативной памяти компьютера и автоматически запускается при загрузке операционной системы.

9.1. Управление Родительским контролем

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



При выборе пункта **Статистика** открывается окно, содержащее сведения о работе модуля **Родительский контроль** в течение текущего сеанса (количество заблокированных расурсов разных категорий, последние разрешенные или заблокированные URL).

При выборе пункта пункта **Настройки** открывается окно настроек модуля **Родительский контроль** (см. Настройка Родительского контроля).

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

Восстановить настройки по умолчанию вы можете в разделе **Восстановление** Основных настроек **Dr.Web Security Space**.

9.2. Настройка Родительского контроля

Изменение настроек Родительского контроля

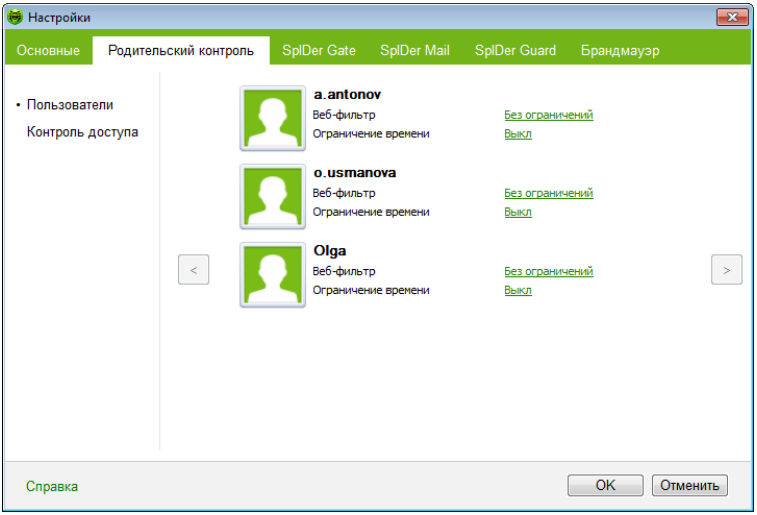
1. Выберите в контекстном меню модуля пункт **Настройки.**
2. Внесите необходимые изменения в разделах настроек.
3. Для того чтобы получить информацию о настройках, расположенных в разделе, нажмите на ссылку **Справка**.
4. По окончании редактирования настроек нажмите кнопку **ОК**.

Раздел Пользователи

В этом разделе производится настройка ограничений по доступу к веб-ресурсам и времени работы пользователей за компьютером и в сети Интернет. Параметры работы задаются отдельно для каждого пользователя операционной системы и отображаются рядом с рисунком для соответствующей учетной записи. В окне настроек учетные записи отображаются автоматически.

Используйте кнопки навигации для перелистывания списка пользователей.

По умолчанию всем пользователем компьютера разрешен неограниченный доступ к ресурсам сети Интернет, ограничения по времени работы отсутствуют.

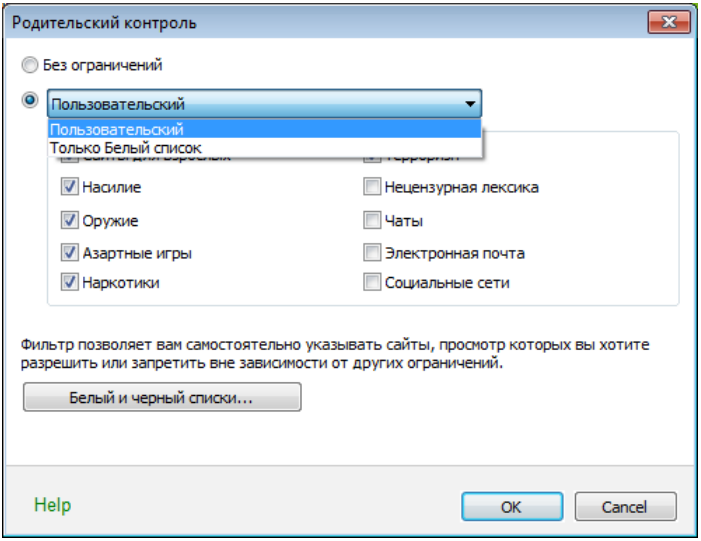


Настройка Веб-фильтра

По умолчанию для всех пользователей установлен режим работы **Без ограничений**. Вы можете изменить режим доступа к веб-страницам и задать белый и черный список ресурсов отдельно для каждого пользователя.

Ограничение доступа к веб-страницам

1. В разделе **Пользователи** настроек модуля **Родительский контроль** найдите в списке учетную запись, для которой требуется настроить ограничения.
2. Щелкните по ссылке в соответствующей графе **Веб-фильтр**. Откроется окно настроек.



