



Dr.WEB

Антивирус для серверов Windows

Руководство администратора

Жасағаныңды қорға

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© «Доктор Веб», 2017. Все права защищены

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

Товарные знаки

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

Ограничение ответственности

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

Версия 11.0

Руководство администратора

06.09.2017

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: <http://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	6
1.1. О чем эта документация	7
1.2. Используемые обозначения и сокращения	8
1.3. Методы обнаружения	8
2. Системные требования	11
3. Установка, изменение и удаление программы	13
3.1. Первая установка	13
3.2. Удаление или изменение программы	16
4. Лицензирование	18
4.1. Способы активации	19
4.2. Продление лицензии	19
4.3. Мастер регистрации	20
5. Начало работы	21
5.1. Проверка антивируса	22
6. Инструменты	24
6.1. Менеджер лицензий	24
6.2. Защита от потери данных	25
6.3. Антивирусная сеть	27
6.4. Менеджер карантина	28
6.5. Поддержка	29
6.5.1. Создание отчета	30
7. Обновление	33
8. Сканер Dr.Web	35
8.1. Запуск проверки	35
8.2. Действия при обнаружении угроз	37
8.3. Запуск Сканера с параметрами командной строки	38
8.4. Консольный сканер	39
8.5. Запуск проверки по расписанию	40
9. Настройки	41
10. Основные настройки	42
10.1. Уведомления	42
10.2. Обновление	45



10.3. Сеть	47
10.4. Самозащита	48
10.5. Dr.Web Cloud	50
10.6. Антивирусная сеть	51
10.7. Устройства	51
10.8. Дополнительно	53
11. Исключения	57
11.1. Файлы и папки	57
11.2. Приложения	59
12. Компоненты защиты	62
12.1. SpIDer Guard	62
12.1.1. Настройка SpIDer Guard	62
12.2. Сканер	67
12.3. Превентивная защита	69
13. Статистика	75
Приложения	76
Приложение А. Дополнительные параметры командной строки	76
Параметры для Сканера и Консольного сканера	76
Параметры для Модуля обновления	82
Коды возврата	85
Приложение Б. Угрозы и способы их обезвреживания	87
Классификация угроз	87
Действия для обезвреживания угроз	92
Приложение В. Принципы именования угроз	93



1. Введение

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

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

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

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

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

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

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

SpIDer Guard – антивирусный сторож, который постоянно находится в оперативной памяти, осуществляя проверку создаваемых файлов и запускаемых процессов, а также обнаруживая проявления вирусной активности.

Модуль обновления – компонент, который позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов Dr.Web, а также производит их автоматическую установку.

Агент Dr.Web – модуль управления, с помощью которого осуществляется запуск и настройка компонентов программы Dr.Web.

Превентивная защита – компонент, контролирующий доступ к критически важным объектам системы, обеспечивающий целостность запущенных приложений и файлов пользователя, а также защиту от эксплойтов.



1.1. О чем эта документация

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

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

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

В Приложениях содержится подробная справочная информация по настройке программы Dr.Web.



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 этом руководстве используются следующие обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
<i>Сигнатура</i>	Новый термин или акцент на термине в описаниях.
<ключевой_файл>	Поля для замены функциональных названий фактическими значениями.
Далее	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
C:\Windows\	Наименования файлов и каталогов, фрагменты программного кода.
<u>Приложение А</u>	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

1.3. Методы обнаружения

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

Методы обнаружения угроз

Сигнатурный анализ

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

Origins Tracing

Это уникальная технология Dr.Web, которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах



механизмы заражения или вредоносное поведение. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения Dr.Web, от таких угроз, как троянская программа-вымогатель Trojan.Encoder.18 (также известная под названием «gprcode»). Кроме того, использование технологии Origins Tracing позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing, добавляется постфикс `.Origin`.

Эмуляция исполнения

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

Эвристический анализ

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

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

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



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



2. Системные требования



Перед установкой программы Dr.Web следует:

- удалить с компьютера другие антивирусные программы для предотвращения возможной несовместимости их резидентных компонентов с резидентными компонентами Dr.Web;
- в Windows Server 2016 отключить Защитник Windows вручную, используя групповые политики;
- установить все рекомендуемые производителем операционной системы критические обновления; если поддержка операционной системы производителем прекращена, рекомендуется перейти на более современную версию операционной системы.

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

Компонент	Требование
Процессор	Полная поддержка системы команд i686.
Операционная система	Для 32-разрядных операционных систем: • Windows Server 2003 с пакетом обновлений SP1; • Windows Server 2008 с пакетом обновлений SP2 или выше. Для 64-разрядных операционных систем: • Windows Server 2008 с пакетом обновлений SP2 или выше; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016.
Свободная оперативная память	512 МБ и больше.
Место на жестком диске	750 МБ для размещения компонентов продукта. Файлы, создаваемые в ходе установки, потребуют дополнительного места.
Разрешение	Рекомендуемое разрешение экрана не менее 800x600.



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.



Для обеспечения правильной работы Dr.Web должны быть открыты следующие порты:

Назначение	Направление	Номера портов
Для обновления (если включена опция обновления по https)	исходящий	443
Для обновления	исходящий	80
Для отправки почтовых уведомлений		25 или 465 (либо в зависимости от настроек почтовых уведомлений)
Для соединения с облачным сервисом Dr.Web Cloud	исходящие	2075 (в том числе для UDP)

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



3. Установка, изменение и удаление программы

Перед установкой Dr.Web обратите внимание на [системные требования](#), а также настоятельно рекомендуется:

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



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

3.1. Первая установка



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

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

- в обычном режиме;
- с параметрами командной строки.

