



Защити созданное

Руководство пользователя

© «Доктор Веб», 2015. Все права защищены.

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

ТОРГОВЫЕ ЗНАКИ

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk и логотипы Dr.WEB являются зарегистрированными товарными знаками «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

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

Dr.Web Security Space
Версия 10.0
Руководство пользователя
29.07.2015

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

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

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

«Доктор Веб»

«Доктор Веб» — российский разработчик средств информационной безопасности.

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

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

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

**Мы благодарны пользователям за поддержку
решений семейства Dr.Web!**



Содержание

1. Введение	7
1.1. О чем эта документация	9
1.2. Используемые обозначения и сокращения	9
1.3. Методы обнаружения	10
2. Системные требования	12
3. Установка, изменение и удаление программы	13
3.1. Первая установка	14
3.2. Удаление или изменение программы	18
4. Лицензирование	20
4.1. Способы активации	21
4.2. Продление лицензии	21
4.3. Мастер регистрации	22
4.3.1. Запуск активации	22
4.3.2. Ввод регистрационных данных	23
4.3.3. Результат активации	24
5. Начало работы	25
5.1. Проверка антивируса	27
6. Инструменты	28
6.1. Менеджер лицензий	28
6.2. Защита от потери данных	29
6.3. Антивирусная сеть	30
6.4. Менеджер Карантина	32
6.5. Поддержка	33
6.5.1. Создание отчета	34
7. Обновление	35
8. Сканер Dr.Web	36
8.1. Запуск проверки	36
8.2. Действия при обнаружении угроз	39
8.3. Настройка Сканера	40
8.4. Запуск Сканера с параметрами командной строки	47



8.5. Консольный сканер	48
8.6. Запуск проверки по расписанию	48
9. Настройки	50
10. Основные настройки	51
10.1. Уведомления	51
10.2. Обновление	55
10.3. Сеть	55
10.4. Самозащита	57
10.5. Dr.Web Cloud	58
10.6. Антивирусная сеть	59
10.7. Устройства	60
10.8. Дополнительно	61
11. Родительский контроль	64
11.1. Настройка модуля Родительский контроль	65
12. Исключения	67
12.1. Вебсайты	67
12.2. Файлы и папки	67
12.3. Программы и процессы	68
12.4. Антиспам	68
13. Компоненты защиты	70
13.1. SpIDer Guard	70
13.1.1. Настройка SpIDer Guard	70
13.2. SpIDer Gate	74
13.2.1. Настройка SpIDer Gate	75
13.3. SpIDer Mail	76
13.3.1. Настройка SpIDer Mail	77
13.4. Антиспам	80
13.5. Брандмауэр Dr.Web	82
13.5.1. Обучение Брандмауэра	82
13.5.1. Настройка Брандмауэра	84
13.6. Dr.Web для Outlook	92
13.6.1. Настройка Dr.Web для Outlook	92
13.6.2. Обнаружение угроз	93
13.6.3. Проверка на спам	96



13.6.4. Регистрация событий	100
13.6.5. Статистика проверки	101
13.7. Превентивная защита	102
Приложения	105
Приложение А. Дополнительные параметры командной строки	105
Параметры для Сканера и Консольного сканера	105
Параметры для Модуля обновления	110
Коды возврата	112
Приложение Б. Угрозы и способы их обезвреживания	114
Классификация угроз	114
Действия для обезвреживания угроз	118
Приложение В. Принципы именования угроз	119



1. Введение

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

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

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

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

Каждое из антивирусных решений **Dr.Web** для операционных систем семейства Microsoft® Windows® включает в состав соответствующий набор из следующих компонентов защиты:

Сканер Dr.Web – антивирусный сканер с графическим интерфейсом, который запускается по запросу пользователя или по расписанию и проводит антивирусную проверку компьютера.

Консольный сканер Dr.Web – версия **Сканера Dr.Web** с интерфейсом командной строки.

SpIDer Guard – антивирусный сторож, который постоянно находится в оперативной памяти, осуществляя проверку создаваемых файлов и запускаемых процессов, 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 **Антиспама Dr.Web**.

Dr.Web для Outlook – подключаемый модуль, который проверяет почтовые ящики Microsoft Outlook на вирусы и спам.

SpIDer Gate – модуль антивирусной проверки HTTP-трафика. При настройках по умолчанию веб-антивирус **SpIDer Gate** автоматически проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих вирусы и другие 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»**, которые позволяют антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании **«Доктор Веб»** в режиме реального времени.

Родительский контроль – компонент, который ограничивает доступ к веб-сайтам, файлам и папкам, а также позволяет ограничить время работы в сети Интернет и за компьютером для каждой учетной записи Windows. Вы можете [подключиться](#) к облачным сервисам компании **«Доктор Веб»**, которые позволяют антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании **«Доктор Веб»** в режиме реального времени.



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 программы **Dr.Web**.



1.1. О чем эта документация

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

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

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

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



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

1.2. Используемые обозначения и сокращения

В данном руководстве используются следующие обозначения:

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов «Доктор Веб» или их компонентов.
<u>Зеленое и подчеркнутое начертание</u>	Ссылки на страницы руководства и веб-сайты.
Моноширинный шрифт	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
<i>Курсив</i>	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак 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. Методы обнаружения

Все антивирусные продукты, разработанные компанией «Доктор Веб», применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Методы обнаружения угроз

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. *Сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в **вирусных базах Dr.Web** составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing™

Это уникальная технология **Dr.Web**, которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы заражения или вредоносное поведение. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения **Dr.Web**, от таких угроз, как троянская программа-вымогатель Trojan.Encoder.18 (также известная под названием «gpcode»). Кроме того, использование технологии **Origins Tracing** позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи **Origins Tracing**, добавляется постфикс `.Origin`.

Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и шифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи *эмулятора* – программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (*буфером эмуляции*). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Эвристический анализ

Работа эвристического анализатора основывается на наборе *эвристик* (предположений, статистическая значимость которых подтверждена опытным путем) о характерных признаках вредоносного и, наоборот, безопасного исполняемого кода. Каждый признак кода имеет определенный вес (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.



Эвристический анализатор также использует технологию **FLY-CODE™** – универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта **Dr.Web**, но и новыми, ранее не исследованными программами. При проверке упакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов **Dr.Web** используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты **Антивирусной Лаборатории «Доктор Веб»** обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту **Dr.Web**, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.



2. Системные требования



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

- удалить с компьютера другие антивирусные программы 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; если поддержка операционной системы производителем прекращена, рекомендуется перейти на более современную версию операционной системы.

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

Компонент	Требование
Процессор	Полная поддержка системы команд i686.
Операционная система	Для 32-разрядных операционных систем: • Windows XP с пакетом обновлений SP2 или выше; • Windows Vista с пакетом обновлений SP2 или выше; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или выше; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10. Возможно, потребуется загрузить с сайта Microsoft и установить обновления ряда системных компонентов. Dr.Web сообщит вам, при необходимости, их наименования и URL.
Свободная оперативная память	512 МБ и больше.
Место на жестком диске	1 ГБ для размещения компонентов продукта. Файлы, создаваемые в ходе установки, потребуют дополнительного места.
Разрешение	Рекомендуемое разрешение экрана не менее 800x600.
Прочее	Для подключаемого модуля Dr.Web для Outlook необходим установленный клиент Microsoft Outlook из состава MS Office: • Outlook 2000 (Outlook 9); • Outlook 2002 (Outlook 10 или Outlook XP); • Office Outlook 2003 (Outlook 11); • Office Outlook 2007; • Office Outlook 2010; • Office Outlook 2013.

Опущенные требования к конфигурации совпадают с таковыми для соответствующих операционных систем.



3. Установка, изменение и удаление программы

Перед установкой **Dr.Web** обратите внимание на [системные требования](#), а также 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 программы и межсетевые экраны для предотвращения возможной несовместимости их резидентных компонентов.



3.1. Первая установка



Установка **Dr.Web** должна выполняться пользователем с правами администратора данного компьютера.

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

- в фоновом режиме;
- в обычном режиме.

