Dr.WEB®

Антивирус
для серверов Windows

Защити созданное

Руководство администратора

Антивирус Dr.Web для серверов Windows
Версия 8.0
Руководство администратора
11.12.2013

«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

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

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

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

Антивирус Dr.Web для серверов 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 **Антивирус Dr.Web для серверов**.

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

- **Сканер Dr.Web®** – антивирусный сканер с графическим интерфейсом, который запускается по запросу пользователя или по расписанию и проводит антивирусную проверку компьютера.
  Существует также версия программы с интерфейсом командной строки (**Консольный сканер Dr.Web®**);
- **SpIDer Guard®** – антивирусный сторож, который постоянно находится в оперативной памяти, осуществляя проверку файлов и памяти «на лету», а также обнаруживая проявления вирусной активности;
- **Модуль обновления Dr.Web** – компонент, который позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов **Dr.Web**, а также производит их автоматическую установку;
- **SpIDer Agent** – модуль управления, с помощью которого осуществляется запуск и настройка компонентов программы **Антивирус Dr.Web для серверов**.

1.1. О чем эта документация

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

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

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

В Приложениях содержится подробная справочная информация по настройке программы **Антивирус Dr.Web для серверов**.

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 обозначения, приведенные в таблице 1.

Таблица 1. Обозначения

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

1.3. Системные требования

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

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

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

Компонент	Требование
Процессор	Полная поддержка системы команд i686.
Операционная система	Для 32-разрядных операционных систем: • Microsoft® Windows Server® 2003 с пакетом обновлений SP1; • Microsoft® Windows Server® 2008. Для 64-разрядных операционных систем: • Microsoft® Windows Server® 2008; • Microsoft® Windows Server® 2008 R2; • Microsoft® Windows Server® 2012; • Microsoft® Windows Server® 2012 R2. Возможно, потребуется загрузить с сайта Microsoft и установить обновления ряда системных компонентов. **Антивирус Dr.Web для серверов** сообщит вам, при необходимости, их наименования и URL.
Свободная оперативная память	512 МБ и больше.
Место на жестком диске	200 МБ для размещения компонентов продукта.

Компонент	Требование
	Файлы, создаваемые в ходе установки, потребуют дополнительного места.
Разрешение	Рекомендуемое разрешение экрана не менее 800x600.
Прочее	Подключение к сети Интернет для обновления вирусных баз и компонентов программы **Антивирус Dr.Web для серверов**.

Антивирус Dr.Web для серверов несовместим с плагинами **Dr.Web для Microsoft Exchange Server**, **Dr.Web для IBM Lotus Domino**, **Dr.Web для Kerio WinRoute**, **Dr.Web для Kerio MailServer**, **Dr.Web для Microsoft ISA Server и Forefront TMG**, **Dr.Web для Qbik WinGate** версий 6.0 и ранее.

1.4. Лицензирование

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

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

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

1.4.1. Ключевой файл

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

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

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

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

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

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

1.4.2. Получение ключевого файла

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

Получение ключевого файла в процессе регистрации на сайте

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

Для получения лицензионного ключевого файла необходим регистрационный серийный номер продукта.

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

Повторная регистрация

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

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

1.4.3. Продление лицензии

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

Замена ключевого файла

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

1.5. Методы обнаружения

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

1. В первую очередь применяется *сигнатурный анализ*. Он выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов (*сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для опознания вируса). При этом сравнение проводится по контрольным суммам сигнатур, что позволяет значительно снизить размер записей в вирусных базах данных, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения и лечения зараженных файлов. **Вирусные базы Dr.Web** составлены таким образом, что благодаря одной записи можно обнаруживать целые классы угроз.
2. После завершения сигнатурного анализа применяется уникальная технология **Origins Tracing™**, которая позволяет определить новые или модифицированные вирусы, использующие известные механизмы заражения файлов. Так, например, эта технология защищает пользователей антивирусных решений **Dr.Web** от таких вирусов, как вирус-шантажист Trojan.Encoder.18 (также известный под названием gpcode). Кроме того, именно введение **Origins Tracing** позволяет значительно снизить количество ложных срабатываний эвристического анализатора.

3. Работа *эвристического анализатора* основывается на неких знаниях (*эвристиках*) о характерных признаках вирусного и, наоборот, безопасного кода. Каждый признак имеет определенный вес (число, показывающее серьезность и достоверность данного признака). На основании суммарного веса, характеризующего каждый конкретный файл, эвристический анализатор вычисляет вероятность заражения файла неизвестным вирусом. Как и любая система проверки гипотез в условиях неопределенности, эвристический анализатор может допускать ошибки как первого (пропуск неизвестных вирусов), так и второго рода (ложная тревога).

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

1.6. Проверка антивируса

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

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

Программа test.com представляет собой 68-байтный COM-файл, в результате исполнения которого на консоль выводится текстовое сообщение: `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`
Файл test.com состоит только из текстовых символов, которые формируют следующую строку:

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

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

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

2. Установка программы

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

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

Перед установкой следует также удалить с компьютера другие антивирусные программы для предотвращения возможной несовместимости их резидентных компонентов.

2.1. Первая установка

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

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

- в фоновом режиме;
- в обычном режиме.

Установка с параметрами командной строки

Для запуска установки программы **Антивирус Dr.Web для серверов** 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):

Параметр	Значение
reboot	Автоматическая перезагрузка компьютера после завершения установки.
lang	Язык продукта. Значение параметра – код языка в формате ISO 639-1.
silent	Установка в фоновом режиме.

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

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

Установка в обычном режиме

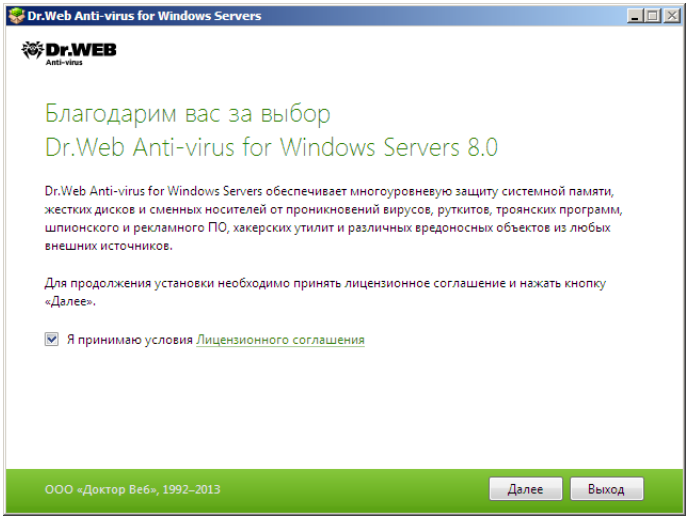
Следуйте указаниям программы установки. На любом шаге до начала копирования файлов на компьютер вы можете выполнить следующее:

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

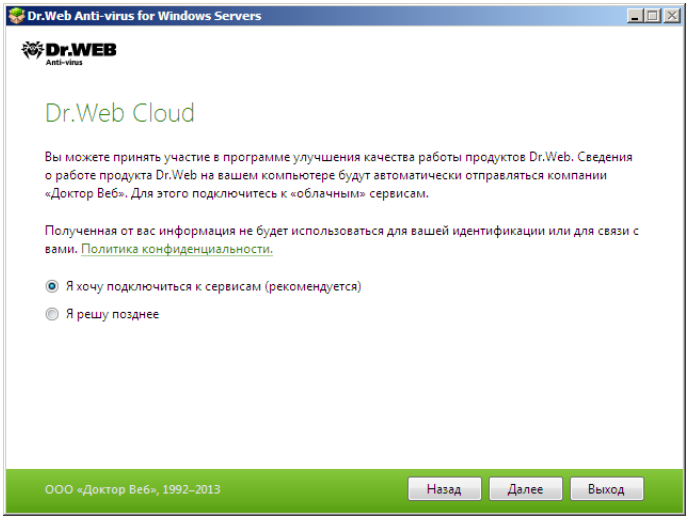
Перед началом установки проверяется актуальность установочного файла. В случае, если существует более новый установочный файл, вам будет предложено его скачать.

Процедура установки:

1. Если на вашем компьютере уже установлен другой антивирус, то программа установки предупредит вас о несовместимости программы **Антивирус Dr.Web для серверов** и иных антивирусных решений, и предложит удалить их.
2. Ознакомьтесь с лицензионным соглашением. Для продолжения установки его необходимо принять.

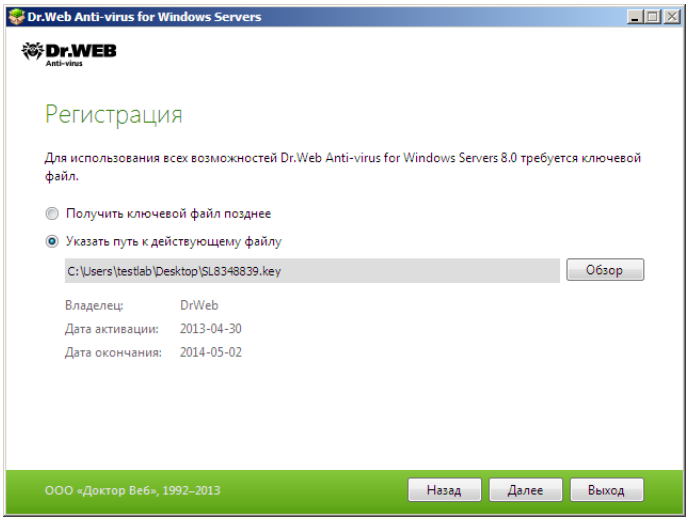


3. Далее вам будет предложено подключиться к программе улучшения качества программного обеспечения.



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

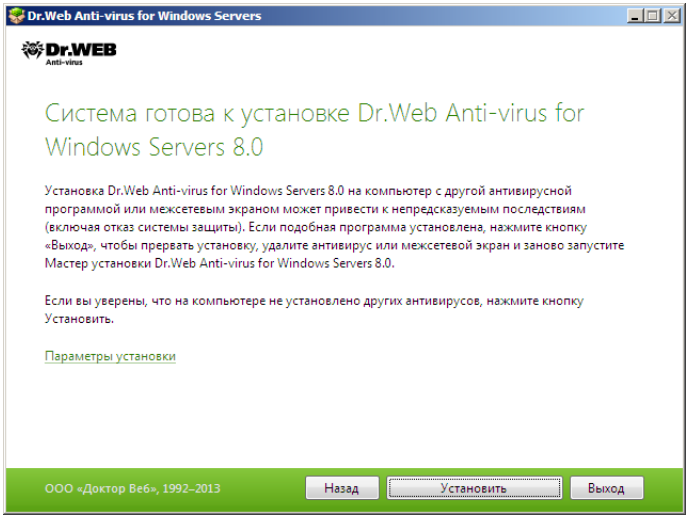
   Нажмите кнопку **Далее**.