Установка с параметрами командной строки

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

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

```
drweb-11.0-srv-win.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 **Отменить**.

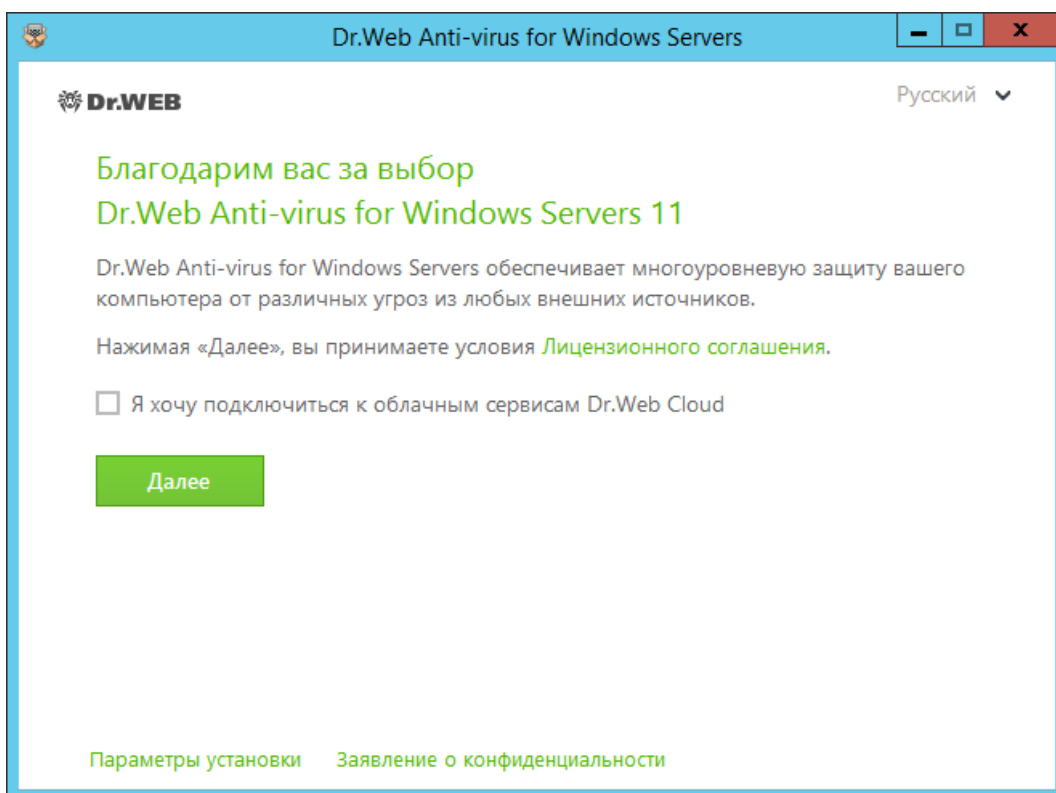
Процедура установки

1. Если на вашем компьютере уже установлен другой антивирус, Мастер установки предупредит вас о несовместимости программы Dr.Web и иных антивирусных решений и предложит удалить их.



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

2. На этом шаге вы можете подключиться к облачным сервисам Dr.Web, которые позволяют осуществлять проверку данных, используя наиболее свежую информацию об угрозах, которая обновляется на серверах компании «Доктор Веб» в режиме реального времени. Опция выключена по умолчанию.



3. Для того чтобы самостоятельно выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры, нажмите **Параметры установки**.



Данная опция предназначена для опытных пользователей. Если вы хотите произвести установку с параметрами по умолчанию, перейдите к пункту 4.

- На первой вкладке вы можете изменить состав устанавливаемых компонентов.
- На второй вкладке вы можете изменить путь установки.
- На третьей вкладке окна установлен флажок **Загрузить обновления во время установки**, чтобы в процессе установки были загружены актуальные вирусные базы и другие модули антивируса. Вам будет предложено настроить создание ярлыков для запуска программы Dr.Web.

Чтобы сохранить изменения, нажмите **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите **Отменить**.

4. Нажмите кнопку **Далее**. Обратите внимание, что тем самым вы принимаете условия лицензионного соглашения.
5. В окне **Мастер регистрации** программа установки предупредит вас о том, что для работы программы Dr.Web необходима лицензия. Выполните одно из следующих действий:
 - если у вас есть ключевой файл и он находится на жестком диске или съемном носителе, выберите **Указать путь к действующему ключевому файлу** и в стандартном окне открытия файла выберите ключевой файл. Для изменения пути нажмите кнопку **Обзор** и выберите другой ключевой файл;
 - для продолжения установки без ключевого файла выберите **Получить лицензию позднее**. В этом случае ни один компонент программы не будет работать до тех пор, пока вы не укажете действительный ключевой файл.

Нажмите кнопку **Далее**.



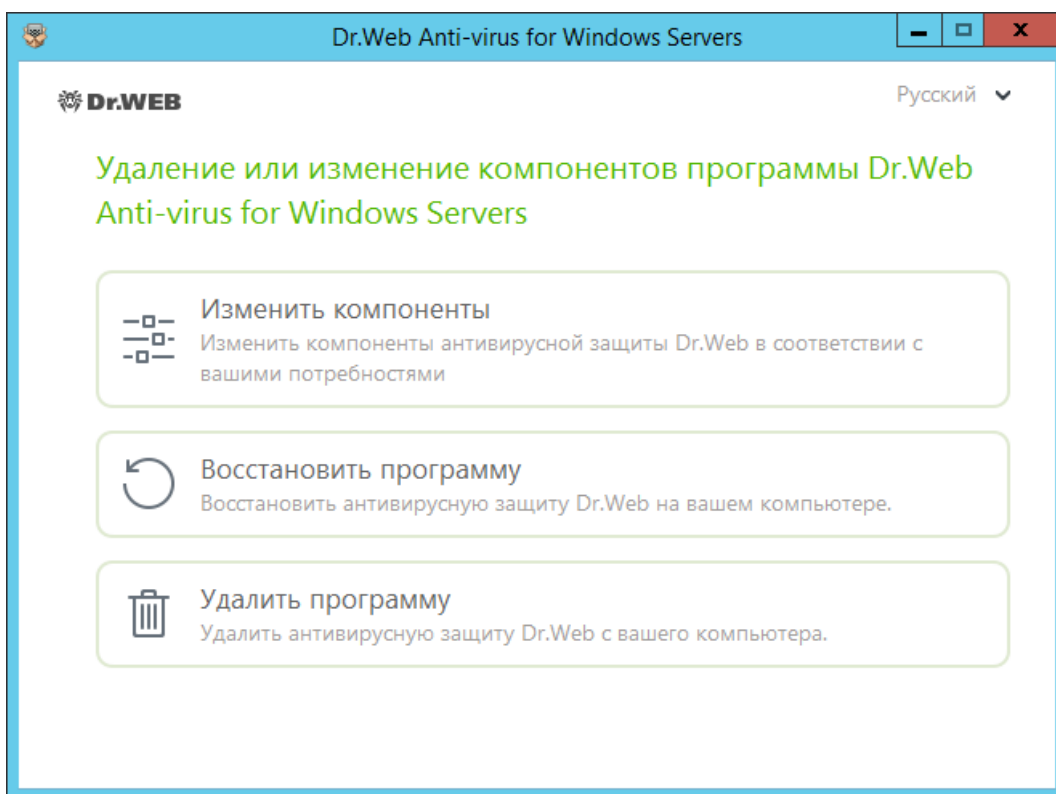
6. Если необходимо задать параметры прокси-сервера, установите флажок **Задать IP-адрес и порт прокси-сервера вручную**. Нажмите кнопку **Установить**.
7. Если в процессе установки вы указали действующий ключевой файл и не снимали флажок **Загрузить обновления во время установки**, будет выполнен процесс обновления вирусных баз и других компонентов программы Dr.Web. Обновление проводится автоматически и не требует дополнительных действий.
8. Для завершения процесса установки выполните перезагрузку компьютера.

3.2. Удаление или изменение программы



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

1. Для удаления или изменения конфигурации Dr.Web путем добавления и удаления отдельных компонентов, запустите компонент удаления программ операционной системы Windows.
2. В открывшемся списке выберите строку с названием программы. Далее для удаления программы полностью нажмите кнопку **Удалить** и перейдите к шагу 6. А для изменения конфигурации Dr.Web, путем добавления и удаления отдельных компонентов, нажмите кнопку **Изменить**, при этом откроется окно Мастера удаления/изменения компонентов программы.





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



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

5. Чтобы удалить все установленные компоненты, выберите пункт **Удалить программу**.
6. В окне **Сохраняемые параметры** установите флажки напротив того, что следует сохранить после удаления программы. Сохраненные объекты и настройки могут использоваться программой при повторной установке. По умолчанию выбраны все опции – **Карантин, Настройки Dr.Web Anti-virus for Windows Servers** и **Защищаемые копии файлов**. Нажмите кнопку **Установить**.
7. В следующем окне для подтверждения удаления Dr.Web введите изображенный код, после чего нажмите кнопку **Удалить программу**.
8. Изменения вступят в силу после перезагрузки компьютера. Процесс перезагрузки можно отложить, нажав кнопку **Позже**. Нажмите кнопку **Перезагрузить сейчас** для немедленного завершения процедуры удаления или изменения состава компонентов Dr.Web.



4. Лицензирование

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

Ключевой файл

Права пользователя на использование Dr.Web хранятся в специальном файле, называемом *ключевым файлом*. При получении ключевого файла в комплекте дистрибутива продукта установка ключевого файла производится автоматически и никаких дополнительных действий не требует.

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

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



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

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

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

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

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

Рекомендуется сохранять *ключевой файл* до истечения срока действия лицензии.



4.1. Способы активации

Активировать лицензию вы можете одним из следующих способов:

- получив ключевой файл во время регистрации лицензии на официальном [сайте](#) «Доктор Веб»;
- указав путь к имеющемуся у вас действительному ключевому файлу в процессе установки либо в [Мастере регистрации](#).

Повторная активация

Повторная активация лицензии может потребоваться в случае утраты ключевого файла.



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

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

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

4.2. Продление лицензии

В некоторых случаях, например, при окончании срока действия лицензии или при изменении характеристик защищаемой системы или требований к ее безопасности, вы можете принять решение о приобретении новой или расширенной лицензии на Dr.Web. В таком случае вам потребуется заменить текущий ключевой файл. Dr.Web поддерживает обновление лицензии на лету, при котором не требуется переустанавливать Dr.Web или прерывать его работу.

Замена ключевого файла

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



4.3. Мастер регистрации

Модуль управления SpIDer Agent после старта проверяет наличие [ключевого файла](#). При его отсутствии модуль предлагает получить ключевой файл через Интернет.

Вы можете указать ключевой файл в процессе установки. Для этого [на 5 шаге](#) установки выберите пункт **Укажите путь к действительному ключевому файлу**.

Вы также можете указать ключевой файл после установки продукта:

1. В [меню](#) SpIDer Agent  выберите пункт **Лицензия**. Откроется окно Менеджера лицензий.
2. Нажмите кнопку **Купить или активировать новую лицензию**. Откроется окно Мастера регистрации.

Активация лицензии



Пользователям Windows XP для активации лицензии необходимо указать действительный ключевой файл, а не серийный номер. Если ключевого файла нет, но есть серийный номер, его необходимо активировать на [сайте](#) компании «Доктор Веб».

Если у вас имеется ключевой файл для активации лицензии, укажите путь к действующему ключевому файлу и нажмите кнопку **Готово**.

Новая лицензия

Чтобы приобрести новую лицензию, продлить или расширить текущую лицензию со скидкой в онлайн-магазине компании «Доктор Веб», нажмите кнопку **Купить**.



5. Начало работы

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



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

Значок SpIDer Agent отражает текущее состояние Dr.Web:

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

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

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



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

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

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

Лицензия. Открывает [Менеджер лицензий](#).

Инструменты. Открывает меню, предоставляющее доступ:

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



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

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

Сканер. Быстрый доступ к запуску разных типов проверки.

Режим работы . Позволяет переключаться между режимом пользователя и режимом администратора. По умолчанию Dr.Web запускается в ограниченном режиме – режиме пользователя, в котором недоступны [Настройки](#) и настройки [Компонентов защиты](#). Для переключения в другой режим, нажмите на замок. При включенном UAC операционная система выдаст запрос на повышение прав. Также для изменения режима потребуется ввести пароль, если в разделе [Настройки](#) вы включили опцию **Защищать паролем настройки Dr.Web**.

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