Установка с параметрами командной строки

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

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

```
drweb-1000-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. Если на вашем компьютере уже установлен другой антивирус, то программа установки предупредит вас о несовместимости программы **Dr.Web** и иных антивирусных решений и предложит удалить их.



Перед началом установки проверяется актуальность установочного файла. В случае, если существует более новый установочный файл, вам будет предложено его скачать.

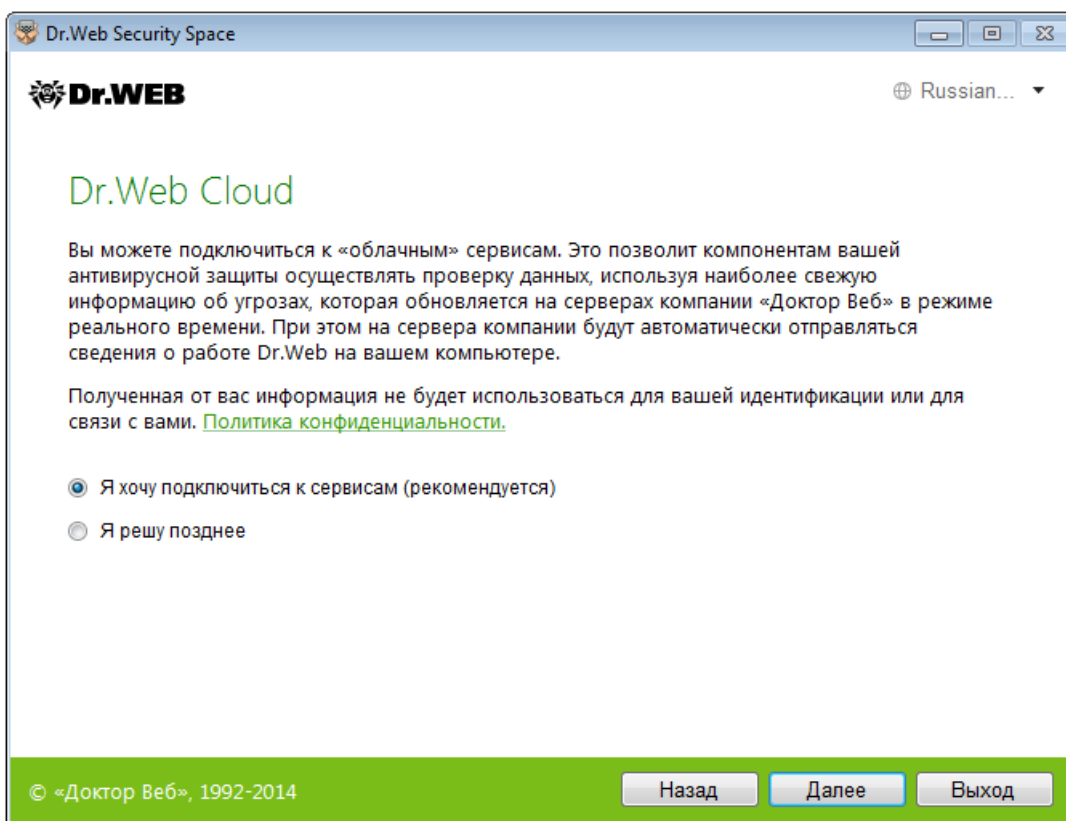
2. В окне приветствия ознакомьтесь с лицензионным соглашением. Для продолжения установки его необходимо принять.

Нажмите кнопку **Далее**.

3. На следующем шаге вам будет предложено установить **Брандмауэр Dr.Web**.

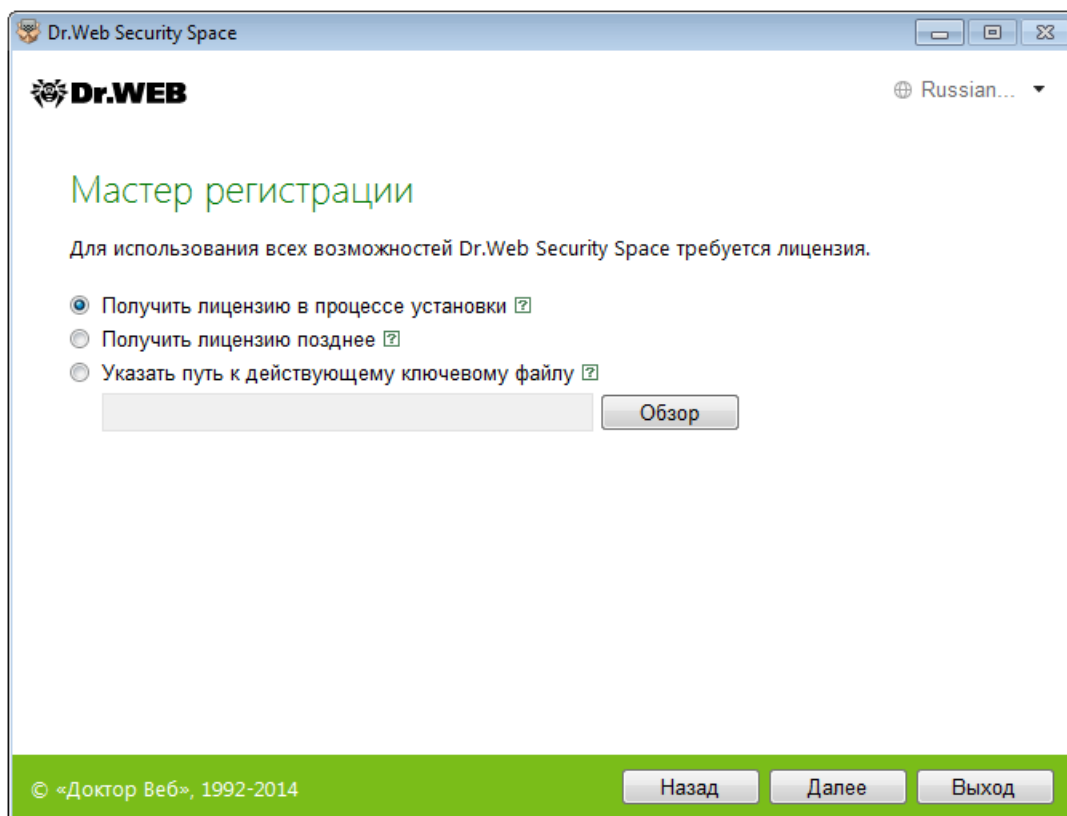
Нажмите кнопку **Далее**.

4. Далее вам будет предложено подключиться к облачным сервисам **Dr.Web**, которые позволят осуществлять проверку данных, используя наиболее свежую информацию об угрозах, которая обновляется на серверах компании «Доктор Веб» в режиме реального времени.



Нажмите кнопку **Далее**.

5. В окне **Мастер регистрации** программа установки предупредит вас о том, что для работы программы **Dr.Web** необходима лицензия.



Выполните одно из следующих действий:

- если у вас есть ключевой файл и он находится на жестком диске или сменном носителе, выберите **Указать путь к действующему ключевому файлу** и в стандартном окне открытия файла выберите ключевой файл. Для изменения пути нажмите кнопку **Обзор** и выберите другой ключевой файл;
- если у вас нет ключевого файла, но вы готовы его получить в процессе установки, выберите **Получить лицензию в процессе установки**;
- для продолжения установки **без лицензии** выберите **Получить лицензию позднее**. Обновления не будут загружаться до тех пор, пока вы не укажете или не получите ключевой файл.

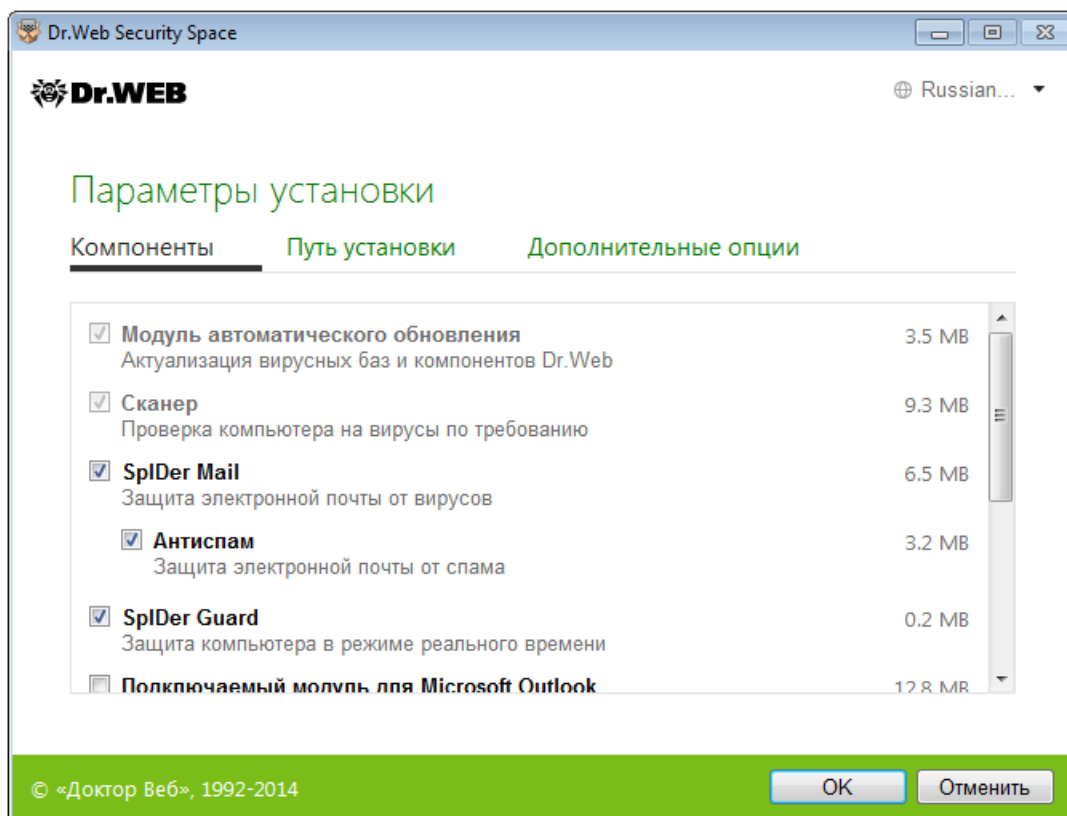
Нажмите кнопку **Далее**.

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 лицензию 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 программы **Dr.Web**.
После того, как все необходимые изменения будут внесены, нажмите кнопку **ОК**.
10. Если на шаге 5 вы выбрали **Получить лицензию 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 программы **Dr.Web**. Обновление проводится автоматически и не требует дополнительных действий.
12. Для завершения процесса установки выполните перезагрузку компьютера.

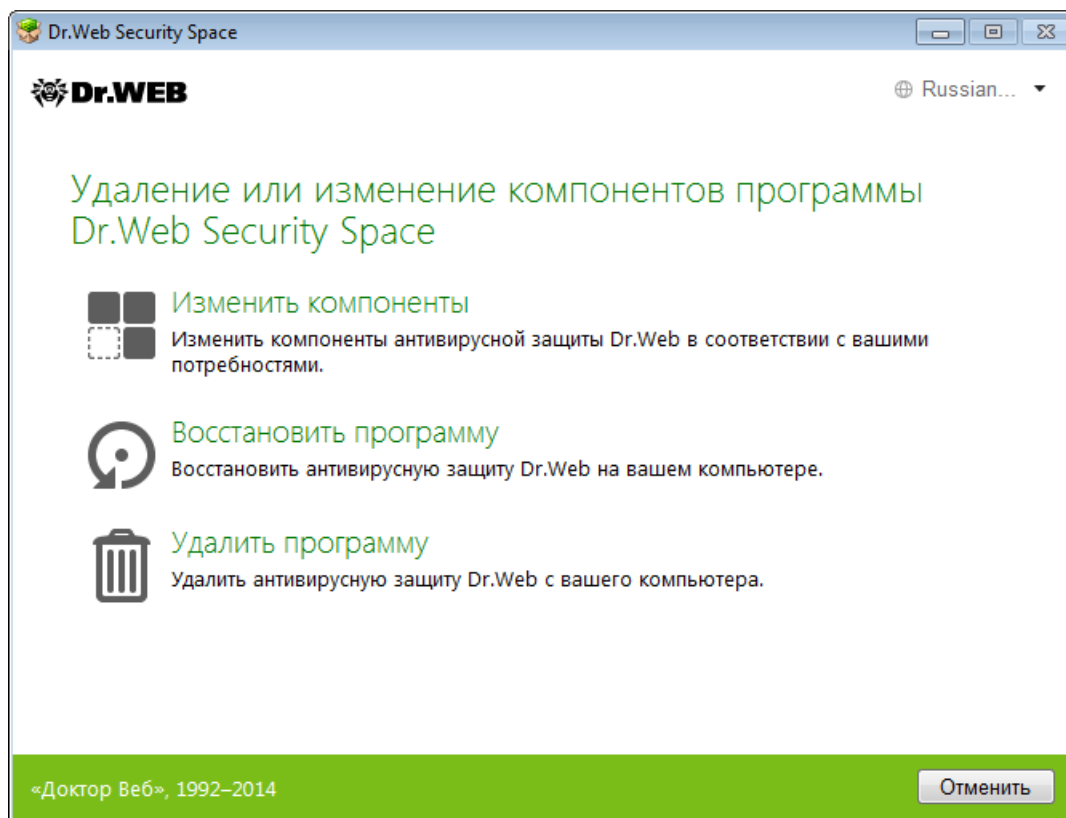


3.2. Удаление или изменение программы



После удаления **Dr.Web** ваш компьютер не будет защищен от вирусов и других вредоносных программ.

1. Для удаления или изменения конфигурации **Dr.Web** путем добавления и удаления отдельных компонентов, выберите (в зависимости от операционной системы):
 - для Windows XP (в зависимости от вида меню «Пуск»):
 - Меню «Пуск»: **Пуск → Панель управления → Установка и удаление программ.**
 - Классическое меню «Пуск»: **Пуск → Настройка → Панель управления → Установка и удаление программ.**
 - для Windows Vista (в зависимости от вида меню «Пуск»):
 - Меню «Пуск»: **Пуск → Панель управления**, далее в зависимости от вида Панели управления:
 - Классический вид: **Программы и компоненты.**
 - Домашняя страница: **Программы → Программы и компоненты.**
 - Классическое меню «Пуск»: **Пуск → Настройка → Панель управления → Программы и компоненты.**
 - для Windows 7 выберите **Пуск → Панель управления**, далее в зависимости от вида Панели управления:
 - Мелкие/крупные значки: **Программы и компоненты.**
 - Категория: **Программы → Удаление программ.**
 - для Windows 8 и Windows 8.1 откройте **Панель управления** любым удобным способом, например, через пункт **Панель управления** в контекстном меню, вызываемом правым щелчком мыши по левому нижнему углу экрана. Далее в зависимости от типа настройки **Просмотр** для Панели управления:
 - Мелкие/крупные значки: **Программы и компоненты.**
 - Категория: **Программы → Удаление программ.**
2. В открывшемся списке выберите строку с названием программы. Далее для удаления программы полностью нажмите кнопку **Удалить** и перейдите к шагу 6. А для изменения конфигурации **Dr.Web**, путем добавления и удаления отдельных компонентов, нажмите кнопку **Изменить**, при этом откроется окно Мастера удаления/изменения компонентов программы.



3. Если необходимо восстановить антивирусную защиту на вашем компьютере, в открывшемся окне выберите пункт **Восстановить программу**.
4. Для изменения конфигурации **Dr.Web** выберите пункт **Изменить компоненты**. В открывшемся окне установите флажки напротив компонентов, которые хотите добавить, и снимите флажки напротив удаляемых компонентов. Определив конфигурацию, нажмите кнопку **Установить**.



При удалении каких-либо компонентов **Dr.Web** откроется окно **Отключение Самозащиты**, в котором необходимо ввести изображенный код подтверждения, после чего нажать кнопку **Установить**.

5. Чтобы удалить все установленные компоненты, выберите пункт **Удалить программу**.
6. В окне **Параметры** установите флажки напротив того, что следует сохранить после удаления программы. Сохраненные объекты и настройки могут использоваться программой при повторной установке. По умолчанию выбраны все опции – **Карантин**, **Настройки Dr.Web Security Space** и **Защищаемые копии файлов**. Нажмите кнопку **Далее**.
7. В следующем окне для подтверждения удаления **Dr.Web** введите изображенный код, после чего нажмите кнопку **Удалить программу**.
8. По просьбе программы перезагрузите компьютер для завершения процедуры удаления или изменения состава компонентов **Dr.Web**.



4. Лицензирование

Для работы **Dr.Web** в течение продолжительного времени требуется лицензия. Приобретение лицензии возможно вместе с продуктом, а также на [сайте](#) компании «**Доктор Веб**». Лицензия позволяет полноценно использовать все возможности продукта на протяжении всего срока действия. Лицензия регулирует права пользователя, установленные в соответствии с пользовательским договором.

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, вы можете активировать демонстрационный период. Он обеспечивает полную функциональность основных компонентов, но срок действия существенно ограничен.



Активация демонстрационного периода на одном и том же компьютере возможна не чаще, чем один раз в год.

Демонстрационный период может быть активирован сроком:

- на 3 месяца. Для этого вам необходимо зарегистрироваться на [сайте](#) компании «**Доктор Веб**» и получить серийный номер;
- на 1 месяц, при этом серийный номер не требуется, регистрационные данные не запрашиваются.

Ключевой файл

Права пользователя на использование **Dr.Web** хранятся в специальном файле, называемом *ключевым файлом*.

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;
- наличие или отсутствие технической поддержки;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать антивирус).

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

- срок действия лицензии не истек;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным*, при этом **Dr.Web** перестает обезвреживать вредоносные программы и пропускает почтовые сообщения без проверки.

Если при установке **Dr.Web** вы не получили ключевой файл и не указали путь к нему, то в этом случае используется *временный* ключевой файл. Такой ключевой файл обеспечивает полную функциональность компонентов программы **Dr.Web**. Однако в [меню](#) **SpIDer Agent** будут отсутствовать пункты **Мой Dr.Web** и **Обновление**, кроме того, обновления не будут загружаться до тех пор, пока вы не активируете лицензию или демонстрационный период либо с помощью **Менеджера лицензий** не укажете путь к действительному ключевому файлу.

Рекомендуется сохранять ключевой файл до истечения срока действия лицензии или демонстрационного периода.



Ключевой файл, полученный для активации демонстрационного периода, может использоваться только на том компьютере, на котором вы проходили регистрацию.

4.1. Способы активации

Активировать лицензию или демонстрационный период вы можете одним из следующих способов:

- с помощью [Мастера регистрации](#) в процессе установки или любой другой момент;
- получив ключевой файл во время регистрации лицензии на [официальном сайте «Доктор Веб»](#);
- указав путь к имеющемуся у вас действительному ключевому файлу в процессе установки либо в [Менеджере лицензий](#).

Повторная активация

Повторная активация лицензии или демонстрационного периода может потребоваться в случае утраты ключевого файла.



В случае повторной активации лицензии или демонстрационного периода выдается тот же ключевой файл, который был выдан ранее, при условии, что срок его действия не истек.

Повторная активация демонстрационного периода на 3 месяца может осуществляться только на том компьютере, на котором вы проходили регистрацию.

При переустановке продукта или в случае, когда лицензия предоставляет право установки продукта на несколько компьютеров, повторная активация серийного номера не требуется. Вы можете использовать ключевой файл, полученный при первой регистрации.

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.

4.2. 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**. В таком случае вам потребуется заменить текущий ключевой файл. **Dr.Web** поддерживает обновление лицензии «на лету», при котором не требуется переустанавливать **Dr.Web** или прерывать его работу.

Замена ключевого файла

1. Чтобы заменить текущую 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** переключится на использование нового ключевых файла.

4.3. Мастер регистрации

Модуль управления **SpIDer Agent** после старта проверяет наличие ключевого файла. При его отсутствии модуль предлагает получить ключевой файл через Интернет.

Ключевой файл может быть получен в процессе установки. Для этого в на 5 шаге установки выберите пункт **Получить лицензию в процессе установки**, при этом будет запущена процедура активации лицензии или демонстрационного периода.

Вы также можете получить ключевой файл, запустив процедуру активации лицензии или демонстрационного периода после установки продукта. Для этого воспользуйтесь одной из следующих опций:

- в меню SpIDer Agent  в области уведомлений Windows выберите пункт **Лицензия**;
- в окне Менеджера лицензий нажмите кнопку **Получить новую лицензию** и в выпадающем списке выберите **через сеть Интернет**.

После запуска процедуры активации откроется окно Мастера регистрации.

Для активации лицензии вам потребуется серийный номер, выданный вам при приобретении **Dr.Web**.

Для ознакомления с работой программы **Dr.Web Security Space** вы можете активировать демонстрационный период:

- на 3 месяца, для этого вам необходимо зарегистрироваться на сайте и получить серийный номер;

После заполнения анкеты на указанный вами адрес электронной почты будет отправлен серийный номер для активации демонстрационного периода на 3 месяца.

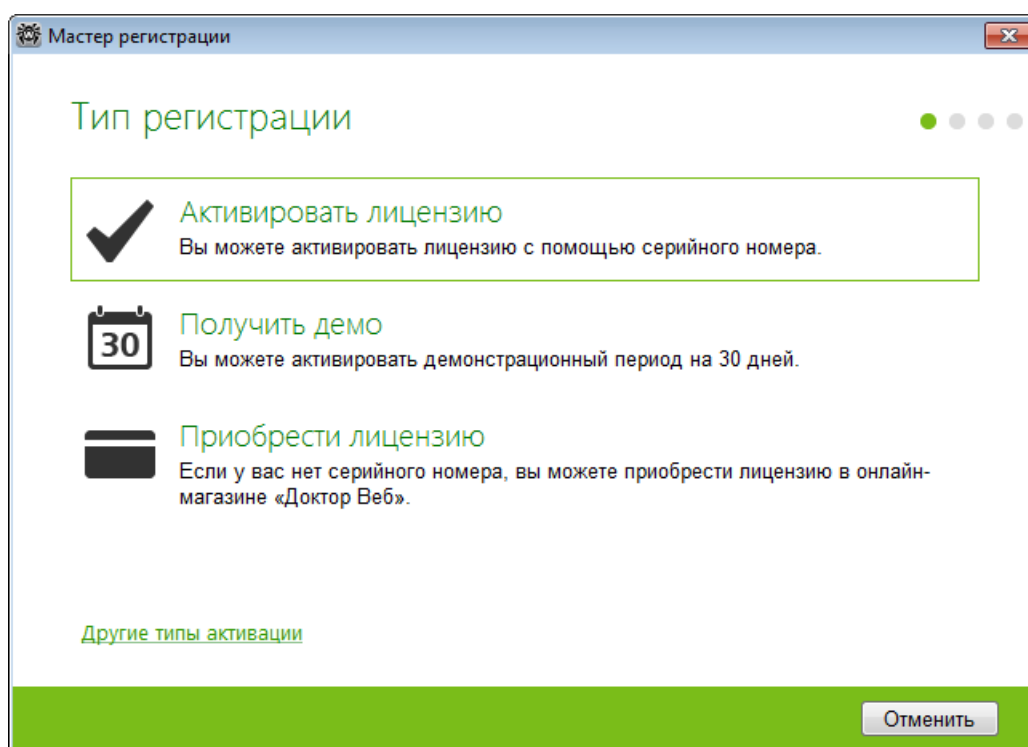
- на 1 месяц, при этом серийный номер не требуется, регистрационные данные не запрашиваются.

4.3.1. Запуск активации

В первом окне вам будет предложено выбрать один из следующих вариантов активации:

- **Активировать лицензию;**
- **Получить демо;**
- **Приобрести лицензию.**

Если у вас имеется серийный номер для активации лицензии или демонстрационного периода на 3 месяца, выберите **Активировать лицензию**. Введите серийный номер и нажмите кнопку **Далее**.



- При вводе серийного номера для активации демонстрационного периода на 3 месяца откроется окно [с результатом активации](#).
- При вводе серийного номера для активации лицензии откроется окно [ввода регистрационных данных](#).



Если вы уже являлись пользователем **Dr.Web**, то вы сможете продлить действие приобретенной лицензии на 150 дополнительных дней. Для этого перед вводом регистрационных данных откроется окно, в котором необходимо указать серийный номер либо путь к ключевому файлу предыдущей регистрации.

Если серийного номера у вас нет, но вы хотите ознакомиться с продуктом, активируйте демонстрационный период на 1 месяц, выбрав **Получить демо**. Нажмите кнопку **Далее**, при этом откроется окно [с результатом активации](#).

Чтобы приобрести лицензию в онлайн-магазине компании **«Доктор Веб»**, выберите **Приобрести лицензию**.

Если у вас уже есть действительный ключевой файл, выберите **Другие типы активации**. В открывшемся окне укажите путь к файлу.

4.3.2. Ввод регистрационных данных

Для регистрации лицензии введите персональные сведения (имя, фамилию, выберите в раскрывающемся списке страну и введите адрес электронной почты). Все перечисленные поля являются обязательными.

Если вы хотите получать по электронной почте новости о продукте, установите соответствующий флажок.

Нажмите кнопку **Далее**.



4.3.3. Результат активации

Если активация закончилась успешно, то выводится соответствующее сообщение. Нажмите на кнопку **Готово**, чтобы перейти к обновлению вирусных баз и других файлов пакета. Данная процедура, как правило, не требует вмешательства пользователя.

Если активация завершилась неудачно, выводится сообщение об ошибке. Нажмите кнопку **Параметры соединения**, чтобы изменить настройки подключения к сети Интернет, либо кнопку **Повторить** для исправления неверно введенных данных.



5. Начало работы

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



Если **SpIDer Agent** не запущен, в меню **Пуск** раскройте группу **Dr.Web** и выберите пункт **SpIDer Agent**.

Значок **SpIDer Agent** отражает текущее состояние **Dr.Web**:

-  – все компоненты, необходимые для защиты компьютера, запущены и работают правильно;
-  – Самозащита **Dr.Web** или важный компонент (сторож **SpIDer Guard**, **Брандмауэр**) отключены, что ослабляет защиту антивируса и компьютера. Включите Самозащиту или отключенный компонент;
-  – ожидается запуск компонентов после старта операционной системы, дождитесь запуска компонентов программы; либо в процессе запуска одного из ключевых компонентов **Dr.Web** возникла ошибка, компьютер находится под угрозой заражения. Проверьте наличие действительного ключевого файла и при необходимости [установите](#) его..

Также, в соответствии с [настройками](#), над значком **SpIDer Agent**  могут появляться различные подсказки-уведомления.

Для доступа к меню **SpIDer Agent** щелкните по значку **SpIDer Agent**  в области уведомлений Windows.



Доступ к настройкам и компонентам защиты, а также отключение компонентов возможны только при работе с правами администратора.

В меню **SpIDer Agent**  сосредоточены основные средства управления и настройки **Dr.Web**.

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.

Лицензия. Открывает [Менеджер лицензий](#).

Инструменты. Открывает меню, предоставляющее доступ:

- к [Защите от потери данных](#);
- к [Антивирусной сети](#);
- к [Менеджеру карантина](#);
- к разделу [Поддержка](#).

Компоненты защиты. Быстрый доступ к списку компонентов защиты, в котором вы можете включить или выключить каждый из компонентов.

Обновление. Информация об актуальности компонентов или вирусных баз. Запускает обновление.

Сканер. Быстрый доступ к запуску разных типов проверки.

Режим работы  . Позволяет переключаться между режимом пользователя и режимом администратора. По умолчанию **Dr.Web** запускается в ограниченном режиме – режиме



пользователя, в котором недоступны [Настройки](#) и настройки [Компонентов защиты](#). Для переключения в другой режим, нажмите на замок. При включенном UAC операционная система выдаст запрос на повышение прав. Также для изменения режима потребуется ввести пароль, если в разделе [Настройки](#) вы включили опцию **Защищать паролем настройки Dr.Web**.

Статистика . Открывает окно, содержащее сведения о работе компонентов в течение текущего сеанса (количество проверенных, зараженных и подозрительных объектов, предпринятые действия и др.).

Настройки . Открывает окно с доступом к основным настройкам, настройкам компонентов защиты, а также модуля **Родительский контроль** и исключениям.



Для доступа к настройкам компонентов и для перехода к онлайн-сервису **Мой Dr.Web** необходимо ввести пароль, если в разделе [Настройки](#) вы включили опцию **Защищать паролем настройки Dr.Web**.

Если вы забыли пароль к настройкам продукта, обратитесь в [службу технической поддержки](#).



5.1. 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**.

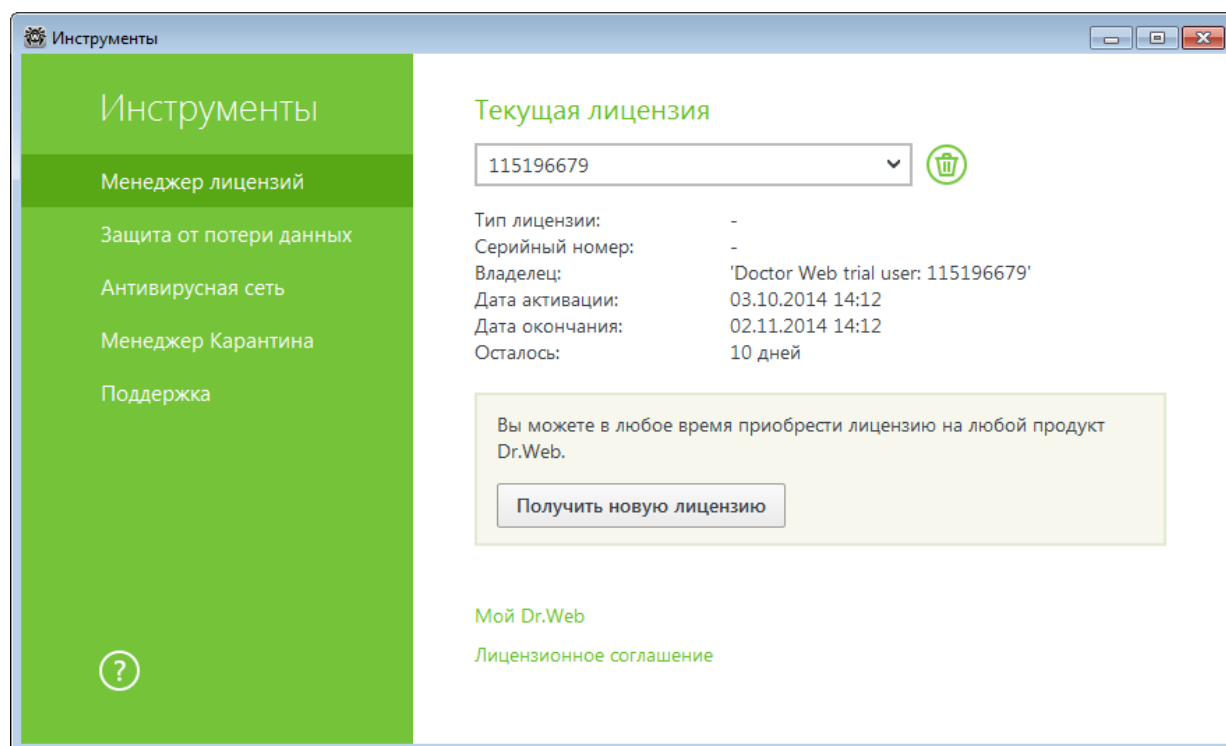


6. Инструменты

6.1. Менеджер лицензий

Менеджер лицензий в доступном виде отображает информацию, содержащуюся в имеющихся у вас [лицензиях Dr.Web](#).

Для доступа к этому окну в [меню SpIDer Agent](#)  выберите пункт **Лицензия**. В верхней части окна приводится информация о выбранной лицензии.



Получение ключевого файла

Для получения ключевого файла с сервера компании **«Доктор Веб»** нажмите кнопку **Получить новую лицензию**. Запустится [Мастер регистрации](#), в котором вы можете активировать новую лицензию, указать путь к ключевому файлу другой лицензии или приобрести лицензию на любой продукт **Dr.Web**.

Для работы программы **Dr.Web** требуется установить в защищаемой системе ключевой файл.

Ссылка **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 и т. д.), продлить срок ее действия, задать вопрос службе поддержки и многое другое.

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

Кнопка  позволяет удалить лицензию, выбранную в списке **Текущая лицензия**. Последнюю действующую лицензию удалить нельзя.



Удалить лицензию можно только в режиме администратора. В режиме пользователя эта кнопка недоступна.

Для работы **Dr.Web** требуется установить в защищаемой системе ключевой файл **Dr.Web**. При получении ключевого файла в процессе установки или в комплекте дистрибутива продукта установка ключевого файла производится автоматически и никаких дополнительных действий не требует.



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

При отсутствии действительного ключевого файла активность всех компонентов **Dr.Web** блокируется.

Менеджер лицензий может выводить оповещения в область уведомлений Windows. Вы можете настроить вывод уведомлений на экран и отправку их на электронную почту.

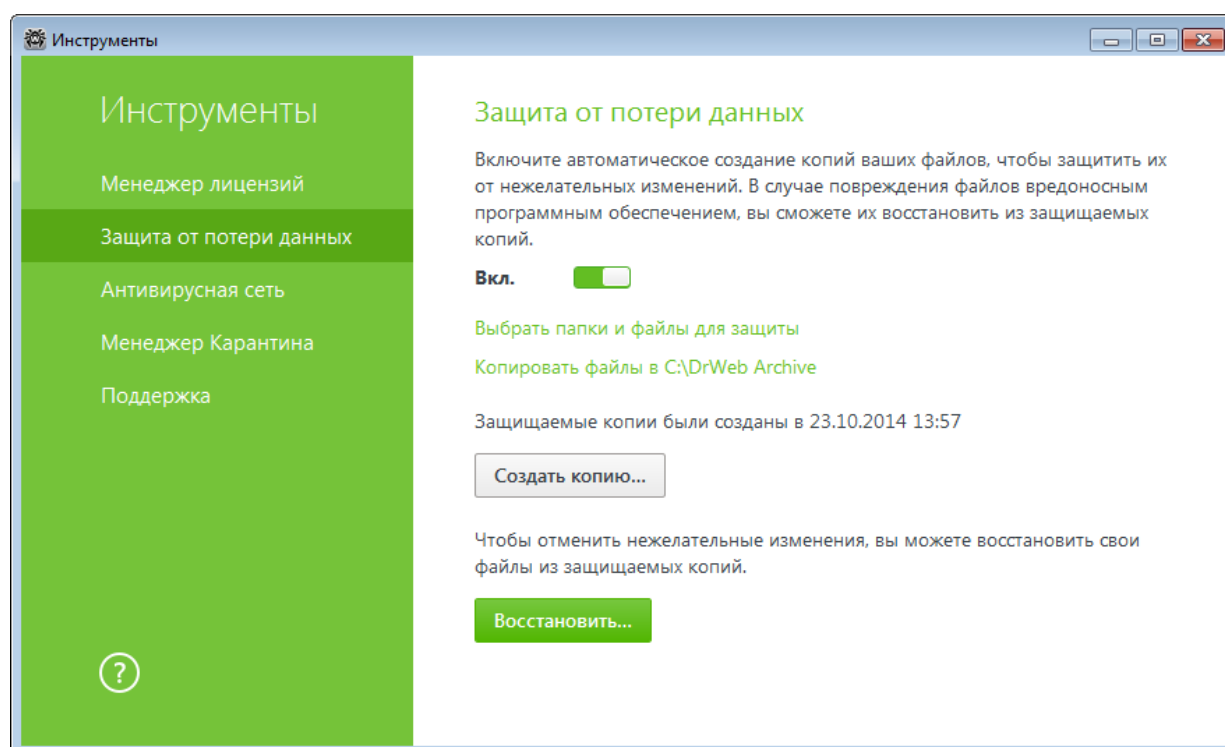
6.2. Защита от потери данных



В режиме пользователя невозможно изменить параметры защиты, а также восстановить файлы из копии. Для выполнения этих действий переключитесь в режим администратора.

Для того чтобы защитить важные файлы от изменений вредоносным программным обеспечением, включите функцию **Защиты от потери данных**. Эта функция позволяет создавать копии содержимого выбранных вами папок.