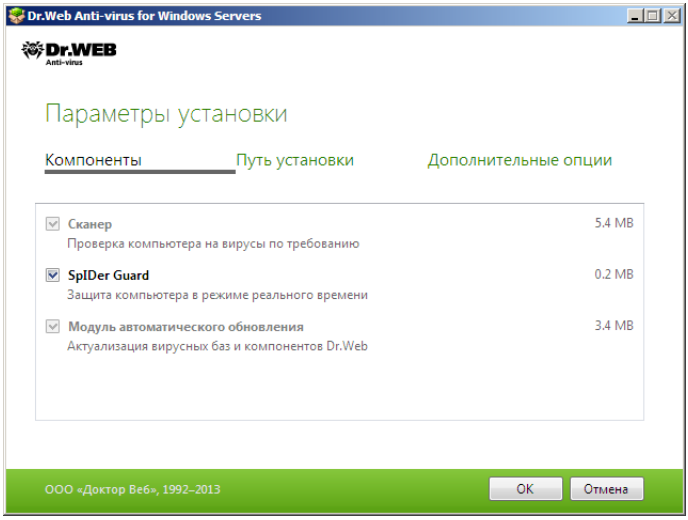
Используйте только ключевой файл варианта программы **Антивирус Dr.Web для серверов**. Ключевой файл должен иметь расширение .key.

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

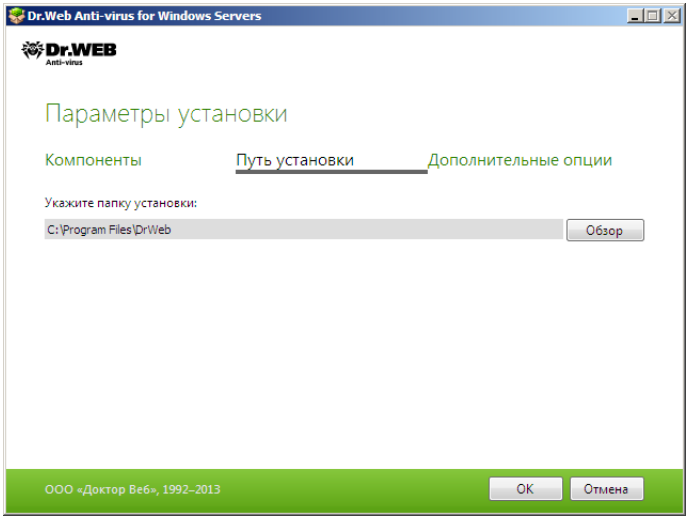
   Для того чтобы самостоятельно выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры установки, нажмите **Параметры установки**. Данная опция предназначена для опытных пользователей.



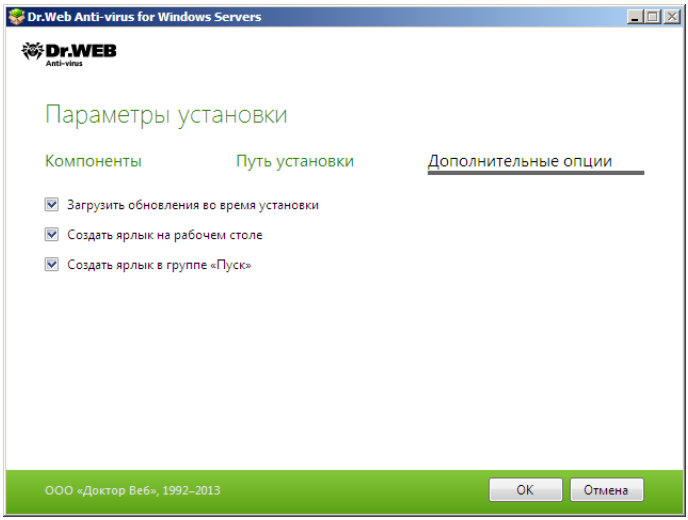
6. Если на предыдущем шаге вы нажали кнопку **Установить,** то перейдите к описанию шага 9. В противном случае откроется окно **Параметры установки**. На первой вкладке вы можете изменить состав устанавливаемых компонентов.



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



8. Если на шаге 4 вы указали действующий ключевой файл, 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 **Антивирус Dr.Web для серверов**.

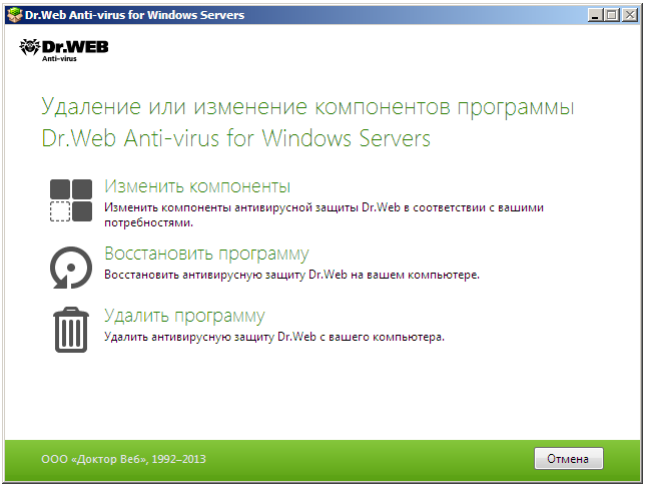


После того, как все необходимые изменения будут внесены, нажмите кнопку **OK**.

9. Если в процессе установки вы указали действующий ключевой файл и на шаге 8 установили флажок **Загрузить обновления во время установки**, а также во время установки по умолчанию, будет выполнен процесс обновления вирусных баз и других компонентов программы **Антивирус Dr.Web для серверов**. Обновление проводится автоматически и не требует дополнительных действий.

2.2. Удаление и изменение программы

1. Запустите программу установки при помощи утилиты установки и удаления программ операционной системы Windows.
2. В открывшемся окне выберите режим работы программы установки:
   - чтобы изменить состав устанавливаемых компонентов, выберите вариант **Изменить компоненты**;
   - чтобы восстановить антивирусную защиту на вашем компьютере, выберите вариант **Восстановить программу**;
   - чтобы удалить все установленные компоненты, выберите пункт **Удалить программу.**



3. Для удаления программы **Антивирус Dr.Web для серверов** или изменения состава компонентов введите код подтверждения, изображенный в открывшемся окне.
4. При необходимости по просьбе программы перезагрузите компьютер для завершения процедуры удаления или изменения состава компонентов.

3. Приступая к работе

Программа установки позволяет установить на компьютер следующие компоненты антивирусной защиты:

- **Сканер Dr.Web** для Windows (с GUI-интерфейсом и консольную версию);
- сторож **SpIDer Guard**;
- **Модуль автоматического обновления Dr.Web**;
- модуль управления **SpIDer Agent**.

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

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

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

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

Организация антивирусной защиты

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

- при помощи **Сканера Dr.Web** произвести проверку всей файловой системы компьютера с предусмотренными по умолчанию (максимальными) настройками подробности проверки;
- сохранить настройки **SpIDer Guard** по умолчанию;
- периодически, по мере обновления вирусных баз, повторять полную проверку компьютера (не реже раза в неделю);
- в случае временного отключения **SpIDer Guard**, если в этот период компьютер подключался к сети Интернет или производилась загрузка файлов со сменного носителя, провести полную проверку немедленно.

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

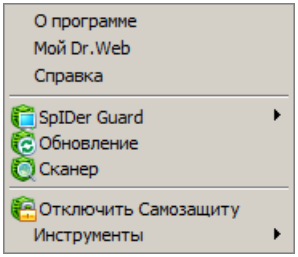
Использование компонентов программы **Антивирус Dr.Web для серверов** подробнее описано в следующих разделах.

3.1. Модуль управления SpIDer Agent

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

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

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



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

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

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

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

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

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

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

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

Отключение самозащиты:

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

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

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

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

- к **Менеджеру лицензий** (см. раздел Менеджер лицензий);
- к настройкам общих параметров работы программы **Антивирус Dr.Web для серверов** (см. Основные настройки) и настройкам отдельных компонентов;
- к **Менеджеру Карантина** (см. Менеджер Карантина);
- к статистике компонентов;
- к Антивирусной сети;
- к созданию отчета.

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

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

Данный пункт отображается только при отсутствии административных привилегий. Например, при работе в среде Windows Server 2008 при включенной системе контроля учетной записи UAC. В противном случае данный пункт недоступен и **SpIder Agent** сразу предоставляет доступ ко всем функциям.

3.2. Основные настройки

Настройки программы **Антивирус Dr.Web для серверов** недоступны в пользовательском режиме.

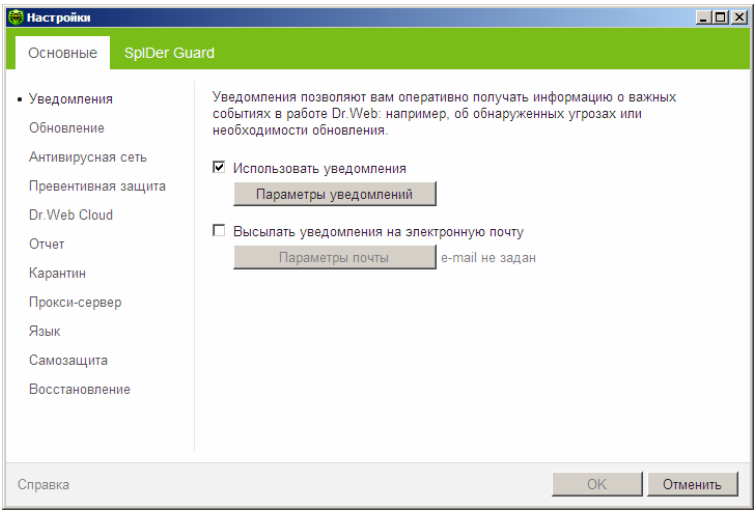
Единый центр управления настройками позволяет задать как общие параметры работы антивирусного комплекса, так и индивидуальные настройки всех компонентов программы **Антивирус Dr.Web для серверов** за исключением **Сканера**.