Настройки . Открывает окно с доступом к основным настройкам, настройкам компонентов защиты и исключениям.



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

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

Справка . Открывает справку.

5.1. Проверка антивируса

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

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



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

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

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

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



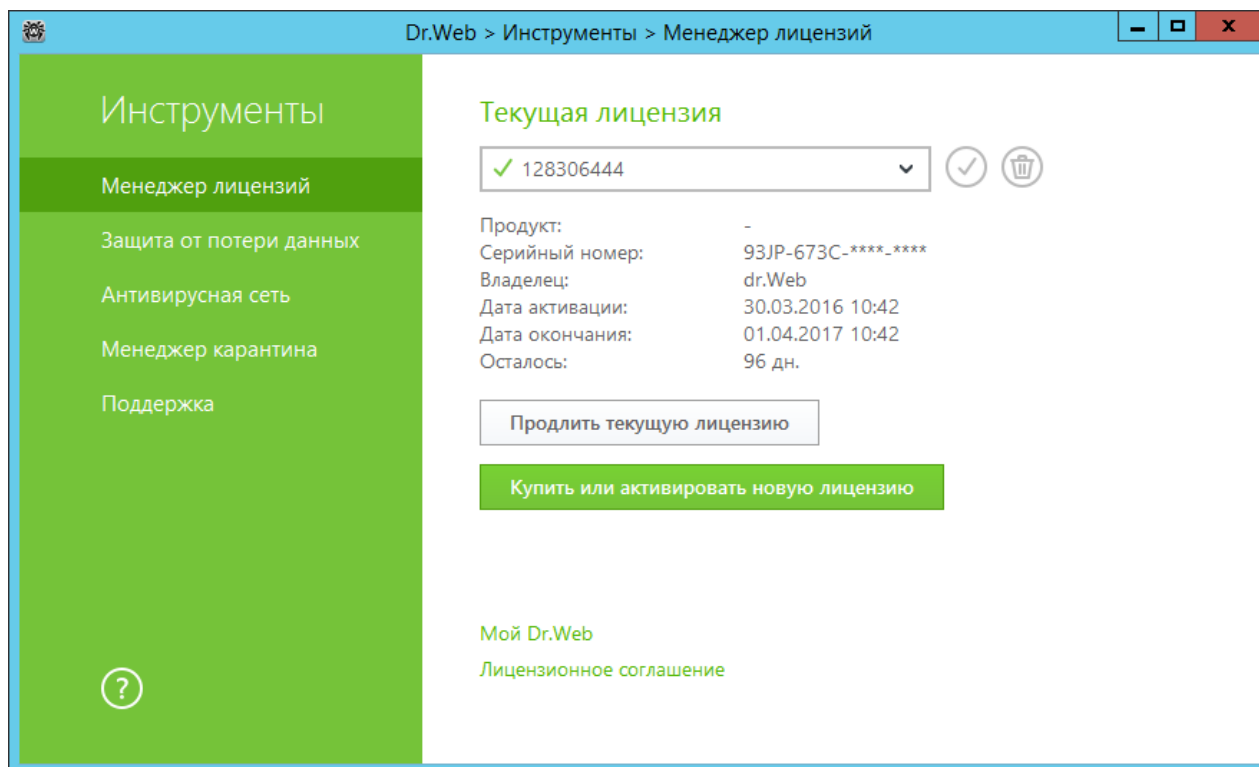
При работе в [оптимальном режиме](#) SpIDer Guard не прерывает запуск тестового файла EICAR и не определяет данную операцию как опасную, так как данный файл не представляет угрозы для компьютера. Однако при копировании или создании такого файла на компьютере SpIDer Guard автоматически обрабатывает файл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



6. Инструменты

6.1. Менеджер лицензий

В этом окне вы можете просмотреть информацию обо всех [лицензиях](#) Dr.Web, хранящихся на вашем компьютере, а также изменить текущую лицензию, продлить ее или купить новую и активировать для использования.



Чтобы просмотреть информацию о лицензии, которая на данный момент не является текущей, выберите ее в выпадающем списке. В режиме администратора кнопка  позволяет удалить просматриваемую лицензию, а  - назначить ее текущей. Обратите внимание, что последнюю действующую лицензию удалить нельзя.

При нажатии кнопки **Купить или активировать новую лицензию** программа откроет окно [Мастера регистрации](#), который подскажет вам дальнейшие действия.

При нажатии кнопки **Продлить текущую лицензию** программа откроет страницу на сайте компании «Доктор Веб», на которую будут переданы параметры используемой лицензии.

Дополнительно

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



Ссылка **Лицензионное соглашение** открывает текст соглашения на сайте компании «Доктор Веб».

6.2. Защита от потери данных

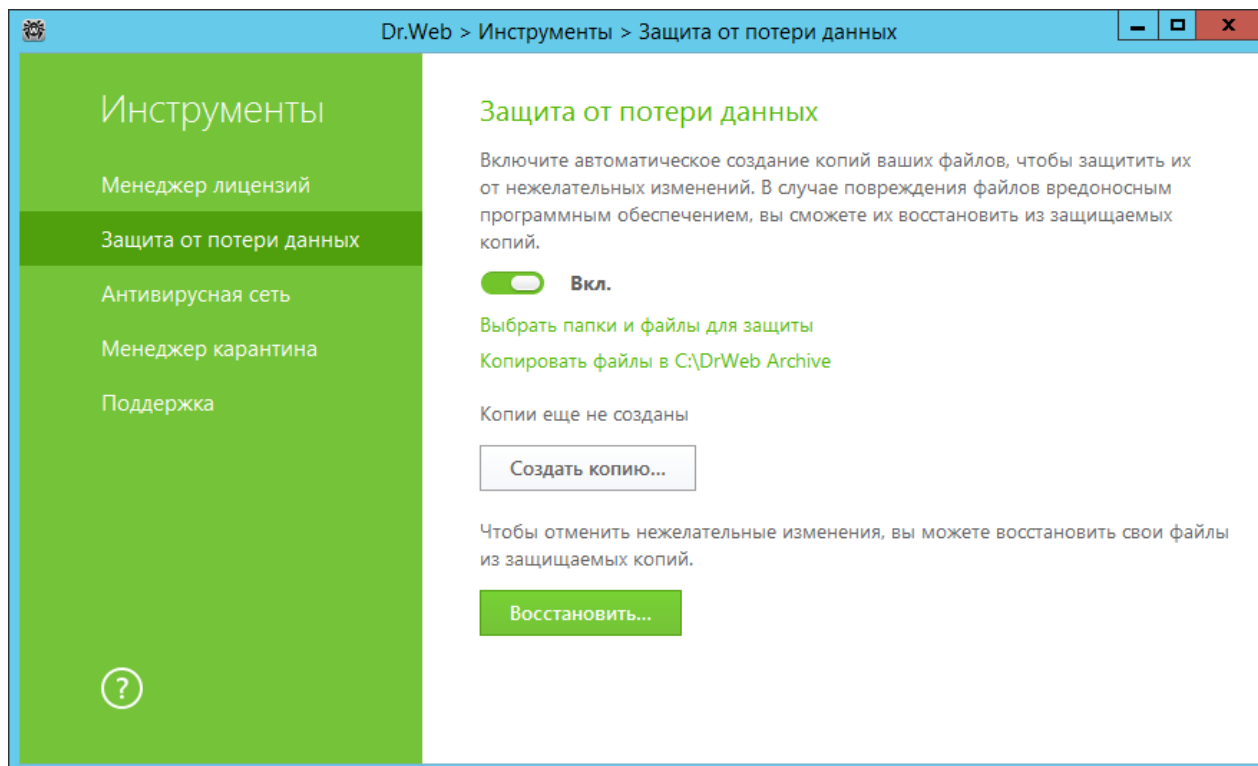


В режиме пользователя невозможно изменить параметры защиты, а также восстановить файлы из копии. Для выполнения этих действий переключитесь в [режим администратора](#).

Защита от потери данных - функция, которая обеспечивает защиту важных файлов от изменений вредоносным программным обеспечением. Эта функция позволяет создавать копии содержимого выбранных вами папок.



Если файл заблокирован на момент создания копии, то он не попадет в резервную копию.



Формирование списка папок и файлов для защиты

Нажмите ссылку **Выбрать папки и файлы для защиты**, чтобы указать объекты, для которых будут созданы защищаемые копии:

- чтобы добавить файл или папку, нажмите кнопку и выберите нужный объект;
- чтобы удалить объект из списка, выберите его и нажмите кнопку .



В любой момент вы можете изменить список объектов.

Параметры создания копий

Нажмите ссылку **Копировать файлы в C:\DrWeb Archive**. В открывшемся окне укажите необходимые параметры.

1. Задайте общие параметры для создаваемых копий:

- укажите диск для хранения копий;
- укажите периодичность, с которой копии объектов будут создаваться. Через указанный промежуток времени Dr.Web будет проверять заданные объекты на наличие изменений и создавать копию, если изменения были внесены;
- при необходимости запретите запуск создания копий при работе от батареи.

2. Задайте ограничения, которые позволят ограничить размер используемого места на диске:

- укажите максимально допустимый объём места на диске, который вы хотите выделить для хранения копий;
- при необходимости вы можете задать ограничение на количество копий;
- выберите одно из действий: в случае превышения одного из указанных ограничений новые копии либо не будут создаваться, либо будут перезаписывать уже существующие копии (начиная с самой старой).

Удаление созданных копий

Вы можете удалить существующие копии, чтобы очистить место на диске (на самих файлах удаление копий не отразится). Для этого нажмите **Копировать файлы в C:\DrWeb Archive**, затем нажмите **Удалить копии**.

Восстановление файлов

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

Запуск создания копий вручную

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



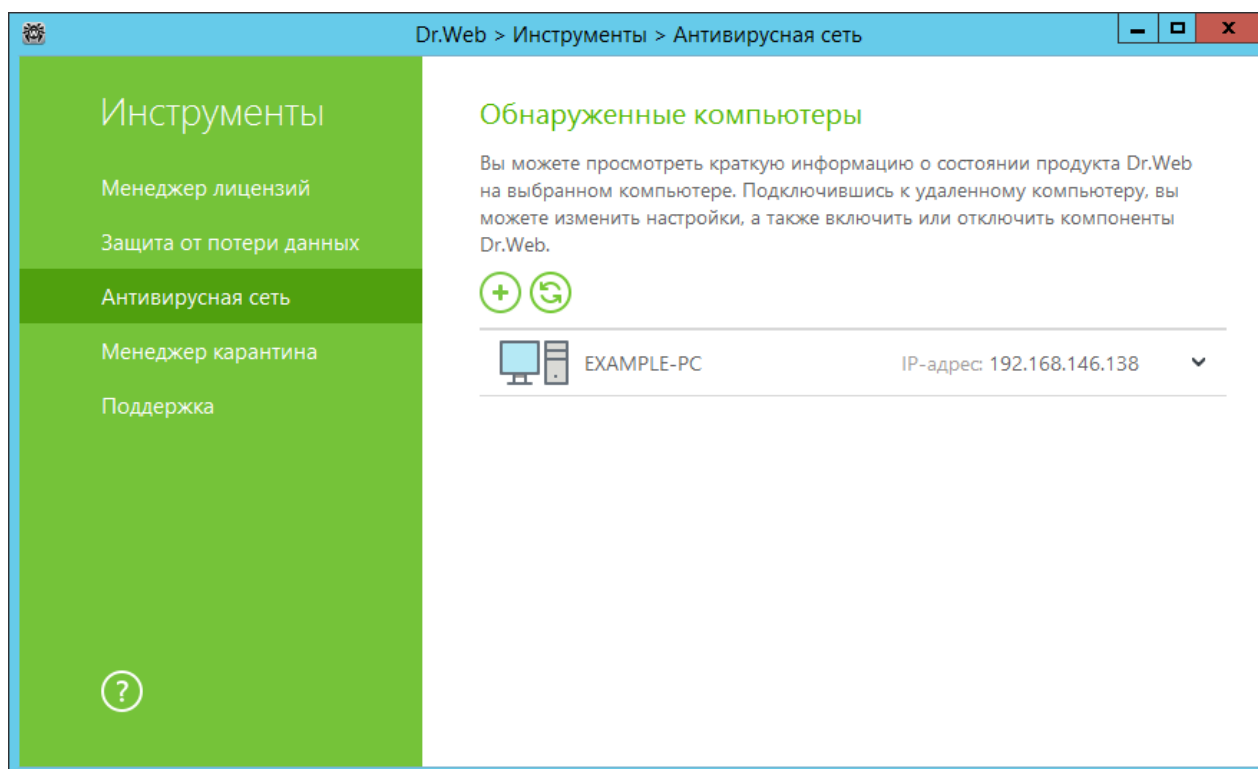
Для работы системы **Защиты от потери данных** требуется не менее 20 ГБ свободного места на том диске, который вы выбрали для хранения копий.



6.3. Антивирусная сеть

Этот компонент позволяет управлять программами Антивирус Dr.Web для Windows, Антивирус Dr.Web для серверов и Dr.Web Security Space в рамках одной версии продукта на других компьютерах в пределах одной локальной сети.

Для удаленной работы с продуктами Dr.Web щелкните значок SpIDer Agent  в области уведомлений Windows и в группе **Инструменты** выберите пункт **Антивирусная сеть**.



Для доступа к удаленному антивирусу, выберите компьютер в списке и нажмите кнопку **Подключиться....** Введите пароль, заданный в настройках удаленного антивируса. В области уведомлений Windows появится значок удаленного SpIDer Agent , а также будет показано уведомление об успешном подключении.

Вы можете просматривать статистику, включать и отключать модули, а также изменять их настройки. Компоненты Антивирусная сеть, Карантин и Сканер недоступны. Настройки и статистика Брандмауэра Dr.Web также недоступны, однако вы можете включить или отключить этот компонент (в случае подключения к продуктам Антивирус Dr.Web для Windows или Dr.Web Security Space). Также вам доступен пункт **Отсоединиться**, при выборе которого завершается установленное соединение с удаленным антивирусом.

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

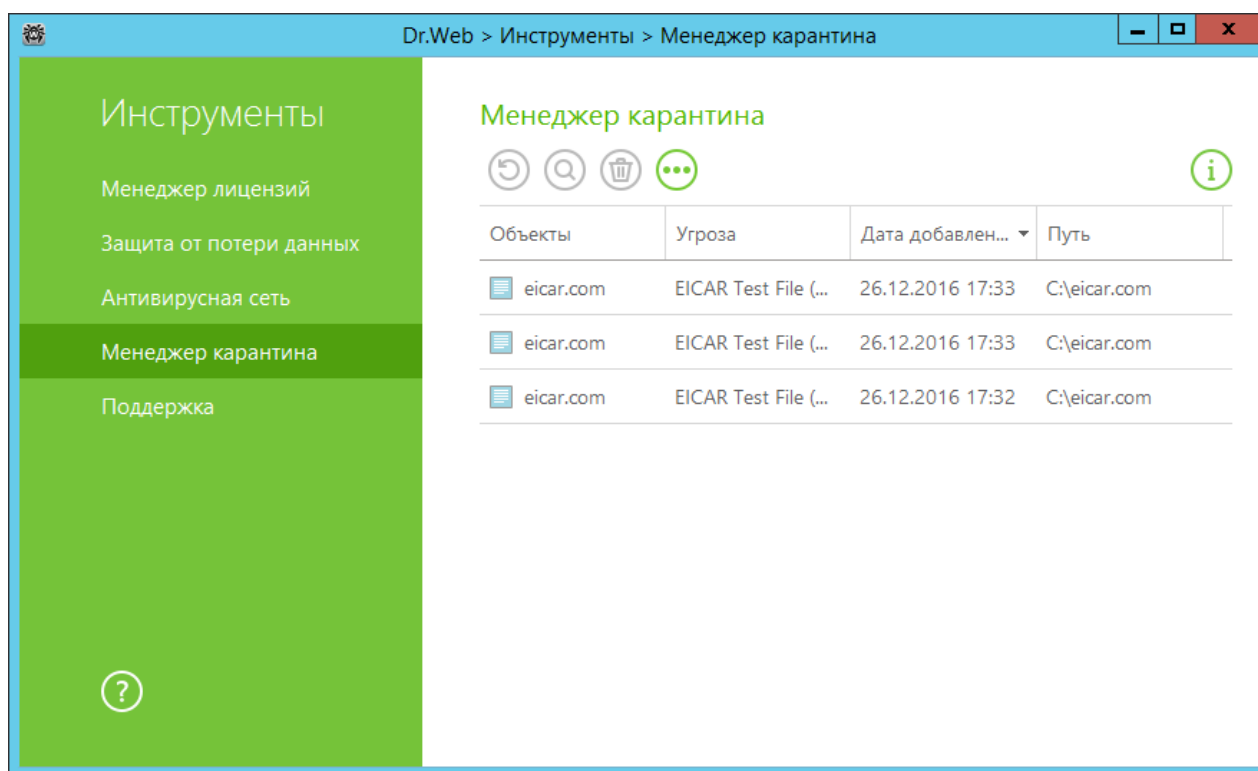


Вы можете установить только одно соединение с удаленным продуктом Dr.Web. При наличии установленного соединения кнопка **Подключиться...** недоступна.

Компьютеры в локальной сети отображаются в списке только в том случае, если в установленном на них продукте Dr.Web разрешено удаленное управление. Вы можете разрешить подключение к программе Dr.Web на вашем компьютере в разделе Антивирусная сеть [Основных настроек](#).

6.4. Менеджер карантина

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



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

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



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

- **Объекты** – список имен объектов, находящихся в карантине;
- **Угроза** – классификация вредоносной программы, определяемая программой Dr.Web при автоматическом перемещении объекта в карантин;
- **Дата добавления** – дата, когда объект был перемещен в карантин;
- **Путь** – полный путь, по которому находился объект до перемещения в карантин.



В окне Менеджера карантина файлы могут видеть только те пользователи, которые имеют к ним доступ. Чтобы отобразить скрытые объекты, необходимо иметь права Администратора.

В контекстном меню объектов доступны следующие кнопки управления:

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



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

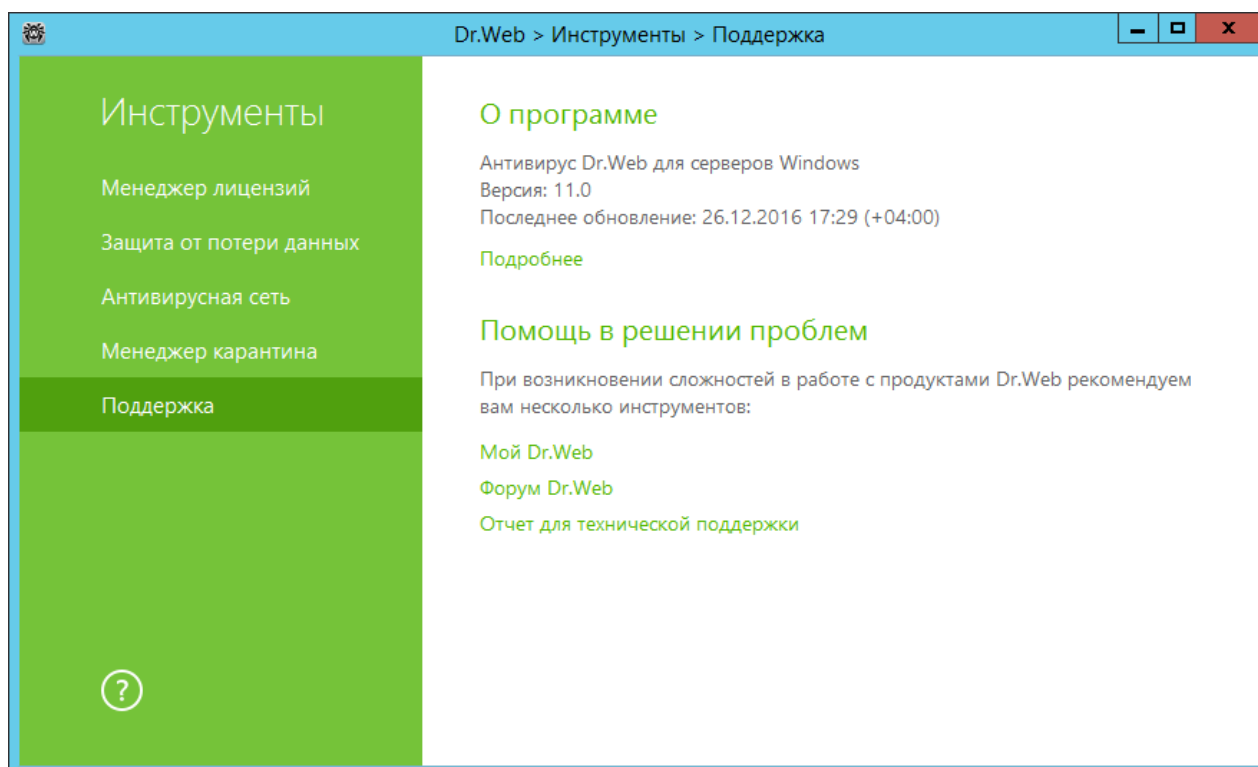
- **Проверить** – повторно проверить объект, перемещенный в карантин;
- **Удалить** – удалить файл из карантина и из системы.

Эти действия доступны также в контекстном меню при нажатии правой кнопкой мыши на один или несколько выбранных объектов.

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

6.5. Поддержка

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



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

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

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

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

Если после этого вам не удалось решить проблему, вы можете заполнить веб-форму вопроса <http://support.drweb.com>.

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

6.5.1. Создание отчета

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

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



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

1. Техническая информация об операционной системе:

- общие сведения о компьютере;
- запущенных процессах;
- запланированных заданиях;
- службах, драйверах;
- браузере по умолчанию;
- установленных приложениях;
- политиках ограничений;
- файле HOSTS;
- о серверах DNS;
- записи системного журнала событий;
- перечень системных каталогов;
- ветви реестра;
- провайдеры Winsock;
- сетевые соединения;
- отчеты отладчика Dr.Watson;
- индекс производительности.

2. Информация об Антивирусных решениях Dr.Web.

3. Информация о подключаемых модулях Dr.Web:

- Dr.Web для IBM Lotus Domino;
- Dr.Web для Kerio MailServer;
- Dr.Web для Kerio WinRoute.

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

Создание отчета из командной строки

Чтобы сформировать отчет, воспользуйтесь следующей командой:

```
/auto
```

Например: `dwsysinfo.exe /auto`

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



Также вы можете использовать команду:

```
/auto/report: [<полный путь к архиву>]
```

где:

- <полный путь к архиву> – путь к файлу отчета.

Например: `dwsysinfo.exe /auto /report:C:\report.zip`



7. Обновление

Для обнаружения вредоносных объектов антивирусы компании «Доктор Веб» используют специальные вирусные базы Dr.Web, в которых содержится информация обо всех известных вредоносных программах. Регулярное обновление позволяет обнаруживать ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев – излечивать ранее неизлечимые зараженные файлы.

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

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

Запуск обновления

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



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

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

Запуск обновления с помощью модуля управления SpIDer Agent

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

Запуск обновления из командной строки

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



Автоматический запуск обновления

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



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



8. Сканер Dr.Web

Сканер Dr.Web для Windows предназначен для антивирусной проверки загрузочных секторов, памяти, а также как отдельных файлов, так и объектов в составе сложных структур (архивы, контейнеры, электронные письма с вложениями). Проверка производится с использованием всех [методов обнаружения](#) угроз. По умолчанию Сканер Dr.Web производит антивирусную проверку всех файлов с использованием как вирусных баз, так и эвристического анализатора (алгоритма, позволяющего с большой вероятностью обнаруживать неизвестные программе вирусы на основе общих принципов их создания). Исполняемые файлы, упакованные специальными упаковщиками, при проверке распаковываются. Проверяются файлы в архивах всех основных распространенных типов (ACE, ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP и др.), файловых контейнерах (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM и др.), а также файлы в составе писем в почтовых ящиках почтовых программ (формат писем должен соответствовать RFC822).

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

Действия по умолчанию являются оптимальными для большинства применений, но при необходимости вы можете изменить их в [окне настройки](#) параметров работы компонента Сканер 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.

8.1. Запуск проверки

Запуск Сканера Dr.Web



При работе под управлением операционных систем Windows Server 2003 и более поздних Сканер Dr.Web рекомендуется запускать с правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут проверены.

1. В [меню](#) SpIDer Agent выберите пункт **Сканер**. Откроется меню быстрого доступа к запуску разных типов проверки.
2. Выберите пункт **Выборочная**, чтобы проверить только указанные вами объекты. Откроется главное окно Сканера Dr.Web.
3. Выберите пункты **Быстрая** или **Полная**, чтобы запустить соответствующие типы проверок.



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**.

Настройка Сканера Dr.Web

Вы можете настроить параметры работы, а также реакции Сканера Dr.Web на обнаруженные угрозы в разделе **Настройки** → **Компоненты защиты** → **Сканер**.

Описание режимов проверки

Быстрая проверка

В данном режиме проверяются:

- загрузочные сектора всех дисков;
- оперативная память;
- корневая папка загрузочного диска;
- системная папка Windows;
- папка Мои Документы;
- временные файлы;
- точки восстановления системы;
- наличие руткитов (если процесс проверки запущен от имени администратора).



Архивы и почтовые файлы в этом режиме не проверяются.

Полная проверка

В данном режиме производится полная проверка оперативной памяти и всех жестких дисков (включая загрузочные секторы), а также осуществляется проверка на наличие руткитов.

Выборочная проверка

При выборе данного режима в окне Сканера Dr.Web 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 **Начать проверку**. Чтобы добавить объекты в список, нажмите кнопку



Процесс проверки

После начала проверки становятся доступными кнопки **Пауза** и **Стоп**. На любом этапе проверки вы можете сделать следующее:

- чтобы приостановить проверку, нажмите кнопку **Пауза**. Чтобы продолжить проверку после паузы, нажмите кнопку **Возобновить**.
- чтобы полностью остановить проверку, нажмите кнопку **Стоп**.



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

8.2. Действия при обнаружении угроз

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



По нажатию кнопки **Обезвредить** действия применяются к объектам в таблице. По умолчанию после окончания проверки обезвреживаются все объекты. При необходимости вы можете вручную выбрать конкретные объекты или группы. Для выбора группы объектов можно воспользоваться клавишами CTRL и SHIFT. Действия для обезвреживания угроз доступны в контекстном меню при нажатии правой кнопкой мыши на один или несколько выбранных объектов.

Выбор действия

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

Существуют следующие ограничения:

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

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



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



Если в [настройках](#) Сканера Dr.Web вы выбрали пункт **Обезвредить обнаруженные угрозы** для настройки **После завершения проверки**, то обезвреживание угроз будет произведено автоматически.

8.3. Запуск Сканера с параметрами командной строки

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

Запуск Сканера из командной строки

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

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

где:

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



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

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

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

8.4. Консольный сканер

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



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

Запуск Консольного сканера

Чтобы запустить Консольный сканер, воспользуйтесь следующей командой:

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

где:

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

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

Список ключей Консольного сканера содержится в [Приложении А](#).

После выполнения Консольный сканер возвращает один из следующих кодов:

- 0 – проверка успешно завершена, инфицированные объекты не найдены;
- 1 – проверка успешно завершена, найдены инфицированные объекты;



- 10 – указаны некорректные ключи;
- 11 – ключевой файл не найден либо не поддерживает Консольный сканер;
- 12 – не запущен Scanning Engine;