Нажмите ссылку **Выбрать файлы и папки для защиты**, чтобы указать объекты, для которых будут созданы защищаемые копии. В любой момент вы можете изменить список объектов. Также вы можете указать диск для хранения копий и периодичность, с которой эти копии будут создаваться. Через указанный промежуток времени **Dr.Web** будет проверять заданные объекты на наличие изменений и создавать копию, если изменения были внесены. Также вы можете удалить копии, чтобы очистить место на диске (на самих файлах удаление копий не отразится), и запретить запуск создания копий при работе от батареи.



В случае, если ваши файлы были повреждены, вы можете восстановить их копии за определенную дату. Для этого в главном окне нажмите кнопку **Восстановить**. В открывшемся окне выберите дату, и актуальные на тот момент копии файлов будут восстановлены в указанную вами папку.

Чтобы запустить создание копий вручную, в главном окне нажмите кнопку **Создать копию**. В открывшемся окне задайте описание для новой копии.

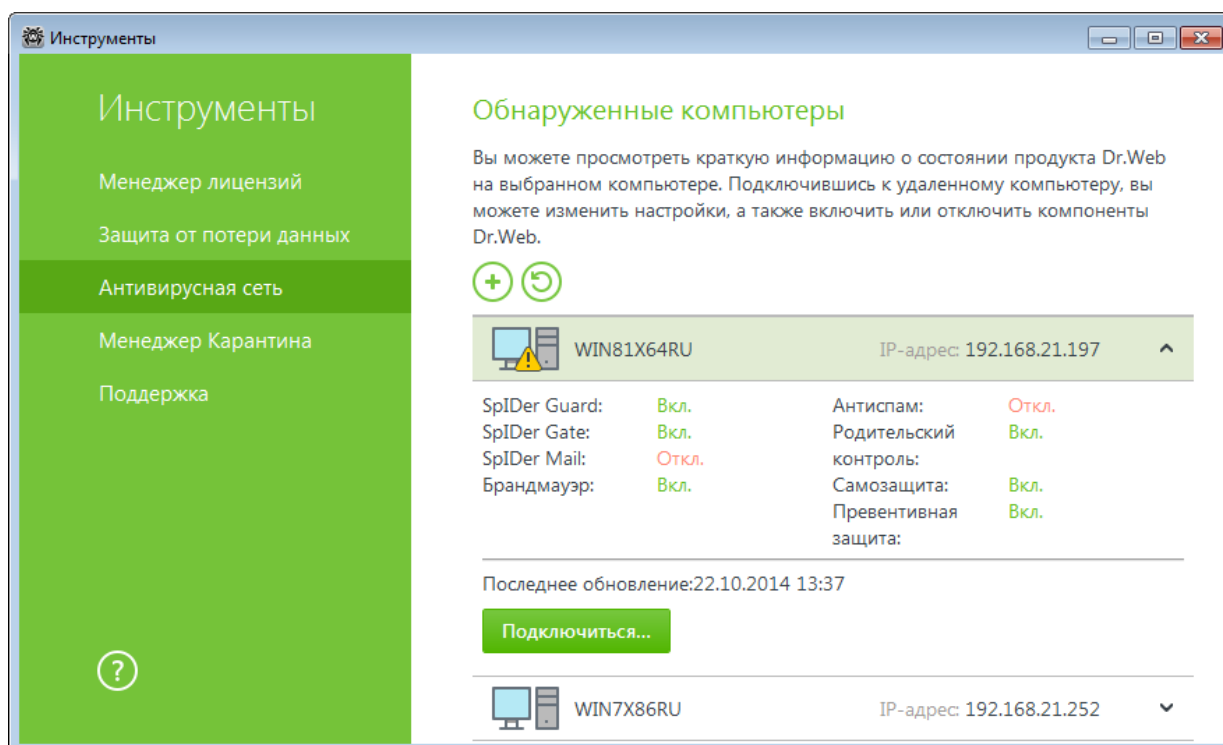


Для создания копий требуется не менее 5 ГБ свободного места на том диске, который вы выбрали для хранения копий.

6.3. Антивирусная сеть

Этот компонент позволяет управлять программами **Антивирус Dr.Web для Windows**, **Антивирус Dr.Web для серверов** и **Dr.Web Security Space** версии 10.0 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 группе **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** , а также будет показано уведомление об успешном подключении.

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 (в случае подключения к продуктам **Антивирус Dr.Web для Windows** или **Dr.Web Security Space**). 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  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 программе **Dr.Web** на вашем компьютере в разделе **Антивирусная сеть** Основных настроек.

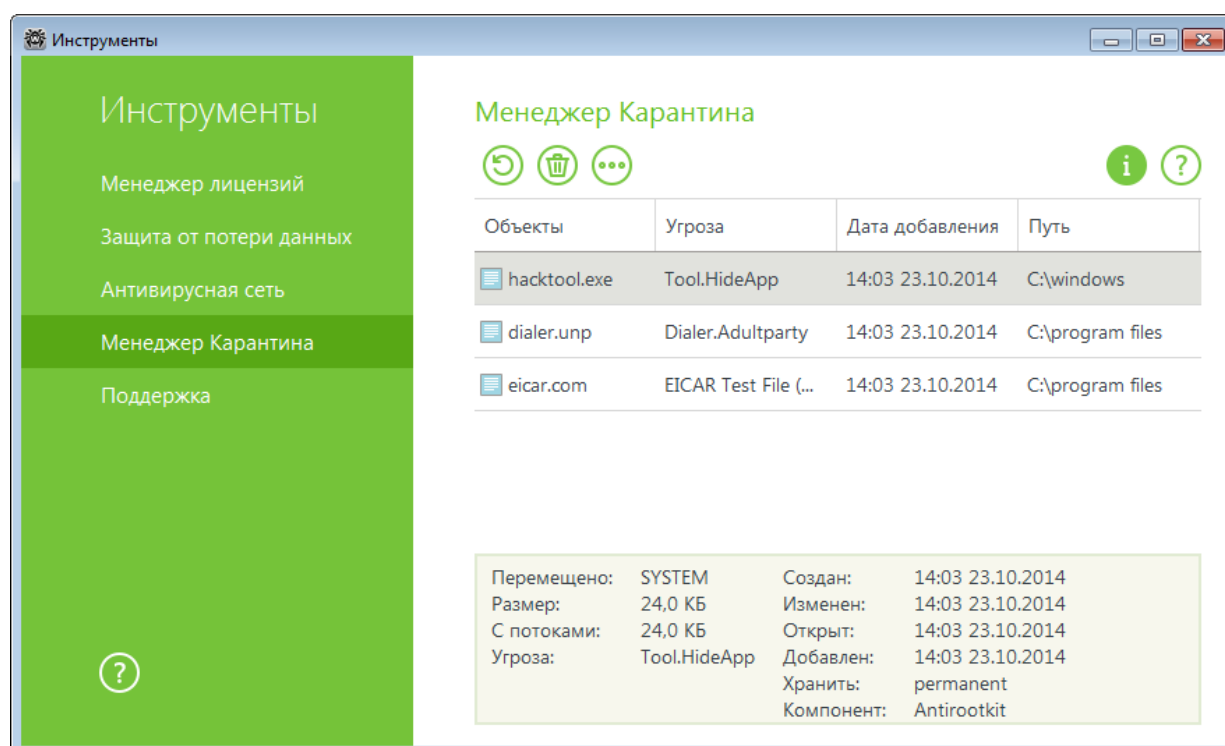


6.4. Менеджер Карантина

Менеджер карантина отображает данные о содержимом карантина, который служит для изоляции файлов, подозрительных на наличие вредоносных объектов. Также в карантин помещаются резервные копии файлов, обработанных **Dr.Web**.

В настройках Менеджера карантина вы можете включить опцию, которая определяет режим изоляции зараженных объектов, обнаруженных на съемных носителях. При включении этой опции подобные угрозы помещаются в папку на том же носителе и не шифруются. При этом папка карантина создается только в том случае, если возможна запись на носитель. Использование отдельных папок и отказ от шифрования на съемных носителях позволяет предотвратить возможную потерю данных.

Для доступа к этому окну в подменю **Инструменты** меню **SpIDer Agent** выберите пункт **Менеджер карантина**.



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

- **Объекты** – список имен объектов, находящихся в карантине;
- **Угроза** – классификация вредоносной программы, определяемая программой **Dr.Web** 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 **Менеджера карантина** файлы могут видеть только те пользователи, которые имеют к ним доступ. Чтобы отобразить скрытые объекты, необходимо иметь права Администратора.

В контекстном меню объектов доступны следующие кнопки управления:

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



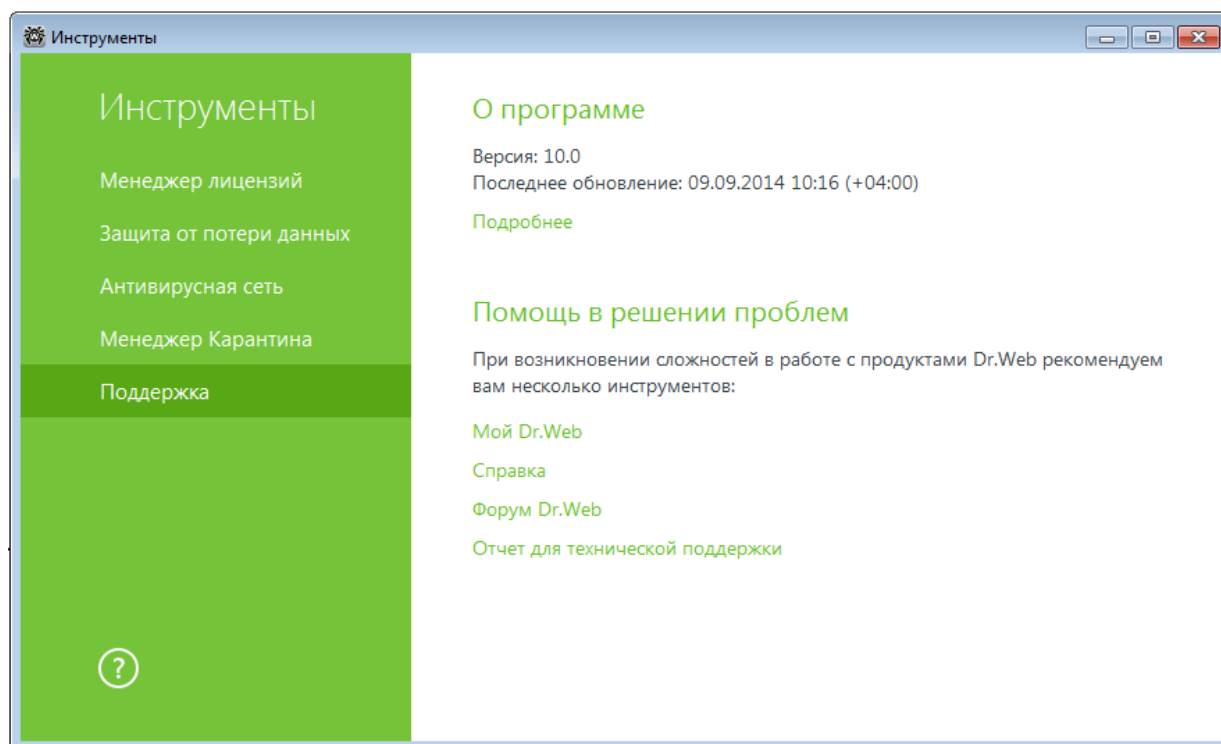
Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

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

Для того чтобы удалить все объекты из карантина, нажмите кнопку  и в выпадающем списке выберите пункт **Удалить все**.

6.5. Поддержка

Этот раздел содержит информацию о версии продукта, составе компонентов и дате последнего обновления, а также полезные ссылки, которые могут помочь вам ответить на вопросы или исправить неполадки, возникшие в процессе работы **Dr.Web**.



Воспользуйтесь одним из следующих инструментов в том случае, если у вас возникли вопросы.

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.

Справка. Открывает справку.

Форум Dr.Web. Открывает форум **Dr.Web** по адресу <http://forum.drweb.com>.

Отчет для технической поддержки. Запускает мастер, который позволит вам [создать отчет](#), содержащий важную информацию о системе и работе компьютера.

Если после этого вам не удалось решить проблему, 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>.



6.5.1. Создание отчета

При обращении в службу технической поддержки компании «Доктор Веб» вы можете сформировать отчет о вашей операционной системе и работе **Dr.Web**.

Отчет будет сохранен в виде архива в папке Doctor Web, расположенном в папке профиля пользователя %USERPROFILE%.

Чтобы сформировать отчет, нажмите соответствующую кнопку. В отчет будет включаться:

1. Техническая информация об операционной системе:
 - общие сведения о компьютере;
 - запущенных процессах;
 - запланированных заданиях;
 - службах, драйверах;
 - браузере по умолчанию;
 - установленных приложениях;
 - политиках ограничений;
 - файле HOSTS;
 - о серверах DNS;
 - записи системного журнала событий;
 - перечень системных каталогов;
 - ветви реестра;
 - провайдеры Winsock;
 - сетевые соединения;
 - отчеты отладчика Dr.Watson;
 - индекс производительности.
2. Информация об **Антивирусных решениях Dr.Web**.
3. Информация о подключаемых модулях **Dr.Web**:
 - **Dr.Web для IBM Lotus Domino**;
 - **Dr.Web для Kerio MailServer**;
 - **Dr.Web для Kerio WinRoute**.

Информация о работе **Антивирусных продуктов Dr.Web** находится в Журнале событий операционной системы Windows, в разделе **Журналы приложений и служб** → **Doctor Web**.



7. Обновление

Для обнаружения вредоносных объектов антивирусы компании «**Доктор Веб**» используют специальные **вирусные базы Dr.Web**, в которых содержится информация обо всех известных вредоносных программах. Регулярное 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 антивирусов **Dr.Web** исправляются обнаруженные в программах ошибки, обновляется справочная система и документация.

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

Запуск обновления

При обновлении **Dr.Web** загрузит все обновленные файлы, соответствующие вашей версии **Dr.Web**, а также новую версию **Dr.Web** в случае ее выхода.



Для обновления **Dr.Web** необходимо иметь доступ к сети Интернет, либо к зеркалу обновлений (локальной или сетевой папке), либо к Антивирусной сети, в которой хотя бы на одном из компьютеров настроено зеркало обновлений.

Настройка необходимых параметров производится в разделе **Обновление** [Основных настроек Dr.Web](#).

Запуск обновления с помощью модуля управления SpIDer Agent

В [меню SpIDer Agent](#)  выберите пункт **Обновление**. Откроется информация об актуальности вирусных баз и компонентов, а также дата последнего обновления. Чтобы запустить процесс обновления, нажмите кнопку **Обновить**.

Запуск обновления из командной строки

Перейдите в папку установки **Dr.Web** (%PROGRAMFILES%\Common Files\Doctor Web\Updater) и запустите drwupsrv.exe. Список параметров вы можете найти в [Приложении А](#).

Автоматический запуск обновления

При автоматическом запуске обновление проводится в фоновом режиме, при этом отчеты записываются в файл dwupdater.log в папке %allusersprofile%\Doctor Web\Logs\.



При обновлении исполняемых файлов, драйверов и библиотек может потребоваться перезагрузка компьютера. В этом случае будет показано соответствующее предупреждение.



8. Сканер Dr.Web

Сканер Dr.Web для Windows предназначен для антивирусной проверки загрузочных секторов, памяти, а также как отдельных файлов, так и объектов в составе сложных структур (архивы, контейнеры, электронные письма с вложениями). Проверка производится с использованием всех [методов обнаружения](#) угроз. 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.

Вы можете [подключиться](#) к облачным сервисам компании «**Доктор Веб**», которые позволяют антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании «**Доктор Веб**» в режиме реального времени.

8.1. Запуск проверки

Запуск Сканера



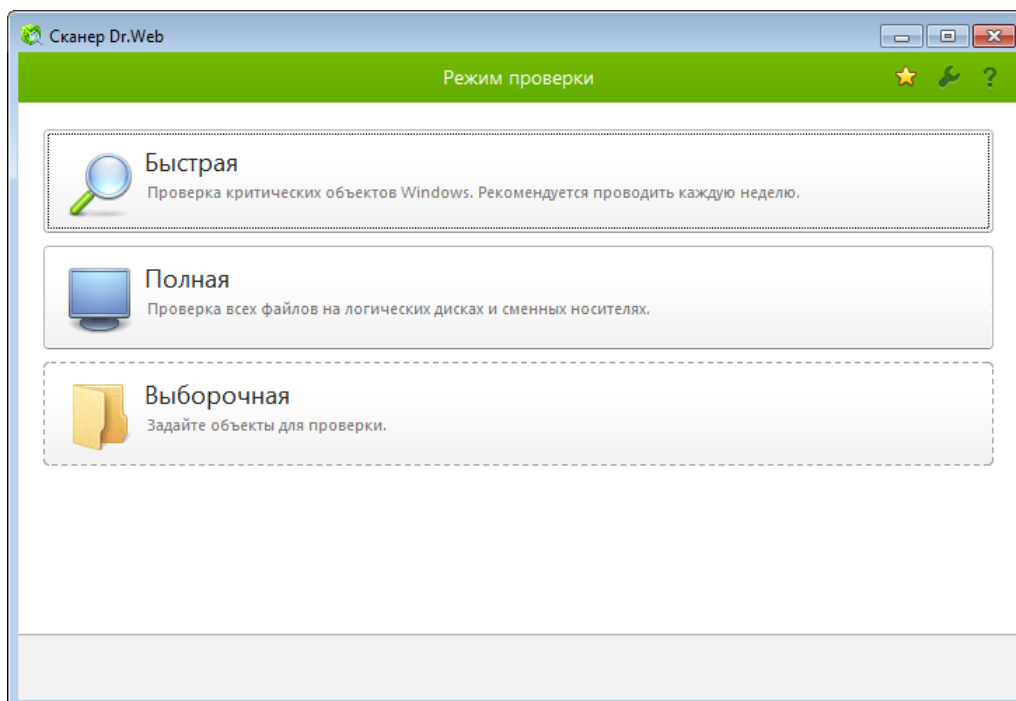
Рекомендуется запускать **Сканер** от имени пользователя, обладающего правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут подвергнуты проверке.

1. Для запуска **Сканера** используйте одно из следующих средств:
 - значок **Сканера** на Рабочем столе;
 - пункт **Сканер** в меню **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. [Запуск Сканера из командной строки](#)).

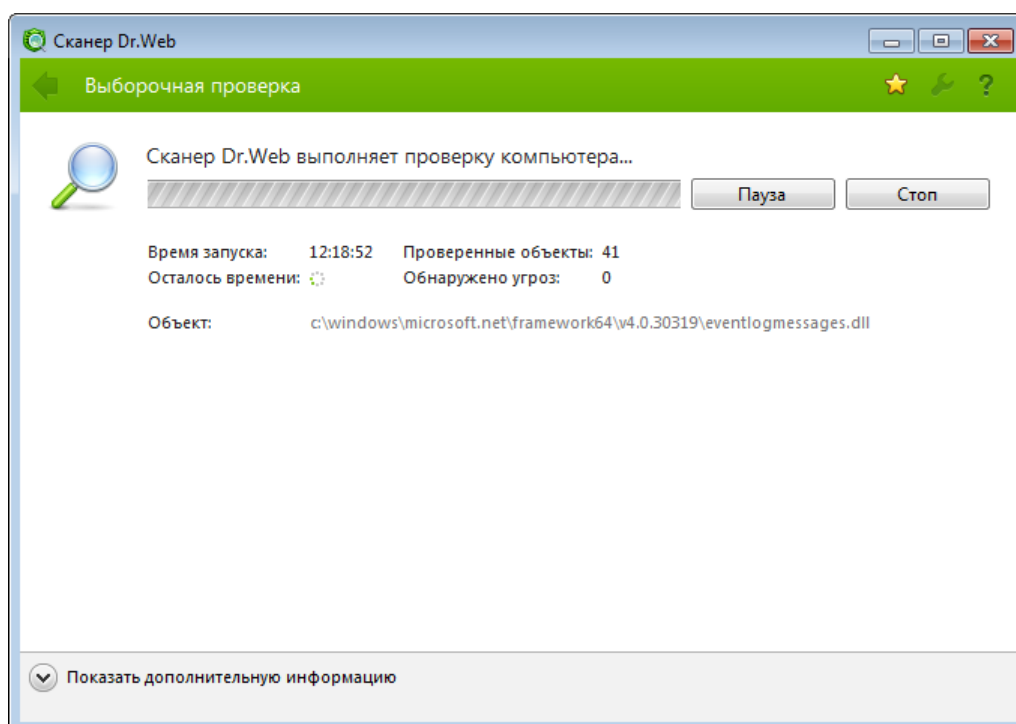
Чтобы запустить **Сканер** с настройками по умолчанию для проверки конкретного файла или каталога, выберите в контекстном меню значка файла или каталога (на Рабочем столе или в Проводнике операционной системы Windows) пункт **Проверить Dr.Web**.



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:

- загрузочные сектора всех дисков;
- оперативная память;
- корневая папка загрузочного диска;



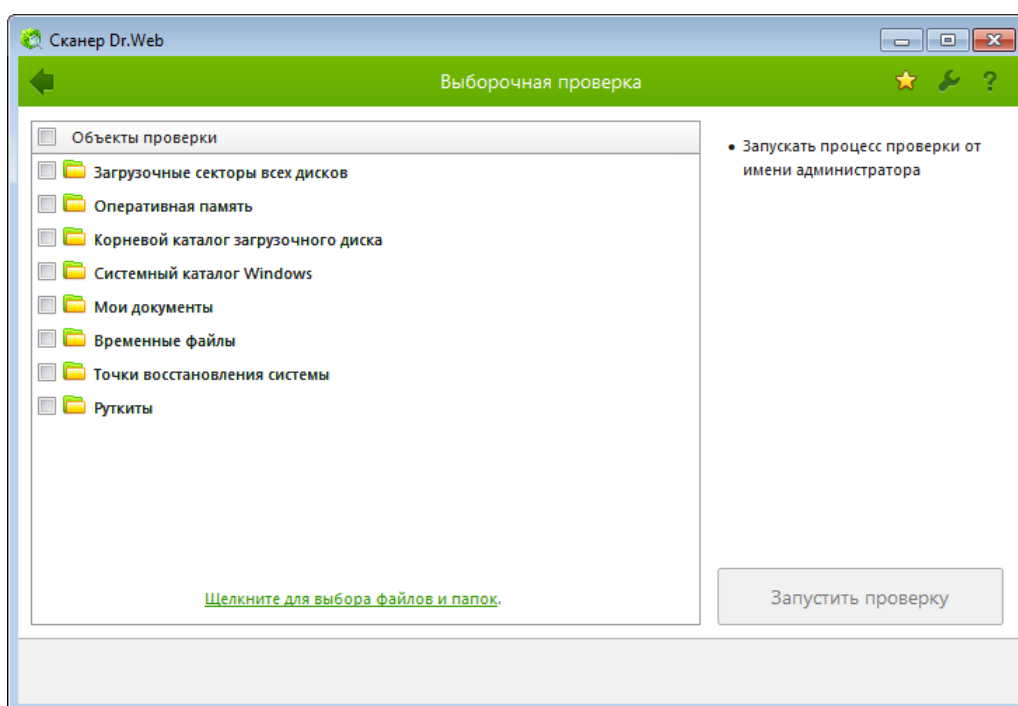
- системная папка Windows;
- папка Мои Документы;
- временные файлы;
- точки восстановления системы;
- наличие руткитов (если процесс проверки запущен от имени администратора).



Архивы и почтовые файлы в режиме быстрой проверки не проверяются.

В режиме *полной проверки* производится полное сканирование оперативной памяти и всех жестких дисков (включая загрузочные сектора), 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** в таблице задаются объекты для проверки: любые файлы и папки, а также такие объекты, как оперативная память, 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**.

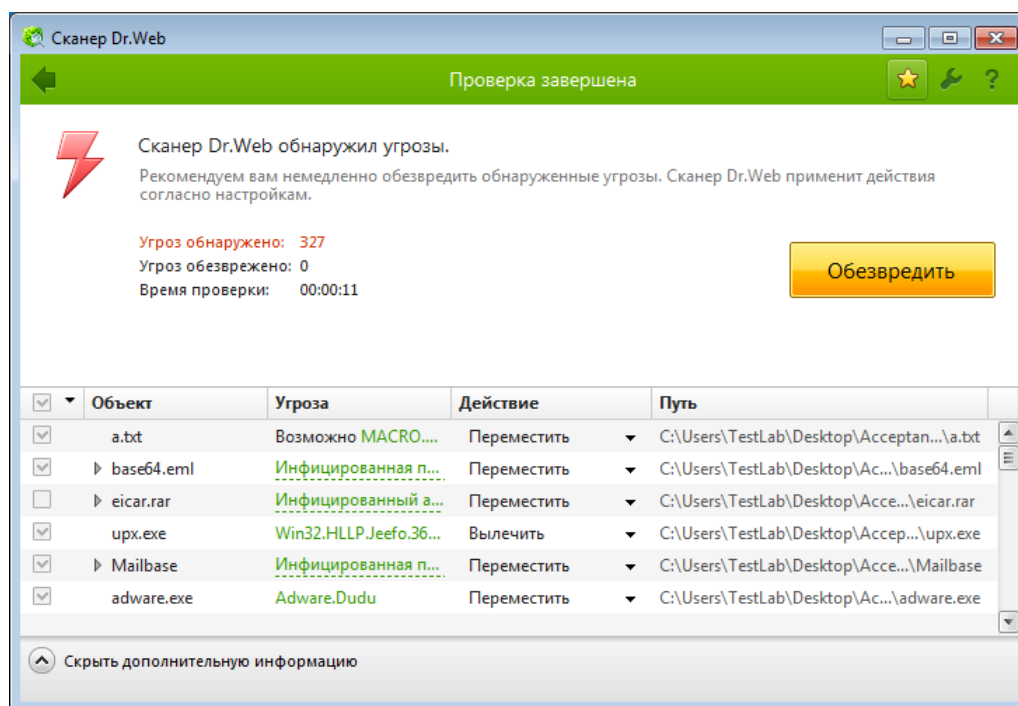


Кнопка **Пауза** недоступна во время проверки оперативной памяти и процессов.



8.2. Действия при обнаружении угроз

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.



По нажатию кнопки **Обезвредить** действия применяются к выбранным объектам в таблице. По умолчанию после окончания проверки для обезвреживания выбраны все объекты. При необходимости вы можете вручную выбрать конкретные объекты или группы объектов, для которых требуется применить действия по нажатию кнопки **Обезвредить**. Для этого используйте флажки рядом с названиями объектов или выпадающее меню в заголовке таблицы.

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 выбранные угрозы одновременно.

Существуют следующие ограничения:

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

Подробный отчет о работе программы сохраняется в файл журнала dwscanner.log, который находится в папке %USERPROFILE%\Doctor Web.



Название столбца	Описание
Объект	В этом столбце указано наименование зараженного или подозрительного объекта (имя файла – если заражен файл, Boot sector в случае зараженного загрузочного сектора, Master Boot Record в случае зараженного MBR жесткого диска).
Угроза	В этом столбце указано наименование вируса или модификации вируса по внутренней классификации « Доктор Веб » (модификацией известного вируса называется код, полученный таким изменением известного вируса, что при этом он опознается сканером, но алгоритмы лечения исходного вируса к нему неприменимы). Для подозрительных объектов указывается, что объект «возможно, инфицирован» и указывается тип возможного вируса по классификации эвристического анализатора.
Действие	Нажмите на стрелочку на этой кнопке, чтобы задать действие для выбранной угрозы (по умолчанию Сканер Dr.Web предлагает оптимальное значение). Вы можете применить указанное на кнопке действие отдельно, без нейтрализации остальных угроз. Для этого нажмите на эту кнопку.
Путь	В этом столбце указан полный путь к соответствующему файлу.



Если в [настройках Сканера Dr.Web](#) вы установили флажок **Автоматически применять действия к угрозам**, то обезвреживание угроз будет произведено автоматически.

8.3. Настройка Сканера



При работе под управлением операционных систем Windows Vista и более поздних **Сканер Dr.Web** рекомендуется запускать от имени пользователя, обладающего правами администратора.

Настройки по умолчанию являются оптимальными для большинства применений **Сканера Dr.Web**, их не следует изменять без необходимости.

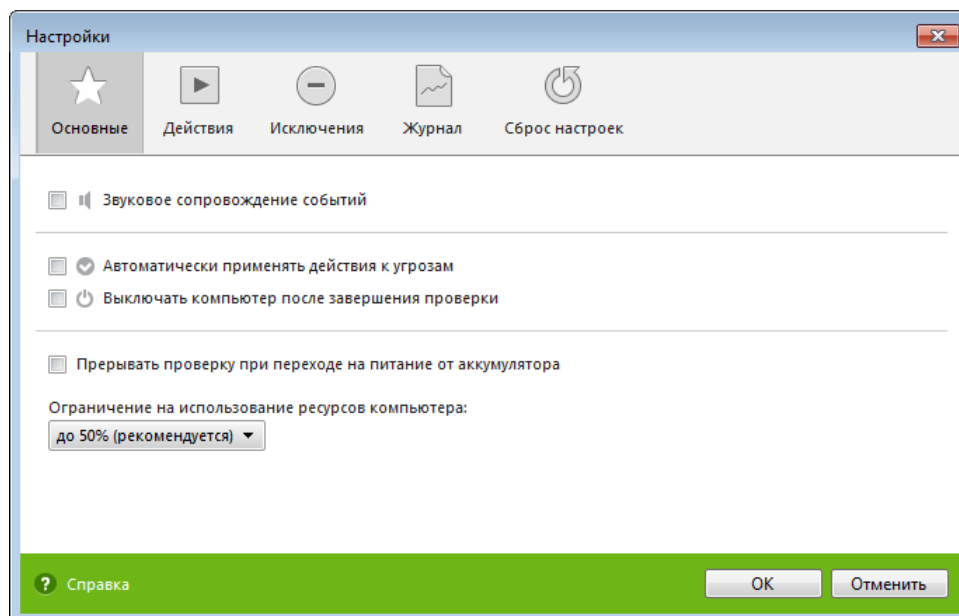
Изменение настроек Сканера Dr.Web

- В [меню SpIDer Agent](#) выберите пункт **Сканер**. Откроется меню быстрого доступа к запуску разных типов проверки.
- Выберите пункт **Выборочная**. Откроется главное окно **Сканера Dr.Web**. Пункты **Быстрая** и **Полная** запустят соответствующие типы проверок (при этом настройки будут недоступны до остановки или окончания проверки).
- На панели инструментов щелкните по иконке настроек . Откроется окно настроек, содержащее следующие разделы:
 - раздел [Основные](#), в котором задаются общие параметры работы **Сканера Dr.Web**;
 - раздел [Действия](#), в котором задается реакция **Сканера Dr.Web** на обнаружение зараженных или подозрительных файлов и вредоносных программ;
 - раздел [Исключения](#), в котором задаются дополнительные ограничения на состав файлов, подлежащих проверке;
 - раздел [Журнал](#), в котором задается режим ведения файла журнала **Сканера Dr.Web**;
 - раздел [Сброс настроек](#), в котором пользователю предоставляется возможность восстановить исходные настройки **Сканера Dr.Web**.
- Для более подробной информации о настройках, задаваемых в каждом разделе, воспользуйтесь кнопкой **Справка** .
- По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.



Раздел Основные

В этом разделе задаются основные параметры работы **Сканера Dr.Web**.



Настройка	Описание
Звуковое сопровождение событий	Установите этот флажок, чтобы Сканер Dr.Web сопровождал каждое событие звуковым сигналом.
Автоматически применять действия к угрозам	Установите этот флажок, чтобы Сканер Dr.Web автоматически применял действия к обнаруженным угрозам.
Выключать компьютер после завершения проверки	Установите этот флажок, чтобы после завершения проверки происходило выключение компьютера. Если при этом установлен флажок Автоматически применять действия к угрозам , перед выключением компьютера Сканер Dr.Web применит заданные действия к обнаруженным угрозам.
Прерывать проверку при переходе на питание от аккумулятора	Установите этот флажок, чтобы при переходе на питание от аккумулятора проверка была прервана.
Ограничение на использование ресурсов компьютера	Эта опция устанавливает ограничение на использование ресурсов компьютера Сканером Dr.Web . По умолчанию задано значение 50%.



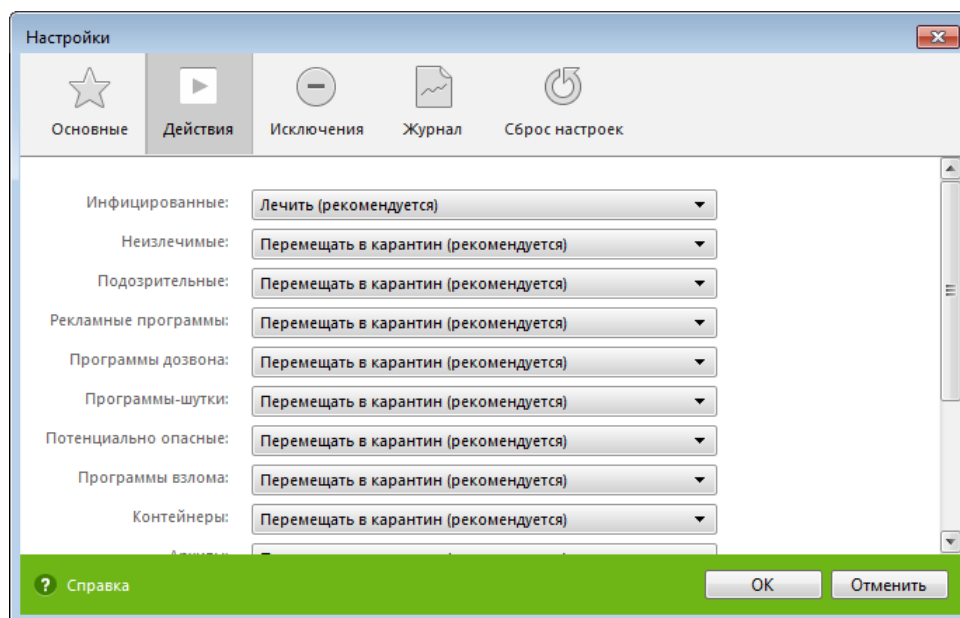
Параметры **Звуковое сопровождение событий**, **Автоматически применять действия к угрозам** и **Выключать компьютер после завершения проверки** доступны для быстрой настройки в главном окне **Сканера Dr.Web** или в окне настройки выборочной проверки. Для этого щелкните по иконке ★ на панели инструментов.



Раздел Действия

Настройка обезвреживания угроз

1. Перейдите в окне настроек в раздел **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, контейнерах и почтовых ящиках. Действия по отношению к вышеуказанным объектам выполняются над всем объектом, а не только над зараженной его частью.
7. Для успешного завершения лечения некоторых зараженных (инфицированных) файлов требуется перезагрузка операционной системы. Вы можете выбрать один из вариантов:
 - **Предлагать перезагрузку;**
 - **Перезагружать компьютер автоматически.** Этот режим может привести к потере несохраненных данных.

Оптимальной реакцией на обнаружение излечимых угроз (например, зараженных вирусами



файлов) является лечение, в ходе которого восстанавливается исходное состояния объекта до заражения. Угрозы других типов рекомендуется перемещать в карантин, что позволяет предотвратить случайную потерю ценных данных. Вы можете выбрать следующие реакции:

Действие	Описание
Лечить	Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, будет отработана реакция, заданная для неизлечимых объектов. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров). Троянские программы при обнаружении удаляются. Это единственное действие, доступное для зараженных загрузочных секторов.
Перемещать в карантин	Переместить объект в специальную папку для изоляции. Для загрузочных секторов никаких действий производиться не будет.
Удалять	Полностью удалить объект из системы. Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропустить объект без выполнения каких-либо действий и не выводить информацию в отчете. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

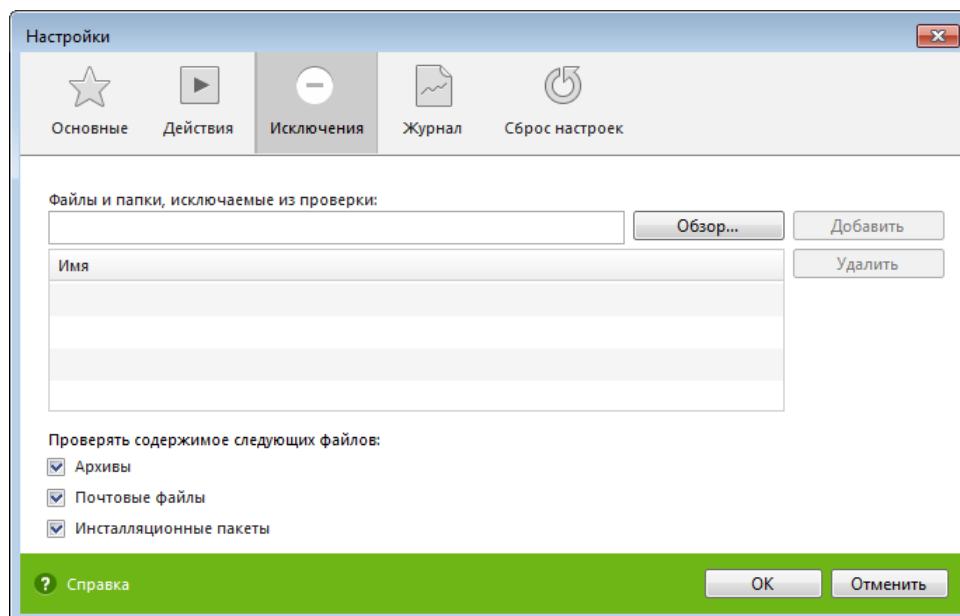


При обнаружении вирусов или подозрительного кода внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров) действия по отношению к угрозам внутри таких объектов выполняются над всем объектом, а не только над зараженной его частью.



Раздел Исключения

В этом разделе задаются дополнительные ограничения на состав файлов, подлежащих проверке.



Здесь можно задать список файлов (масок файлов), которые не будут проверяться (из проверки будут исключены все файлы с данным именем.) В таком качестве могут выступать временные файлы (файлы подкачки) и т. п.

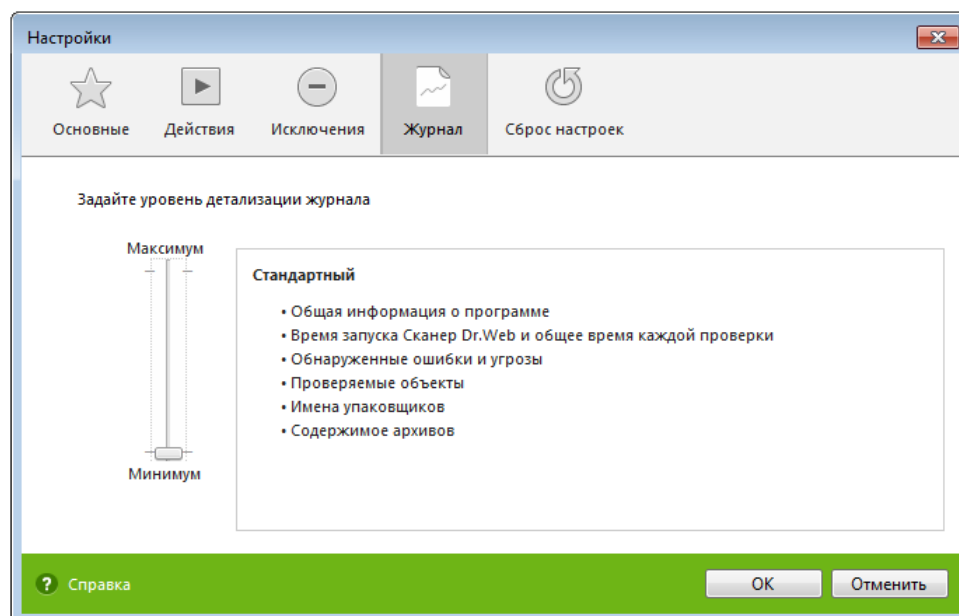
Также вы можете указать, требуется ли проводить проверку содержимого архивов, почтовых файлов и инсталляционных пакетов.



Раздел Журнал

В этом разделе вы можете настроить параметры ведения файла журнала.

Журнал **Сканера Dr.Web** хранится в файле dwscanner.log, расположенном в папке %USERPROFILE%\Doctor Web. Рекомендуется периодически анализировать файл журнала.



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

Вы можете задать одну из следующих степеней детальности ведения журнала:

- **Стандартный** – в данном режиме в журнале фиксируются такие события, как проведение обновлений, запуск и остановка **Сканера Dr.Web**, обнаруженные угрозы, а также данные об именах упаковщиков и содержимом проверяемых архивов. При необходимости вы можете добавить такие объекты в список **исключений**, что может снизить нагрузку на компьютер. Данный режим ведения журнала походит для большинства применений;
- **Отладочный** – в данном режиме в журнале фиксируется максимальное количество информации о работе **Сканера Dr.Web**, что может привести к значительному увеличению файла журнала. Рекомендуется использовать этот режим только при возникновении проблем в работе **Сканера Dr.Web** или по просьбе технической поддержки компании «Доктор Веб».

Для **Стандартного** режима разрешенный размер журнала равен 10 МБ. Размер файла в отладочном режиме не ограничен.

После завершения проверки при превышении максимального размера файл журнала урезается до:

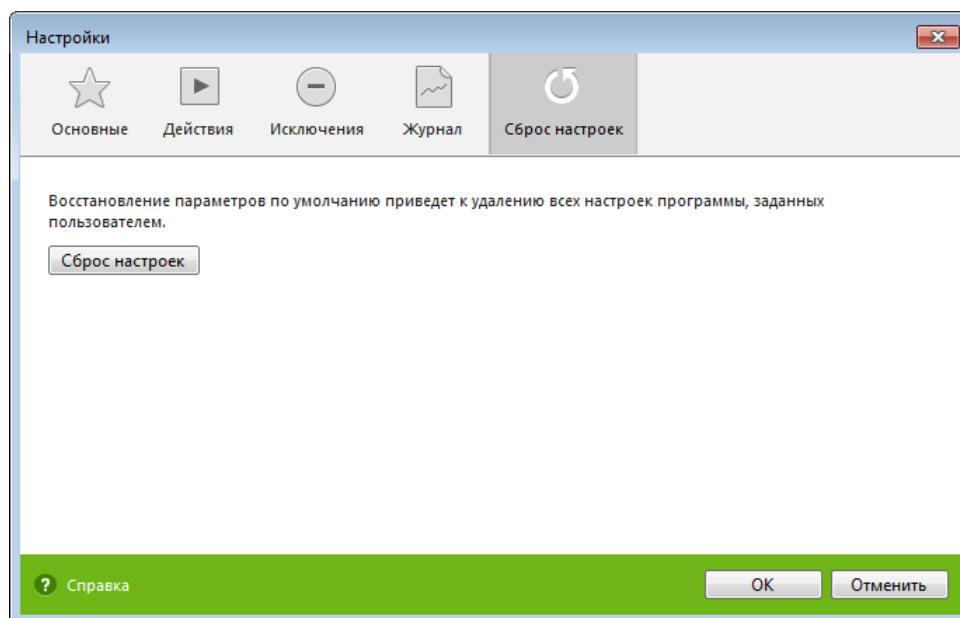
- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер (таким образом информация сохраняется до следующего запуска проверки).



При запуске проверки файл журнала урезается до размера, заданного настройками.

Раздел Сброс настроек

В разделе восстановления стандартных настроек вы можете восстановить настройки работы **Сканера Dr.Web**. Для этого нажмите кнопку **Восстановить значения по умолчанию**.





8.4. Запуск Сканера с параметрами 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 [<ключи>] [<объекты>]
```