Общая настройка Антивирус Dr.Web для серверов

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

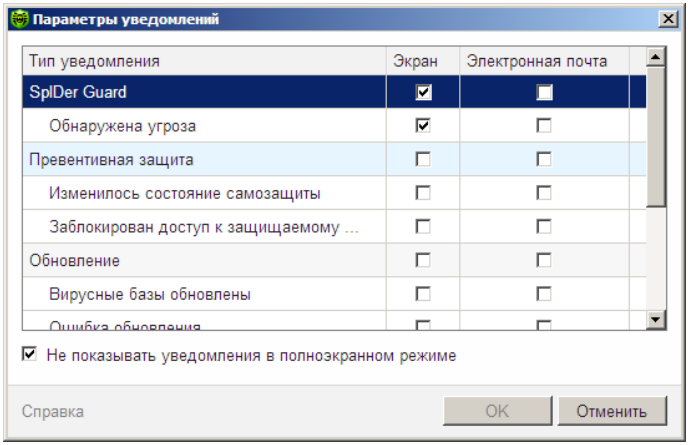
3.2.1. Раздел Уведомления

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



Настройка уведомлений

1. Чтобы включить режим нотификации о событиях, установите флажок **Использовать уведомления**.
2. Нажмите кнопку **Параметры уведомлений**. Откроется окно со списком возможных уведомлений.



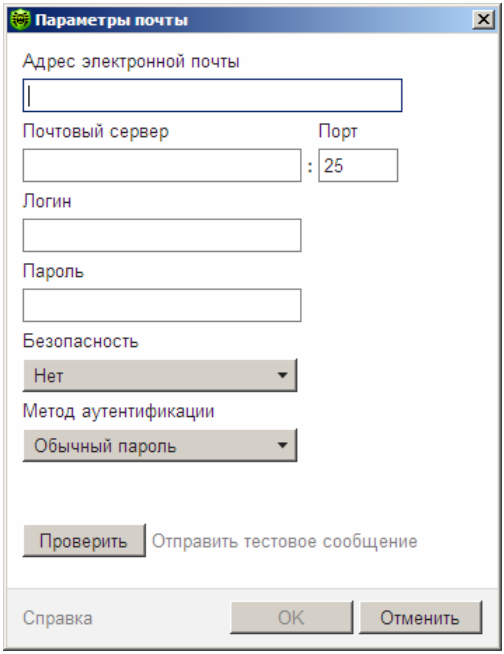
3. Выберите уведомления, которые вы хотите получать, и установите соответствующие флажки. Чтобы отображать экранные уведомления, устанавливайте флажок в столбце **Экран**. Чтобы получать оповещения по почте, устанавливайте флажок в столбце **Почта**.
4. При необходимости задайте дополнительные параметры отображения экранных оповещений:

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

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

Настройка почтовых уведомлений

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



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

Настройка	Описание
Адрес	Укажите почтовый адрес, на который вы хотите получать оповещения выбранных типов.

Настройка	Описание
Почтовый сервер	Укажите адрес почтового сервера, который должен использовать **Антивирус Dr.Web для серверов** для отправки почтовых оповещений.
Порт	Укажите порт почтового сервера, к которому должен подключаться **Антивирус Dr.Web для серверов** для отправки почтовых оповещений.
Логин	Укажите имя учетной записи для подключения к почтовому серверу.
Пароль	Укажите пароль учетной записи для подключения к почтовому серверу.
Безопасность	Выберите параметры безопасности при подключении к почтовому серверу.
Метод аутентификации	Выберите метод аутентификации, используемый для подключения к почтовому серверу.

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

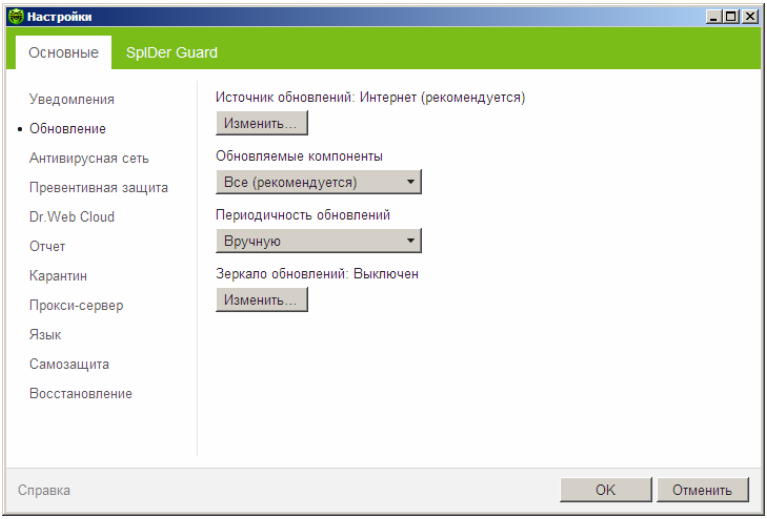
Временное отключение уведомлений

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

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

3.2.2. Раздел Обновление

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

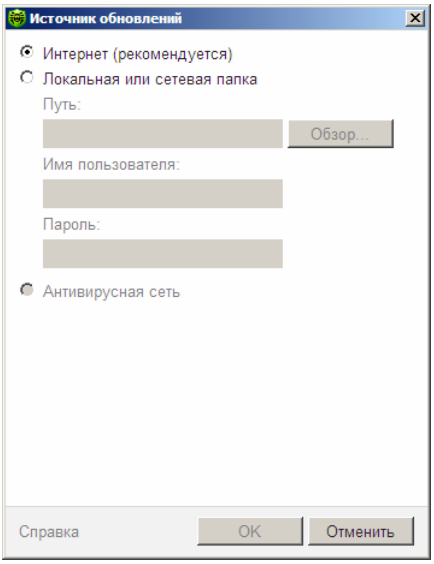


Настройка	Описание
Источник обновлений	Вы можете указать удобный для вас источник обновлений.
Обновляемые компоненты	Вы можете выбрать один из вариантов загрузки обновлений: • **Все (рекомендуется)**, при котором загружаются обновления как для **вирусных баз Dr.Web**, так и для антивирусного ядра и других программных компонентов программы **Антивирус Dr.Web для серверов**;

Настройка	Описание
	• **Только базы**, при котором загружаются только обновления **вирусных баз Dr.Web** и антивирусного ядра; другие компоненты программы **Антивирус Dr.Web для серверов** не обновляются.
Периодичность обновлений	Вы можете выбрать периодичность, с которой будет производиться проверка на наличие обновлений.
Зеркало обновлений	Вы можете создать зеркало обновлений, которое смогут использовать другие компьютеры в локальной сети, на которых установлен продукт **Dr.Web**.

Источник обновлений

Для того чтобы выбрать источник обновлений, нажмите кнопку **Изменить.**

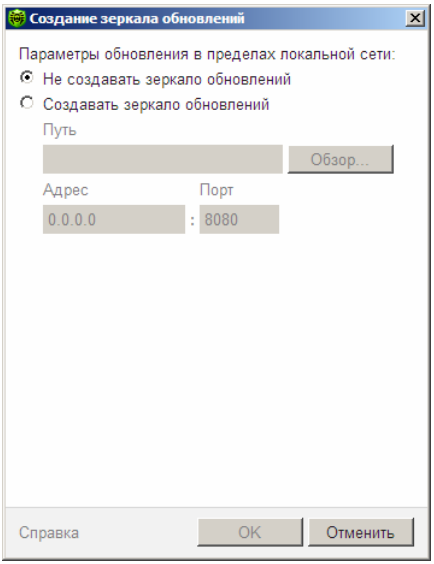


В открывшемся окне укажите удобный для вас источник обновлений:

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

Создание зеркала обновлений

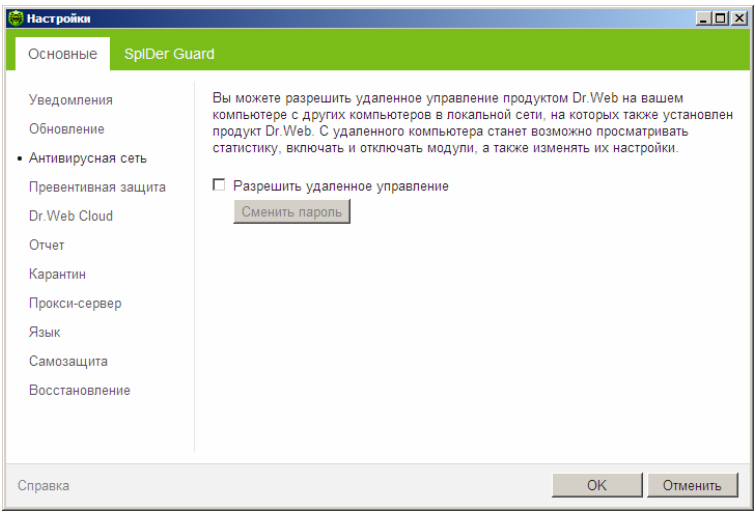
Чтобы ваш компьютер могли использовать как источник обновлений другие компьютеры в локальной сети, на которых установлен продукт **Dr.Web**, нажмите кнопку **Изменить** в пункте **Зеркало обновлений** и в открывшемся окне выберите Создавать зеркало обновлений. Укажите путь к папке, в которую будут копироваться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



3.2.3. Раздел Антивирусная сеть

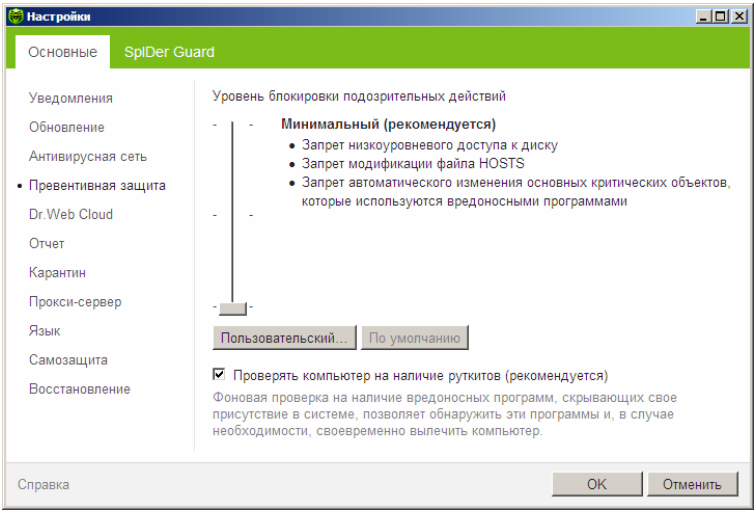
В данном разделе вы можете разрешить удаленное управление вашим антивирусом с других компьютеров локальной сети при помощи компонента Антивирусная сеть. Вхождение в состав антивирусной сети позволяет создавать на вашем компьютере зеркала обновлений, а также удаленно контролировать состояние антивирусной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

Для предотвращения несанкционированного доступа к настройкам программы **Антивирус Dr.Web для серверов** на вашем компьютере необходимо задать пароль для удаленного управления.