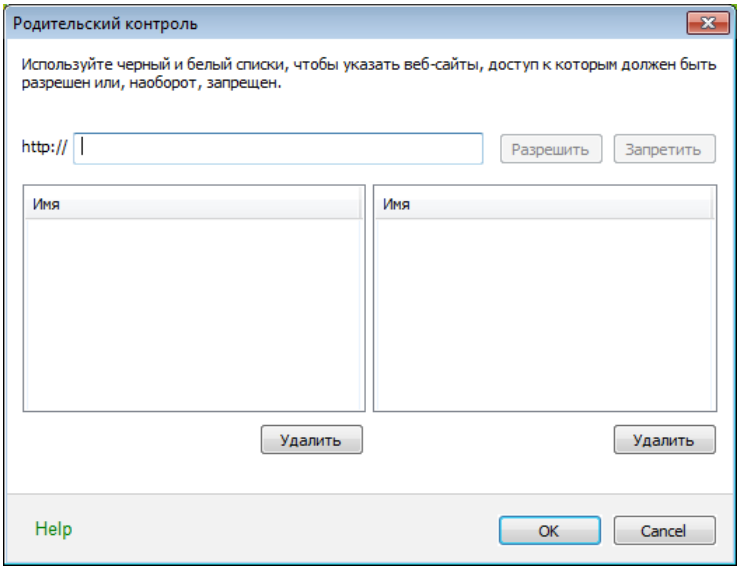
3. Выберите вариант доступа к веб-ресурсам:
   - **Без ограничений –** ограничений на доступ к веб-ресурсам нет.
   - **Пользовательский –** вы можете указать категории тех ресурсов, доступ к которым вы хотите ограничить. Также в этом режиме вы можете самостоятельно указывать сайты, доступ к которым будет запрещаться или разрешаться вне зависимости от других ограничений. Для задания списков нажмите кнопку **Белый и черный списки.**
   - **Только Белый список –** запрещается доступ ко всем веб-ресурсам, кроме указанных в «белом» списке веб-сайтов. Для задания списка разрешенных ресурсов нажмите кнопку **Белый и черный списки.**

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

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

Формирование списка доменных адресов

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



- если вы хотите добавить в список определенный сайт, введите его полный адрес (прим.: www.example.com). Доступ ко всем ресурсам, расположенным на этом сайте, будет определяться данной записью;
- если вы хотите разрешить/запретить доступ к тем веб-сайтам, в адресе которых содержится определенный текст, введите в поле этот текст. (Прим.: **example**. Доступ к адресам **example**.com, **example**.test.com, test.com/**example**, test.**example**222.ru и т.п. будет определяться данной записью);

В том случае, когда введенная строка содержит символ ".",

данная строка будет рассматриваться как имя домена. Тогда доступ ко всем ресурсам, находящиеся на этом домене, будет определяться данной записью. Если данная строка содержит и символ "/" (прим.: **example.com/test**), то та часть, что стоит слева от символа, будет считаться доменным именем, а части справа от символа – частью разрешенного на данном домене адреса (т.о. будут обрабатываться такие адреса как **example.com/test**11, template**.example.com/test**22 и т.п.).

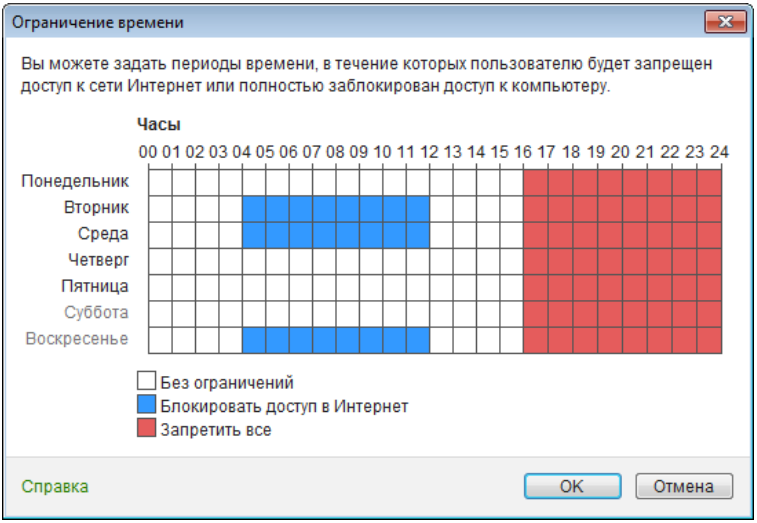
2. Выполните одно из следующих действий, чтобы добавить запись в список:
   - чтобы добавить запись «белый» список и разрешить пользователю доступ к указанным веб-ресурсам, нажмите кнопку **Разрешить;**
   - чтобы добавить запись «черный» список и запретить пользователю доступ к указанным веб-ресурсам, нажмите кнопку **Запретить.**
3. Чтобы удалить какой-либо ресурс из списка, выберите его в этом списке и нажмите кнопку **Удалить.**

Ограничение времени работы

По умолчанию всем пользователям разрешено работать за компьютером и в сети Интернет неограниченное время. Вы можете изменить режим доступа для каждого отдельного пользователя.

Ограничение времени доступа к сети Интернет

1. В разделе **Пользователи** настроек модуля **Родительский контроль** найдите в списке учетную запись, для которой требуется настроить ограничения.
2. Щелкните по ссылке в соответствующей графе **Ограничение времени**. Откроется окно настроек.