где:

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

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

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

Параметры – ключи командной строки, которые задают настройки программы. При их отсутствии проверка выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их). Ключи начинаются с символа «/» и, как и остальные параметры командной строки, разделяются пробелами.



8.5. Консольный сканер

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



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

Запуск Консольного сканера

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

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

где:

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

Ключ начинается с символа «/», несколько ключей разделяются пробелами. Список объектов проверки может быть пуст или содержать несколько элементов, разделенных 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.

8.6. 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 просмотра параметров задания 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 установленных компонентов входит Брандмауэр, то после установки программы **Dr.Web** 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.



9. Настройки



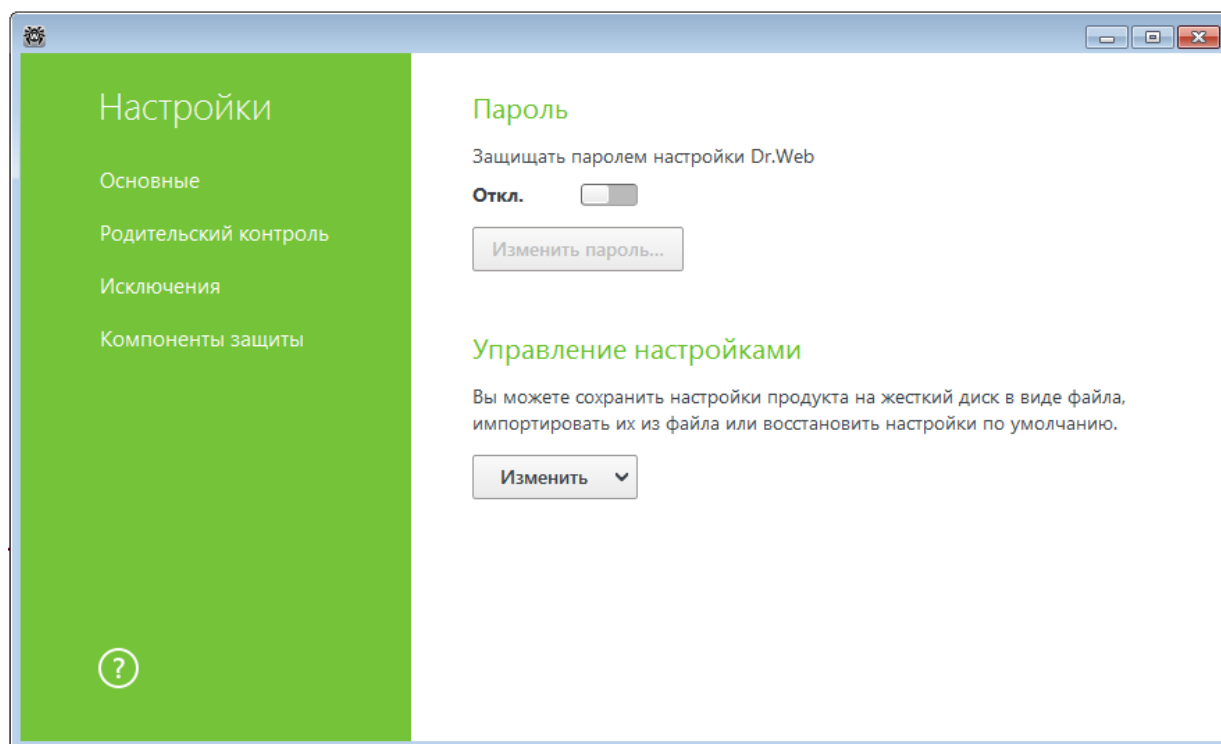
Настройки доступны только при работе с правами администратора.

Защита паролем

Чтобы ограничить доступ к настройкам **Dr.Web** на вашем компьютере включите опцию **Защищать паролем настройки Dr.Web**. В открывшемся окне задайте пароль, который будет запрашиваться при обращении к настройкам **Dr.Web**, подтвердите его ввод и нажмите кнопку **ОК**.



Если вы забыли пароль к настройкам продукта, обратитесь в [службу технической поддержки](#).



Управление настройками

Чтобы восстановить настройки по умолчанию, в выпадающем списке выберите пункт **Сбросить настройки**.

Если вы уже настроили работу антивируса на другом компьютере и хотите использовать те же настройки, в выпадающем списке выберите пункт **Импортировать**.

Если вы хотите использовать свои настройки на других компьютерах, в выпадающем списке выберите пункт **Экспортировать**, а затем воспользуйтесь аналогичной вкладкой на другом компьютере.



10. Основные настройки



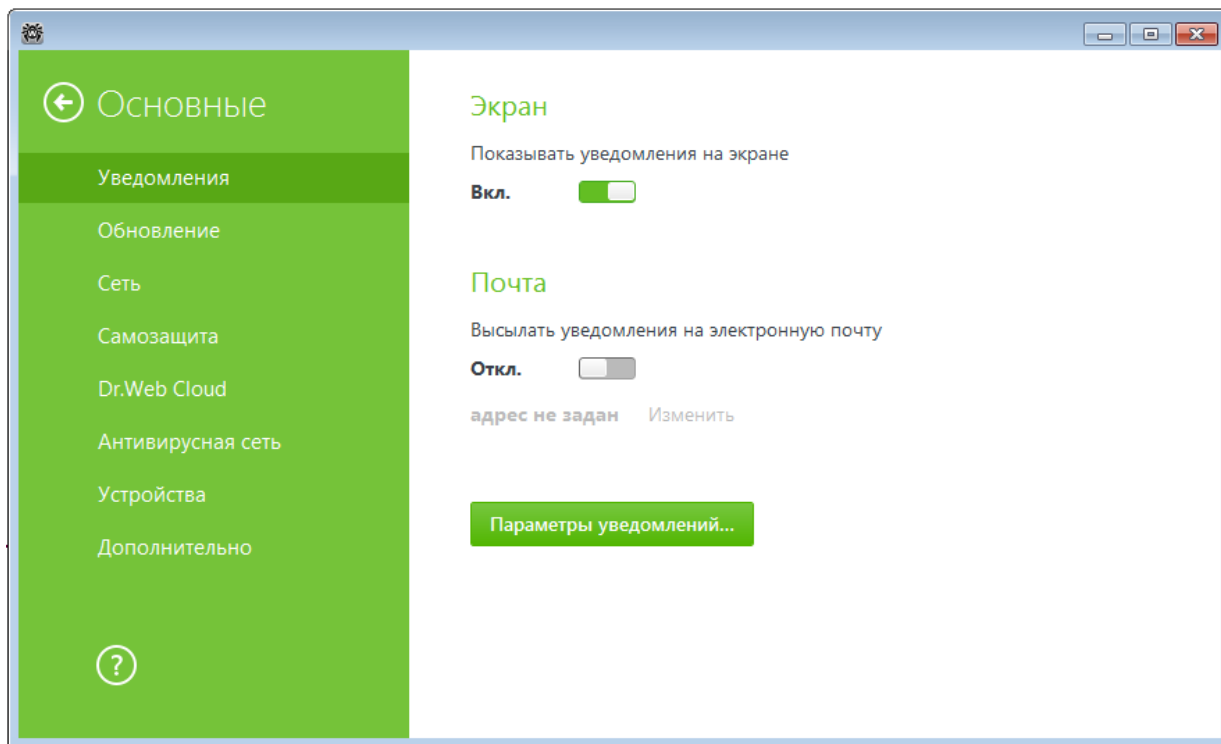
Для доступа к основным настройкам **Dr.Web** запрашивается пароль, если в разделе [Настройки](#) вы установили флажок **Защищать паролем настройки Dr.Web**.

Настройки **Dr.Web** доступны только при запуске с правами администратора.

Единый центр управления настройками позволяет задать как общие параметры работы антивирусного комплекса.

10.1. 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.



Уведомления, которые выводятся на экран

Включите соответствующую опцию, чтобы получать подсказки-уведомления в виде всплывающего окна над значком **SpIDer Agent**  в области уведомлений Windows.



Уведомления по почте

Чтобы включить режим нотификации о событиях по почте, включите опцию **Высылать уведомления на электронную почту**.

1. Убедитесь, что в окне **Параметры уведомлений** выбраны нужные типы оповещений.
2. Нажмите кнопку **Изменить**, чтобы задать параметры почты. Откроется окно настройки параметров.
3. Укажите следующую информацию:

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

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

Параметры уведомлений

Параметры уведомлений

Тип уведомления	Экран	Почта
Обнаружена угроза	☒	☐
Важные	☒	☐
Критичные	☒	☐
Малозначительные	☒	☐

☒ Не показывать уведомления в полноэкранном режиме

☒ Отображать уведомления Брандмауэра на отдельном экране в полноэкранном режиме

ОК

Отменить

?



1. Нажмите кнопку **Параметры уведомлений**.
2. Выберите уведомления, которые вы хотите получать, и установите соответствующие флажки. Чтобы отображать экранные уведомления, установите флажок в столбце **Экран**. Чтобы получать оповещения по почте, устанавливайте флажок в столбце **Почта**.
3. 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.

4. Если вы выбрали одно или несколько почтовых уведомлений, настройте [отправку почты](#) с вашего компьютера.
5. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для отказа от них.

Тип уведомления	Описание
Обнаружена угроза	Установите этот флажок, чтобы получать уведомления об обнаруженных угрозах. Снимите флажок, чтобы не получать подобных уведомлений. По умолчанию уведомления включены.
Важные уведомления	Установите этот флажок, чтобы получать следующие важные уведомления: • об истечении времени работы за компьютером, • о заблокированных попытках изменения системной даты, • о появлении новой версии продукта, • об устаревании вирусных баз. Снимите этот флажок, чтобы не получать перечисленные уведомления. По умолчанию уведомления включены.
Критичные уведомления	Установите этот флажок, чтобы получать следующие критичные уведомления: • о том, что срок действия вашей лицензии заканчивается, • об ошибке создания защищаемой копии, • об обнаружении соединений, ожидающих ответа Брандмауэра. Снимите этот флажок, чтобы не получать перечисленные уведомления. По умолчанию уведомления включены.
Малозначительные уведомления	Установите этот флажок, чтобы получать следующие малозначительные уведомления: • об успешном обновлении, • о неуспешном завершении обновления, • об истечении времени работы в Интернет, • о том, что определенный URL был заблокирован, • о том, что попытка доступа к защищаемому объекту заблокирована.