- 255 – проверка прервана пользователем.

8.5. Запуск проверки по расписанию

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

Для просмотра параметров задания откройте **Панель управления** (расширенный вид) → **Администрирование** → **Планировщик заданий**.

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

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

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



9. Настройки

Для доступа к настройкам откройте меню SpIDer Agent  и запустите **Настройки**  в [режиме администратора](#).

Защита паролем

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



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

Управление настройками

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

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

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



10. Основные настройки

Чтобы получить доступ к основным настройкам Dr.Web, откройте меню SpIDer Agent , запустите **Настройки**  в режиме администратора и выберите раздел **Основные**.



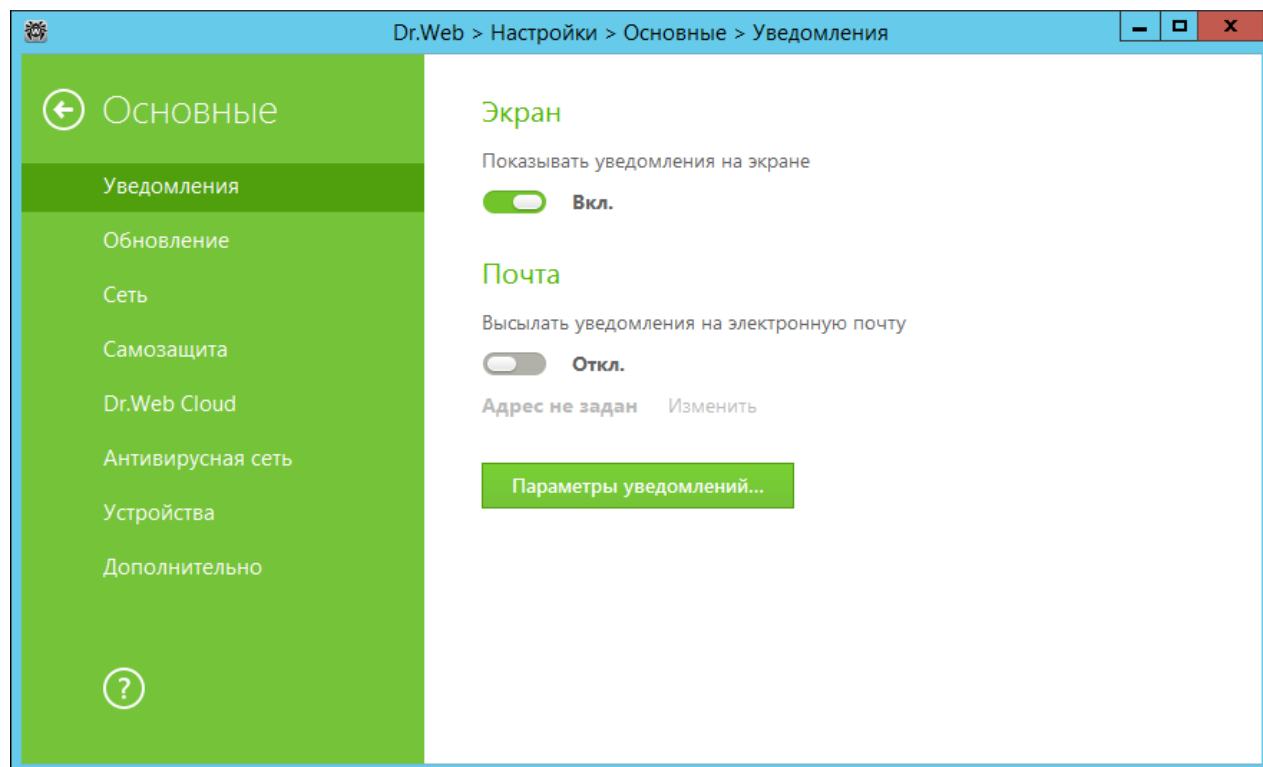
Для доступа к основным настройкам Dr.Web запрашивается пароль, если в разделе Настройки вы установили флажок **Защищать паролем настройки Dr.Web**.

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

10.1. Уведомления

Уведомления, которые выводятся на экран

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





Уведомления по почте

Чтобы получать уведомления о событиях по почте, выполните следующие действия:

1. Включите опцию **Высылать уведомления на электронную почту**.
2. В появившемся окне введите адрес электронной почты, на который вы хотите получать уведомления. Использование этого адреса необходимо будет подтвердить на шаге 7.
3. Нажмите **Далее**.
4. Укажите данные учетной записи, с которой будут отправляться уведомления.
 - Если список почтовых серверов содержит необходимый сервер, выберите его, а затем укажите логин и пароль от вашей учетной записи.
 - Если список почтовых серверов не содержит необходимый сервер, выберите **Указать вручную** и в открывшемся окне заполните необходимые поля.

Настройка	Описание
Сервер SMTP	Укажите адрес почтового сервера, который должен использовать Dr.Web для отправки почтовых оповещений.
Порт	Укажите порт почтового сервера, к которому должен подключаться Dr.Web для отправки почтовых оповещений.
Логин	Укажите имя учетной записи для подключения к почтовому серверу.
Пароль	Укажите пароль учетной записи для подключения к почтовому серверу.
Использовать SSL/TLS	Установите этот флажок, если хотите, чтобы при передаче сообщений использовалось SSL/TLS шифрование.
NTLM-аутентификация	Установите этот флажок, если хотите, чтобы авторизация производилась по протоколу NTLM.

5. Нажмите **Отправить тестовое сообщение**, если хотите проверить, что учетная запись указана верно. Сообщение придет на тот адрес, с которого должны отправляться уведомления (настроенный на шаге 4).
6. Нажмите **Далее**.
7. Введите код подтверждения, который придет на электронный адрес, указанный для получения уведомлений на шаге 2. Если код не придет в течение 10 минут, нажмите кнопку **Отправить код повторно**. Если вы не введете код подтверждения, уведомления на этот адрес отправляться не будут.
8. Чтобы изменить адрес электронной почты и другие параметры, нажмите **Изменить** и повторите все действия, начиная с шага 2.
9. Нажмите кнопку **Параметры уведомлений** и установите нужные типы уведомлений. По умолчанию все типы уведомлений, отправляемые на почту, отключены.



Параметры уведомлений

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

Тип уведомления	Описание
Обнаружена угроза	Установите флажки внутри этой группы, чтобы получать уведомления об угрозах, обнаруженных SpIDer Guard. Снимите флажки, чтобы не получать подобных уведомлений. По умолчанию уведомления включены.
Критичные уведомления	Установите флажки внутри этой группы, чтобы получать критичные уведомления о следующих событиях: • ошибка создания защищаемой копии. Снимите флажки, чтобы не получать перечисленные уведомления. По умолчанию уведомления включены.
Важные уведомления	Установите флажки внутри этой группы, чтобы получать важные уведомления о следующих событиях: • заблокировано устройство; • попытка доступа к защищаемому объекту заблокирована Превентивной защитой; • заблокирована попытка изменения системных даты и времени; • доступна новая версия продукта; • вирусные базы устарели. Снимите флажки, чтобы не получать перечисленные уведомления. По умолчанию уведомления включены.
Малозначительные уведомления	Установите флажки внутри этой группы, чтобы получать малозначительные уведомления о следующих событиях: • успешное обновление; • ошибка обновления; Снимите флажки, чтобы не получать перечисленные уведомления. По умолчанию уведомления выключены.
Лицензия	Установите флажки внутри этой группы, чтобы получать уведомления о следующих событиях: • срок действия вашей лицензии заканчивается; • действующая лицензия не найдена; • текущая лицензия заблокирована.



3. При необходимости задайте дополнительные параметры отображения экранных оповещений:

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

4. Если вы выбрали одно или несколько почтовых уведомлений, настройте [отправку почты](#) с вашего компьютера.

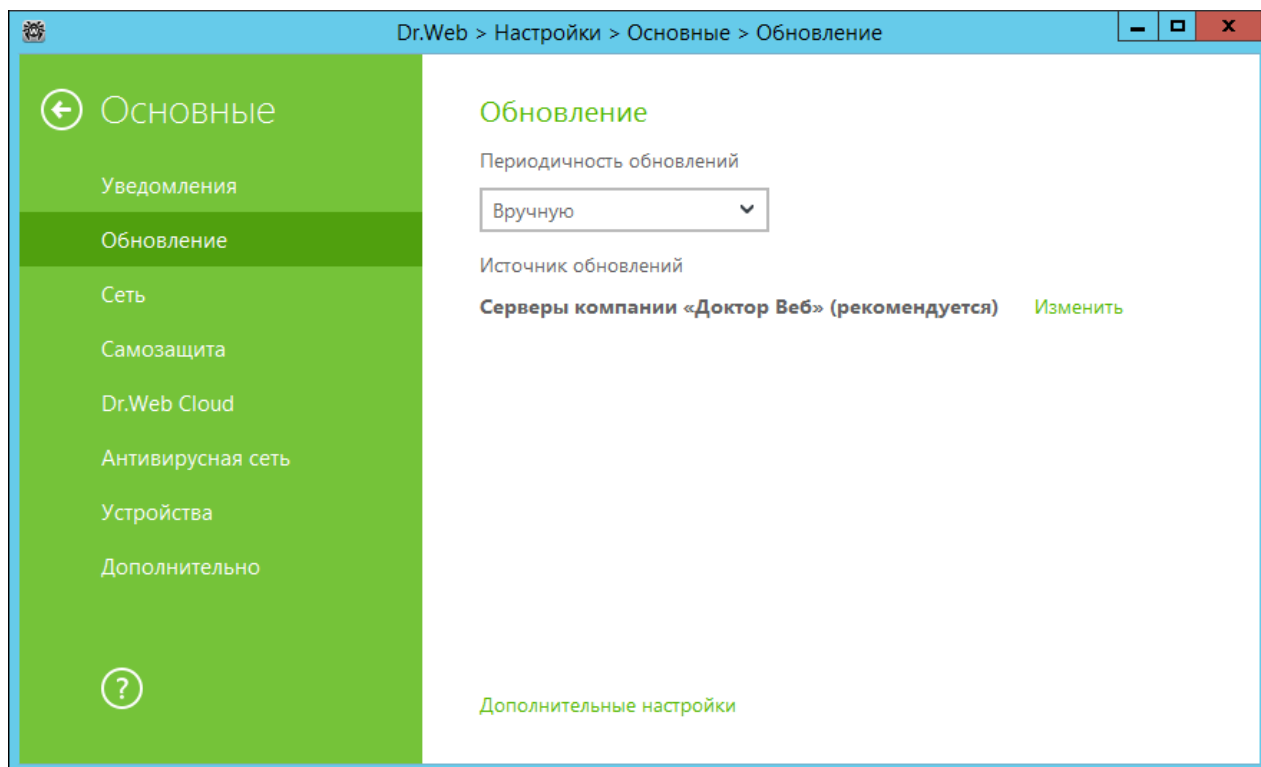


Уведомления о некоторых событиях не входят в перечисленные группы и всегда показываются пользователю:

- установка приоритетных обновлений, для которых требуется перезагрузка;
- перезагрузка для завершения обезвреживания угроз;
- перезагрузка для включения/выключения гипервизора;
- запрос на разрешение процессу модификации объекта;
- успешное подключение к удаленному компьютеру в Антивирусной сети.

10.2. Обновление

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



Основные настройки обновления

Периодичность обновлений. Задайте необходимую периодичность, с которой будет производиться проверка на наличие обновлений. По умолчанию установлено оптимальное значение (30 минут), которое позволяет поддерживать информацию об угрозах в актуальном состоянии.

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

- **Серверы компании «Доктор Веб» (рекомендуется).** 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.

Если вы хотите загружать обновления по безопасному протоколу, включите опцию **Использовать HTTPS-соединение**.



Дополнительные настройки

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 Dr.Web;
- **Только базы**, при котором загружаются только обновления вирусных баз Dr.Web и антивирусного ядра; другие компоненты Dr.Web не обновляются.

Создание зеркала обновлений

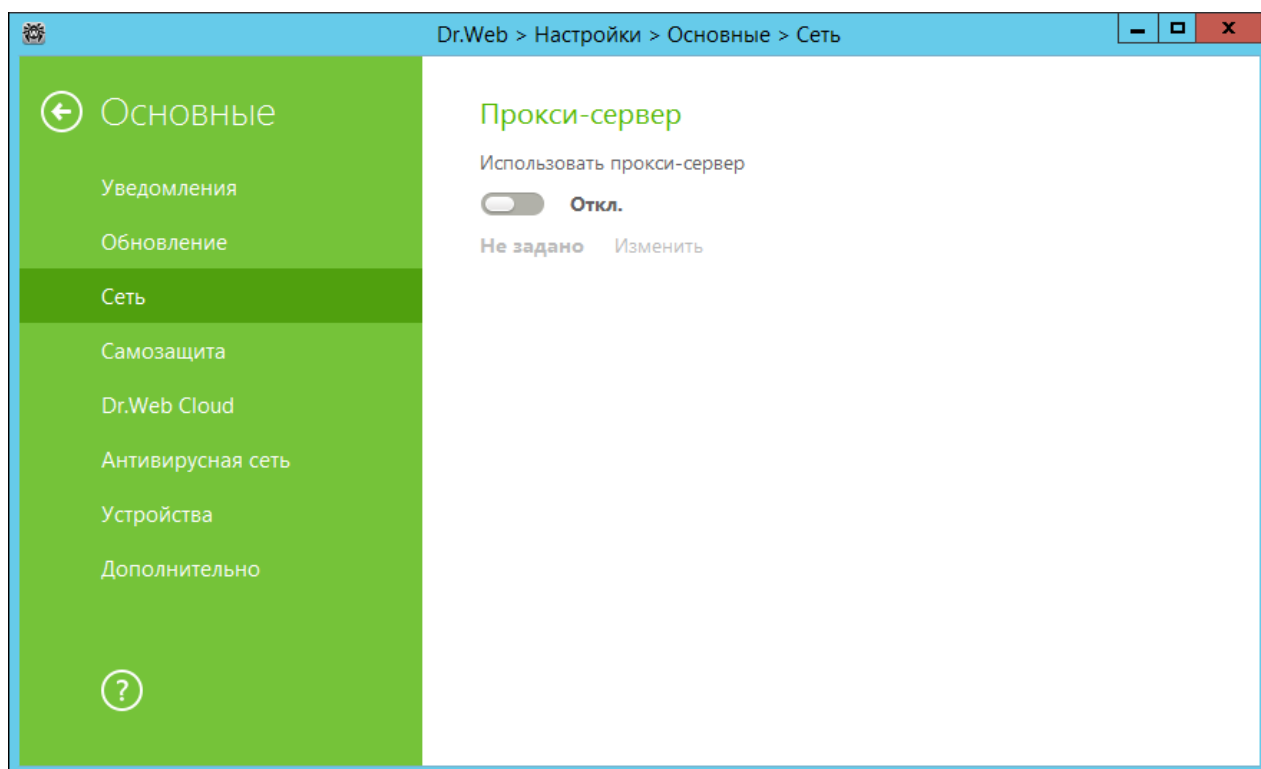
Чтобы ваш компьютер могли использовать как источник обновлений другие компьютеры в локальной сети, на которых установлен продукт Dr.Web, разверните **Дополнительные настройки** и включите соответствующую опцию. Нажмите **Изменить**, чтобы указать путь к папке, в которую будут копироваться обновления. 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.