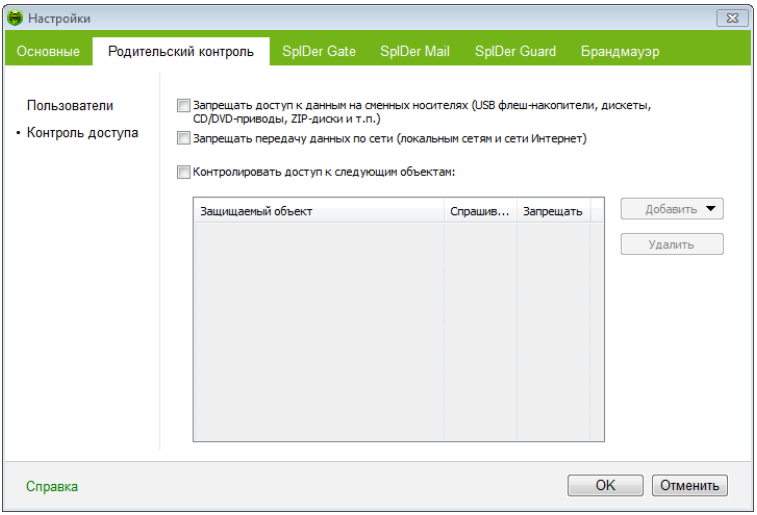


3. Выберите дни недели и часы, когда требуется запретить пользователю выход в Интернет, и выделите соответствующие временные квадраты синим цветом. Методы выделения:
   - чтобы выделить один квадрат, щелкните по нему один раз левой кнопкой мыши;
   - чтобы одновременно выделить несколько расположенных рядом квадратов, один раз щелкните левой кнопкой мыши по первому квадрату и, удерживая кнопку нажатой, выделите весь необходимый период.
4. Выберите дни недели и часы, когда требуется запретить пользователю работу за компьютером, и выделите соответствующие временные квадраты красным цветом.
5. По окончании редактирования нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Раздел Контроль доступа

В данном разделе вы можете запретить запись данных на съемные носители, а также ограничить доступ к конкретным устройствам, папкам или файлам на вашем компьютере. Также вы можете запретить передачу данных по локальным сетям дома или на предприятии и сети Интернет.

Настройки контроля доступа применяются для всех учетных записей Windows.



Формирование списка ресурсов ограниченного доступа

1. Установите флажок **Ограничивать доступ к следующим объектам**.
2. Нажмите кнопку **Добавить** и выберите тип объекта. Вы можете ограничить доступ к конкретному файлу или папке, отдельному устройству или целому класс устройств.

Правила ограничения доступа классу устройств являются более приоритетными, чем отдельные правила для конкретных устройств данного типа. Например, если вы запретите доступ ко всем сменным носителям, то добавленное ранее правило для определенного флеш-накопителя перестанет действовать.

3. Добавьте объект к списку и выберите один из следующий вариантов ограничения доступа к добавленному в список объекту:
   - **Спрашивать –** выводить на экран оповещение при попытке доступа к файлу, папке или устройству. В окне оповещения вы сможете выбрать разрешить или запретить доступ к объекту;
   - **Запрещать –** автоматически блокировать доступ к объекту всем процессам.
4. При необходимости повторите шаги 1 и 2 для добавления других устройств, папок и файлов.
5. Чтобы возобновить доступ к объекту, выберите соответствующий элемент в списке и нажмите кнопку **Удалить**.

10. Брандмауэр Dr.Web

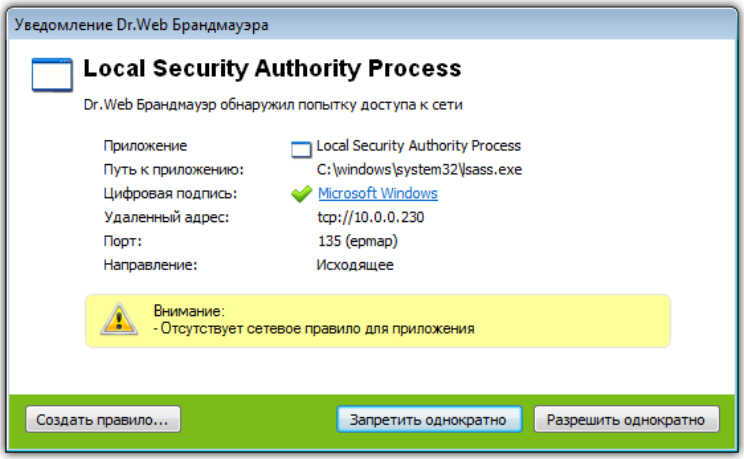
Dr.Web® Брандмауэр предназначен для защиты вашего компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети. Этот компонент позволяет вам контролировать подключение и передачу данных по сети Интернет и блокировать подозрительные соединения на уровне пакетов и приложений.

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.