Тип уведомления	Описание
	Снимите этот флажок, чтобы не получать перечисленные уведомления. По умолчанию уведомления включены.



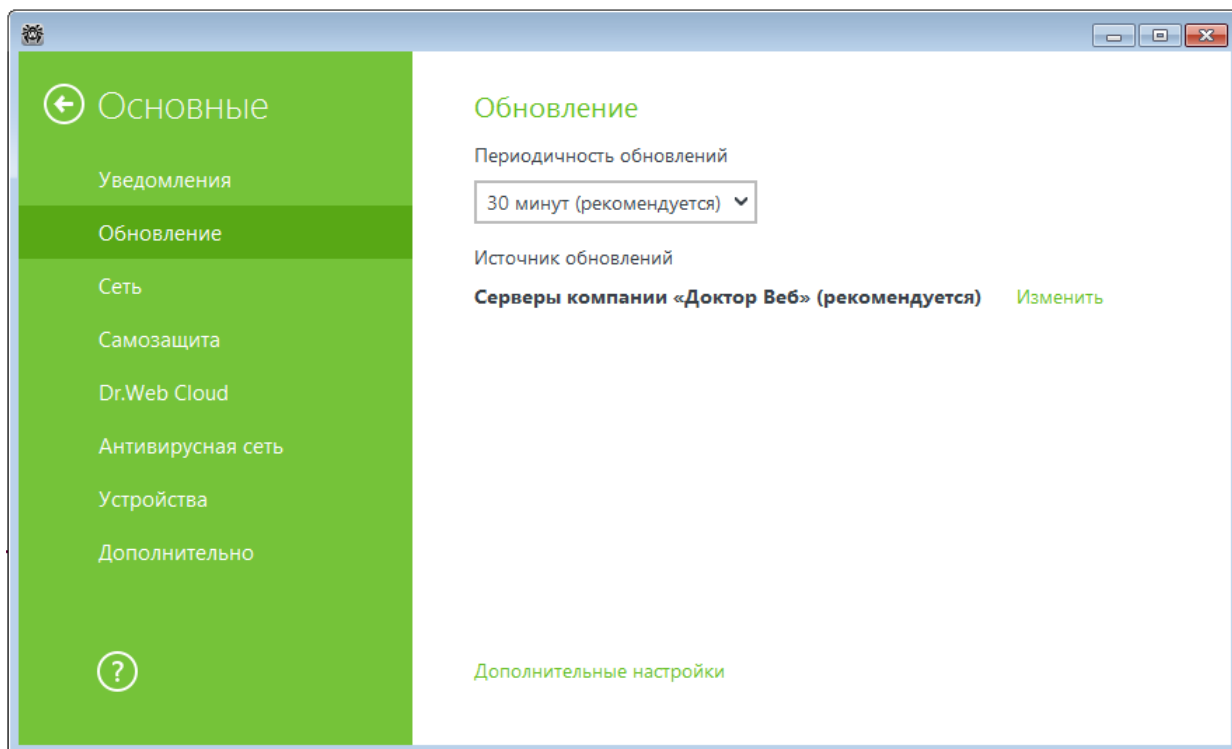
Уведомления о некоторых событиях не входят в перечисленные группы и всегда показываются пользователю:

- установка приоритетных обновлений, для которых требуется перезагрузка;
- запрос на разрешение процессу модификации объекта;
- успешное подключение к удаленному компьютеру в Антивирусной сети;
- активирован демонстрационный период, рекомендуется приобрести лицензию;
- текущая лицензия заблокирована.



10.2. Обновление

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



10.3. Сеть

Использование прокси-сервера

При необходимости вы можете включить использование прокси-сервера и задать настройки подключения к нему. Нажмите **Изменить**, чтобы задать настройки подключения к прокси-серверу:

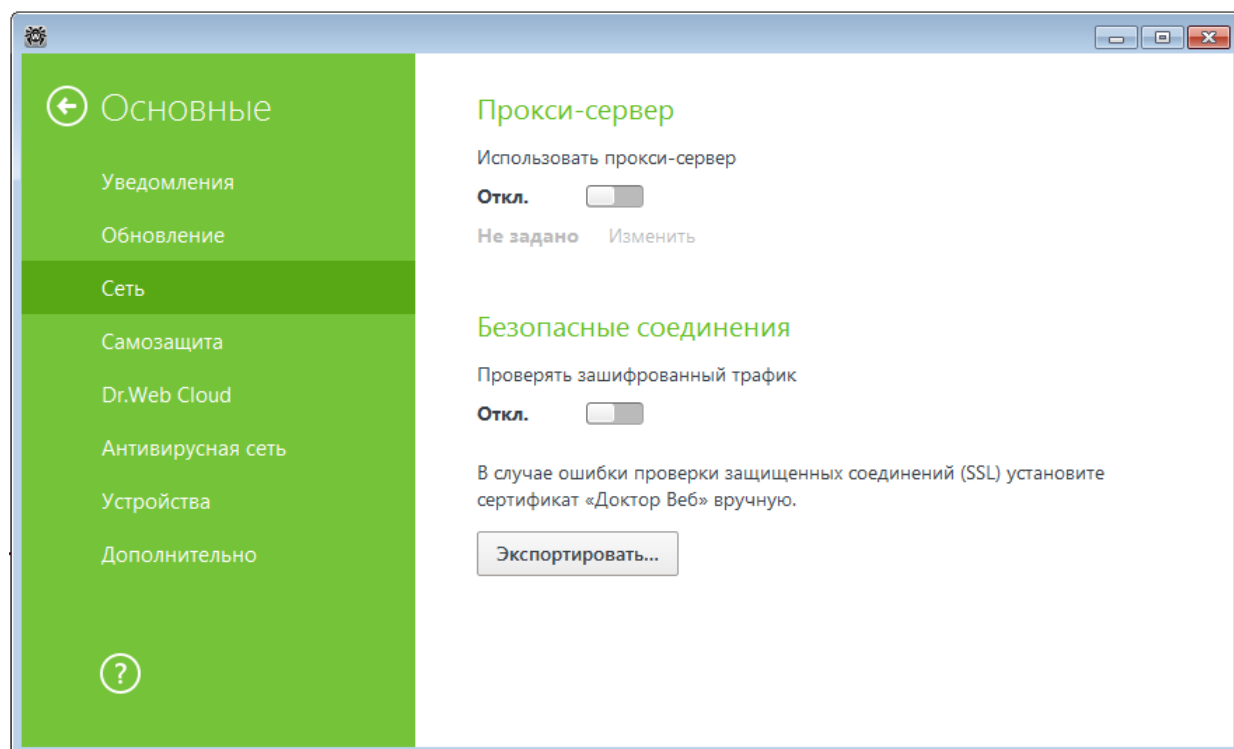
Настройка	Описание
Адрес	Укажите адрес прокси-сервера.
Порт	Укажите порт прокси-сервера.
Пользователь	Укажите имя учетной записи для подключения к прокси-серверу.
Пароль	Укажите пароль учетной записи, используемой для подключения к прокси-серверу.
Тип авторизации	Выберите тип авторизации, требуемый для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

Безопасные соединения

Вы можете включить в проверку данные, передаваемые по безопасным протоколам. Для этого включите соответствующую опцию. Если клиент, который получает и передает такие данные, не обращается к хранилищу сертификатов системы Windows, то необходимо будет экспортировать



сертификат.



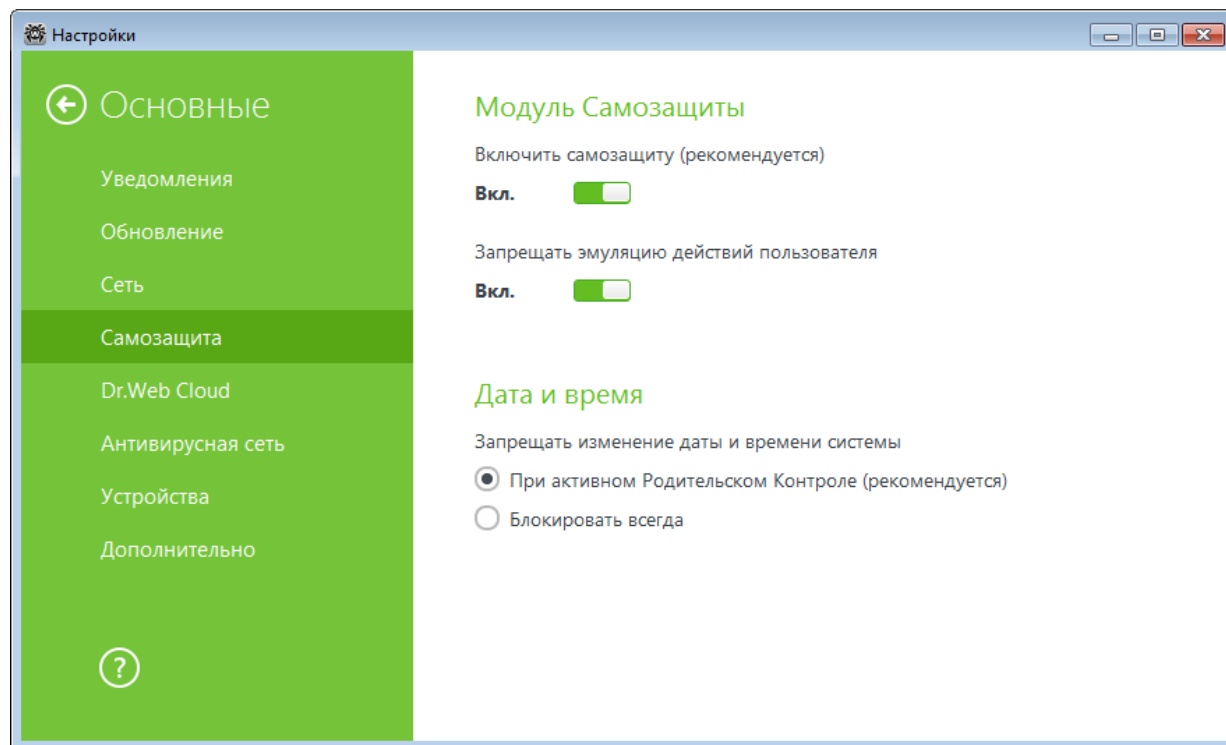
Сертификат «Доктор Веб»

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, а в **SpIDer Mail** – 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 удобную для вас папку.



10.4. Самозащита

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



Настройка **Включить Самозащиту** позволяет защитить файлы и процессы программы **Dr.Web** от несанкционированного доступа. Отключать Самозащиту не рекомендуется.



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

Для того чтобы произвести возврат к точке восстановления системы, необходимо отключить модуль Самозащиты.

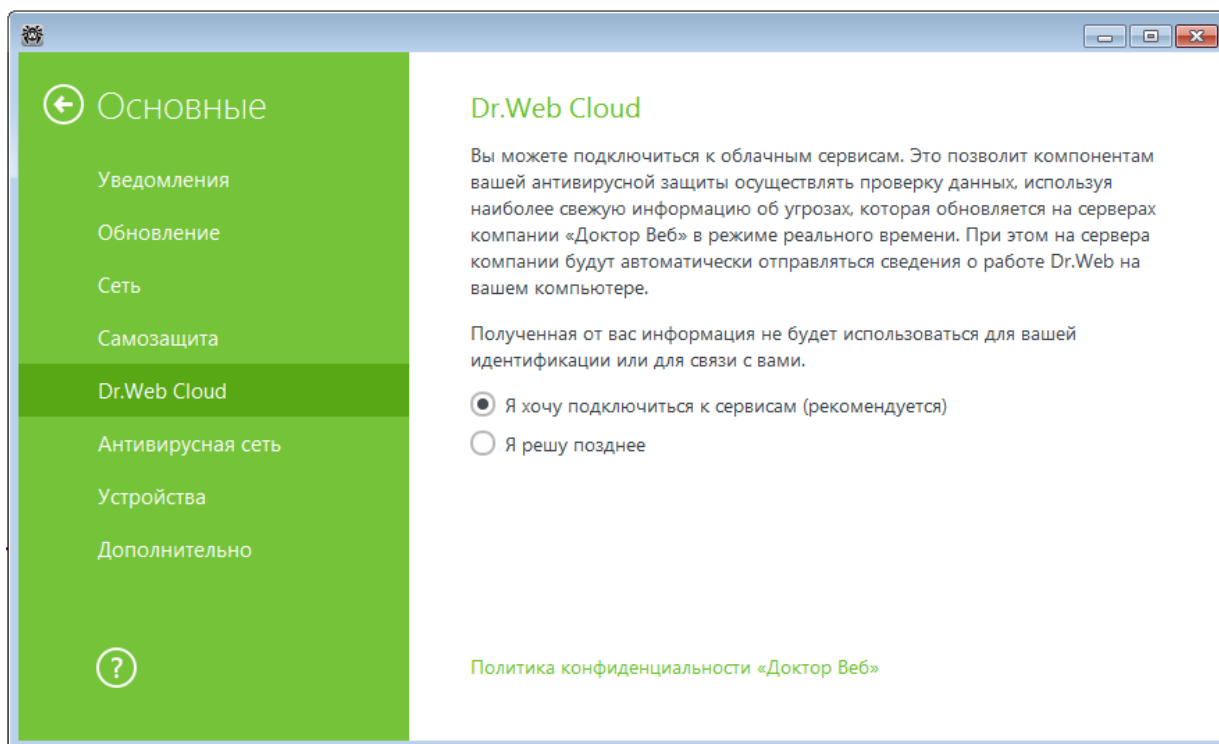
Настройка **Запрещать эмуляцию действий пользователя** позволяет предотвратить любые изменения в работе программы **Dr.Web**, производимые автоматизированно. В том числе будет запрещено исполнение скриптов, эмулирующих работу пользователя с программой **Dr.Web** и запущенных самим пользователем.

Настройка **Запрещать изменение даты и времени системы** позволяет заблокировать ручное и автоматическое изменение системных даты и времени, а также часового пояса. Это ограничение устанавливается для всех пользователей системы. Данная настройка позволит точнее работать функции ограничения времени в модуле **Родительский контроль**. В случае, если в модуле **Родительский контроль** заданы ограничения времени работы за компьютером или в сети Интернет, эта настройка включается автоматически. Вы можете настроить [получение уведомлений](#) в том случае, если осуществлялась попытка изменить системное время.



10.5. 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

Dr.Web Cloud Checker позволяет антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании «Доктор Веб» в режиме реального времени.

В зависимости от [настроек обновления](#) информация об угрозах, используемая компонентами вашей антивирусной защиты, может устаревать. Использование облачных сервисов позволяет гарантированно оградить пользователей вашего компьютера от сайтов с нежелательным содержанием, а также от инфицированных файлов.

Программа улучшения качества ПО

При участии в программе на сервера компании «Доктор Веб» будут автоматически отправляться обезличенные сведения о работе программы **Dr.Web** 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.

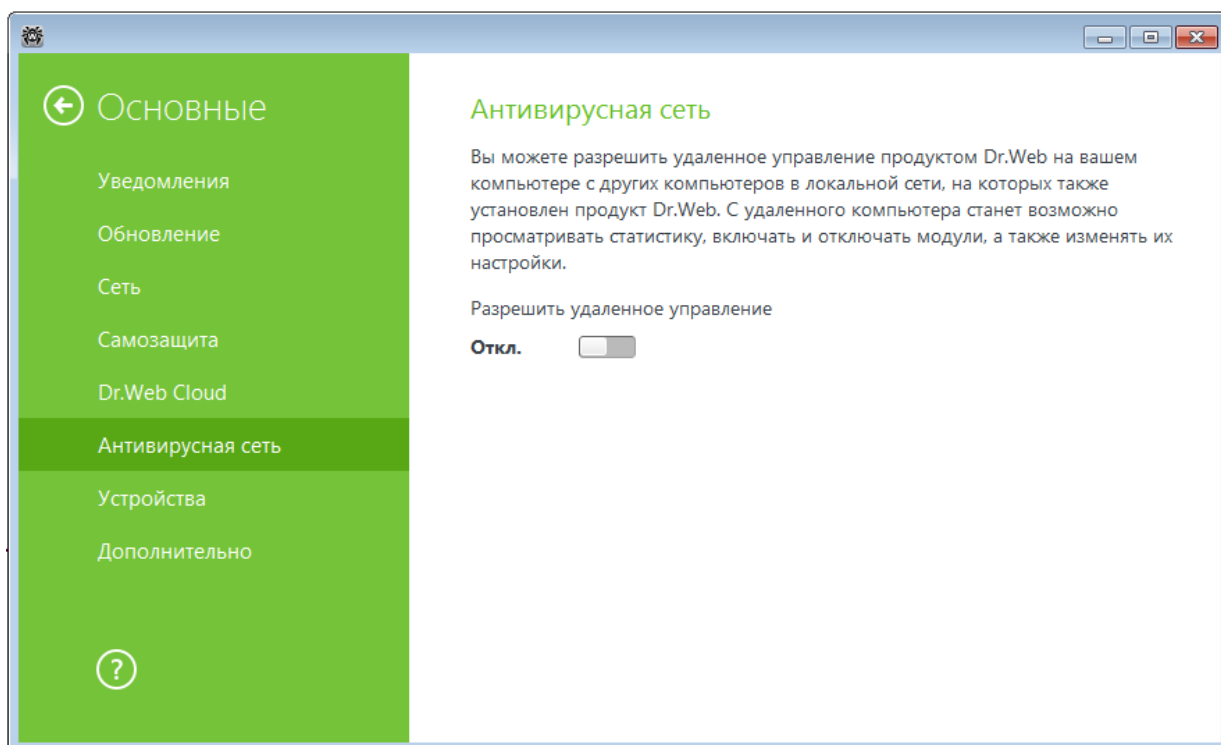
Нажмите на ссылку **Политика конфиденциальности «Доктор Веб»**, чтобы ознакомиться с политикой конфиденциальности на официальном [сайте](#) компании «Доктор Веб».



10.6. 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 удаленно контролировать состояние антивирусной защиты (просматривать статистику, включать и отключать компоненты **Dr.Web**, изменять их настройки), а также получать обновления через локальную сеть. Чтобы использовать компьютер как источник обновлений для других компьютеров антивирусной сети, на которых установлен продукт **Dr.Web**, на нём нужно настроить [зеркало обновлений](#).

Для удаленного управления **Dr.Web** на вашем компьютере необходимо будет вводить пароль. Вы можете использовать пароль, который автоматически генерируется при включении опции, или задать свой.





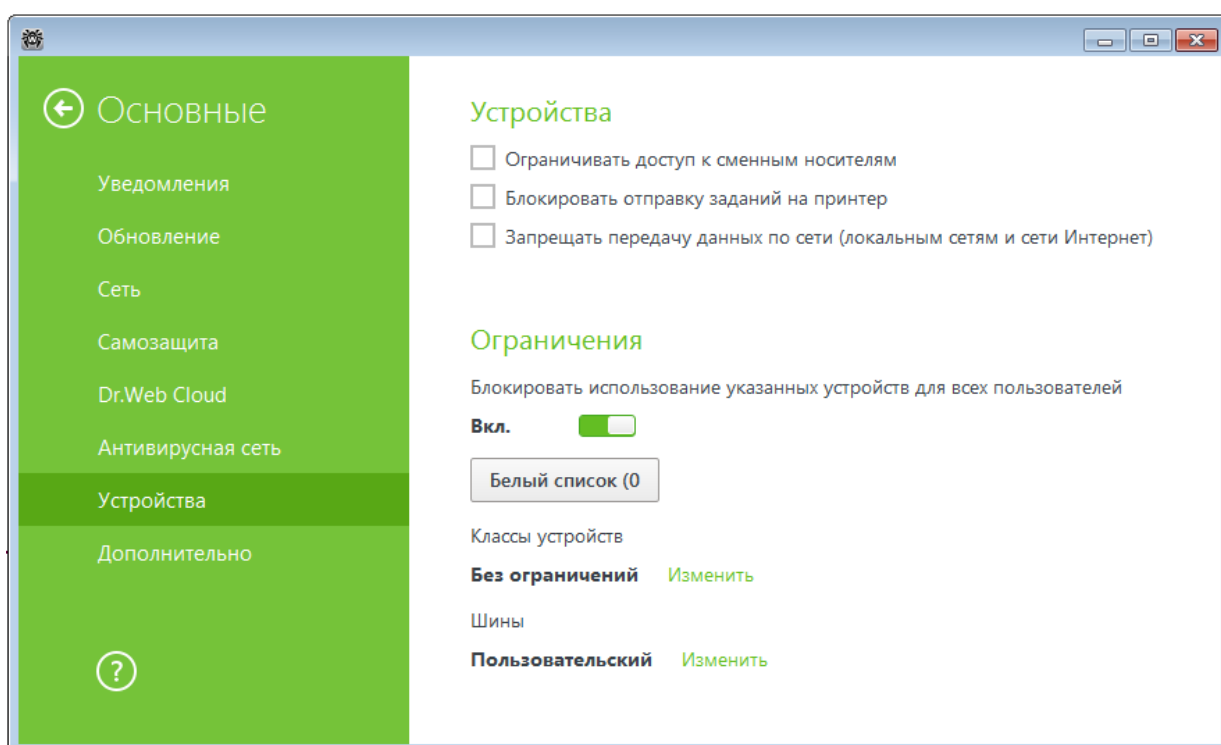
10.7. Устройства



Настройки контроля доступа применяются для всех учетных записей Windows.

Устройства

Чтобы блокировать доступ к данным на сменных носителях (USB флеш-накопителях, дискетах, CD/DVD приводах, ZIP-дисках и т. п.), включите соответствующую опцию. Для того чтобы нельзя было передать на принтер задания на печать, установите флажок **Блокировать отправку заданий на принтер**. По умолчанию опция отключена. Также вы можете запретить передачу данных по локальным сетям и сети Интернет.



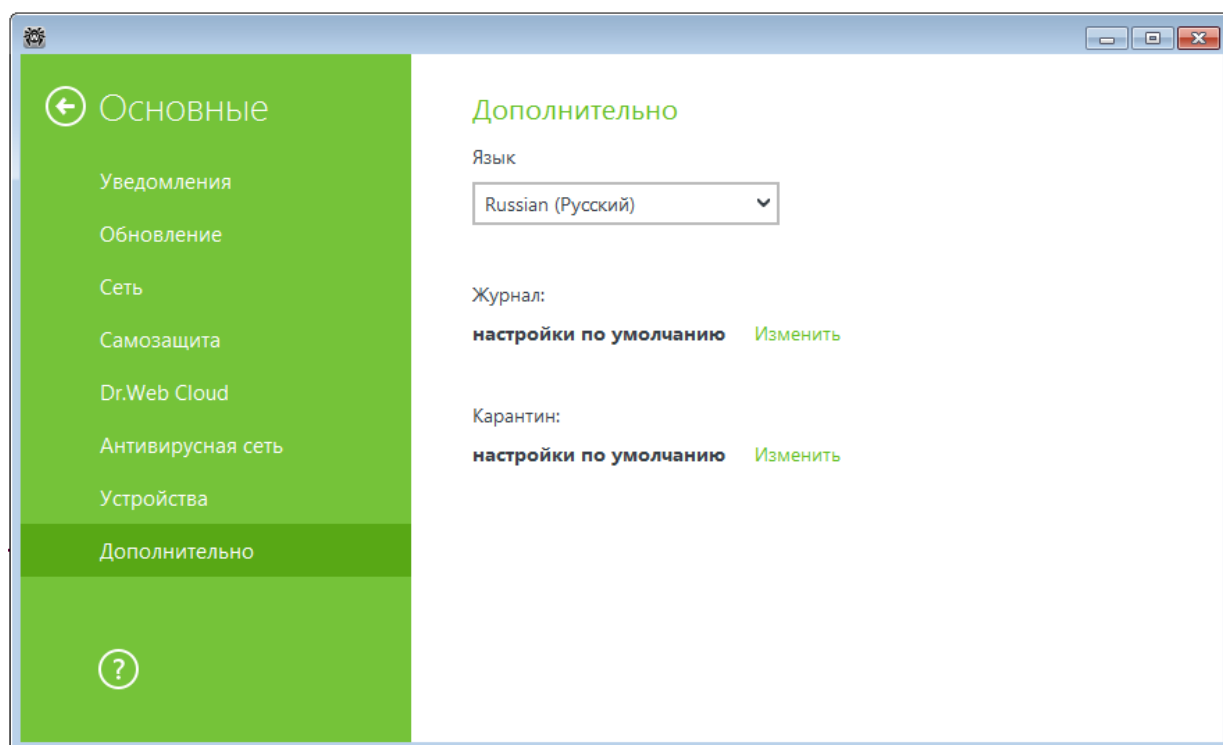
Классы устройств и шин

Чтобы заблокировать доступ к выбранным классам устройств и шин, включите соответствующую опцию. Сформируйте список таких объектов, нажав кнопку **Изменить**. Если при этом вы хотите иметь доступ к каким-либо конкретным устройствам, добавьте их в белый список. Чтобы добавить устройства в белый список, убедитесь, что оно подключено к компьютеру, затем нажмите кнопку **Добавить**. В открывшемся окне выберите нужный объект, при необходимости просмотрев дополнительную информацию об устройстве в нижнем поле. Также эту информацию вы можете просмотреть и после добавления устройства в белый список.