10.3. Сеть

Использование прокси-сервера

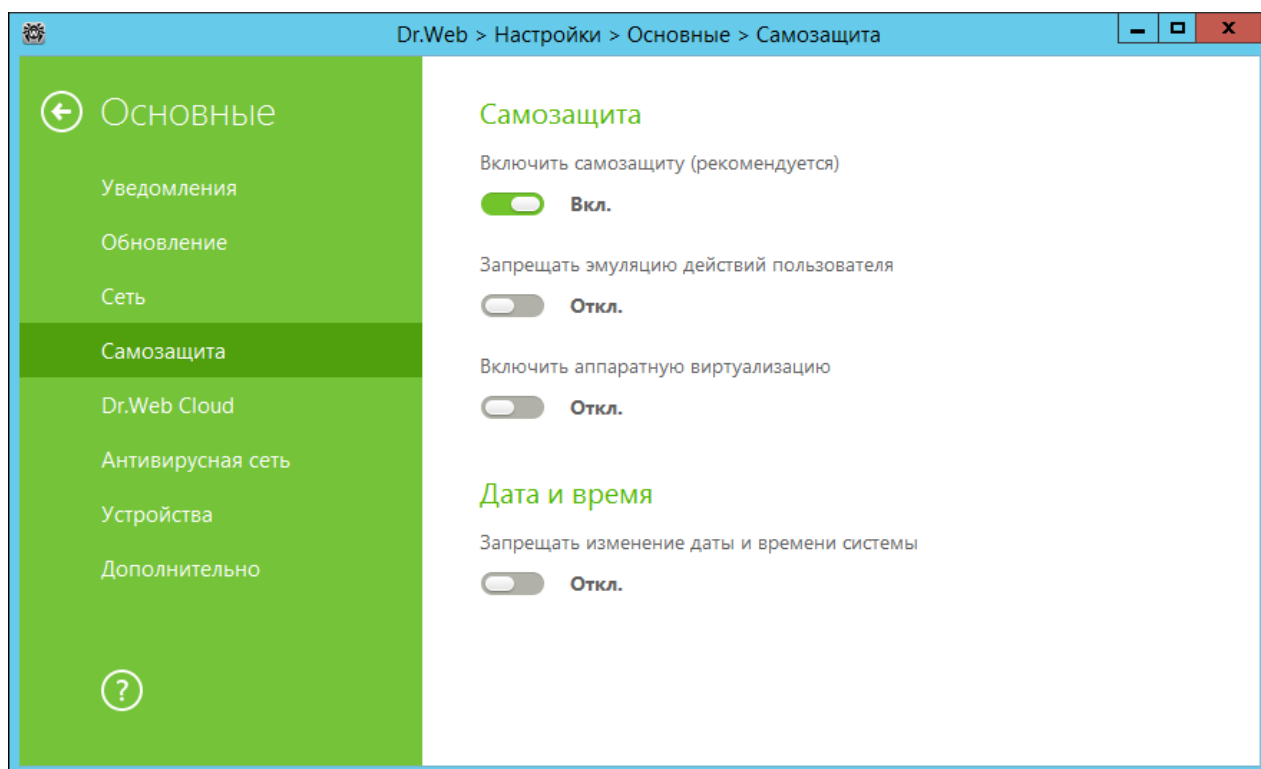
При необходимости вы можете включить использование прокси-сервера и задать настройки подключения к нему. Нажмите **Изменить**, чтобы задать настройки подключения к прокси-серверу:

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



10.4. Самозащита

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





Самозащита

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



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

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

Настройка **Запрещать эмуляцию действий пользователя** позволяет предотвратить изменения в настройках Dr.Web, производимые автоматизированно. В том числе будет запрещено исполнение скриптов, эмулирующих работу пользователя с Dr.Web и запущенных самим пользователем (например, скриптов для изменения настроек Dr.Web, удаления лицензии и других действий, направленных на изменение работы Dr.Web).

Настройка **Использовать аппаратную виртуализацию** позволяет использовать больше возможностей компьютера для обнаружения и лечения угроз, а также для усиления самозащиты Dr.Web. Для включения этой опции потребуется перезагрузка компьютера.



Аппаратная виртуализация работает только в том случае, если аппаратные особенности вашего компьютера и операционная система поддерживают аппаратную виртуализацию.

Включение этой опции может вызвать конфликт совместимости со сторонним программным обеспечением.

При возникновении проблем отключите эту опцию.

Для 32-разрядных операционных систем аппаратная виртуализация не поддерживается.

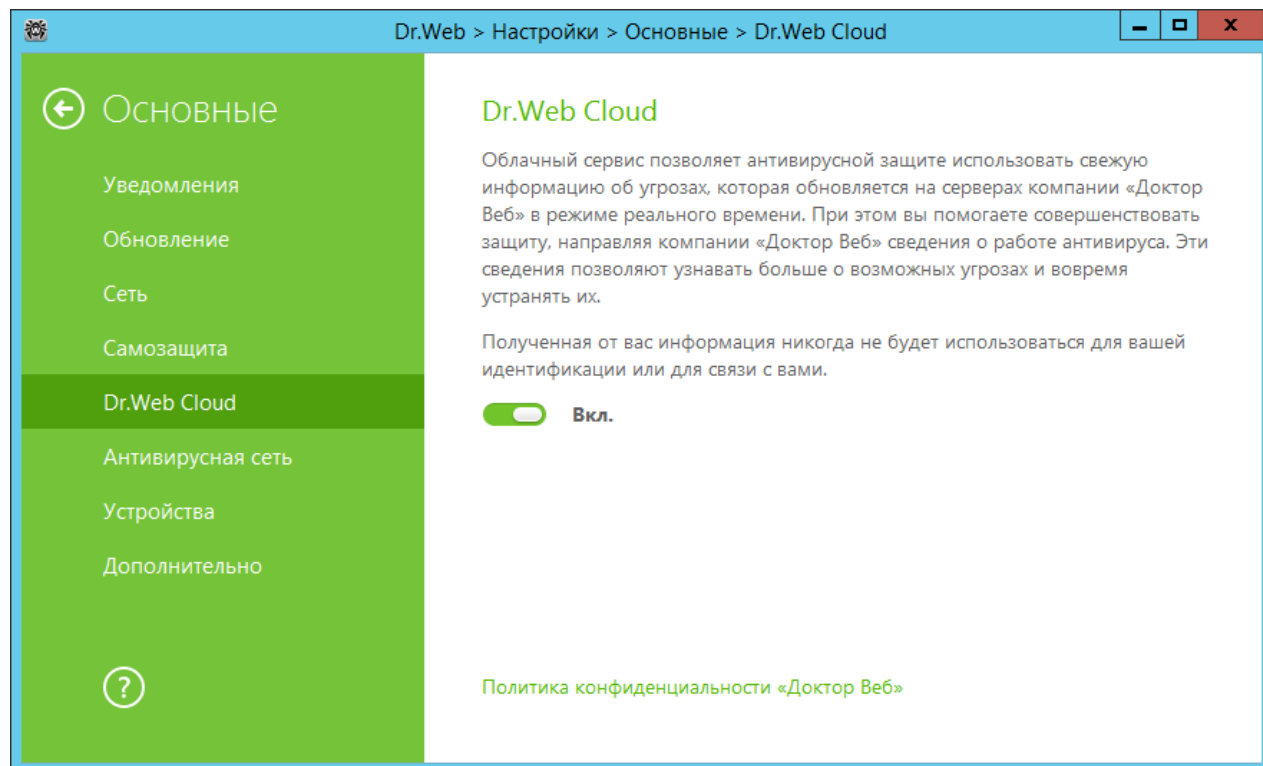
Дата и время

Настройка **Запрещать изменение даты и времени системы** позволяет заблокировать ручное и автоматическое изменение системных даты и времени, а также часового пояса. Это ограничение устанавливается для всех пользователей системы. Вы можете настроить [получение уведомлений](#) в том случае, если осуществлялась попытка изменить системное время.



10.5. Dr.Web Cloud

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



Облачные сервисы

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

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

Программа улучшения качества ПО

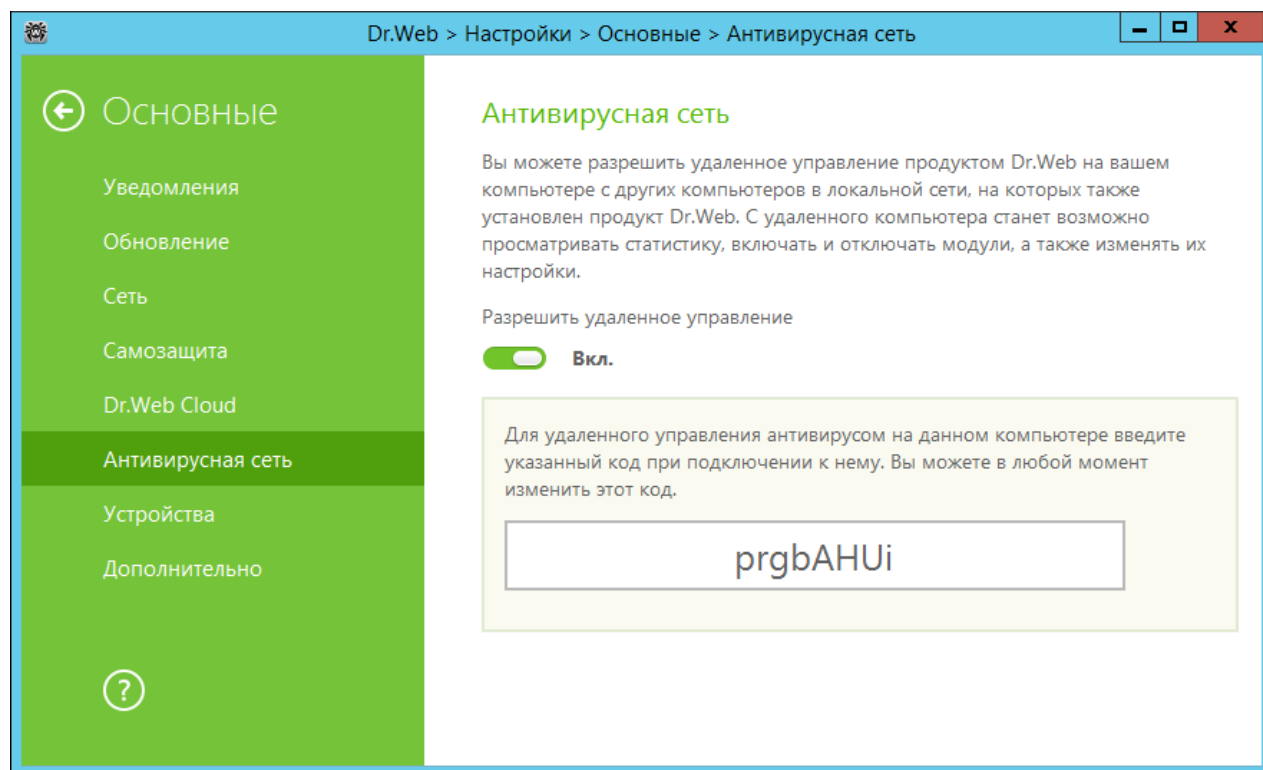
При участии в программе на сервера компании «Доктор Веб» будут автоматически отправляться обезличенные сведения о работе программы Dr.Web на вашем компьютере. Полученная информация не будет использоваться для идентификации пользователя или связи с ним.

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



10.6. Антивирусная сеть

В данном разделе вы можете разрешить удаленное управление вашим антивирусом с других компьютеров локальной сети при помощи компонента [Антивирусная сеть](#). Вхождение в состав антивирусной сети позволяет удаленно контролировать состояние антивирусной защиты (просматривать статистику, включать и отключать компоненты Dr.Web, изменять их настройки), а также получать обновления через локальную сеть. Чтобы использовать компьютер как источник обновлений для других компьютеров антивирусной сети, на которых установлен продукт Dr.Web, на нём нужно настроить [Зеркало обновлений](#).



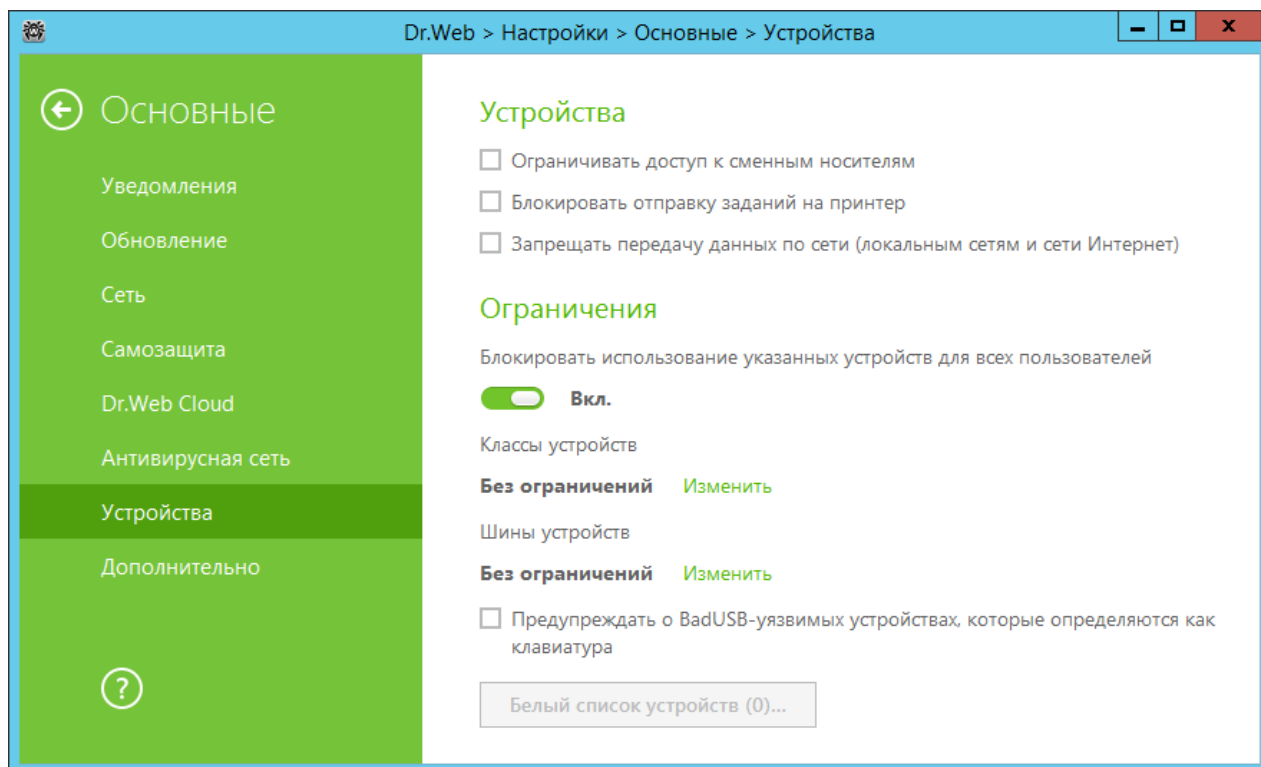
Для удаленного управления Dr.Web на вашем компьютере необходимо будет вводить пароль. Вы можете использовать пароль, который автоматически генерируется при включении опции, или задать свой.

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

10.7. Устройства



Настройки контроля доступа применяются для всех учетных записей Windows.



Устройства

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

Некоторые инфицированные USB-устройства могут опознаваться компьютером как клавиатура. Чтобы Dr.Web проверял, действительно ли подключенное устройство является клавиатурой, включите опцию **Предупреждать о BadUSB-уязвимых устройствах, которые определяются как клавиатура**.

Классы устройств и шин

Чтобы заблокировать доступ к выбранным классам устройств и шин, включите соответствующую опцию. Сформируйте список таких объектов, нажав кнопку **Изменить**. В открывшемся окне выберите те классы устройств или шин, доступ к которым должен быть заблокирован. Чтобы сохранить изменения, нажмите **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите **Отменить**.

Белый список устройств

Если вы ограничили доступ к каким-либо классам устройств или шин, вы можете отдельно разрешить доступ к определенным устройствам, добавив их в белый список. Также в белый



список можно добавить конкретное устройство, чтобы не проверять его на наличие BadUSB-уязвимости.

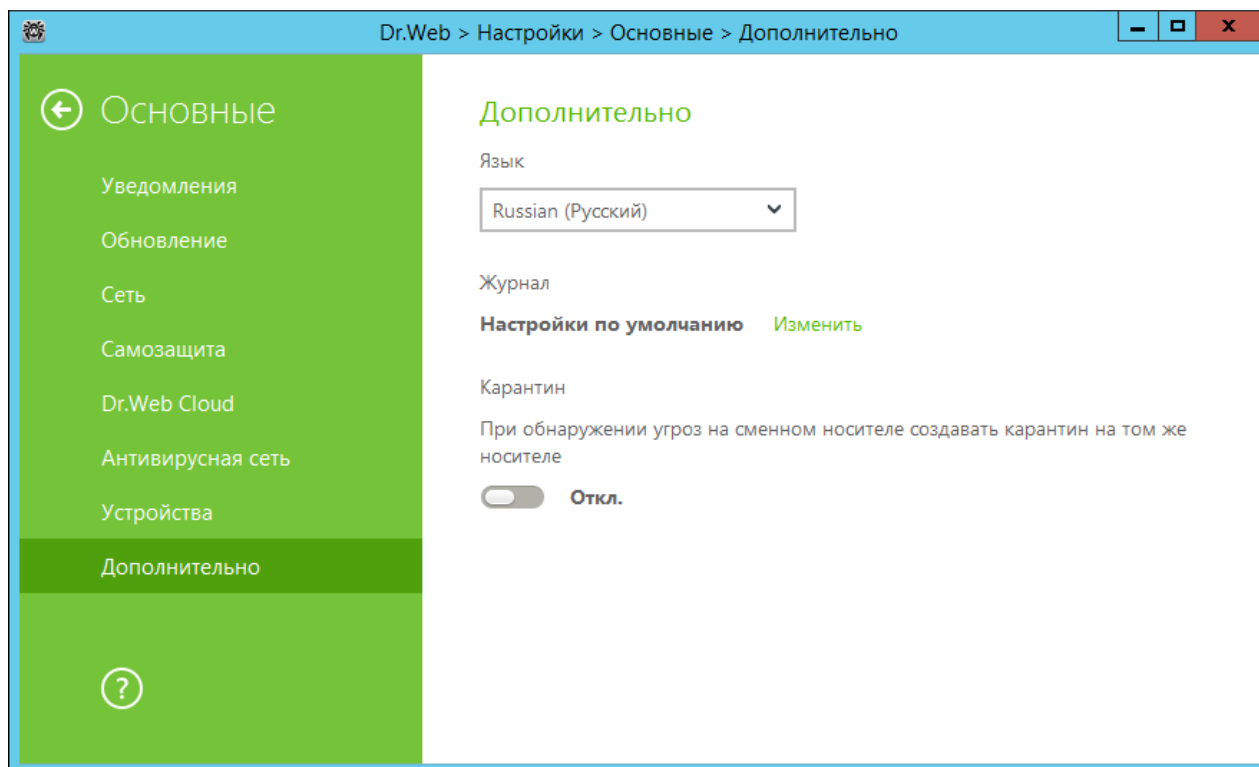
Для добавления устройства в белый список выполните следующие действия:

1. Нажмите кнопку **Белый список устройств** (эта кнопка становится активна, если заданы ограничения).
2. Убедитесь, что устройство подключено к компьютеру.
3. Нажмите кнопку . В открывшемся окне нажмите кнопку **Обзор** и выберите нужное устройство. Для удобства можно воспользоваться фильтром, и тогда в таблице отобразятся только подключенные или только отключенные устройства. Нажмите кнопку **ОК**.
4. Для устройств с файловой системой вы можете настроить правила доступа. Для этого в столбце **Правило** выберите один из режимов: **Разрешать все** или **Только чтение**. Чтобы добавить новое правило для конкретного пользователя, нажмите . Чтобы удалить правило, нажмите .
5. Чтобы сохранить изменения, нажмите **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите **Отменить**. Вы вернётесь к белому списку устройств.
6. Для того чтобы отредактировать набор правил для устройства, выберите его в списке и нажмите .
7. Чтобы удалить набор правил для устройства, выберите его в списке и нажмите .

10.8. Дополнительно

В данном разделе задаются язык настроек, параметры журнала и Карантина.

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



Настройки Журнала

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



По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ (для компонента SpIDer Guard - 100 МБ). При превышении максимального размера файл журнала урезается до:

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

По умолчанию для всех компонентов программы Dr.Web журнал ведется в стандартном режиме, фиксирующем следующую информацию:

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



Компонент	Информация
Сканер	В данном режиме в журнале фиксируются такие события, как проведение обновлений, запуск и остановка Сканера Dr.Web, обнаруженные угрозы, а также данные об именах упаковщиков и содержимом проверяемых архивов.
Обновление Dr.Web	Список обновленных файлов программы Dr.Web и статусы их загрузки, информация о работе вспомогательных скриптов, дата и время проведения обновления, информация о перезапуске компонентов программы Dr.Web после обновления.