3.2.4. Раздел Превентивная защита

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



Уровень превентивной защиты

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

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

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

При необходимости полного контроля за доступом к критическим объектам Windows вы можете поднять уровень защиты до **Параноидального**. В данном случае вам также будет доступен интерактивный контроль за загрузкой драйверов, автоматическим запуском программ и работой системных служб.

Пользовательский режим

Данный режим позволяет гибко настроить реакцию программы **Антивирус Dr.Web для серверов** на определенные действия, которые могут привести к заражению вашего компьютера.

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

Фоновая проверка на заражение

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

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

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

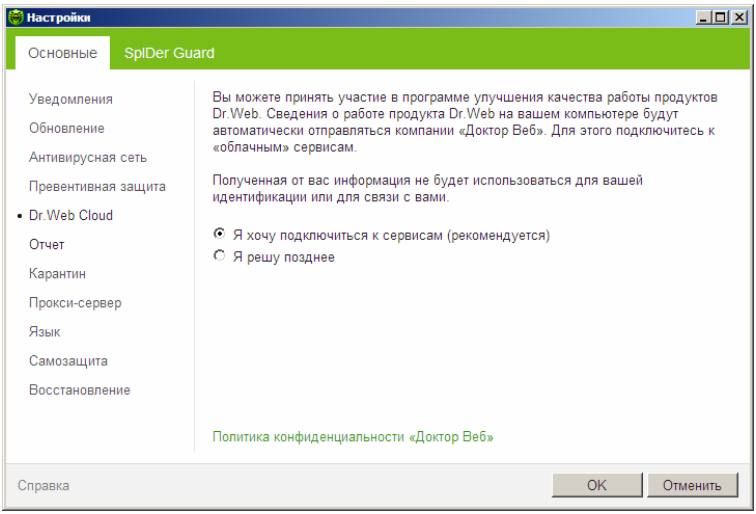
При обнаружении угроз **Антируткит Dr.Web** оповещает вас об угрозе и нейтрализует опасные воздействия.

При проведении фоновой проверки на наличие руткитов из проверки исключаются файлы и папки, заданные на вкладке Исключения компонента **SpIDer Guard**.

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

3.2.5. Раздел Dr.Web Cloud

В данном разделе вы можете подключиться к программе улучшения качества работы продуктов **Dr.Web**.



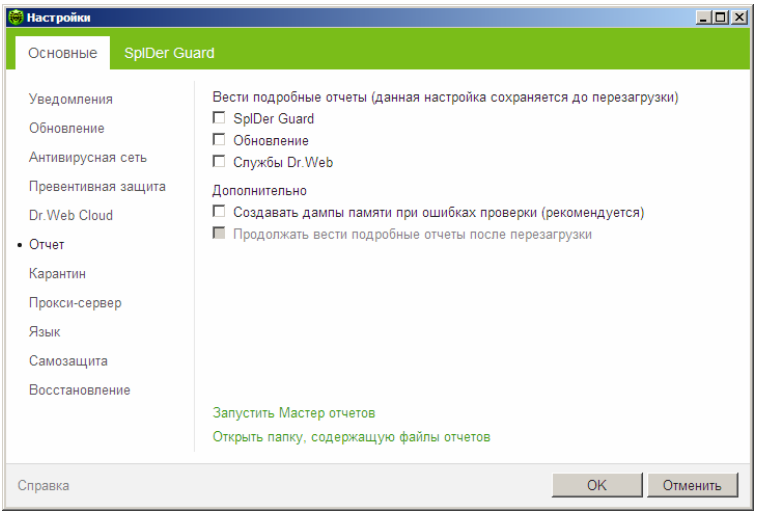
Программа улучшения качества ПО

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

3.2.6. Раздел Отчет

В данном разделе вы можете настроить параметры ведения файлов отчетов для компонентов программы **Антивирус Dr.Web для серверов**.



По умолчанию для всех компонентов программы **Антивирус Dr.Web для серверов** отчеты ведутся в стандартном режиме, фиксирующем следующую информацию:

Компонент	Информация
SpIDer Guard	Проведение обновлений, запуск и останов сторожа **SpIDer Guard**, вирусные события, данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых составных объектов (архивов, файлов электронной почты или файловых контейнеров).

Компонент	Информация
	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.
Модуль обновления	Список обновленных файлов программы **Антивирус Dr.Web для серверов** и статусы их загрузки, информация о работе вспомогательных скриптов, дата и время проведения обновления, информация о перезапуске компонентов программы **Антивирус Dr.Web для серверов** после обновления.
Службы Dr.Web	Информация о компонентах **Dr.Web**, изменение настроек компонентов, включение и выключение компонентов, события превентивной защиты, подключение к антивирусной сети.

Просмотр файлов отчетов

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

Включение подробных отчетов

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

1. Чтобы включить режим ведения подробного отчета для одного из компонентов программы **Антивирус Dr.Web для серверов**, установите соответствующий флажок.

2. По умолчанию подробный отчет ведется до первой перезагрузки операционной системы. Если необходимо зафиксировать поведение компонента в период до и после перезагрузки, установите флажок **Продолжать вести подробные отчеты после перезагрузки**.
3. Сохраните изменения.

По умолчанию файлы отчета имеют ограниченный размер, равный 10 МБ.

Дополнительные настройки

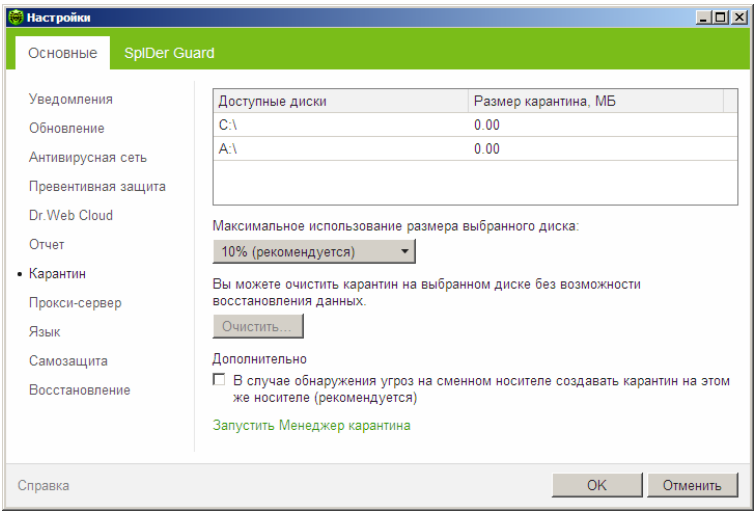
Настройка **Создавать дампы памяти при ошибках проверки (рекомендуется)** позволяет сохранять максимум полезной информации о причинах некорректной работы компонентов, что позволит специалистам компании **«Доктор Веб»** в дальнейшем провести более полный анализ проблемы и предложить ее решение. Рекомендуется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

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

3.2.7. Раздел Карантин

В данном разделе вы можете настроить параметры работы Карантина программы **Антивирус Dr.Web для серверов**, оценить его размер, а также удалить все изолированные файлы с конкретного диска.

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



Ограничение размера Карантина

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

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

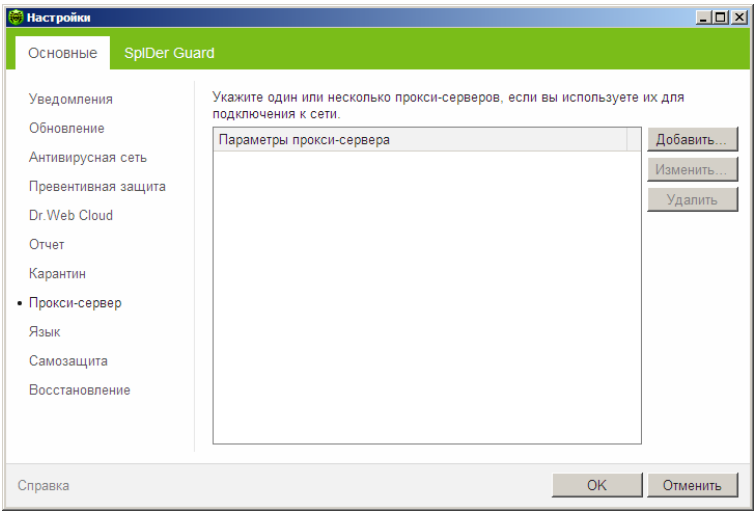
Очистка Карантина

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

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

3.2.8. Раздел Прокси-сервер

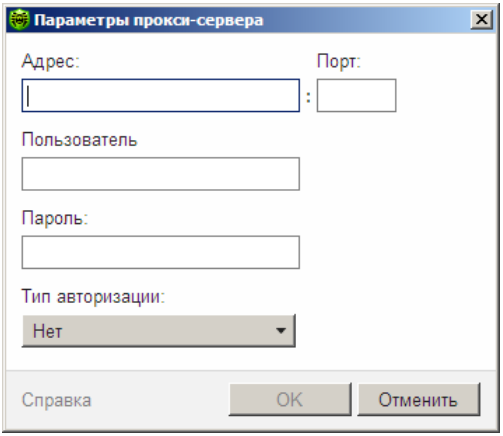
В данном разделе вы можете настроить параметры доступа к сети для **Модуля обновления**.