10.8. Дополнительно

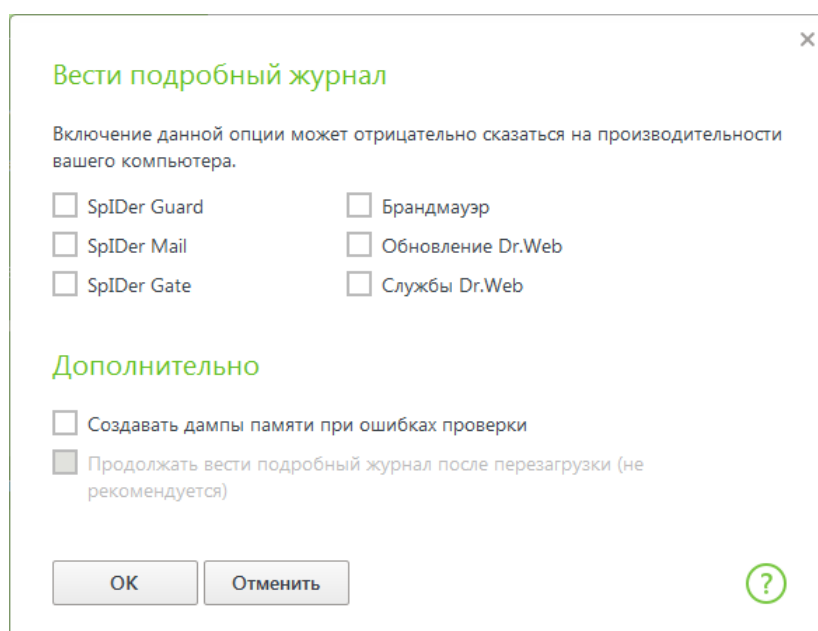
В данном разделе вы можете задать дополнительные настройки работы антивирусной защиты.



Вы можете выбрать из выпадающего списка язык программы. Список языков пополняется автоматически и содержит все доступные на текущий момент локализации графического интерфейса программы **Dr.Web**.

Настройки Журнала

Для управления настройками журнала нажмите соответствующую кнопку **Изменить**.





По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер.

По умолчанию для всех компонентов программы **Dr.Web** журнал ведется 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. 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 журнала. При включении режима ведения подробного журнала собираются данные о сетевых пакетах (рсар-логи).
Обновление Dr.Web	Список обновленных файлов программы Dr.Web и статусы их загрузки, информация о работе вспомогательных скриптов, дата и время проведения обновления, информация о перезапуске компонентов программы Dr.Web после обновления.
Службы Dr.Web	Информация о компонентах Dr.Web , изменение настроек компонентов, включение и выключение компонентов, события превентивной защиты, подключение к антивирусной сети.

Создание дампов памяти

Настройка **Создавать дампы памяти при ошибках проверки** позволяет сохранять полезную информацию о работе некоторых компонентов **Dr.Web**, что позволит специалистам компании **«Доктор Веб»** в дальнейшем провести более полный анализ проблемы и предложить ее решение. Рекомендуется включать данную настройку по просьбе сотрудников технической поддержки **«Доктор Веб»** или при возникновении ошибок проверки файлов или обезвреживания угроз. Дамп памяти сохраняется в виде файла с расширением .dmp в папке %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\.

Включение подробных журналов



При ведении подробного журнала фиксируется максимальное количество информации о работе компонентов **Dr.Web**. Это приведёт к отключению ограничения на размер файлов журнала и снизит производительность работы **Dr.Web** и операционной системы. Использовать этот режим следует только при возникновении проблем в работе компонентов или по просьбе технической поддержки компании **«Доктор Веб»**.



1. Чтобы включить режим ведения подробного журнала для одного из компонентов программы **Dr.Web**, установите соответствующий флажок.
2. По умолчанию подробный журнал ведется до первой перезагрузки операционной системы. Если необходимо зафиксировать поведение компонента в период до и после перезагрузки, установите флажок **Продолжать вести подробный журнал после перезагрузки (не рекомендуется)**.
3. Сохраните изменения.

Настройки Карантина

Для управления настройками карантина нажмите соответствующую кнопку **Изменить**.

Вы можете настроить параметры работы Карантина **Dr.Web** оценить его размер, а также удалить все изолированные файлы с конкретного диска.

Папка карантина создается отдельно на каждом логическом диске, где были обнаружены подозрительные файлы.

Очистка Карантина

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



11. Родительский контроль

С помощью модуля **Родительский контроль** осуществляется ограничение доступа пользователей к веб-сайтам, файлам и папкам, а также контролируется время работы в сети Интернет и за компьютером для каждой учетной записи Windows.

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.

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 **Родительский контроль**.

Вы можете подключиться к облачным сервисам компании **«Доктор Веб»**, которые позволяют антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании **«Доктор Веб»** в режиме реального времени.



11.1. Настройка модуля Родительский контроль



Для доступа к настройкам модуля **Родительский контроль** запрашивается пароль, если в разделе **Настройки** вы включили опцию **Защищать паролем настройки Dr.Web**.

Настройка параметров модуля Родительский контроль для разных пользователей

Выберите в левой панели имя пользователя, для которого вы хотите настроить ограничения доступа. В основной части окна отображаются заданные для этого пользователя настройки. По умолчанию всем пользователям компьютера разрешен неограниченный доступ к ресурсам сети Интернет и к локальным ресурсам, ограничения по времени работы отсутствуют. Для изменения настроек нажмите **Изменить** напротив нужной вам опции.



Вы можете **настроить** вывод уведомлений о действиях модуля **Родительский контроль** на экран и отправку этих уведомлений на электронную почту.

Интернет

По умолчанию для каждого пользователя установлен режим **Без ограничений**. Для изменения настроек, в выпадающем списке выберите другой режим.

Блокировать по категориям

В этом режиме 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.

Блокировать всё, кроме сайтов из белого списка

В этом режиме запрещается доступ ко всем веб-ресурсам, кроме указанных в белом списке веб-сайтов.

Безопасный поиск

В любом из режимов, кроме режима **Без ограничений**, вы можете включить опцию **Безопасный поиск**, которая влияет на выдачу результатов поисковых систем. Эта функция позволяет исключить нежелательные ресурсы из результатов поиска.

Время

В этом разделе производится настройка ограничений по времени работы пользователей за компьютером и в сети Интернет.

По умолчанию пользователям разрешено работать за компьютером и в сети Интернет неограниченное время.



Ограничение времени доступа

1. Выберите дни недели и часы, когда требуется запретить пользователю выход в Интернет, и выделите соответствующие временные квадраты синим цветом.
 - 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.
2. Выберите дни недели и часы, когда требуется запретить пользователю работу за компьютером, и выделите соответствующие временные квадраты красным цветом.
 - чтобы выделить один квадрат, дважды щелкните по нему левой кнопкой мыши;
 - чтобы одновременно выделить несколько расположенных рядом квадратов, дважды щелкните левой кнопкой мыши по первому квадрату и, удерживая кнопку нажатой, выделите весь необходимый период.



При включении ограничений времени работы за компьютером или в сети Интернет, автоматически включается опция **Запрещать изменение даты и времени системы** в разделе [Самозащита](#) основных настроек.

Файлы и папки

По умолчанию для каждого пользователя нет ограничений на доступ к файлам и папкам. Включите соответствующую опцию и добавьте объекты, доступ к которым вы хотите запретить.

Обратите внимание, что ограничение доступа не гарантируется при обращении к заданным объектам из внешних источников или из других операционных систем, установленных на компьютере.



12. Исключения

12.1. Вебсайты

Если вы хотите получить доступ к сайтам, которые не рекомендуются к посещению компанией «Доктор Веб», добавьте их в исключения. Доступ к сайтам из списка будет разрешен, однако антивирусная проверка этих сайтов сохраняется. По умолчанию список пуст. Если адрес сайта добавлен в белый список, то доступ к нему будет предоставляться вне зависимости от других настроек **SpIDer Gate**. Обратите внимание, если такой сайт добавлен одновременно и в черный список модуля **Родительский контроль**, и в исключения, доступ к нему будет заблокирован.

Формирование списка доменных адресов

1. В поле ввода укажите доменное имя или часть доменного имени веб-сайта, доступ к которому вы хотите разрешить вне зависимости от других ограничений.
 - чтобы добавить в список определенный сайт, введите его адрес (например, `www.example.com`). Доступ ко всем ресурсам, расположенным на этом сайте, будет разрешен;
 - чтобы разрешить доступ к тем веб-сайтам, в адресе которых содержится определенный текст, введите в поле этот текст. Пример: если вы введете текст `example`, то доступ к адресам `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru` и т. п. будет разрешен;
 - чтобы разрешить доступ к определенному домену, укажите имя домена с символом «.». В таком случае доступ ко всем ресурсам, находящимся в этом домене, будет разрешен. Если при указании домена используется символ «/», то та часть подстроки, что стоит слева от символа «/», будет считаться доменным именем, а части справа от символа – частью разрешенного на данном домене адреса. Пример: если вы введете текст `example.com/test`, то будут разрешены такие адреса как `example.com/test11`, `template.example.com/test22` и т. п.

Введенная строка при добавлении в список может быть преобразована к универсальному виду.

2. Нажмите кнопку . Указанный адрес появится в списке.
3. При необходимости повторите шаги 1 и 2 для добавления других адресов. Чтобы удалить адрес из белого списка, выберите соответствующий элемент в списке и нажмите кнопку .

12.2. Файлы и папки

В этом разделе задается список папок и файлов, которые исключаются из проверки **SpIDer Guard**. В таком качестве могут выступать папки карантина антивируса, рабочие папки некоторых программ, временные файлы (файлы подкачки) и т. п.

По умолчанию список пуст. Добавьте к исключениям конкретные папки и файлы или используйте маски, чтобы запретить проверку определенной группы файлов.

Формирование списка исключений

Чтобы добавить папку или файл к списку исключений, выполните одно из следующих действий:



- чтобы указать конкретный существующий файл или папку, нажмите . В открывшемся окне нажмите кнопку **Обзор** и выберите папку или файл в стандартном окне открытия файла. Вы можете вручную ввести полный путь к файлу или папке в поле ввода, а также отредактировать запись в поле ввода перед добавлением ее в список;
 - чтобы исключить из проверки все файлы или папки с определенным именем, введите это имя в поле ввода. Указывать путь к папке или файлу при этом не требуется;
 - чтобы исключить из проверки файлы или папки определенного вида, введите определяющую их маску в поле ввода;
 - нажмите кнопку **ОК**. Выбранный файл или папка появится в списке;
 - при необходимости повторите шаги 1 и 2 для добавления других файлов или папок. Чтобы удалить файл или папку из списка исключений, выберите соответствующий элемент в списке и нажмите кнопку .
-
- `C:\folder` или `C:\folder\**` – исключает из проверки все файлы в папке `C:\folder`. В подпапках файлы будут проверяться.
 - `C:\folder\*` – исключает из проверки все файлы в папке `C:\folder` и всех подпапках на любом уровне.
 - `C:\folder\*.txt` – исключает из проверки файлы `*.txt` в папке `C:\folder`. В подпапках файлы `*.txt` будут проверяться.
 - `C:\folder\*\*.txt` – исключает из проверки файлы `*.txt` только в подпапках первого уровня папки `C:\folder`.
 - `C:\folder\**\*.txt` – исключает из проверки файлы `*.txt` в подпапках любого уровня папки `C:\folder`. В самой папке `C:\folder` файлы `*.txt` будут проверяться.

12.3. Программы и процессы

В этом разделе задается список папок и файлов, которые исключаются из проверки компонентами **SpIDer Guard**, **SpIDer Gate** и **SpIDer Mail**.

Формирование списка исключений

1. Чтобы добавить программу или процесс к списку исключений нажмите . В открывшемся окне нажмите кнопку **Обзор** и выберите файл в стандартном окне открытия файла.
2. В окне настройки укажите, какие компоненты не должны проводить проверку выбранного файла.
3. Нажмите кнопку **ОК**. Выбранная программа или процесс появится в списке.
4. При необходимости повторите действия для добавления других программ.
5. Чтобы удалить файл из списка исключений, выберите соответствующий элемент в списке и нажмите .

12.4. Антиспам

В этом окне задаются списки отправителей, письма которых почтовым сторожем **SpIDer Mail** пропускаются или расцениваются как спам без проведения анализа.



Если адрес отправителя добавлен в белый список, то письмо не подвергается анализу на содержание спама. Если адрес отправителя добавлен в черный список, то письму без дополнительного анализа присваивается статус спама. По умолчанию оба списка пусты.

Задание списков антиспама

1. Введите в поле ввода почтовый адрес отправителя или маску, задающую почтовые адреса отправителей, чьи письма вы хотите обрабатывать автоматически без проведения анализа. Метод ввода:
 - чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, `name@pochta.ru`). Все письма, полученные с этого адреса, будут обрабатываться без анализа;
 - чтобы добавить в список отправителей, использующих похожие адреса электронной почты, используйте символы «*» и «?», чтобы заменить отличающуюся часть адреса. При этом символ «*» замещает любую последовательность символов, а символ «?» – один (любой) символ. Пример: если вы введете адрес `name*@pochta.ru`, то письма от отправителей с адресами вида **name@pochta.ru**, **name1@pochta.ru**, **name_moj@pochta.ru** и т. п. будут обрабатываться без анализа;
 - чтобы гарантированно получать или блокировать письма с почтовых адресов в конкретном домене, используйте символ «*» вместо имени пользователя. Пример: чтобы задать все письма от адресантов из домена `pochta.ru`, введите `*@pochta.ru`.
2. Чтобы добавить введенный адрес в список, нажмите кнопку .
3. При необходимости повторите шаги 1 и 2 для добавления других адресов. Чтобы удалить адрес из списка, выберите соответствующий элемент в списке и нажмите кнопку .



13. Компоненты защиты

13.1. 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.

Файлы внутри архивов и почтовые ящики не проверяются. Если какой-либо файл в архиве или почтовом вложении инфицирован, то вредоносный объект будет обнаружен сторожем при извлечении файла до появления возможности заражения компьютера. Для предотвращения проникновения на ваш компьютер вредоносных объектов, распространяемых посредством электронной почты, используйте почтовый сторож **SpIDer Mail**.

При обнаружении зараженных объектов сторож **SpIDer Guard** применяет к ним действия согласно установленным настройкам. Соответствующим изменением настроек вы можете изменить автоматическую реакцию сторожа на вирусные события.

Вы можете подключиться к облачным сервисам компании «**Доктор Веб**», которые позволяют антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании «**Доктор Веб**» в режиме реального времени.

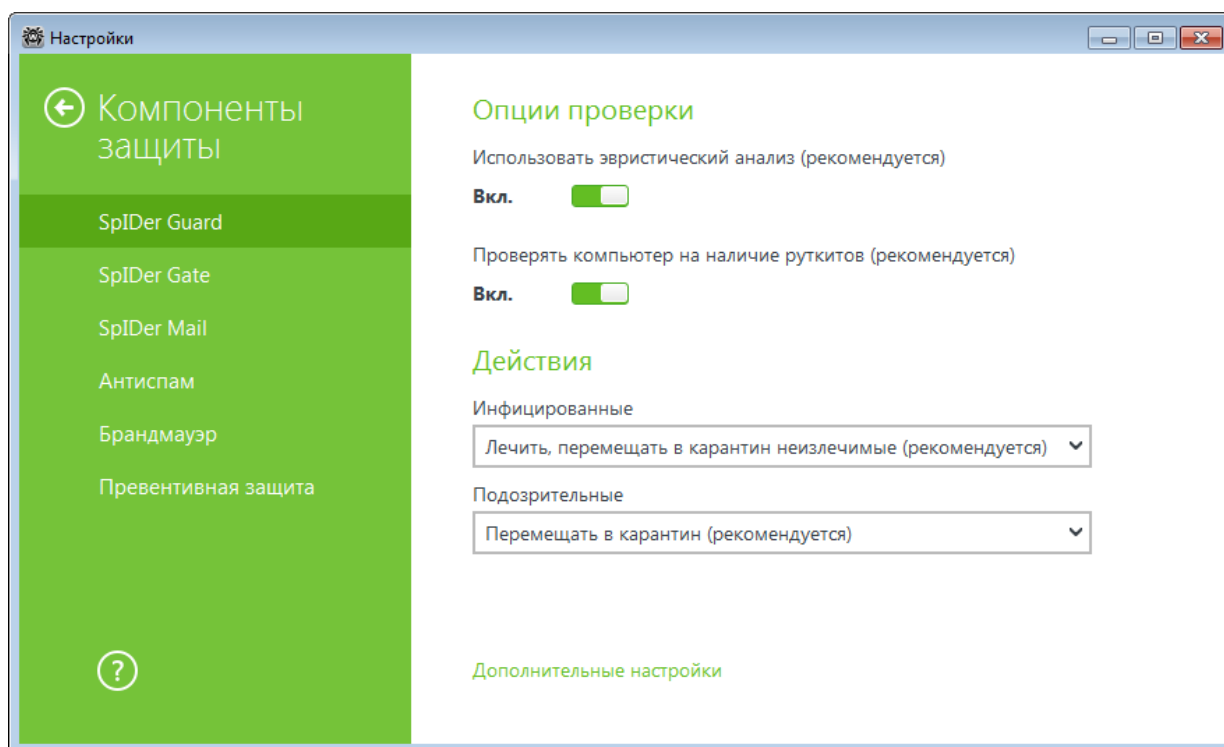
По умолчанию **SpIDer Guard** запускается автоматически при каждой загрузке операционной системы, при этом запущенный сторож **SpIDer Guard** не может быть выгружен в течение текущего сеанса работы операционной системы.

13.1.1. Настройка SpIDer Guard



Для доступа к настройкам сторожа **SpIDer Guard** запрашивается пароль, если в разделе Настройки вы включили опцию **Защищать паролем настройки Dr.Web**.

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



Опции проверки

Эвристический анализ

По умолчанию **SpIDer Guard** проводит проверку, используя [эвристический анализатор](#). Если опция отключена, проверка проводится только по сигнатурам известных вирусов.

Фоновая проверка на заражение

Входящий в состав **Dr.Web 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 системном BIOS компьютера и таких критических областях Windows, как объекты автозагрузки, запущенные процессы и модули, оперативная память, MBR/VBR дисков и др.

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.



При проведении фоновой проверки на наличие руткитов из проверки исключаются файлы и папки, заданные на [соответствующей вкладке](#).

Чтобы включить фоновую проверку, включите опцию **Проверять компьютер на наличие руткитов (рекомендуется)**.



Выключение **SpIDer Guard** не влияет на фоновую проверку. Если настройка включена, фоновая проверка осуществляется независимо от того, включен или выключен **SpIDer Guard**.

Действия

В этом разделе задается реакция сторожа **SpIDer Guard** на обнаружение зараженных или подозрительных файлов и вредоносных программ.

Реакция задается отдельно для каждой категории объектов:

- **Инфицированные объекты**, зараженные известным и (предположительно) излечимым вирусом;
- **Подозрительные объекты**, предположительно зараженные вирусом или содержащие вредоносный объект;
- различные потенциально опасные объекты.

Вы можете изменить реакцию сторожа **SpIDer Guard** на обнаружение каждого типа объектов в отдельности. Состав доступных реакций при этом зависит от типа вирусного события.

По умолчанию сторож **SpIDer Guard** пытается вылечить файлы, зараженные известным и потенциально излечимым вирусом, остальные наиболее опасные объекты – перемещает в [Карантин](#). Программы-шутки, программы взлома и неблагонадежные объекты по умолчанию *игнорируются*. Реакции сторожа **SpIDer Guard** аналогичны соответствующим реакциям **Сканера Dr.Web**.

Существуют следующие действия, применяемые к обнаруженным объектам:

Действие	Описание
Лечить, перемещать в карантин неизлечимые	Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов.
Лечить, удалять неизлечимые	Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов.
Удалить	Удалить объект. Для загрузочных секторов никаких действий производиться не будет.
Перемещать в карантин	Переместить объект в специальную папку Карантина . Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропустить объект без выполнения каких-либо действий и не выводить оповещения. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.



Сторож **SpIDer Guard** не проверяет составные объекты, поэтому никакие действия над ними или входящими в их состав файлами не производятся.

Резервные копии обработанных объектов сохраняются в [Карантине](#).

Режим проверки

В данной группе настроек задается, при каких действиях с объектом должна производиться его проверка сторожем **SpIDer Guard**.

Настройка	Описание
Оптимальный (рекомендуется)	Используется по умолчанию. В данном режиме проверка производится только в следующих случаях: • для объектов на жестких дисках – при запуске или создании файлов, а также попытке записи в существующие файлы или загрузочные сектора; • для объектов на сменных носителях – при любом обращении к файлам или загрузочным секторам (чтение, запись, запуск).
Параноидальный	В данном режиме при любом обращении (создание, чтение, запись, запуск) производится проверка всех файлов и загрузочных секторов на жестких и сетевых дисках, а также сменных носителях.



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](#).

Режим **Оптимальный** рекомендуется использовать после [проверки](#) всех жестких дисков при помощи **Сканера Dr.Web**. При этом будет исключено проникновение на компьютер новых вирусов или других вредоносных программ через сменные устройства, но при этом не будет проводиться повторной проверки уже проверенных, чистых, объектов.

Установка режима **Параноидальный** обеспечивает максимальный уровень защиты, но значительно увеличивает нагрузку на компьютер.

В любом из режимов проверка объектов на сетевых дисках или съемных носителях производится только при установке соответствующих флажков в группе настроек **Дополнительные возможности**.



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

Файлы внутри архивов и почтовые ящики по умолчанию не проверяются. Отказ от проверки архивов и электронной почты в условиях постоянной работы сторожа **SpIDer Guard** не ведет к проникновению вирусов на компьютер, а лишь откладывает момент их обнаружения. При распаковке зараженного архива или открытии зараженного письма операционная система производит попытку записать инфицированный объект на диск, при этом сторож **SpIDer Guard** неминуемо обнаруживает вредоносный объект.



Дополнительные возможности

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

Здесь вы можете задать проверку:

- файлов запускаемых процессов вне зависимости от их расположения (эта опция включена по умолчанию);
- установочных файлов;
- файлов на сетевых дисках;
- файлов и загрузочных секторов на съемных носителях (эта опция включена по умолчанию).

Также **SpIDer Guard** по умолчанию блокирует автоматический запуск активного содержимого внешних носителей данных (CD/DVD-дисков, флэш-памяти и т. д.). 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 отключить опцию **Блокировать автозапуск со сменных носителей**.

13.2. 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»**, которые позволяют антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании **«Доктор Веб»** в режиме реального времени.