Служба Dr.Web	Информация о компонентах Dr.Web, изменение настроек компонентов, включение и выключение компонентов, события превентивной защиты, подключение к антивирусной сети.

Создание дампов памяти

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

Включение подробных журналов



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

1. Чтобы включить режим ведения подробного журнала для одного из компонентов программы Dr.Web, установите соответствующий флажок.
2. По умолчанию подробный журнал ведётся до первой перезагрузки операционной системы. Если необходимо зафиксировать поведение компонента в период до и после перезагрузки, установите флажок **Продолжать вести подробный журнал после перезагрузки (используйте только по запросу технической поддержки компании «Доктор Веб»)**.
3. Сохраните изменения.



Настройки Карантина

Вы можете включить опцию, которая определяет режим изоляции зараженных объектов, обнаруженных на съемных носителях. При включении этой опции подобные угрозы помещаются в папку на том же носителе и не шифруются. При этом папка карантина создается только в том случае, если возможна запись на носитель. Использование отдельных папок и отказ от шифрования на съемных носителях позволяет предотвратить возможную потерю данных. Если опция выключена, обнаруженная угроза перемещается в карантин на локальном диске.

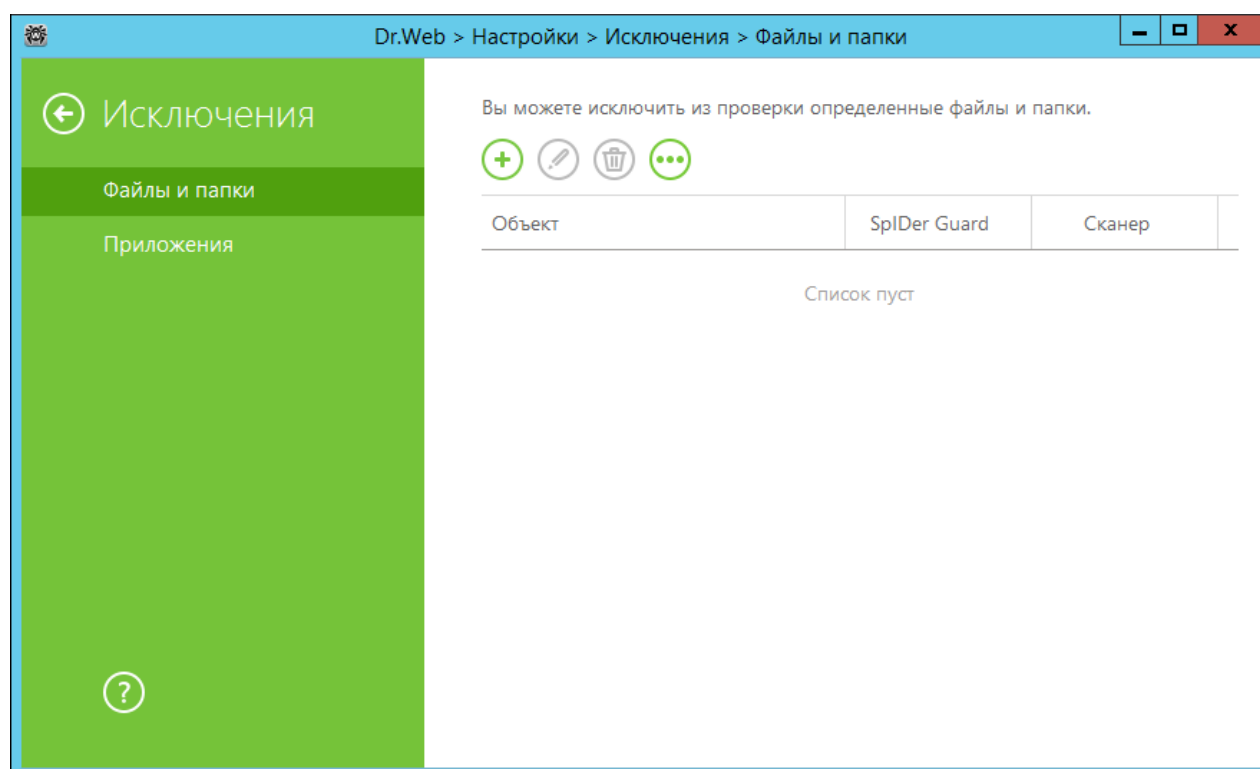


11. Исключения

11.1. Файлы и папки

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

По умолчанию список пуст. Добавьте к исключениям конкретные папки и файлы или используйте маски, чтобы запретить проверку определенной группы файлов. Каждый добавляемый объект можно исключить из проверки как обоих компонентов, так и каждого в отдельности.



Формирование списка исключений

1. Чтобы добавить папку или файл к списку исключений, выполните одно из следующих действий:
 - чтобы указать конкретный существующий файл или папку, нажмите кнопку . В открывшемся окне нажмите кнопку **Обзор** и выберите папку или файл в стандартном окне открытия файла. Вы можете вручную ввести полный путь к файлу или папке в поле ввода, а также отредактировать запись в поле ввода перед добавлением ее в список;



- чтобы исключить из проверки файл с определенным именем, введите имя файла, включая расширение, в поле ввода. Указывать путь к файлу при этом не требуется;
 - чтобы исключить из проверки файлы или папки определенного вида, введите определяющую их маску в поле ввода.
2. В окне настройки укажите, какие компоненты не должны проводить проверку выбранного файла.
 3. Нажмите кнопку **ОК**. Выбранный файл или папка появится в списке.
 4. Для того чтобы отредактировать исключение, выберите нужный элемент в списке и нажмите .
 5. При необходимости повторите шаги 1 и 2 для добавления других файлов или папок. Чтобы удалить файл или папку из списка исключений, выберите соответствующий элемент в списке и нажмите кнопку .

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 этом месте в имени должен находиться именно этот символ.

Примеры задания исключений:

- file.txt – исключает из проверки все файлы с именем file и расширением .txt во всех папках.
- C:\folder\file.txt – исключает из проверки файл file.txt в папке C:\folder.
- file* – исключает из проверки все файлы с любыми расширениями, имя которых начинается с file, во всех папках.
- file.* – исключает из проверки все файлы с именем file и любым расширением во всех папках.
- file – исключает из проверки все файлы с именем file без расширения во всех папках.
- C:\folder или C:\folder** – исключает из проверки все подпапки и файлы в папке C:\folder.
- C:\folder* – исключает из проверки все файлы в папке C:\folder и всех подпапках на любом уровне вложенности.
- C:\folder*.txt – исключает из проверки файлы *.txt в папке C:\folder. В подпапках файлы *.txt будут проверяться.
- C:\folder**.txt – исключает из проверки файлы *.txt только в подпапках первого уровня вложенности папки C:\folder.
- C:\folder***.txt – исключает из проверки файлы *.txt в подпапках любого уровня вложенности папки C:\folder. В самой папке C:\folder файлы *.txt будут проверяться.



Работа с объектами в списке

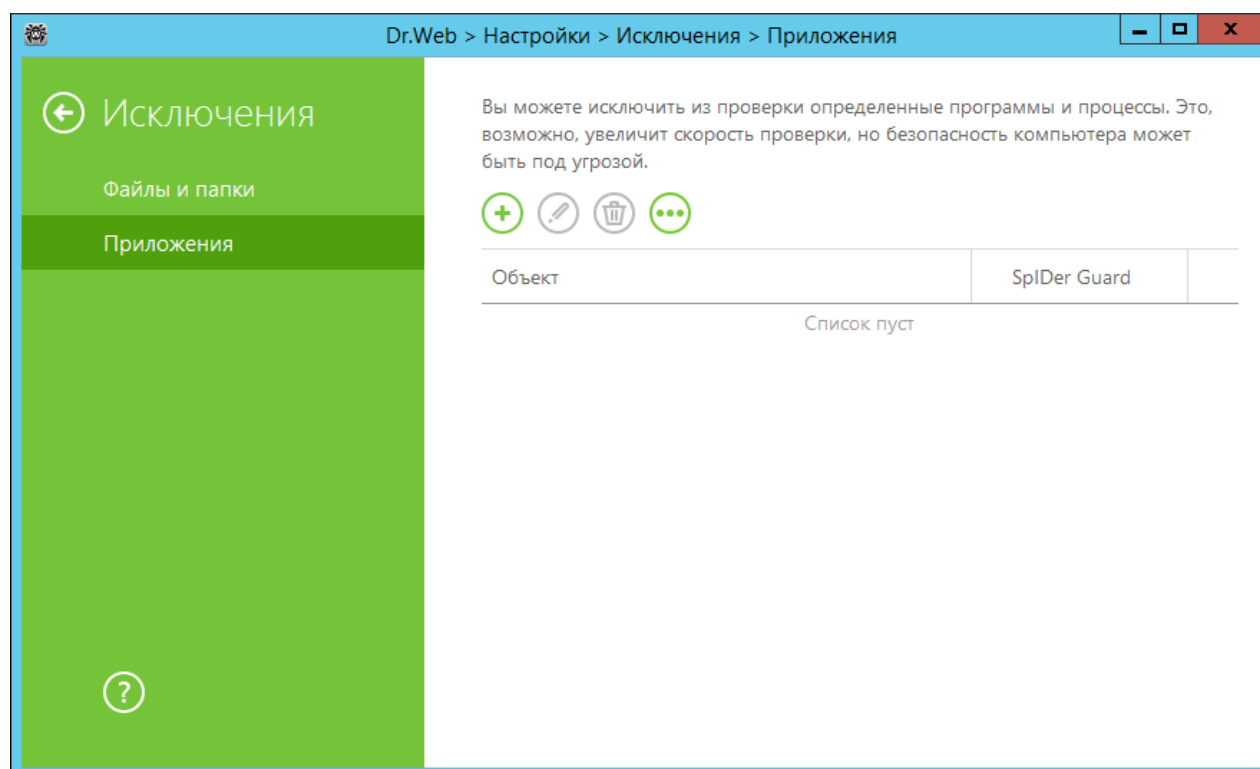
При нажатии кнопки  доступны следующие действия:

- **Экспорт** – эта опция позволяет сохранить созданный список исключений, чтобы использовать его на другом компьютере, на котором установлен Dr.Web.
- **Импорт** – эта опция позволяет использовать список исключений, созданный на другом компьютере.
- **Очистить все** – эта опция позволяет удалить все объекты из списка исключений.

11.2. Приложения

В этом разделе задается список программ и процессов, которые исключаются из проверки компонентом SpIDer Guard .

По умолчанию список пуст.



Формирование списка исключений

1. Чтобы добавить программу или процесс к списку исключений, нажмите . Выполните одно из следующих действий:
 - в открывшемся окне нажмите кнопку **Обзор** и выберите приложение в стандартном окне открытия файла. Вы можете вручную ввести полный путь к приложению в поле ввода;



- чтобы исключить приложение из проверки, введите его имя в поле ввода. Указывать полный путь к приложению при этом не требуется (например: `example.exe`);
 - чтобы исключить из проверки приложения определенного вида, введите определяющую их маску в поле ввода;
 - вы можете исключить из проверки приложение по имени переменной, если в настройках системных переменных задано имя и значение этой переменной.
2. В окне настройки укажите, что SpIDer Guard не должен проводить проверку выбранного приложения.
 3. Нажмите кнопку **ОК**. Выбранное приложение появится в списке.
 4. При необходимости повторите действия для добавления других программ.
 5. Для того чтобы отредактировать исключение, выберите нужный элемент в списке и нажмите .
 6. Чтобы удалить приложение из списка исключений, выберите соответствующий элемент в списке и нажмите .

Маска задает общую часть имени объекта, при этом:

- символ «*» заменяет любую, возможно пустую, последовательность символов;
- символ «?» заменяет любой, но только один символ;

Примеры задания исключений:

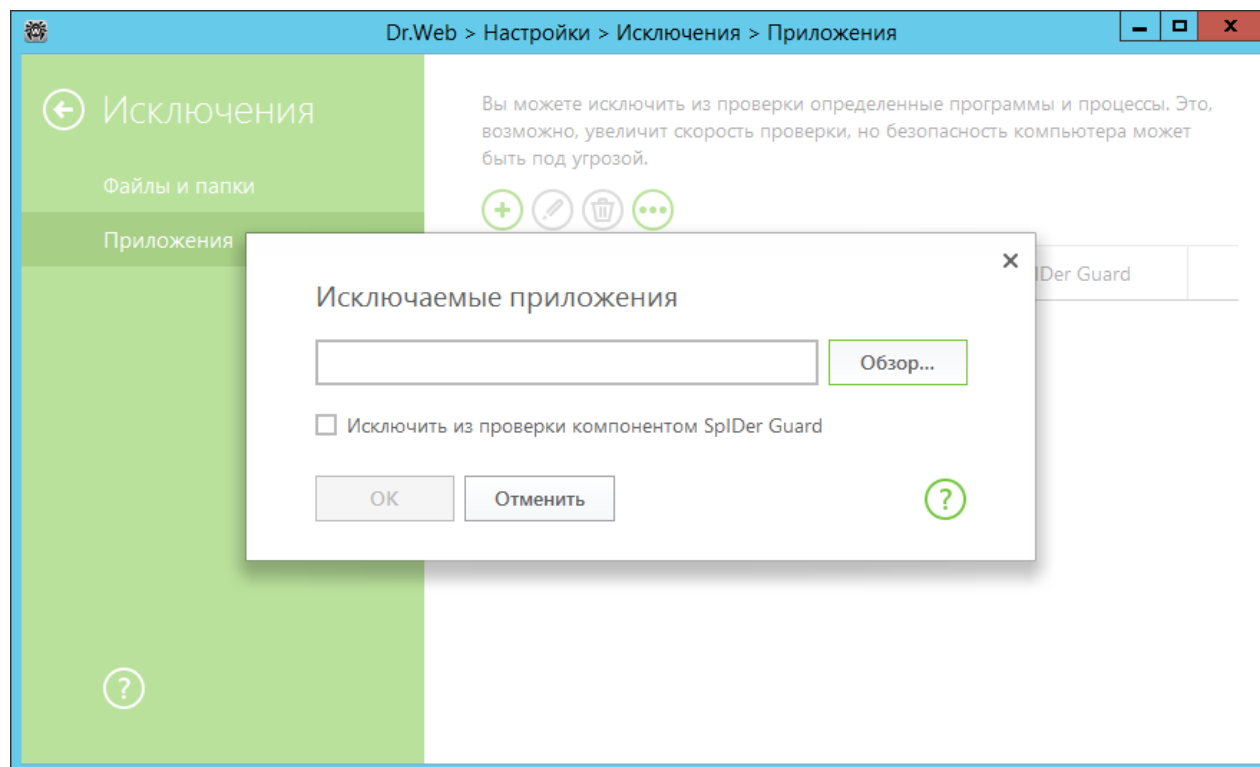
- `C:\Program Files\folder\example.exe` – исключает из проверки приложение `example.exe` в папке `C:\Program Files\folder`.
- `C:\Program Files\folder\*.exe` – исключает из проверки приложения в папке `C:\Program Files\folder`. В подпапках приложения будут проверяться.
- `C:\Program Files\*\*.exe` – исключает из проверки приложения только в подпапках первого уровня вложенности папки `C:\Program Files`.
- `C:\Program Files\**\*.exe` – исключает из проверки приложения в подпапках любого уровня вложенности папки `C:\Program Files`. В самой папке `C:\Program Files` приложения будут проверяться.
- `C:\Program Files\folder\exam*.exe` – исключает из проверки любые приложения, в папке `C:\Program Files\folder`, названия которых начинаются с "exam". В подпапках эти приложения будут проверяться.