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

Формирование списка прокси-серверов

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



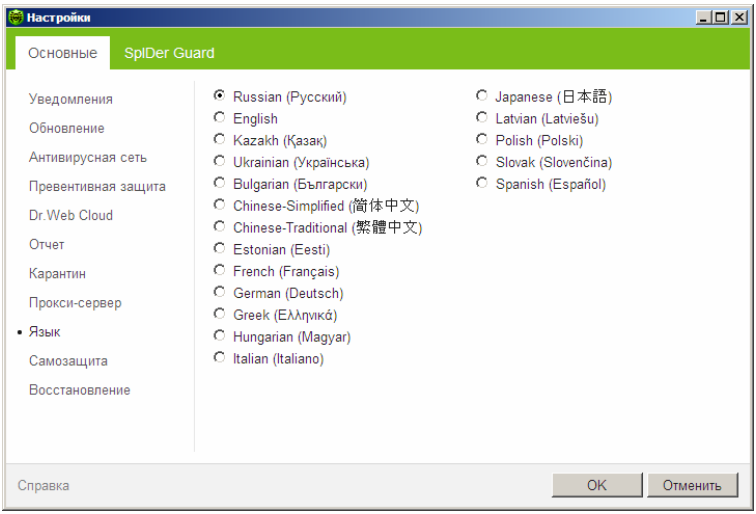
3. Укажите настройки подключения к прокси-серверу:

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

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

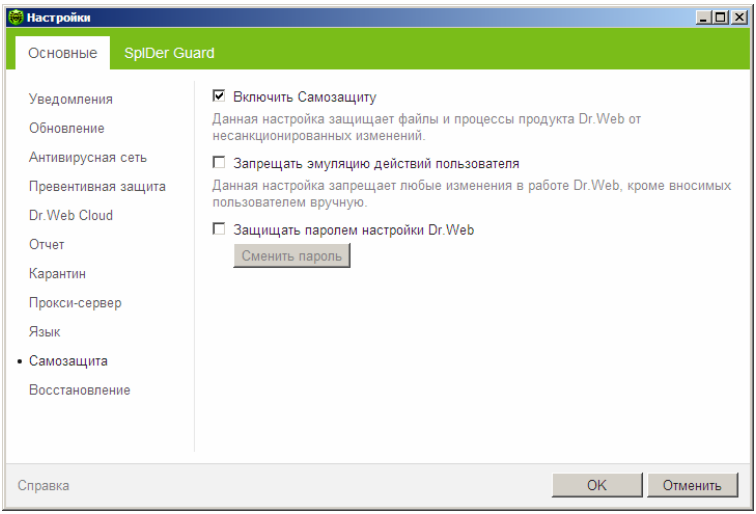
3.2.9. Раздел Язык

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



3.2.10. Раздел Самозащита

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



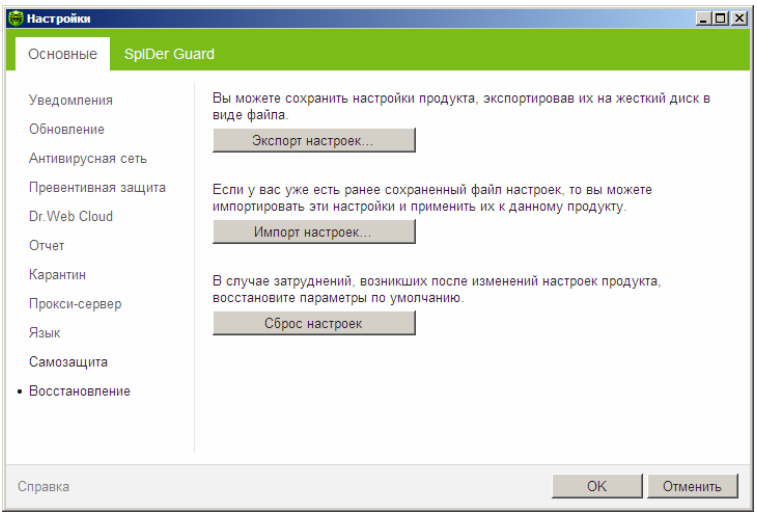
Настройка **Включить самозащиту** позволяет защитить файлы и процессы программы **Антивирус Dr.Web для серверов** от несанкционированного доступа. Отключать самозащиту не рекомендуется.

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

Настройка **Защищать паролем настройки Dr.Web** позволяет установить пароль для доступа к настройкам программы **Антивирус Dr.Web для серверов** на вашем компьютере. Задайте пароль, который будет запрашиваться при обращении к настройкам программы **Антивирус Dr.Web для серверов**.

3.2.11. Раздел Восстановление

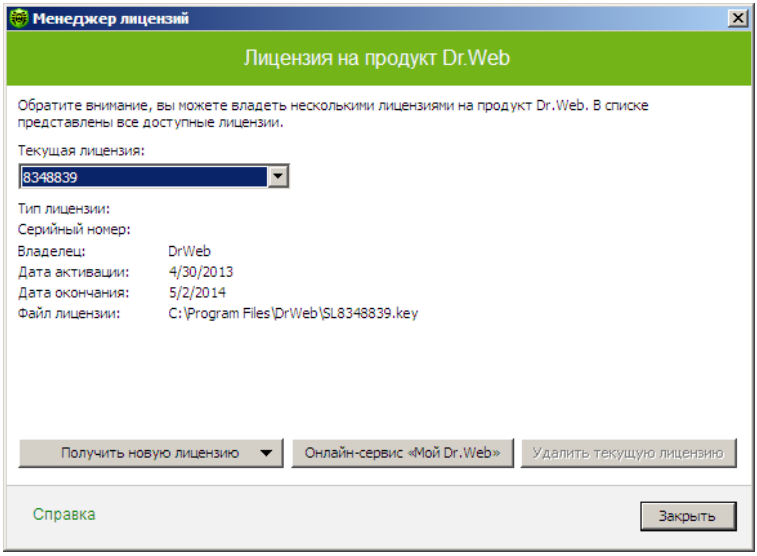
В данном разделе вы можете восстановить настройки программы **Антивирус Dr.Web для серверов** по умолчанию, а также экспортировать или импортировать их.



3.3. Менеджер лицензий

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

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



Установка полученного ключевого файла

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

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

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

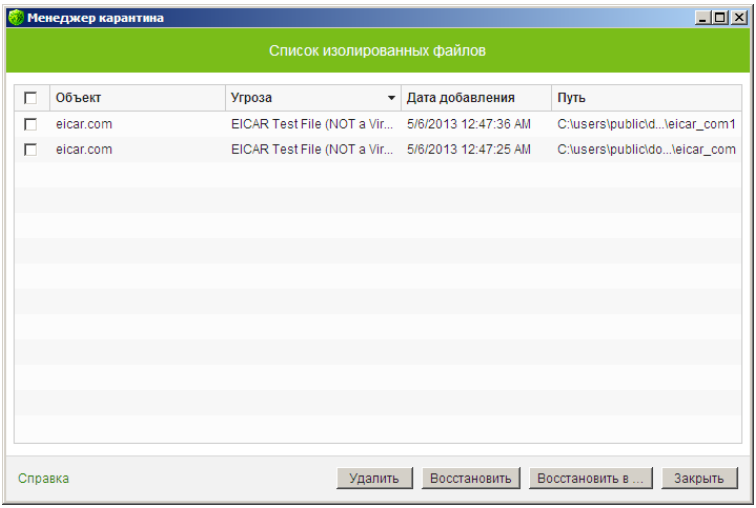
При работе программы ключевой файл по умолчанию должен находиться в каталоге установки. **Антивирус Dr.Web для серверов** регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа не модифицируйте ключевой файл.

При отсутствии действительного ключевого файла активность всех компонентов блокируется.

3.4. Менеджер Карантина

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

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



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

- **Объект** – список имен объектов, находящихся в карантине;

- **Угроза** – классификация вредоносной программы, определяемая **Антивирусом Dr.Web для серверов** при автоматическом перемещении объекта в карантин;
- **Дата добавления** – дата, когда объект был перемещен в **Карантин**;
- **Путь** – полный путь, по которому находился объект до перемещения в карантин.

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

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

В окне карантина доступны следующие кнопки управления:

- **Восстановить** – переместить файл из карантина и восстановить первоначальное местоположение файла на компьютере (восстановить файл под тем же именем и в папку, в которой он находился до перемещения в карантин);
- **Восстановить в** – переместить файл под заданным именем в нужную папку;

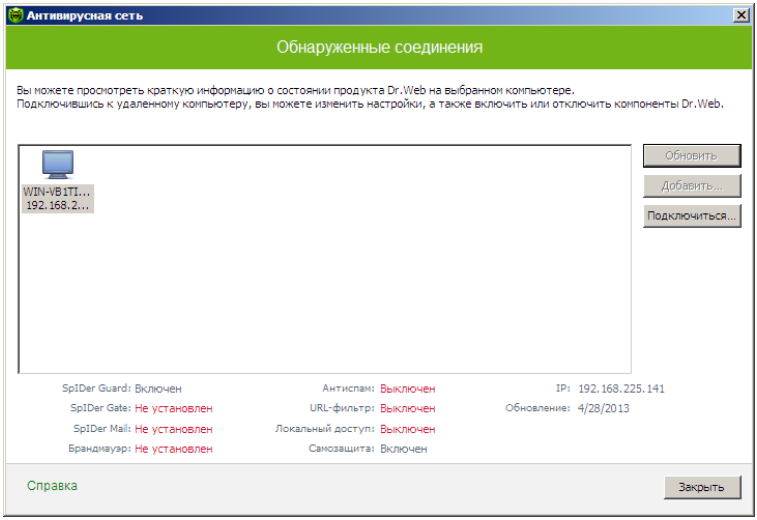
Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

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

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

3.5. Антивирусная сеть

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



Для доступа к удаленному антивирусу, выберите компьютер в списке и нажмите кнопку **Подключиться**. Введите пароль, заданный в настройках удаленного антивируса. В области уведомлений Windows появится значок удаленного **SpIDer Agent**. Пользователь антивируса, к которому вы подключились, получит уведомление в виде всплывающей подсказки.

При работе с удаленным антивирусом вам доступны следующие пункты (набор компонентов варьируется в зависимости от того, к какому продукту **Dr.Web** установлено подключение):

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

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

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

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

Компоненты **Антивирусная сеть**, **Карантин** и **Сканер** недоступны. Настройки и статистика **Брандмауэра Dr.Web** также недоступны, однако вы можете включить или отключить этот компонент (в случае подключения к продуктам **Антивирус Dr.Web** 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 **Добавить** и введите IP-адрес.