10.1. 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:



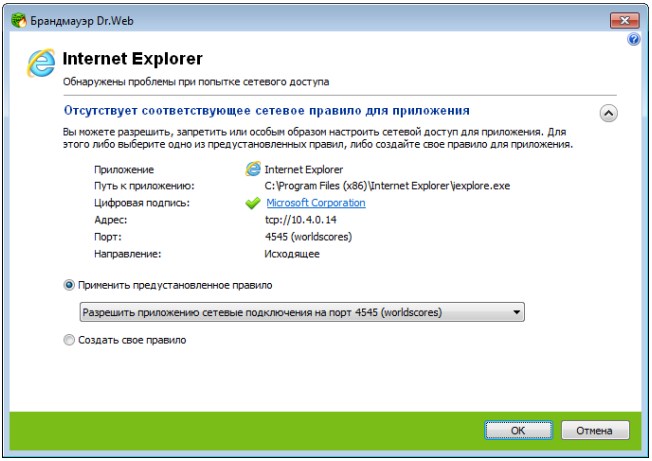
При работе под ограниченной учетной записью (Гость) **Брандмауэр Dr.Web** не выдает пользователю предупреждения о попытках доступа к сети. Предупреждения будут выдаваться под учетной записью с правами администратора, если такая сессия активна одновременно с гостевой.

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.

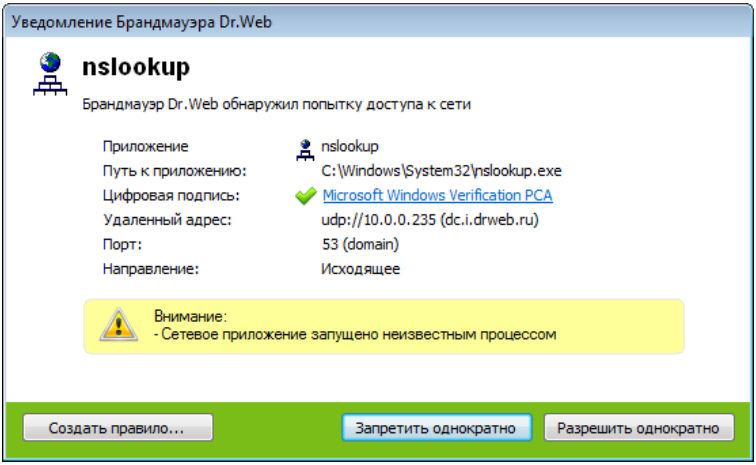
2. Примите решение о подходящей для данного случая операции и выберите соответствующее действие в нижней части окна:
   - чтобы однократно блокировать данное подключение, выберите действие **Запретить однократно**;
   - чтобы однократно позволить приложению данное подключение, выберите действие **Разрешить 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.

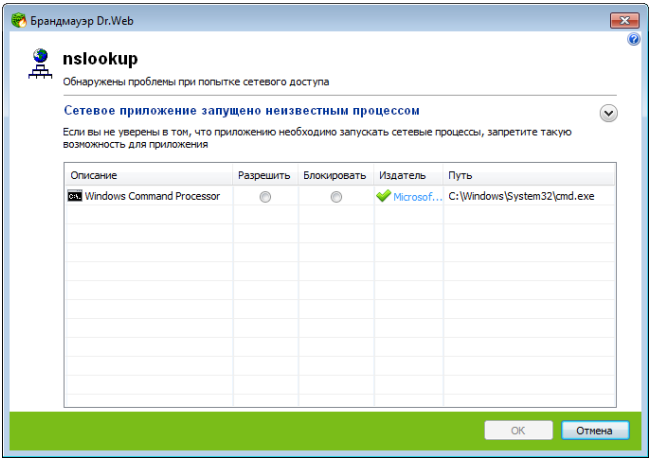
Для создания правил необходимы права администратора.

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:



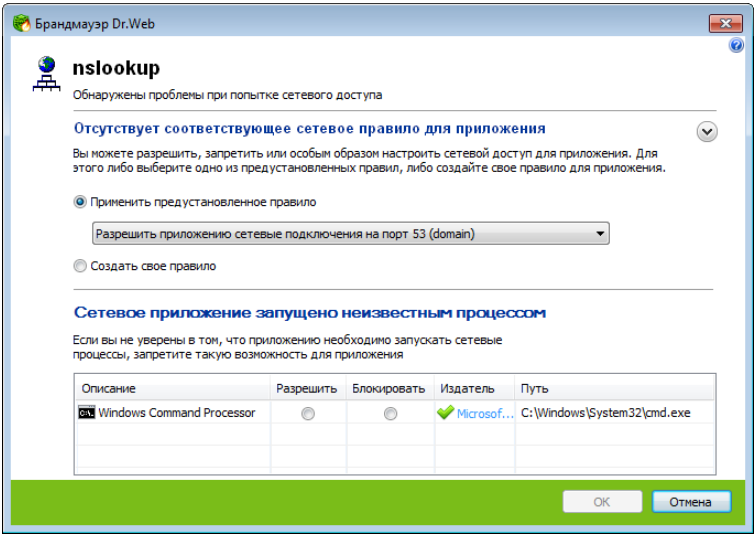
Правила для родительских процессов

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:

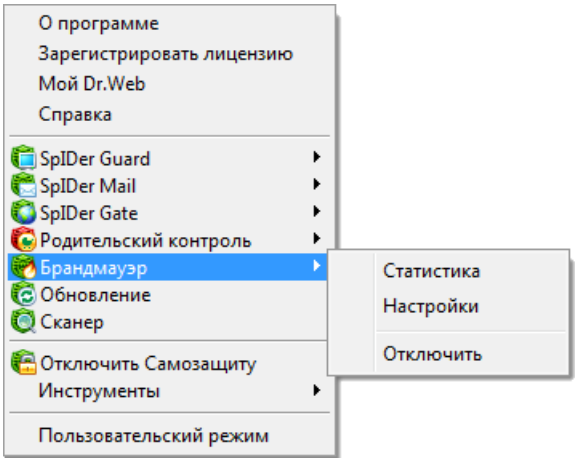

Брандмауэр Dr.Web
nslookup
Обнаружены проблемы при попытке сетевого доступа
Отсутствует соответствующее сетевое правило для приложения
Вы можете разрешить, запретить или особым образом настроить сетевой доступ для приложения. Для этого либо выберите одно из предустановленных правил, либо создайте свое 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

10.2. 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** выдает сообщение об ошибке доступа. При этом в меню **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.

Основные средства настройки и управления **Брандмауэром** сосредоточены в группе **Брандмауэр** контекстного меню **SpIDer Agent**:



Группа **Брандмауэр** включает следующие пункты:

Пункт меню	Описание
Статистика	Открывает окно, содержащее сведения об обработанных **Брандмауэром** событиях
Настройки	Данный пункт недоступен в пользовательском режиме. Предоставляет доступ к основной части настраиваемых параметров **Брандмауэра**. Восстановить параметры работы программы, используемые по умолчанию, а также экспортировать или импортировать настройки вы можете в разделе **Восстановление** Основных настроек **Dr.Web Security Space**.
Отключить/ Запустить	Данный пункт недоступен в пользовательском режиме. Позволяет временно отключить или заново запустить межсетевой экран. Пункт **Запустить** появляется в меню в том случае, когда работа **Брандмауэра** была приостановлена.

Временное отключение Брандмауэра

Вы можете временно отключать межсетевой экран.

Отключение функций Брандмауэра

Данное действие невозможно в пользовательском режиме.

Прибегайте к этой возможности с осторожностью.

1. Откройте контекстное меню значка **SpIDer Agent**.
2. В подменю **Брандмауэр** выберите пункт **Отключить**.

При отключении **Брандмауэра** запрашивается код подтверждения или пароль (если в разделе **Самозащита** Основных настроек **Dr.Web Security Space** вы установили флажок **Защищать паролем настройки Dr.Web**).

Восстановление функций Брандмауэра

1. Откройте контекстное меню значка **SpIDer Agent**  .
2. В подменю **Брандмауэр** выберите пункт **Запустить**.

10.3. Настройка Брандмауэра

Настройки **Брандмауэра** недоступны в пользовательском режиме.

Для начала работы с **Брандмауэром** необходимо:

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

По умолчанию **Брандмауэр** работает в режиме обучения. Вне зависимости от режима работы производится 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.

Основные средства настройки и управления сетевым фильтром **Брандмауэр Dr.Web** сосредоточены в группе **Брандмауэр** контекстного меню **SpIDer Agent**.

Настройка сетевого фильтра

1. Откройте контекстное меню значка **SpIDer Agent** .
2. В подменю **Брандмауэр** выберите пункт **Настройки**. Откроется вкладка **Брандмауэр** окна настроек **Dr.Web Security Space**, содержащая следующие разделы:
   - раздел Приложения, в котором задаются параметры фильтрации на уровне приложений;
   - раздел Родительские процессы, в котором задаются правила запуска приложений различными процессами и другими приложениями;
   - раздел Интерфейсы, в котором задаются параметры фильтрации на уровне сетевых пакетов;

- раздел Дополнительно, в котором задается режим работы **Брандмауэра**.

3. Внесите необходимые изменения. Для получения информации о настройках, расположенных в разделе, нажмите на ссылку **Справка**.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

10.3.1. Раздел Приложения

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.

В данном разделе 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**.

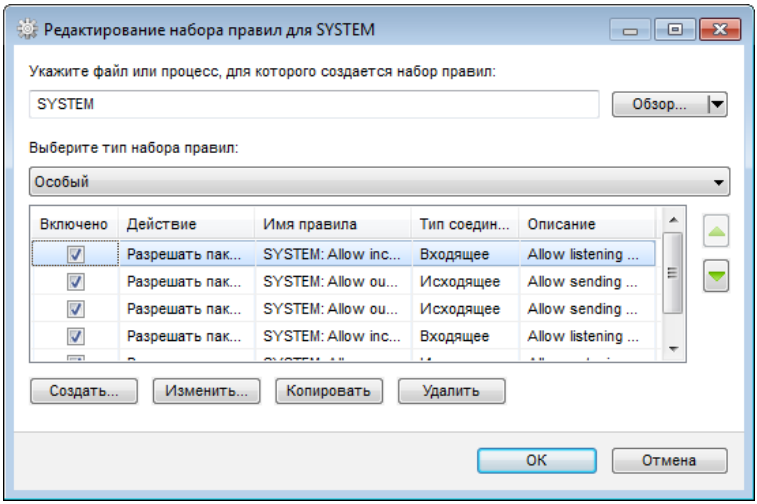
Для каждой программы может быть не более одного набора правил фильтрации.

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.