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

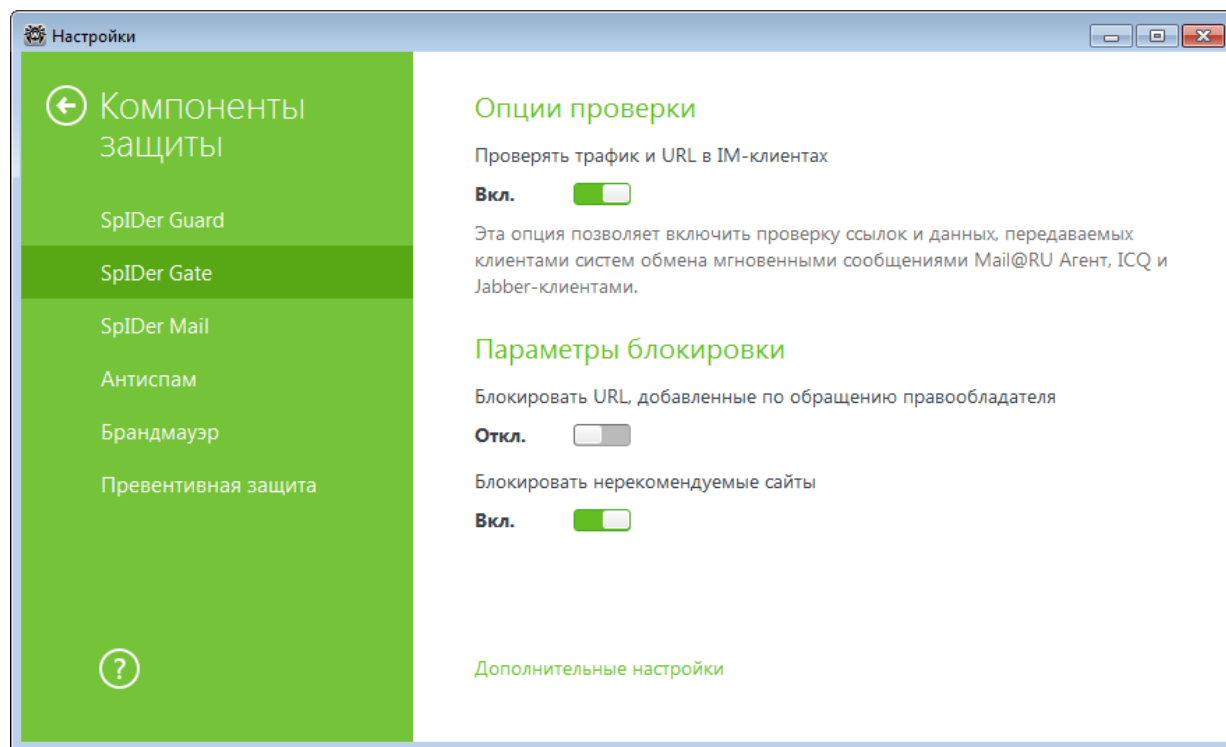


13.2.1. Настройка SpIDer Gate



Для доступа к настройкам веб-антивируса **SpIDer Gate** запрашивается пароль, если в разделе [Настройки](#) вы включили опцию **Защищать паролем настройки Dr.Web**.

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



Проверка трафика IM-клиентов

В группе **Опции проверки** вы можете включить проверку ссылок и данных, передаваемых клиентами систем обмена мгновенными сообщениями (Mail@RU Агент, ICQ и клиентов, работающих по протоколу Jabber). Проверяется только входящий трафик. По умолчанию опция включена.

Ссылки, передаваемые в сообщениях, проверяются согласно настройкам **SpIDer Gate**: ссылки на веб-сайты, известные как источники распространения вирусов, блокируются автоматически, ссылки на нерекомендуемые сайты и URL, добавленные по обращению правообладателя, блокируются в том случае, если включены соответствующие настройки в разделе **Параметры блокировки**. При этом учитываются [белый список веб-сайтов](#) и [приложения, исключаемые из проверки](#).

Файлы, передаваемые клиентами систем обмена мгновенными сообщениями, также проверяются. При обнаружении угрозы передача такого файла блокируется, если включена соответствующая настройка в разделе **Блокировать программы**. Вирусы блокируются автоматически, если опция **Проверять трафик и URL в IM-клиентах** включена.

Параметры блокировки

В группе **Параметры блокировки** вы можете установить автоматическую блокировку доступа к



URL, добавленных по обращению правообладателя (для этого установите соответствующий флажок), а также к нерекомендованным сайтам, известным как неблагонадежные (для этого установите флажок **Блокировать нерекомендуемые сайты**). В разделе **Исключения** вы можете [указать сайты](#), доступ к которым должен быть разрешен, несмотря на установленные ограничения.



SpIDer Gate по умолчанию блокирует доступ к веб-сайтам, известным как источники вирусов или вредоносных программ других типов. При этом учитывается список приложений, [исключаемых из проверки](#).

Блокировка программ

Веб-антивирус **SpIDer Gate** может блокировать следующие вредоносные программы:

- подозрительные;
- потенциально опасные;
- программы дозвона;
- программы взлома;
- рекламные программы;
- программы-шутки.

По умолчанию блокируются подозрительные и рекламные программы, а также программы дозвона.

Блокировка объектов

SpIDer Gate может блокировать непроверенные или повреждённые объекты. По умолчанию эти опции выключены.

Дополнительные возможности

Вы можете настроить проверку архивов и инсталляционных пакетов. По умолчанию опция проверки архивов и инсталляционных пакетов отключена.

Также 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 сторожу отдавать данные быстрее, тем самым повышая скорость работы с сетью. Однако при более частых проверках повышается нагрузка на процессор.

Также вы можете выбрать тип проверяемого HTTP-трафика. По умолчанию проверяется только входящий трафик. При этом учитываются заданные действия, [белый список веб-сайтов](#) и [приложения, исключаемые из проверки](#).

13.3. 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.



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.

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. подраздел [Настройка SpIDer Mail](#)):

- из зараженных писем удаляется вредоносная информация (это действие называется *лечением письма*), затем они доставляются обычным образом;
- письма с подозрительными объектами перемещаются в виде отдельных файлов в [Карантин](#), почтовой программе посылается сообщение об этом (это действие называется *перемещением письма*). Перемещенные письма удаляются с POP3- или IMAP4-сервера;
- незараженные письма и письма, не прошедшие проверки, передаются без изменений (*пропускаются*).

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

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.

13.3.1. Настройка SpIDer Mail

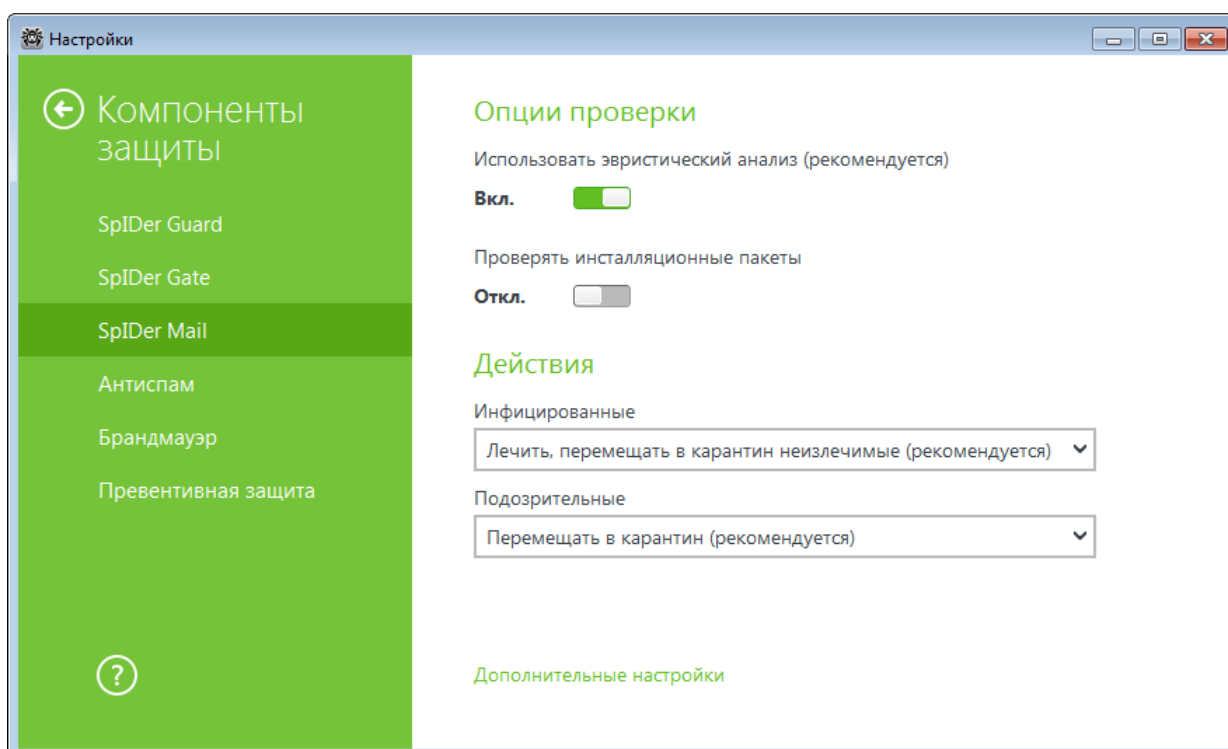


Для доступа к настройкам почтового сторожа **SpIDer Mail** запрашивается пароль, если в разделе [Настройки](#) вы включили опцию **Защищать паролем настройки Dr.Web**.

Настройки программы по умолчанию являются оптимальными для большинства применений, их



не следует изменять без необходимости.



Особенности проверки

Эта группа настроек задает дополнительные параметры проверки электронной почты:

- использование эвристического анализа – в данном режиме используются специальные механизмы, позволяющие выявить в электронной почте подозрительные объекты, с большой вероятностью зараженные еще неизвестными вирусами. Чтобы отключить эвристический анализ, снимите флажок **Использовать эвристический анализатор (рекомендуется)**;
- проверка инсталляционных пакетов. Эта настройка по умолчанию выключена.

Действия

По умолчанию почтовый сторож **SpIDer Mail** пытается вылечить письма, зараженные известным и потенциально излечимым вирусом. Неизлечимые и подозрительные письма, а также рекламные программы и программы дозвона перемещаются в Карантин. Остальные письма передаются почтовым сторожем без изменений (*пропускаются*).

Реакции почтового сторожа **SpIDer Mail** аналогичны соответствующим реакциям **Сканера Dr.Web**.

Вы можете предписать почтовому сторожу **SpIDer Mail** следующие реакции:

Действие	Описание
Лечить, перемещать в карантин неизлечимые	Восстановить состояние письма до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для инфицированных писем, зараженных известным излечимым вирусом, за исключением троянских программ, которые при обнаружении удаляются. Лечение файлов в архивах невозможно вне зависимости от типа вируса.



Действие	Описание
Лечить, удалять неизлечимые	Восстановить состояние письма до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален.
Удалять	Удалить письмо. В этом случае электронное письмо не пересылается адресату, вместо этого почтовой программе передается сообщение о совершенной операции.
Перемещать в карантин	Переместить письмо в специальную папку Карантина . В этом случае письмо не пересылается адресату, вместо этого почтовой программе передается сообщение о совершенной операции.
Игнорировать	Передать письмо без выполнения каких-либо действий над ним.

В случае обнаружения вредоносных объектов в почте любая из указанных настроек, кроме действия **Игнорировать**, приводит к отказу в передаче письма.

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 в последствие проверять **Сканером Dr.Web**.



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

После выполнения предписанного действия почтовый сторож **SpIDer Mail** по умолчанию может выводить соответствующее оповещение в область уведомлений Windows. Вы можете [настроить](#) вывод уведомлений на экран и отправку их на электронную почту.

Действия над письмами

В данной группе настроек указываются дополнительные действия над электронными письмами, обработанными почтовым сторожем **SpIDer Mail**.

Настройка	Описание
Вставка заголовка 'X-Antivirus' в сообщения	Установлена по умолчанию. При использовании данной настройки в заголовок всех писем, обработанных почтовым сторожем SpIDer Mail , добавляется информация о проверке электронного сообщения и версии Dr.Web . Вы не можете изменить формат добавляемого заголовка.
Удалять модифицированные письма на сервере	При использовании данной настройки входящие письма, удаленные или перемещенные в карантин почтовым сторожем SpIDer Mail , удаляются с почтового сервера независимо от настроек почтовой программы.

Оптимизация проверки

Вы можете задать условие, при выполнении которого сложноустроенные письма, проверка которых является чрезмерно трудоемкой, признаются непроверенными. Для этого включите опцию **Тайм-аут проверки письма** и задайте максимальное время, в течение которого письмо проверяется. По истечении указанного времени почтовый сторож **SpIDer Mail** прекратит проверку письма.



Проверка архивов

Включите опцию **Проверять архивы**, чтобы **SpIDer Mail** проверял содержимое архивов, передаваемых по электронной почте. При этом будут доступны следующие настройки:

- **Максимальный размер файла при распаковке.** Если распакованный архив превысит указанный размер, то почтовый сторож **SpIDer Mail** не будет распаковывать и проверять его;
- **Максимальный коэффициент сжатия архива.** Если коэффициент сжатия превышает указанный, то почтовый сторож **SpIDer Mail** не будет распаковывать и проверять его;
- **Максимальный уровень вложенности в архив.** Если уровень вложенности превышает заданное значение, то почтовый сторож **SpIDer Mail** проверит архив только до указанного уровня.

Для включения одного или нескольких параметров оптимизации установите соответствующие флажки.



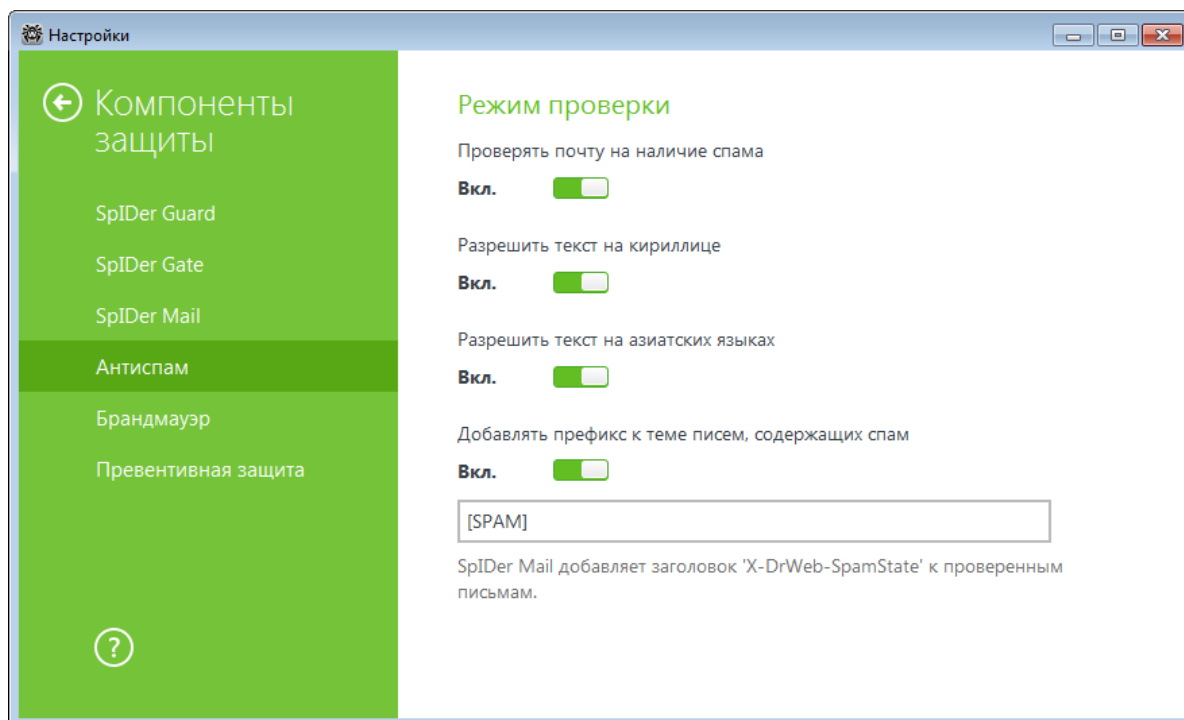
Ограничения для параметра отсутствуют, если задано значение 0.

13.4. Антиспам

Антиспам Dr.Web

Технологии антиспам-фильтра **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. Такое сравнение, в сочетании с данными о размерах изображений, обычно используемых отправителями спама, защищает пользователей от спам-сообщений, содержащих ссылки на веб-страницы;
- **семантический анализ** — сравнение слов и выражений сообщения со словами и идиомами, типичными для спама, производится по специальному словарю. Анализ подвергается 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.



По умолчанию осуществляется проверка входящих писем на спам. Чтобы входящая корреспонденция не проверялась спам-фильтром, отключите соответствующую опцию.

Укажите, какие письма не следует причислять к спаму и каким образом пометить отфильтрованные сообщения.

Настройка	Описание
Добавлять префикс к заголовку писем, содержащих спам	По умолчанию данный флажок установлен, в начало темы спам-писем добавляется подстрока «[SPAM]». Данная настройка указывает почтовому сторожу SpIDer Mail добавлять указанный префикс к темам писем, распознаваемых как спам. 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.
Белый и черный списки	Нажмите, чтобы задать список отправителей, чьи электронные письма вы хотите гарантированно пропускать без проверки на спам или гарантированно блокировать.

Обработка писем спам-фильтром

Почтовый сторож **SpIDer Mail** добавляет ко всем проверенным письмам следующие заголовки:

- X-DrWeb-SpamState: <значение>, где <значение> указывает на то, является ли письмо спамом (Yes) по мнению почтового сторожа **SpIDer Mail** или нет (No);
- X-DrWeb-SpamVersion: <версия>, где <версия> – версия библиотеки **Антивспам Dr.Web**;
- X-DrWeb-SpamReason: <рейтинг спама>, где <рейтинг спама> – перечень оценок по различным критериям принадлежности к спаму.

Используйте эти заголовки и префикс в теме письма (если соответствующий флажок установлен) для настройки фильтрации спама вашей почтовой программой.



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

Для повышения качества работы спам-фильтра, вы можете сообщать об ошибках распознавания спама.

Исправление ошибок распознавания

1. При обнаружении ошибки в работе спам-фильтра, создайте новое письмо и приложите к нему неправильно распознанное сообщение. Письма, отправленные в тексте письма, анализироваться не будут.
2. Отправьте письмо с вложением на один из следующих адресов:
 - письмо, ошибочно оцененное как спам, – на адрес vrnonspam@drweb.com;
 - спам, нераспознанный системой, – на адрес vrspam@drweb.com.

13.5. Брандмауэр Dr.Web

Брандмауэр Dr.Web 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.

13.5.1. 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.

Правила для приложений

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.
Адрес	Протокол и адрес хоста, к которому совершается попытка подключения.
Порт	Порт, по которому совершается попытка подключения.
Направление	Направление соединения.

- 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](#).
- Нажмите кнопку **ОК**. **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

- При обнаружении попытки подключения к сети со стороны приложения, запущенного неизвестной для **Брандмауэра** программой, ознакомьтесь с информацией об исполняемом файле родительской программы.
- Когда вы примете решение о подходящей для данного случая операции, выполните одно из следующих 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](#).
- Нажмите кнопку **ОК**. **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 как для приложений, так и для родительских процессов.



13.5.1. Настройка Брандмауэра



Для доступа к настройкам **Брандмауэра** запрашивается пароль, если в разделе [Настройки](#) вы включили опцию **Защищать паролем настройки Dr.Web**.

Для начала работы с **Брандмауэром** необходимо:

- выбрать режим работы программы;
- [настроить список](#) авторизованных приложений;
- настроить параметры для известных сетей.

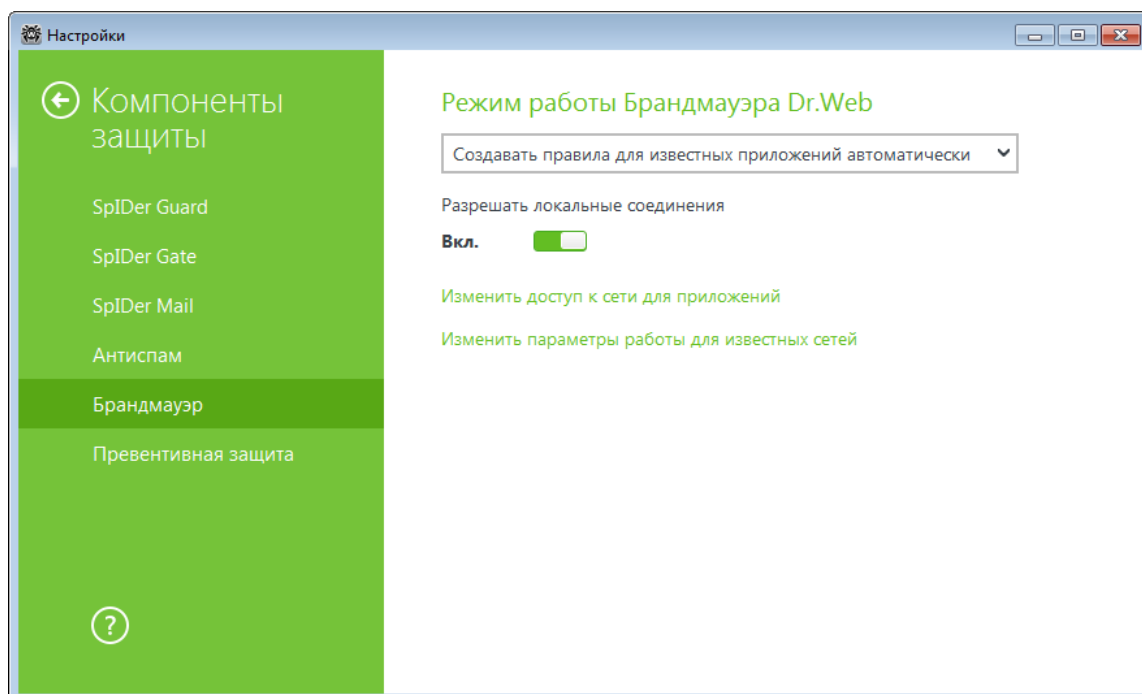
По умолчанию **Брандмауэр** автоматически создает правила для известных приложений. Вне зависимости от режима работы производится регистрация событий.

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

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.



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.





Выбор режима работы

Выберите один из следующих режимов работы:

- **Разрешать неизвестные соединения** — режим, при котором всем неизвестным приложениям предоставляется доступ к сетевым ресурсам;
- **Создавать правила для известных приложений автоматически** — режим, 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. Известные соединения обрабатываются **Брандмауэром** согласно заданным правилам фильтрации.

Создавать правила для известных приложений автоматически

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.

Разрешать неизвестные соединения

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.

Параметры для приложений

Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам, а также разрешить или запретить этим приложениям запуск других процессов. Вы можете задавать правила как для пользовательских, так и для системных приложений.



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

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.



Если вы создали блокирующее правило для процесса или установили режим **Блокировать неизвестные соединения**, а потом отключили блокирующее правило или изменили режим работы, блокировка будет действовать до повторной попытки установить соединение, инициированной самим процессом.

Для приложений, которые уже удалены с вашего компьютера, правила не удаляются автоматически. Вы можете удалить такие правила, выбрав пункт **Удалить неиспользуемые правила** в контекстном меню списка.

В окне **Новый набор правил для приложения** (или **Редактирование набора правил**) вы можете настроить доступ приложения к сетевым ресурсам, а также запретить или разрешить запуск других приложений.

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

При работе **Брандмауэра** в режиме обучения, вы можете инициировать создание правила непосредственно из окна оповещения о попытке несанкционированного подключения.



Запуск других приложений

Чтобы разрешить или запретить приложению запускать другие приложения, в выпадающем списке **Запуск сетевых приложений** выберите:

- **Разрешать**, чтобы разрешить приложению запускать процессы;
- **Запрещать**, чтобы запретить приложению запускать процессы;
- **Не задано**. В этом случае на это приложение будут распространяться настройки выбранного [режима работы Брандмауэра](#).

Доступ к сетевым ресурсам

1. Выберите режим доступа к сетевым ресурсам:
 - **Разрешать все** – все соединения приложения будут разрешены;
 - **Запрещать все** – все соединения приложения запрещены;
 - **Не задано**. В этом случае на это приложение будут распространяться настройки выбранного [режима работы Брандмауэра](#).
 - **Пользовательский** – в этом режиме вы можете создать набор правил, разрешающих или запрещающих те или иные соединения приложения.
2. Если был выбран **Пользовательский** режим доступа к сетевым ресурсам, то ниже отобразится таблица с информацией о наборе правил для данного приложения.

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.
Направление	Направление соединения: • Входящее – правило применяется, если соединение инициируется из сети к программе на вашем компьютере; • Исходящее – правило применяется, если соединение инициируется программой на вашем компьютере; • Любое – правило применяется вне зависимости от направления соединения.
Описание	Пользовательское описание правила.

3. При необходимости отредактируйте предустановленный или создайте новый набор правил для приложения:
 - 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 набора правил нажмите кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отменить** для отказа от изменений.



Правила фильтрации регулируют сетевое взаимодействие программы с конкретными хостами сети.

Создание правила

Задайте следующие параметры правила:

Параметр	Описание
Общее	
Имя правила	Имя создаваемого/редактируемого правила.
Описание	Краткое описание правила.
Действие	Указывает на действие, выполняемое Брандмауэром при попытке программы подключиться к сети Интернет: • Блокировать пакеты – блокировать попытку подключения; • Разрешать пакеты – разрешить подключение.
Состояние	Состояние правила: • Включено – правило применяется; • Отключено – правило временно не применяется.
Направление	Направление соединения: • Входящее – правило применяется, если соединение иницируется из сети к программе на вашем компьютере; • Исходящее – правило применяется, если соединение иницируется программой на вашем компьютере; • Любое – правило применяется вне зависимости от направления соединения.
Ведение журнала	Режим ведения журнала: • Включено – регистрировать события; • Отключено – не сохранять информацию о правиле.
Настройки правила	
Протокол	Протоколы сетевого и транспортного уровня, по которым осуществляется подключение. Поддерживаются следующие протоколы сетевого уровня: • IPv4; • IPv6; • IP all – протокол IP любой версии. Поддерживаются следующие протоколы транспортного уровня: • TCP; • UDP; • TCP & UDP – протокол TCP или UDP; • RAW.
Локальный адрес/ Удаленный 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 .
Локальный порт/ Удаленный 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 .