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

Компьютеры в локальной сети отображаются в списке только в том случае, если в установленном на них продукте **Dr.Web** разрешено удаленное управление. Вы можете разрешить подключение к программе **Антивирус Dr.Web для серверов** на вашем компьютере в разделе **Антивирусная сеть** Основных настроек.

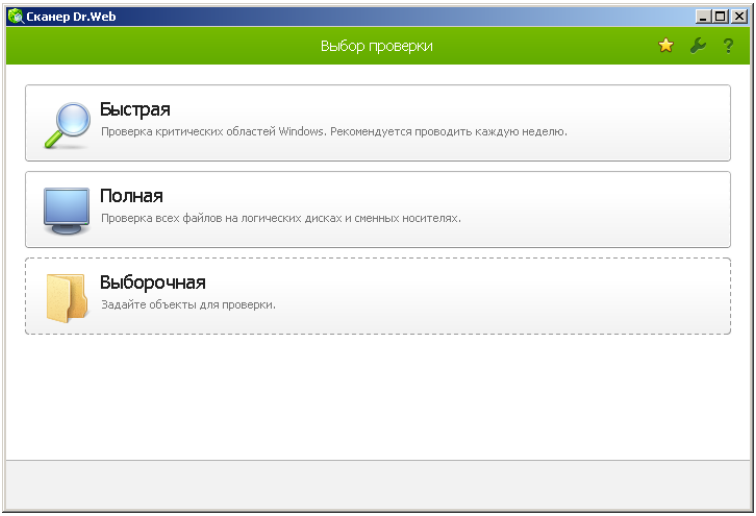
Пункт **Антивирусная сеть** доступен только в Административном режиме.

4. Сканер Dr.Web

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

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

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



4.1. Проверка компьютера

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

Запуск Сканера

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

1. Для запуска **Сканера** используйте одно из следующих средств:
   - значок **Сканера** на Рабочем столе;

- пункт **Сканер** контекстного меню значка **SpIDer Agent** в области уведомлений Windows;
- пункт меню **Сканер Dr.Web** в папке **Dr.Web** Главного меню Windows (открывается по кнопке **Пуск**);
- специальную команду операционной системы Windows (подробнее см. 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**.

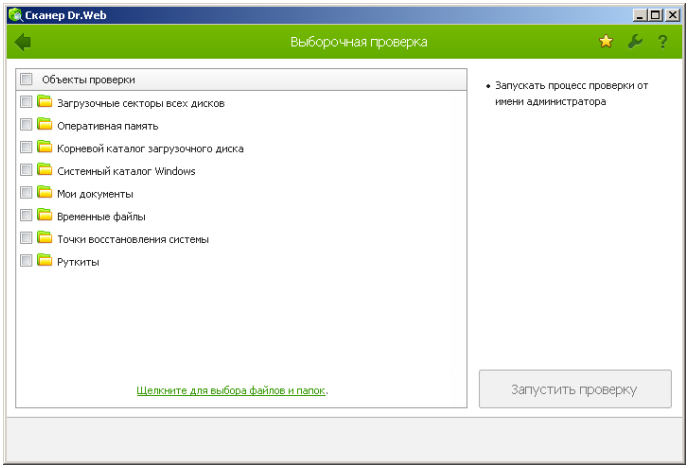
   Во время *быстрой проверки* проверяются:

   - оперативная память;
   - загрузочные секторы всех дисков;
   - корневой каталог загрузочного диска;
   - системный каталог Windows;
   - папка Мои Документы;
   - временный каталог системы;
   - временный каталог пользователя;
   - наличие руткитов (если процесс проверки запущен от имени администратора).

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

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

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

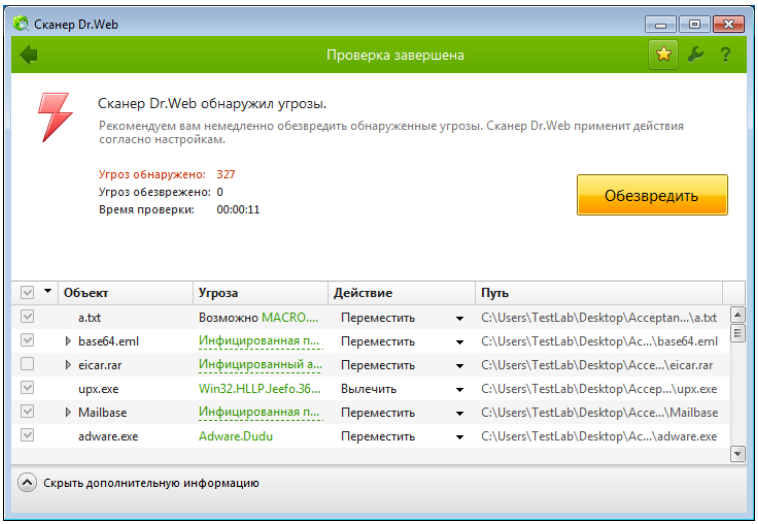


5. После начала проверки в правой части окна становятся доступными кнопки **Пауза** и **Стоп**. На любом этапе проверки вы можете сделать следующее:
   - чтобы приостановить проверку, нажмите кнопку **Пауза**. Для того чтобы возобновить проверку после паузы, нажмите кнопку **Продолжить**;
   - чтобы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

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

4.2. Действия при обнаружении 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.

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

Существуют следующие ограничения:

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

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

4.3. Настройка Сканера

Изменение настроек программы

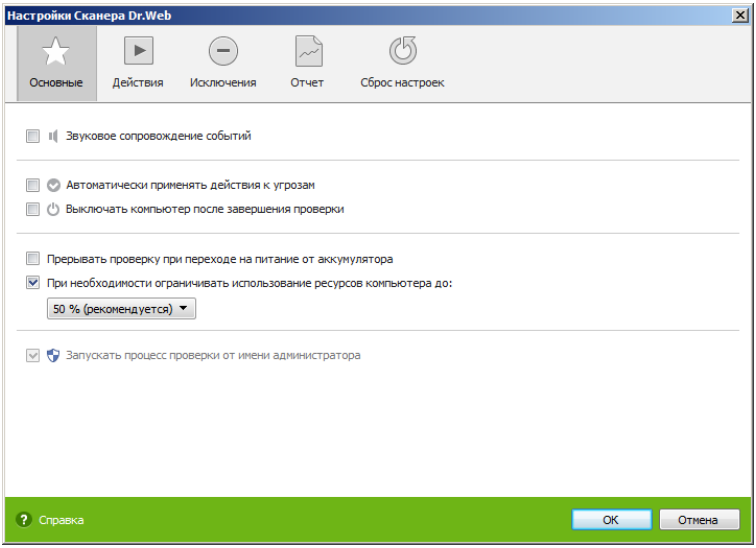
1. Чтобы вызвать **Настройки Сканера**, щелкните на панели инструментов иконку **Настройки**  .

   Откроется окно настроек, содержащее несколько вкладок.

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

Вкладка Основные

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

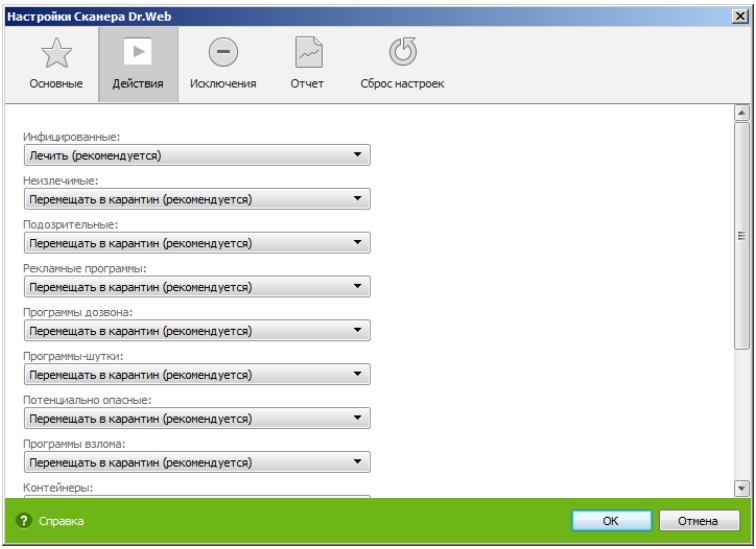


Вы можете включить звуковое сопровождение событий, а также указать **Сканеру Dr.Web** автоматически применять действия к угрозам и настроить взаимодействие программы с операционной системой.

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

Настройка обезвреживания угроз

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

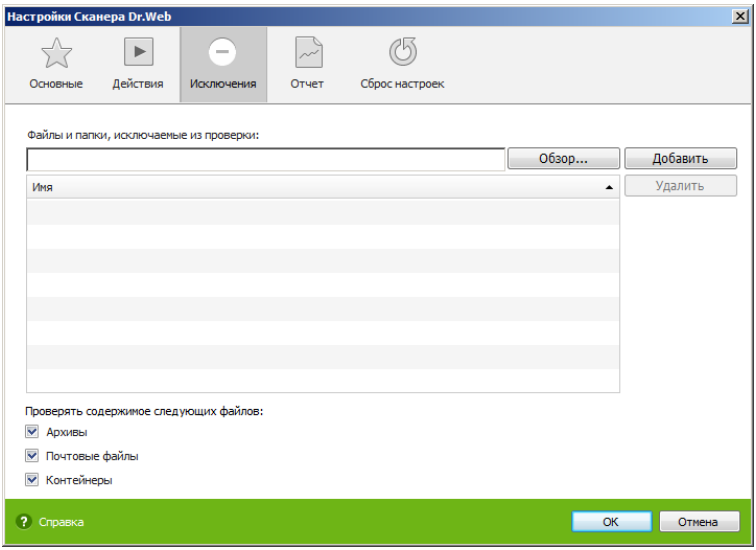


2. Выберите в выпадающем списке **Инфицированные** реакцию **Сканера** на обнаружение инфицированного объекта.
3. Выберите в выпадающем списке **Неизлечимые** реакцию **Сканера** на обнаружение неизлечимого объекта. Это действие аналогично рассмотренному в предыдущем пункте, с той разницей, что вариант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

6. Аналогично настраиваются автоматические действия **Сканера** при обнаружении вирусов или подозрительного кода в файловых архивах, инсталляционных пакетах и почтовых ящиках. Действия по отношению к вышеуказанным объектам выполняются над всем объектом, а не только над зараженной его частью. По умолчанию во всех этих случаях предусмотрено информирование.
7. Для успешного завершения лечения некоторых зараженных (инфицированных) файлов требуется перезагрузка операционной системы. Вы можете выбрать один из вариантов:
   - **Перезагружать компьютер автоматически.** Этот режим может привести к потере несохраненных данных;
   - **Предлагать перезагрузку**.