Для доступа к этому окну в настройках **Брандмауэра** выберите раздел **Приложения** и нажмите кнопку **Создать** или выберите приложение и нажмите кнопку **Изменить.**

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; • **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

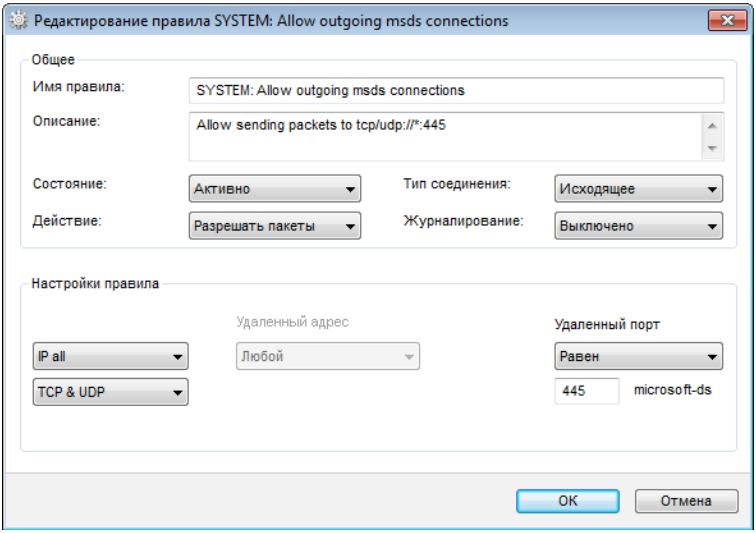
1. В открывшемся окне задайте программу или процесс, для которых будет применяться набор правил. Для этого выполните одно из следующих действий:
   - чтобы задать набор правил для программы, нажмите кнопку **Обзор** и выберите исполняемый файл программы;
   - чтобы задать набор правил для процесса, нажмите стрелку на кнопке **Обзор,** выберите **Запущенное приложение** и укажите процесс;
2. Выберите тип правила:
   - **Разрешать все** – все соединения приложения будут разрешены;

- **Запрещать все** – 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.


Редактирование правила SYSTEM: Allow outgoing msds connections
Общее
Имя правила:
SYSTEM: Allow outgoing msds connections
Описание:
Allow sending packets to tcp/udp://*:445
Состояние:
Активно
Тип соединения:
Исходящее
Действие:
Разрешать пакеты
Журналирование:
Выключено
Настройки правила
Удаленный адрес
Удаленный порт
IP all
Любой
Равен
TCP & UDP
445
microsoft-ds
OK
Отмена

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.

10.3.2. Раздел 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.

10.3.3. Раздел 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.

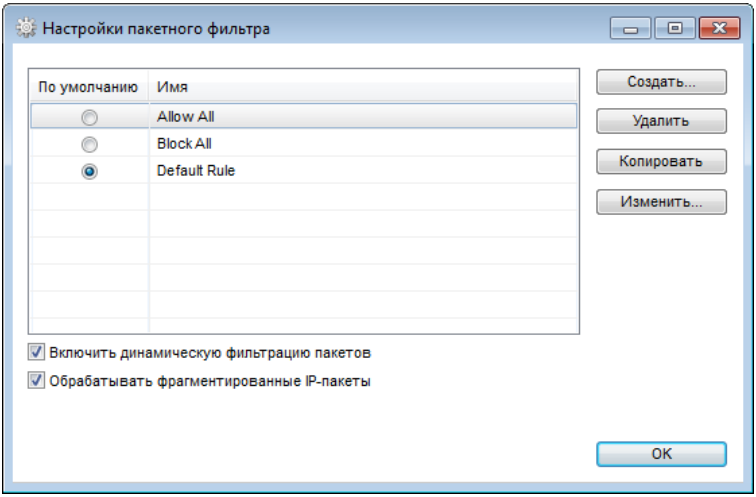
Брандмауэр поставляется со следующими предустановленными наборами правил:

- **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:

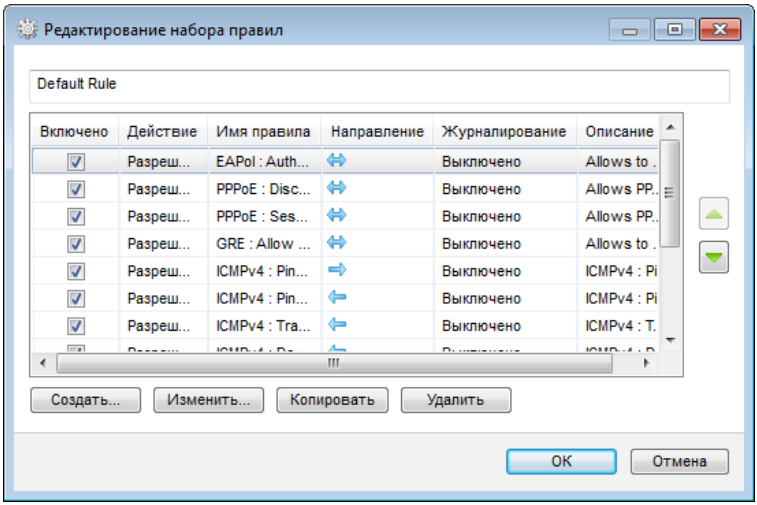
Флажок	Описание
Включить динамическую фильтрацию пакетов	Установите этот флажок, чтобы учитывать при фильтрации состояние TCP-соединения и пропускать только те пакеты, содержимое которых соответствует текущему состоянию. В таком случае все пакеты, передаваемые в рамках соединения, но не соответствующие 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.
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.