Параметры для сетей

В разделе **Интерфейсы** 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 **Показать все**. 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**.

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:

- **Default Rule** — правила, описывающие наиболее часто встречающиеся конфигурации сети и распространенные атаки (используется по умолчанию для всех новых интерфейсов);
- **Allow All** — все пакеты пропускаются;
- **Block All** — все пакеты блокируются.

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

Набор правил для интерфейса

Чтобы задать параметры работы пакетного фильтра, в окне настроек **Брандмауэра** выберите раздел **Интерфейсы** и нажмите кнопку **Настроить**. 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 следующих 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 дополнительные настройки фильтрации пакетов, в окне **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.

Для каждого правила в списке предоставляется следующая краткая информация:

Параметр	Описание
Включено	Состояние правила.
Действие	Указывает на действие, выполняемое Брандмауэром при обработке пакета: • Блокировать пакеты – блокировать пакет; • Разрешать пакеты – передать пакет.
Имя правила	Имя правила.
Направление	Направление соединения: • – правило применяется, если пакет принимается из сети; • – правило применяется, если пакет отправляется с вашего компьютера; • – правило применяется вне зависимости от направления соединения.



Параметр	Описание
Введение журнала	Режим регистрации событий. Указывает на то, какая информация должна быть занесена в журнал: • Только заголовки — заносить в журнал только заголовки пакетов; • Весь пакет — заносить в журнал пакеты целиком; • Отключено — 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 **Отменить** 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	Направление соединения: • Входящее — правило применяется, если пакет принимается из сети; • Исходящее — правило применяется, если пакет отправляется с вашего компьютера; • Любое — правило применяется вне зависимости от направления соединения.



Параметр	Описание
Режим ведения журнала	Режим регистрации событий. Указывает на то, какая информация должна быть занесена в журнал: • Весь пакет — заносить в журнал пакеты целиком; • Только заголовки — заносить в журнал только заголовки пакетов; • Отключено — 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.



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.

13.6. Dr.Web для Outlook

Основные функции компонента

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

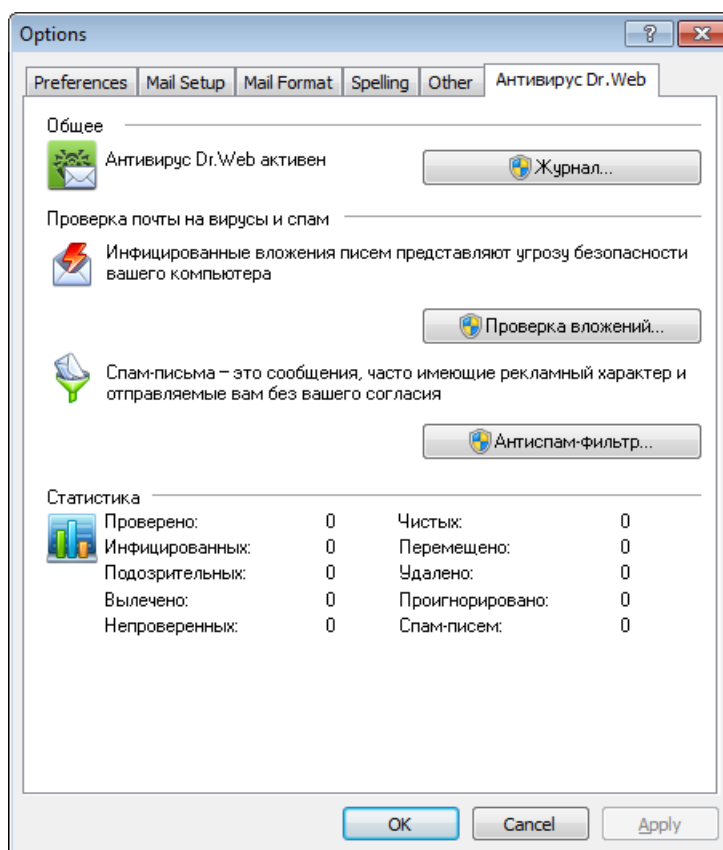
- антивирусная проверка вложенных файлов входящих почтовых сообщений;
- проверка почты, поступающей по зашифрованному соединению SSL;
- проверка почтовых сообщений на спам;
- обнаружение и нейтрализация вредоносного программного обеспечения;
- использование эвристического анализатора для дополнительной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

13.6.1. 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 **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.

13.6.2. 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.

Вредоносные объекты

Dr.Web для Outlook обнаруживает следующие вредоносные объекты:

- инфицированные объекты;
- файлы-бомбы или архивы-бомбы;
- рекламные программы;
- программы взлома;

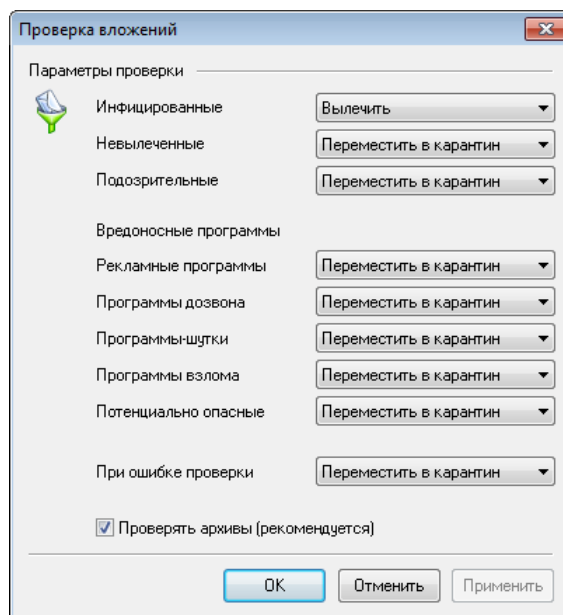


- программы дозвона;
- программы-шутки;
- потенциально опасные программы;
- шпионские программы;
- троянские программы;
- компьютерные черви и вирусы.

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** (для Microsoft Outlook 2010 в разделе **Файл** → **Параметры** → **Надстройки** необходимо выбрать **Dr.Web для Outlook** и нажать кнопку **Параметры надстройки**) нажмите кнопку **Проверка вложений**.



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;
- флажок **Проверять архивы (рекомендуется)** позволяет включить или отключить проверку вложенных файлов, представляющих собой архивы. Установите этот флажок 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 папке [Карантина](#);
- **Пропустить** – означает, что объект будет пропущен без изменений.



13.6.3. 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** (для Microsoft Outlook 2010 в разделе **Файл** → **Параметры** → **Надстройки** необходимо выбрать **Dr.Web для Outlook** и нажать кнопку **Параметры надстройки**) нажмите кнопку **Спам-фильтр**. Откроется окно настроек Спам-фильтра.

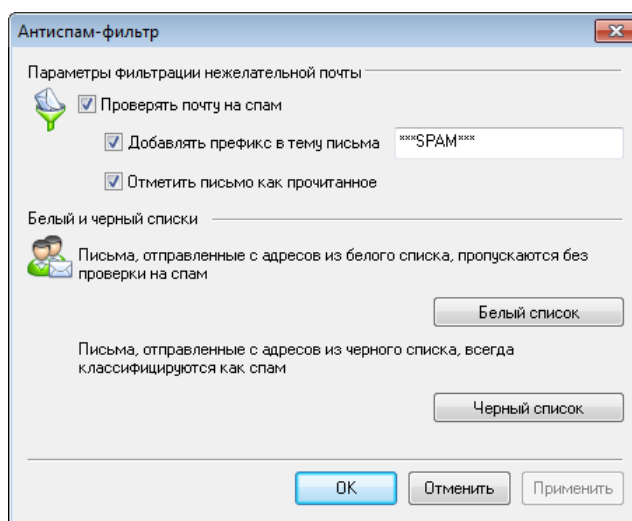


Окно **Спам-фильтр** доступно только при наличии у пользователя прав администратора системы.

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.

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:

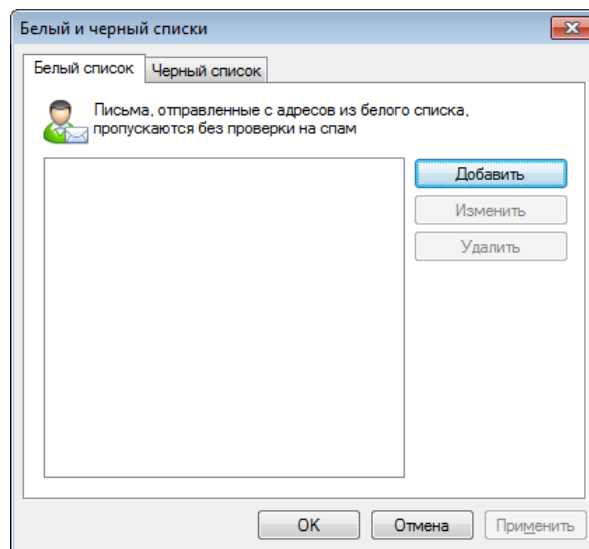
- письма, ошибочно принятые за спам, следует отправлять на адрес vrnonspam@drweb.com;
- нераспознанные и пропущенные спам-сообщения следует отправлять на адрес vrspam@drweb.com.

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

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 адресантов 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 адресантов 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 пометить как спам письма с почтовых адресов в конкретном домене, используйте символ `*` вместо имени пользователя. Например, чтобы пометить как спам все письма от адресантов из домена `spam.ru`, введите `*@spam.ru`;
- чтобы гарантированно пометить как спам письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте символ `*` вместо имени домена. Например, чтобы пометить как спам все письма от адресантов 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.



13.6.4. 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.

Журнал операционной системы

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

- сообщения о запуске и остановке программы;
- параметры ключевого файла: действительность или недействительность лицензии, срок действия лицензии (информация заносится при запуске программы, в процессе ее работы и при замене 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 день до окончания срока).

Чтобы просмотреть журнал 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**.

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 день до окончания срока).



Настройка регистрации событий

1. На вкладке **Антивирус Dr.Web** нажмите кнопку **Журнал**. Откроется окно настроек журнала.
2. Для максимальной детализации регистрируемых событий установите флажок **Вести подробный журнал**. По умолчанию события регистрируются в обычном режиме.



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

3. 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 папка, в которой хранится журнал.

13.6.5. 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 **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 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.



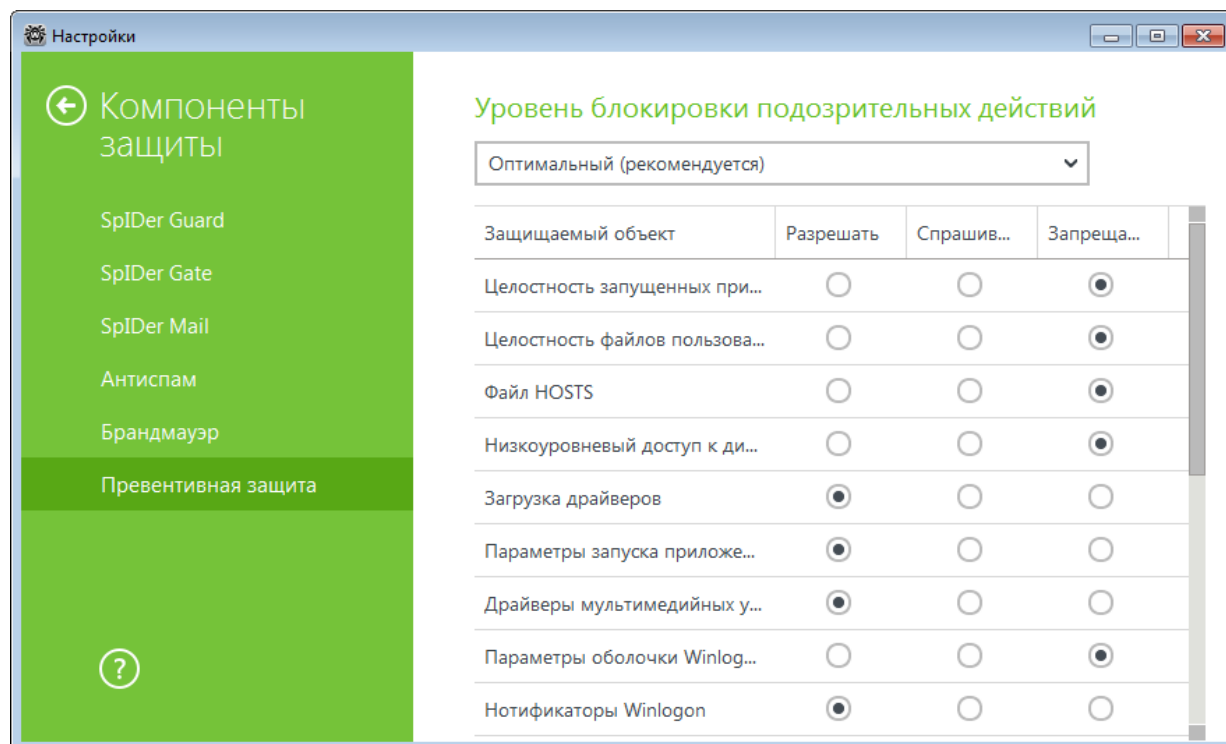
По умолчанию статистика сохраняется в файле drwebforoutlook.stat, который находится в папке %USERPROFILE%\Doctor Web.



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

13.7. Превентивная защита

В данном разделе вы можете настроить реакцию **Dr.Web** на действия сторонних приложений, которые могут привести к заражению вашего компьютера.



Уровень превентивной защиты

В режиме работы **Оптимальный**, установленном по умолчанию, **Dr.Web** запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют 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 и автоматическим запуском программ.

В режиме работы **Пользовательский** вы можете выбрать уровни защиты для каждого объекта по своему усмотрению.



Защищаемый объект	Описание
Целостность запущенных приложений	Данная настройка позволяет отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера. Не отслеживается поведение тех процессов, которые добавлены в исключения .
Целостность файлов пользователей	Данная настройка позволяет отслеживать процессы, которые модифицируют пользовательские файлы по известному алгоритму, свидетельствующему о том, что такие процессы являются угрозой безопасности компьютера. Не отслеживается поведение тех процессов, которые добавлены в исключения . Для того чтобы защитить свои данные от несанкционированных изменений, вы можете настроить создание защищаемых копий важных файлов.
HOSTS файл	Файл HOSTS используется операционной системой для упрощения доступа к сети Интернет. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
Низкоуровневый доступ к диску	Данная настройка позволяет запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
Загрузка драйверов	Данная настройка позволяет запрещать приложениям загрузку новых или неизвестных драйверов.
Критические области Windows	Прочие настройки позволяют защищать от модификации ветки реестра (как в системном профиле, так и в профилях всех пользователей). Доступ к Image File Execution Options: - Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Доступ к User Drivers: - Software\Microsoft\Windows NT\CurrentVersion\Drivers32 - Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Параметры оболочки Winlogon: - Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Нотификаторы Winlogon: - Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Автозапуск оболочки Windows: - Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Ассоциации исполняемых файлов: - Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи) - Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (ключи) Политики ограничения запуска программ (SRP): - Software\Policies\Microsoft\Windows\Safer Плагины Internet Explorer (BHO): - Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Автозапуск программ: - Software\Microsoft\Windows\CurrentVersion\Run - Software\Microsoft\Windows\CurrentVersion\RunOnce - Software\Microsoft\Windows\CurrentVersion\RunOnceEx - Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup - Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup - Software\Microsoft\Windows\CurrentVersion\RunServices - Software\Microsoft\Windows\CurrentVersion\RunServicesOnce



Защищаемый объект	Описание
	Автозапуск политик: • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Конфигурация безопасного режима: • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network Параметры Session Manager: • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows Системные службы: • System\CurrentControlSet\Services



Если при установке важных обновлений от Microsoft или при установке и работе программ (в том числе программ дефрагментации) возникают проблемы, временно отключите превентивную защиту.



Вы можете [настроить](#) вывод уведомлений о действиях превентивной защиты на экран и отправку этих уведомлений на электронную почту.



Приложения

Приложение А. Дополнительные параметры командной строки

Ключи командной строки используются для задания параметров программам, которые могут быть запущены путем открытия на выполнение исполняемого файла. Это относится к **Сканеру Dr.Web**, **Консольному сканеру** и к **Модулю автоматического обновления**. При этом ключи могут задавать параметры, отсутствующие в конфигурационном файле, а для тех параметров, которые в нем заданы, имеют более высокий приоритет.

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

Ключи перечислены в алфавитном порядке.

Параметры для Сканера и 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:<коэффициент_сжатия> – максимальный уровень сжатия. Если сканер определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка не производится. По умолчанию – без ограничений.

/ARL:<уровень_вложенности> – максимальный уровень вложенности проверяемого архива. По умолчанию – без ограничений.

/ARS:<размер> – максимальный размер проверяемого архива, в килобайтах. По умолчанию – без ограничений.

/ART:<размер> – порог проверки уровня сжатия (минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия), в килобайтах. По умолчанию – без ограничений.

/ARX:<размер> – 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 папки (проверять подпапки). По умолчанию опция включена.

/E:<количество_потоков> – 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 проверке подвергаются все файлы.

/FR:<регулярное_выражение> – проверять файлы по регулярному выражению. По умолчанию проверке подвергаются все файлы.

/FULL – произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы). (Только для **Сканера**).

/FX:<маска> – не проверять файлы, соответствующие маске. (Только для **Консольного 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 угроз. 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 папке, что и сканер. По умолчанию используется drweb32.key или другой подходящий из папки C:\Program Files\DrWeb\.

/LITE – произвести стартовую проверку системы, при которой проверяются оперативная память и загрузочные секторы всех дисков, 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_попыток> – установить максимальное число попыток вылечить файл. По умолчанию – без ограничений.

/NB – не создавать резервные копии вылеченных/удалённых файлов. По умолчанию опция отключена.

/NI[:X] – уровень использования ресурсов системы, в процентах. Определяет количество памяти используемой для проверки и системный приоритет 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:

O – низший.

L – низкий.

N – обычный. Приоритет по умолчанию.

H – высокий.

M – максимальный.



/PAL:<уровень_вложенности> – максимальный уровень вложенности упаковщиков исполняемого файла. Если уровень вложенности превышает указанный, проверка будет производиться только до указанного уровня вложенности. По умолчанию – 1000.

/QL – вывести список всех файлов, помещённых в карантин на всех дисках. (Только для **Консольного Сканера**).

/QL:<имя_логического_диска> – вывести список всех файлов, помещённых 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), находящиеся 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**).

/RA:<имя_файла> – дописать отчет о работе программы в указанный файл. По умолчанию – запись в файл журнала не производится.

/REP – проверять по символьным ссылкам. По умолчанию опция отключена.

/RP:<имя_файла> – записать отчет о работе программы в указанный файл. По умолчанию – запись в файл журнала не производится.

/RPC:<сек> – тайм-аут 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**).

/RPCN:<имя_хоста> – использовать указанное имя хоста для вызовов RPC. (Только для **Консольного Сканера**).

/RPCP:<протокол> – использовать указанный протокол RPC. Возможно использование протоколов: lpc, pr, tcr. (Только для **Консольного Сканера**).

/SCC – выводить содержимое составных объектов. По умолчанию опция отключена.

/SCN – выводить название инсталляционного пакета. По умолчанию опция отключена.

/SLS – выводить логи на экран. По умолчанию опция включена. (Только для **Консольного Сканера**).

/SPN – выводить название упаковщика. По умолчанию опция отключена.

/SPS – отображать процесс проведения проверки. По умолчанию опция включена. (Только для **Консольного Сканера**).

/SST – выводить время проверки объекта. 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.

/W: <сек> – 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)
- /AAR: <действие> – действия с инфицированными архивами (возможные действия: DQIR)
- /ACN: <действие> – действия с инфицированными инсталляционными пакетами (возможные действия: DQIR)
- /ADL: <действие> – действия с программами дозвона (возможные действия: DQIR)
- /ANT: <действие> – действия с программами взлома (возможные действия: DQIR)
- /AIC: <действие> – действия с неизлечимыми файлами (возможные действия: DQR)
- /AIN: <действие> – действия с инфицированными файлами (возможные действия: CDQR)
- /AJK: <действие> – действия с программами-шутками (возможные действия: DQIR)
- /AML: <действие> – действия с инфицированными почтовыми файлами (возможные действия: QIR)
- /ARW: <действие> – действия с потенциально опасными файлами (возможные действия: DQIR)
- /ASU: <действие> – действия с подозрительными файлами (возможные действия: DQIR)

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:

/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.

Для ключа /FL модификатор «-» означает: проверить пути, перечисленные в указанном файле, и удалить этот файл.

Для ключей /ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W значение параметра «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 вместо dwscancl 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 (=dwupdater.log) arg	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.
-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>.



Параметр	Описание
-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.
--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.
-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	Вирусов или подозрений на вирусы не обнаружено.
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.



Код возврата	Событие
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.

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



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

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

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

Компьютерные черви

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

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

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

Троянские программы (тройанские кони, трояны)

Этот тип вредоносных программ не способен к саморепликации. Трояны подменяют какую-либо из часто запускаемых программ и выполняют 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 различные распространенные ПО, которое может использоваться для взлома, а также некоторые программы, использующие методы социальной инженерии (получение конфиденциальной информации у пользователей путем введения их в заблуждение).

Шпионские программы

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

Такие программы тайно закладываются на компьютер вместе с каким-либо программным обеспечением или при просмотре определенных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты от присутствия шпионских программ на компьютере – нестабильная работа браузера и замедление производительности системы.

Рекламные программы

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

Программы-шутки

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

Программы дозвона

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



Все вышеперечисленные типы программ считаются вредоносными, т. к. представляют угрозу либо данным пользователя, либо его правам на конфиденциальность информации. К вредоносным не принято причислять программы, не скрывающие своего внедрения в систему, программы для рассылки спама и анализаторы трафика, хотя потенциально и они могут при определенных обстоятельствах нанести вред пользователю.

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

Ниже приведены некоторые виды хакерских атак и интернет-мошенничества:

- *Атаки методом подбора пароля* – специальная троянская программа вычисляет необходимый для проникновения в сеть пароль методом подбора на основании заложенного в эту программу словаря паролей или генерируя случайные последовательности символов.
- *DoS-атаки* (отказ обслуживания) и *DDoS-атаки* (распределенный отказ обслуживания) – вид сетевых атак, граничащий с терроризмом, заключающийся в отправке огромного числа запросов с требованием услуги на атакуемый сервер. При достижении определенного количества запросов (ограниченного аппаратными возможностями сервера), сервер перестает с ними справляться, что приводит к отказу в обслуживании. DDoS-атаки отличаются от DoS-атак тем, что осуществляются сразу с большого количества IP-адресов.
- *Почтовые бомбы* – один из простейших видов сетевых атак. Злоумышленником посылается на компьютер пользователя или почтовый сервер компании одно огромное сообщение, или множество (десятки тысяч) почтовых сообщений, что приводит к выводу системы из строя. В антивирусных продуктах **Dr.Web** для почтовых серверов предусмотрен специальный механизм защиты от таких атак.
- *Сниффинг* – вид сетевой атаки, также называется «пассивное прослушивание сети». Несанкционированное прослушивание сети и наблюдение за данными, которое производится при помощи специальной невредоносной программы – пакетного сниффера, который осуществляет перехват всех сетевых пакетов домена, за которым идет наблюдение.
- *Спуфинг* – вид сетевой атаки, заключающейся в получении обманным путем доступа в сеть посредством имитации соединения.
- *Фишинг (Phishing)* – технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т. д. При помощи спамерских рассылок или почтовых червей потенциальным жертвам рассылаются подложные письма, якобы от имени легальных организаций, в которых их просят зайти на подделанный преступниками интернет-сайт такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию, в последствии используемую злоумышленниками для кражи денег со счета жертвы и в других преступлениях.
- *Вишинг (Vishing)* – технология интернет-мошенничества, разновидность фишинга, отличающаяся использованием вместо электронной почты war diallers (автонабирателей) и возможностей Интернет-телефонии (VoIP).



Действия 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 ОС 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;
- HLLD – 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 работать в Интернете анонимно 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.