Вкладка Исключения

На этой вкладке задаются дополнительные ограничения на состав файлов, подлежащих проверке.

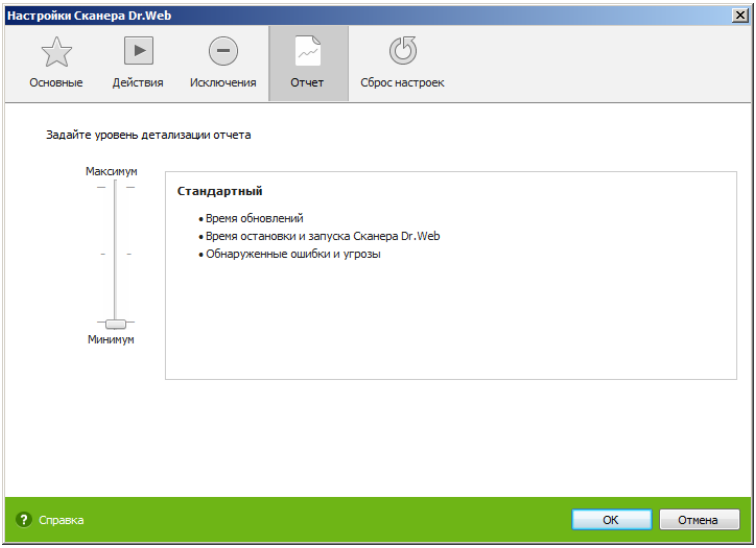


Здесь можно задать список файлов (масок файлов), которые не будут проверяться (из проверки будут исключены все файлы с данным именем.) В таком качестве могут выступать временные файлы (файлы подкачки) и т. п.

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

Вкладка Отчет

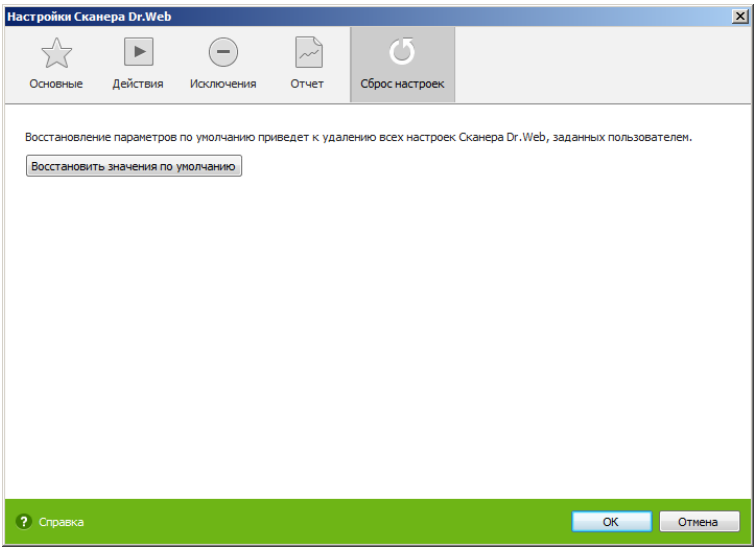
На этой вкладке вы можете настроить параметры ведения файла отчета.



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

Вкладка Сброс настроек

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



4.4. Запуск Сканера из командной строки

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

Запуск Сканера из командной строки

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

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

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

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

4.5. Консольный сканер

Также в состав программы **Антивирус Dr.Web для серверов** 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

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

Список объектов для проверки может быть пуст или содержать несколько элементов, разделенных пробелами.
Все ключи командной строки начинается с символа «/» и разделяются пробелами. Список ключей **Консольного сканера** содержится в Приложении А.

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

0 – проверка успешно завершена, инфицированные объекты не найдены;

1 – проверка успешно завершена, найдены инфицированные объекты;

10 – указаны некорректные ключи;

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

12 – не запущен **Scanning Engine**;

255 – проверка прервана пользователем.

4.6. Запуск проверки по расписанию

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

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

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

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

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

5. SpIDer Guard

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

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

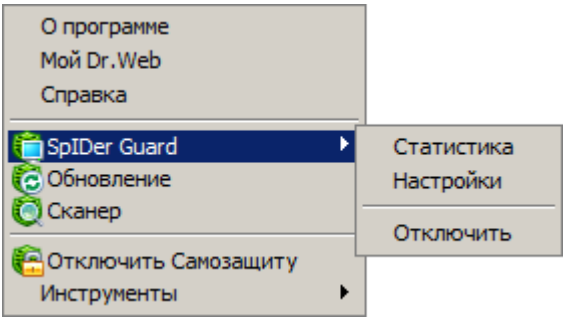
Соответствующим изменением настроек вы можете задать автоматическую реакцию сторожа **SpIDer Guard** на вирусные события. Вы сможете следить за ней с помощью окна статистики и файла отчета.

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

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

5.1. Управление SpIDer Guard

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



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

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

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

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

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

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

5.2. Настройка SpIDer Guard

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

Изменение настроек сторожа

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

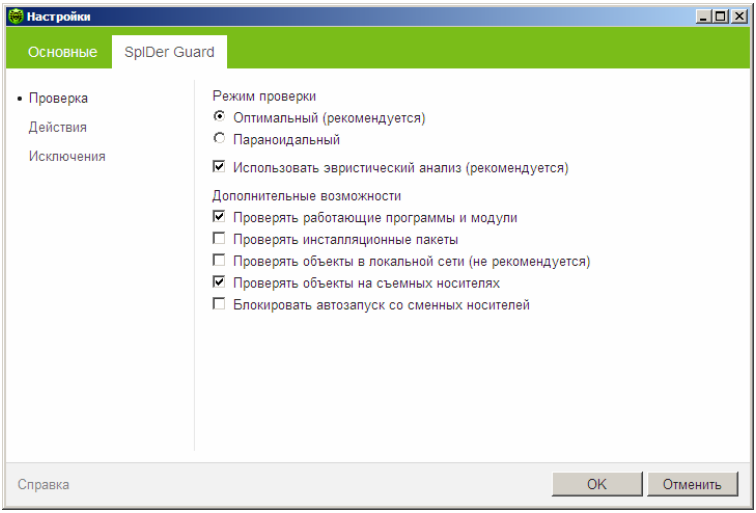
Раздел Проверка

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

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

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

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



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

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

Здесь вы можете задать проверку:

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

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

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

Настройка действий

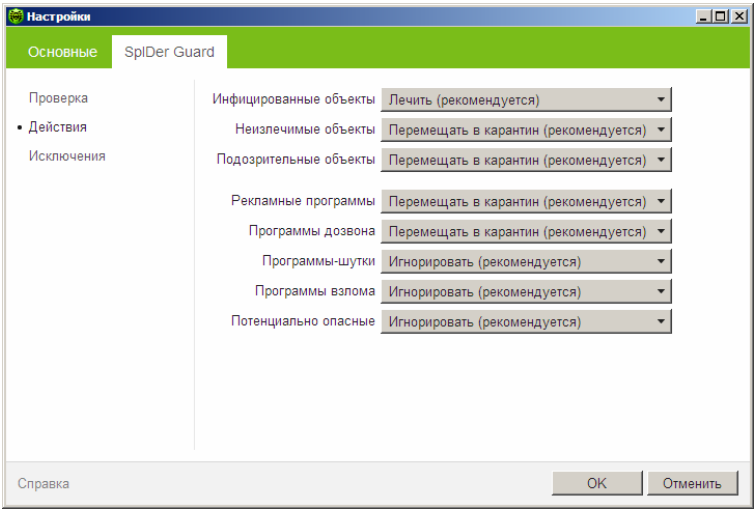
В разделе **Действия** вы можете настроить автоматические действия сторожа с зараженными объектами.

Состав доступных реакций зависит от типа вирусного события.

Реакции **Лечить**, **Перемещать в карантин, Игнорировать** и **Удалить** аналогичны таким же реакциям **Сканера**. Действия с обнаруженными угрозами рассмотрены выше, см. Действия для обезвреживания угроз.

Изменение настроек сторожа

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



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

Задание исключений

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

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

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

Вы можете формировать список исключений следующим образом:

- чтобы указать конкретный существующий каталог или файл, нажмите кнопку **Обзор** и выберите каталог или файл в стандартном окне открытия файла. Вы можете вручную ввести полный путь к файлу или каталогу в поле ввода, а также отредактировать запись в поле ввода перед добавлением ее в список;
- чтобы исключить из проверки все файлы или каталоги с определенным именем, введите это имя в поле ввода. Указывать путь к каталогу или файлу при этом не требуется;
- чтобы исключить из проверки файлы или каталоги определенного вида, введите определяющую их маску в поле ввода. Маска задает общую часть имени объекта. При этом:
    - символ «*» заменяет любую, возможно пустую, последовательность символов;
    - символ «?» заменяет любой, но только один символ;

- остальные символы маски ничего не заменяют и означают, что на данном месте в имени файла или каталога должен находиться именно этот символ.

Пример:

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

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

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

6. Автоматическое обновление

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

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

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

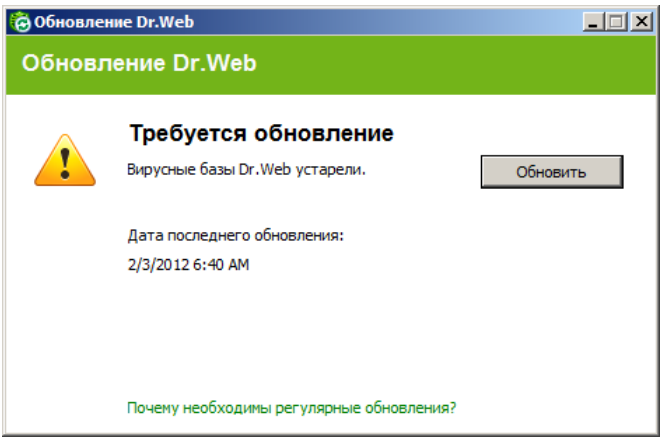
6.1. Запуск обновления

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

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

После запуска **Модуля обновления** появится диалоговое окно, в котором отображается информация об актуальности вирусных баз и компонентов, а также дата последнего обновления. При необходимости из этого окна вы можете запустить обновление. Настроить необходимые параметры вы можете в разделе **Обновление** Основных настроек работы программы.