Параметр	Описание
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: • **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.

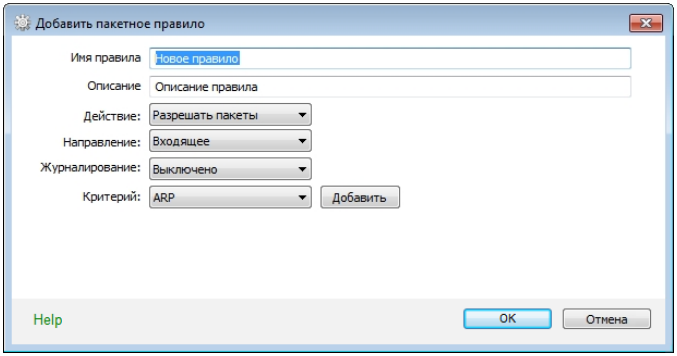
4. Используйте стрелочки справа от списка, чтобы определить порядок выполнения правил. Правила выполняются последовательно, согласно очередности в списке.
5. По окончании редактирования списка нажмите кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отмена** для отказа от изменений.

Те пакеты, для которых нет правил в наборе, автоматически блокируются. Исключения составляют те пакеты, которые разрешаются правилами в Фильтре приложений.

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:

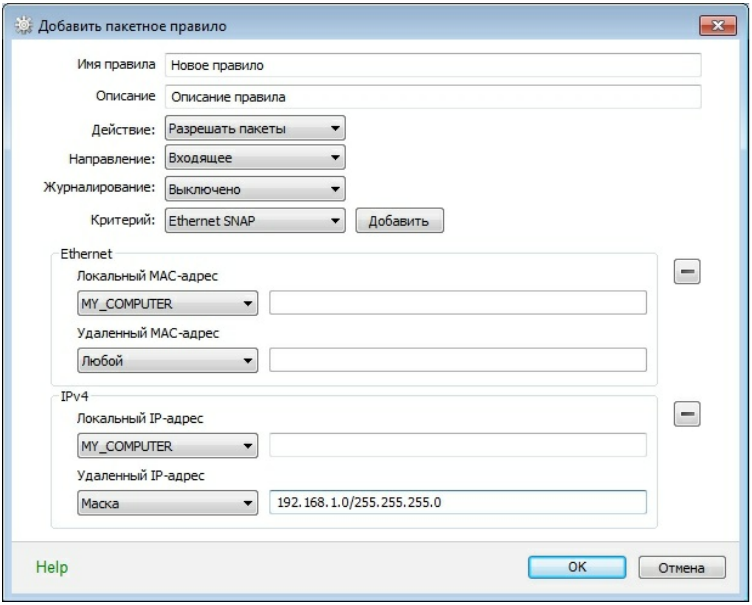
Параметр	Описание
Имя правила	Имя создаваемого/редактируемого правила.
Описание	Краткое описание правила.
Действие	Указывает на действие, выполняемое **Брандмауэром** при обработке пакета: • **Блокировать пакеты** – блокировать пакет; • **Разрешать пакеты** – передать пакет.
Направление	Отправитель пакета: • **Входящее** – правило применяется, если принимается пакет из сети; • **Исходящее** – правило применяется, если пакет отправляется с вашего компьютера;

Параметр	Описание
	• **Любое** – правило применяется вне зависимости от того, кто является отправителем пакета.
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.
Критерий	Критерий фильтрации. Например, транспортный или сетевой протокол. Чтобы добавить критерий фильтрации, выберите нужный критерий в выпадающем списке и нажмите кнопку **Добавить**. Вы можете добавить любое необходимое количество критериев. Для некоторых заголовков доступны дополнительные критерии фильтрации.

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

Если вы не добавите ни одного критерия фильтрации, то данное правило будет разрешать или блокировать все пакеты (в зависимости от настройки в поле **Действие**).

Например, правило для пакетного фильтра, разрешающее все пакеты из подсети, может выглядеть следующим образом:



Если в данном правиле внутри заголовка IPv4 для параметров **Локальный IP-адрес** и **Удаленный IP-адрес** указать значение **Любой**, правило сработает для любого пакета, содержащего заголовок IPv4 и отправленного с физического адреса локального компьютера.

10.3.4. Раздел Дополнительно

В этом разделе 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

Настройка **Разрешать локальные соединения** позволяет 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.

10.4. 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.

Для доступа к журналам откройте контекстное меню значка **SpIDer Agent** и в группе **Брандмауэр** выберите пункт **Статистика.**

10.4.1. 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; • **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).

10.4.2. 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; • **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.**

10.4.3. 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.
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**.

11. 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.