Отчёт записывается в файл dwupdater.log, который находится в каталоге %allusersprofile%\Application Data\Doctor Web\Logs\ (в Windows Server 2008 в каталоге %allusersprofile%\Doctor Web\Logs\).



Запуск обновления

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

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

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

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

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

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

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

Приложения

Приложение А. Дополнительные параметры командной строки

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

Ключи начинаются с символа «/» и, как и остальные параметры командной строки, разделяются пробелами. Параметры перечислены в алфавитном порядке.

Параметры для 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:` <*число*> – максимальный уровень сжатия. Если сканер определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка не производится. По умолчанию – без ограничений.
- `/ARL:` <*число*> – максимальный уровень вложенности проверяемого архива. По умолчанию – без ограничений.

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

- /LITE – произвести стартовую проверку системы, при которой проверяются оперативная память, загрузочные секторы всех дисков, а также провести проверку на наличие руткитов. (Только для **Сканера**).
- /LN – проверять файлы, на которые указывают ярлыки. По умолчанию – опция отключена.
- /LS – проверять под учетной записью LocalSystem. По умолчанию опция отключена.
- /MA – проверять почтовые файлы. По умолчанию опция включена.
- /MC: <*число*> – установить максимальное число попыток вылечить файл. По умолчанию – без ограничений.
- /NB – не создавать резервные копии вылеченных/ удаленных файлов. По умолчанию опция отключена.
- /NI[:X] – уровень использования ресурсов системы, в процентах. Определяет количество памяти используемой для проверки и системный приоритет задачи проверки. По умолчанию – без ограничений.
- /NOREBOOT – отменяет перезагрузку и выключение после проверки. (Только для **Сканера**).
- /NT – проверять NTFS-потоки. По умолчанию опция включена.
- /OK – выводить полный список проверяемых объектов, сопровождая незараженные пометкой **Ok**. По умолчанию опция отключена.
- /P: <*приоритет*> – приоритет запущенной задачи проверки в общей очереди задач на проверку:
  - *0* – низший.
  - *L* – низкий.
  - *N* – обычный. Приоритет по умолчанию.
  - *H* – высокий.
  - *M* – максимальный.
- /PAL: <*число*> – максимальный уровень вложенности упаковщиков исполняемого файла. Если уровень вложенности превышает указанный, проверка будет производиться только до указанного уровня вложенности. По умолчанию – 1000.

- /RA: *<имя файла>* – дописать отчет о работе программы в указанный файл. По умолчанию отчет не создается.
- /RP: *<имя файла>* – записать отчет о работе программы в указанный файл. По умолчанию отчет не создается.
- /RPC: *<число>* – таймаут соединения с Scanning Engine, в секундах. По умолчанию – 30 секунд. (Только для **Консольного Сканера**).
- /RPCD – использовать динамический идентификатор RPC. (Только для **Консольного Сканера**).
- /RPCE – использовать динамический целевой адрес RPC. (Только для **Консольного Сканера**).
- /RPCE: *<целевой_адрес>* – использовать указанный целевой адрес RPC. (Только для **Консольного Сканера**).
- /RPCH: *<имя_хоста>* – использовать указанное имя хоста для вызовов RPC. (Только для **Консольного Сканера**).
- /RPCP: *<протокол>* – использовать указанный протокол RPC. Возможно использование протоколов: lpc, np, tcp. (Только для **Консольного Сканера**).
- /QL – вывести список всех файлов, помещенных в карантин на всех дисках. (Только для **Консольного Сканера**).
- /QL: *<имя_логического_диска>* – вывести список всех файлов, помещенных в карантин на указанном логическом диске. (Только для **Консольного Сканера**).
- /QNA – выводить пути в двойных кавычках.
- /QR[:[d][:p]] – удалить файлы с указанного диска *<d> (имя_логического_диска)*, находящие в карантине дольше *<p> (количество)* дней. Если *<d>* и *<p>* не указаны, то будут удалены все файлы, находящиеся в карантине, со всех логических дисков. (Только для **Консольного Сканера**).
- /QUIT – закрыть **Сканер** после проверки (вне зависимости от того, были ли применены действия к обнаруженным угрозам). (Только для **Сканера**).
- /REP – проверять по символьным ссылкам. По умолчанию опция отключена.

- `/SCC` – выводить содержимое составных объектов. По умолчанию опция отключена.
- `/SCN` – выводить название инсталляционного пакета. По умолчанию – опция отключена.
- `/SILENTMODE` – запустить проверку в фоновом режиме. Если при проверке будут обнаружены угрозы, откроется окно **Сканера Dr.Web** со списком угроз. В противном случае окно не будет отображено. (Только для **Сканера**).
- `/SLS` – выводить логи на экран. По умолчанию – опция включена. (Только для **Консольного Сканера**).
- `/SPN` – выводить название упаковщика. По умолчанию – опция включена.
- `/SPS` – отображать процесс проведения проверки. По умолчанию – опция включена. (Только для **Консольного Сканера**).
- `/SST` – выводить время проверки файла. По умолчанию – опция отключена.
- `/TB` – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.
- `/TM` – выполнять поиск угроз в оперативной памяти (включая системную область Windows).
- `/TR` – проверять системные точки восстановления.
- `/W:`*<число>* – максимальное время проверки, в секундах. По умолчанию – без ограничений.
- `/WCL` – вывод, совместимый с drwebwcl. (Только для **Консольного Сканера**).
- `/X:S[:R]` – по окончании проверки перевести машину в указанный режим: выключение/перезагрузка/ждущий режим/спящий режим.

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

- /AAD: <*действие*> – действия для рекламных программ (возможные действия: *DQIR*, по умолчанию – информирование)
- /AAR: <*действие*> – действия с инфицированными архивами (возможные действия: *DQIR*, по умолчанию – информирование)
- /ACN: <*действие*> – действия с инфицированными инсталляционными пакетами (возможные действия: *DQIR*, по умолчанию – информирование)
- /ADL: <*действие*> – действия с программами дозвона (возможные действия: *DQIR*, по умолчанию – информирование)
- /AHT: <*действие*> – действия с программами взлома (возможные действия: *DQIR*, по умолчанию – информирование)
- /AIC: <*действие*> – действия с неизлечимыми файлами (возможные действия: *DQR*, по умолчанию – информирование)
- /AIN: <*действие*> – действия с инфицированными файлами (возможные действия: *CDQR*, по умолчанию – информирование)
- /AJK: <*действие*> – действия с программами-шутками (возможные действия: *DQIR*, по умолчанию – информирование)
- /AML: <*действие*> – действия с инфицированными почтовыми файлами (возможные действия: *QIR*, по умолчанию – информирование)
- /ARW: <*действие*> – действия с потенциально опасными файлами (возможные действия: *DQIR*, по умолчанию – информирование)

- /ASU: *<действие>* – действия с подозрительными файлами (возможные действия: *DQIR*, по умолчанию – информирование)

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

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

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

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

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

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

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

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

Параметры для Модуля обновления

Общие параметры:

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

Параметры команды инициализации (init):

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

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

Параметры команды обновления (update):

Параметр	Описание
-p [--product] arg	Название продукта. Если название указано, то будет произведено обновление только этого продукта. Если продукт не указан и не указаны конкретные компоненты, будет произведено обновление всех продуктов. Если указаны компоненты, будет произведено обновление указанных компонентов.
-n [--component] arg	Перечень компонентов, которые необходимо обновить до определенной модификации. Формат: *<name>*, *<target revision>*.

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

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

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

Приложение Б. Угрозы и способы их обезвреживания

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

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

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

Классификация угроз

Компьютерные вирусы

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

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

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

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

Большинство вирусов обладают той или иной защитой от обнаружения. Способы защиты постоянно совершенствуются и вместе с ними разрабатываются новые технологии борьбы.

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

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

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

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

Компьютерные черви

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

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

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

Троянские программы (троянские кони, трояны)

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

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

Руткит

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

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

Программы взлома

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

Шпионские программы

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

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

Рекламные программы

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

Программы-шутки

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

Программы дозвона

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

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

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

Ниже приведены некоторые виды хакерских атак и интернет-мошенничества:

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

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

Действия для обезвреживания угроз

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

1. *Лечение* – действие, применяемое к вирусам, червям и троянам. Оно подразумевает удаление вредоносного кода из зараженных файлов либо удаление функциональных копий вредоносных программ, а также, по возможности, восстановление работоспособности пораженных объектов (т. е. возвращение структуры и функционала программы к состоянию, которое было до заражения). Далеко не все вредоносные программы могут быть вылечены, однако именно продукты **«Доктор Веб»** предоставляют самые эффективные алгоритмы лечения и восстановления файлов, подвергшихся заражению.

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

Приложение В. Принципы именования угроз

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

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

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

Основные префиксы

Префиксы операционной системы

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

- `Win` – 16-разрядные программы ОС Windows 3.1;
- `Win95` – 32-разрядные программы ОС Windows 95, ОС Windows 98, ОС Windows Me;
- `WinNT` – 32-разрядные программы ОС Windows NT, ОС Windows 2000, ОС Windows XP, ОС Windows Vista;
- `Win32` – 32-разрядные программы различных сред ОС Windows 95, ОС Windows 98, ОС Windows Me и ОС Windows NT, ОС Windows 2000, ОС Windows XP, ОС Windows Vista;
- `Win32.NET` – программы в 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;
- HLLO – вирусы, перезаписывающие код программы жертвы;
- HLLP – вирусы-паразиты;
- HLLC – вирусы-спутники.

К группе префиксов языка разработки можно также отнести:

- Java – вирусы для среды виртуальной машины Java.

Троянские кони

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

- PWS – троянец, ворующий пароли;
- Backdoor – троянец с RAT-функцией (*Remote Administration Tool* – утилита удаленного администрирования);
- IRC – троянец, использующий для своего функционирования среду Internet Relayed Chat channels;

- DownLoader – троянец, скрытно от пользователя загружающий различные вредоносные файлы из Интернета;
- MulDrop – троянец, скрытно от пользователя загружающий различные вирусы, содержащиеся непосредственно в его теле;
- Proxy – троянец, позволяющий злоумышленнику 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.

Приложение Г. Техническая поддержка

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

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

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

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

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