11.1. Запуск обновления

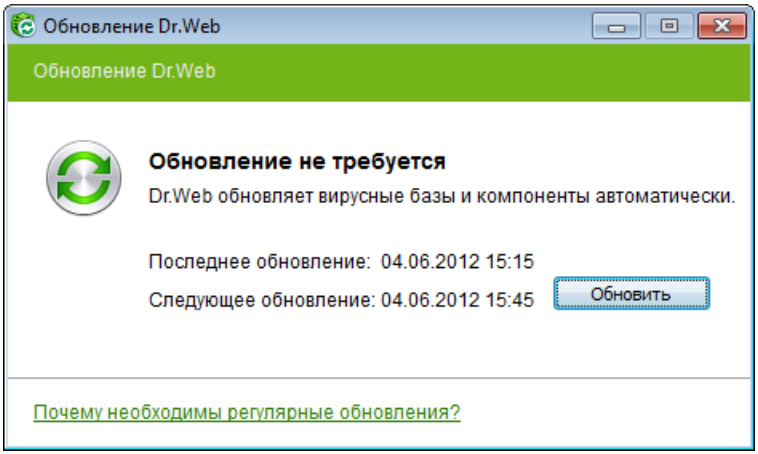
Для запуска **Модуля обновления** вы можете использовать одно из следующих средств:

- в режиме командной строки вызвать исполняемый файл drwupsrv.exe из каталога установки **Dr.Web Security Space** ;
- 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 в разделе **Обновление** Основных настроек работы **Dr.Web Security Space** .

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 **Dr.Web Security Space** могут быть

заблокированы; пользователю выдается соответствующее сообщение.

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

После успешной проверки ключевого файла происходит обновление. Программа автоматически загружает все обновленные файлы, соответствующие вашей версии **Dr.Web Security Space**, 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**).
- `/AC` – проверять инсталляционные пакеты. По умолчанию – опция включена.
- `/AFS` – использовать прямой слеш при указании вложенности внутри архива. По умолчанию – опция отключена.
- `/AR` – проверять архивы. По умолчанию – опция включена.
- `/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 проверять директории (проверять поддиректории). По умолчанию – опция включена.
- /E: *<число>* – провести проверку в указанное количество потоков.
- /FAST – произвести быструю проверку системы. (Только для **Сканера**).
- /FL: *<имя_файла>* – проверять пути, указанные в файле.
- /FM: *<маска>* – проверять файлы по маске. По умолчанию – проверяются все файлы.
- /FR: *<регулярное_выражение>* – проверять файлы по регулярному выражению. По умолчанию – проверяются все файлы.
- /FX: *<маска>* – не проверять файлы, соответствующие маске. (Только для **Консольного Сканера**).
- /FULL – произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы). (Только для **Сканера**).
- /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` – проверять файлы, на которые указывают ярлыки. По умолчанию – опция отключена.
- `/LS` – проверять 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 проверки и системный приоритет задачи проверки. По умолчанию – без ограничений.
- `/NOREBOOT` – отменяет перезагрузку и выключение после проверки. (Только для **Сканера**).
- `/NT` – проверять NTFS-потоки. По умолчанию – опция включена.
- `/OK` – выводить полный список проверяемых объектов, сопровождая незараженные пометкой **Ok**. По умолчанию – опция отключена.
- `/P`: <*приоритет*> – приоритет запущенной задачи проверки в общей очереди задач на проверку:
  - *0* – низший.
  - *L* – низкий.
  - *N* – обычный. Приоритет по умолчанию.
  - *H* – высокий.
  - *M* – максимальный.
- `/PAL`: <*число*> – максимальный уровень вложенности упаковщиков исполняемого файла. Если уровень вложенности превышает указанный, проверка будет производиться только до указанного уровня вложенности. 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 карантин на указанном логическом диске. (Только для **Консольного Сканера**).
- /QNA – выводить пути в двойных кавычках.
- /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**).
- /QUIT – закрыть **Сканер** после проверки (вне зависимости от того, были ли применены действия к обнаруженным угрозам). (Только для **Сканера**).
- /REP – проверять 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.
- /SILENTMODE – запустить проверку в фоновом режиме. Если при проверке будут обнаружены угрозы, откроется окно **Сканера Dr.Web** со списком угроз. В противном случае окно не будет отображено. (Только для **Сканера**).
- /SLS – выводить логи на экран. По умолчанию – опция включена. (Только для **Консольного Сканера**).
- /SPN – выводить название упаковщика. По умолчанию – опция включена.
- /SPS – отображать процесс проведения проверки. По умолчанию – опция включена. (Только для **Консольного Сканера**).
- /SST – выводить время проверки файла. По умолчанию – опция отключена.
- /TB – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.
- /TM – выполнять поиск угроз в оперативной памяти (включая системную область Windows).
- /TR – проверять системные точки восстановления.
- /TS – выполнять поиск угроз в файлах автозапуска (по папке Автозагрузка, системным ini-файлам, реестру Windows).
- /W:<*число*> – максимальное время проверки, в секундах. По умолчанию – без ограничений.
- /WCL – вывод, совместимый с drwebwcl. (Только для **Консольного Сканера**).
- /X: S[:R] – по окончании проверки 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: проверять 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:\

проверить 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, download - скачать.
-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 удаления (uninstall):

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.
-k [--password] arg	Пароль пользователя прокси-сервера.

Параметр	Описание
-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 В. 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. 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.