- `example.exe` – исключает из проверки все приложения с именем `example` и расширением `.exe` во всех папках.
- `example*` – исключает из проверки приложения любого типа, имена которых начинаются с `example`, во всех папках.
- `example.*` – исключает из проверки все приложения с именем `example` и любым расширением во всех папках.
- `%EXAMPLE_PATH%\example.exe` – исключает из проверки приложение по имени системной переменной. Имя системной переменной и её значение можно задать в настройках операционной системы.



Для операционной системы Windows 7 и выше: **Панель управления** → **Система** → **Дополнительные параметры системы** → **Дополнительно** → **Переменные среды** → **Системные переменные**.

Имя переменной в примере: `EXAMPLE_PATH`.

Значение переменной в примере: `C:\Program Files\folder`.



Работа с объектами в списке

При нажатии кнопки  доступны следующие действия:

- **Экспорт** – эта опция позволяет сохранить созданный список исключений, чтобы использовать его на другом компьютере, на котором установлен Dr.Web.
- **Импорт** – эта опция позволяет использовать список исключений, созданный на другом компьютере.
- **Очистить все** – эта опция позволяет удалить все объекты из списка исключений.



12. Компоненты защиты

12.1. SpIDer Guard

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

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

Файлы внутри архивов и почтовые ящики не проверяются. Если какой-либо файл в архиве или почтовом вложении инфицирован, то вредоносный объект будет обнаружен сторожем при извлечении файла до появления возможности заражения компьютера.

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

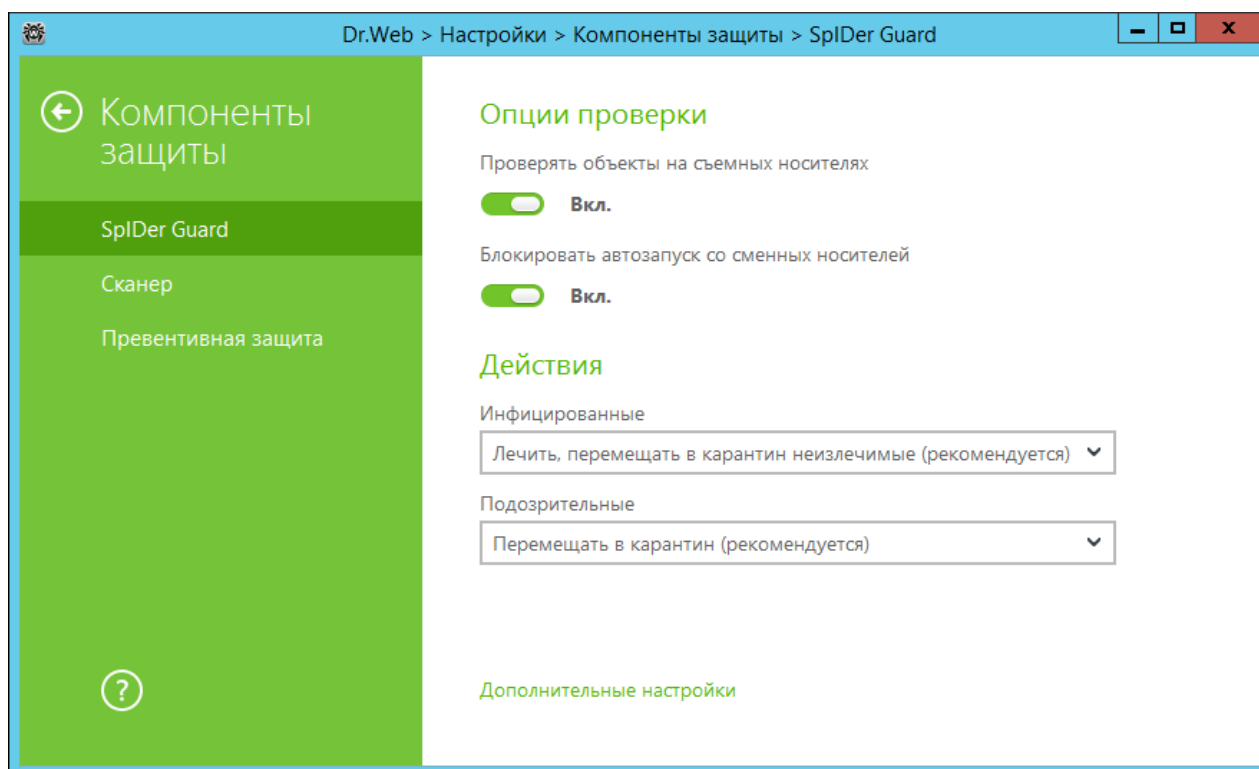
По умолчанию SpIDer Guard запускается автоматически при каждой загрузке операционной системы, при этом запущенный сторож SpIDer Guard не может быть выгружен в течение текущего сеанса работы операционной системы.

12.1.1. Настройка SpIDer Guard



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

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



Опции проверки

SpIDer Guard по умолчанию проверяет объекты на съемных носителях данных (CD/DVD-диски, флеш-памяти и т. д.), а также блокирует автоматический запуск их активного содержимого. Использование этих настроек помогает предотвратить заражение вашего компьютера через съемные носители.



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

Действия

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

Реакция задается отдельно для каждой категории объектов:

- **Инфицированные** - объекты, зараженные известным и (предположительно) излечимым вирусом;
- **Подозрительные** - объекты, предположительно зараженные вирусом или содержащие вредоносный объект;
- различные потенциально опасные объекты. Чтобы развернуть весь список объектов, нажмите ссылку **Дополнительные настройки**.



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

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

Существуют следующие действия, применяемые к обнаруженным объектам:

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



Сторож SpIDer Guard не проверяет составные объекты (архивы, файлы электронной почты или файловые контейнеры), поэтому никакие действия над ними или входящими в их состав файлами не производятся.

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



Режим проверки

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

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



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

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

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

В любом из режимов проверка объектов на сетевых дисках или съемных носителях производится только при включении соответствующих опций в группе настроек **Опции проверки**.



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

Файлы внутри архивов и почтовые ящики по умолчанию не проверяются. Отказ от проверки архивов и электронной почты в условиях постоянной работы сторожа SpIDer Guard не ведет к проникновению вирусов на компьютер, а лишь откладывает момент их обнаружения. При распаковке зараженного архива или открытии зараженного письма



операционная система производит попытку записать инфицированный объект на диск, при этом сторож SpIDer Guard неминуемо обнаруживает вредоносный объект.

Дополнительные возможности

Эта группа настроек позволяет задать параметры проверки на лету, которые будут применяться вне зависимости от выбранного режима работы сторожа SpIDer Guard. Вы можете включить:

- использование эвристического анализатора;
- проверку загружаемых программ и модулей;
- проверку установочных файлов;
- проверку файлов на сетевых дисках (не рекомендуется);
- проверку компьютера на наличие руткитов (рекомендуется).

Эвристический анализ

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

Фоновая проверка на заражение

Входящий в состав Dr.Web Антируткит позволяет в фоновом режиме проводить проверку вашей операционной системы на наличие сложных угроз и при необходимости проводит лечение активного заражения. По умолчанию эта опция включена.

Если опция включена, Антируткит Dr.Web постоянно находится в памяти. В отличие от проверки файлов на лету, проводимой сторожем SpIDer Guard, поиск руткитов производится в системном BIOS компьютера и таких критических областях Windows, как объекты автозагрузки, запущенные процессы и модули, оперативная память, MBR/VBR дисков и др.

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

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



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

Фоновая проверка на руткиты включена по умолчанию.



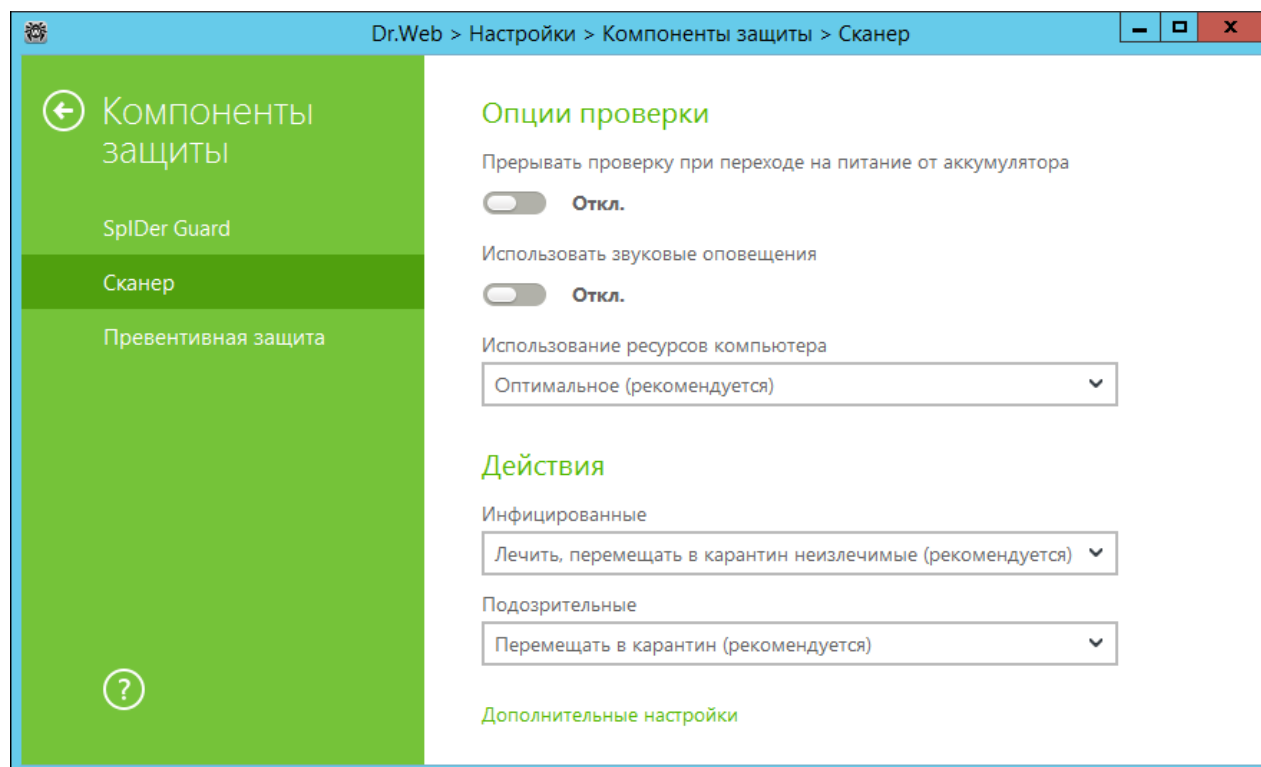
Выключение SpIDer Guard не влияет на фоновую проверку. Если настройка включена, фоновая проверка осуществляется независимо от того, включен или выключен SpIDer Guard.

12.2. Сканер



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

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



Опции проверки

В этой группе доступны общие параметры работы Сканера Dr.Web:

- **Прерывать проверку при переходе на питание от аккумулятора.** Включите эту опцию, чтобы при переходе на питание от аккумулятора проверка была прервана. По умолчанию опция отключена.
- **Использовать звуковые оповещения.** Включите эту опцию, чтобы Сканер Dr.Web сопровождал каждое событие звуковым сигналом. По умолчанию опция отключена.
- **Использование ресурсов компьютера.** Эта опция устанавливает ограничение на использование ресурсов компьютера Сканером Dr.Web. По умолчанию задано оптимальное значение.



Действия

В этом разделе задается реакция Сканера на обнаружение зараженных или подозрительных файлов и вредоносных программ.

Реакция задается отдельно для каждой категории объектов:

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

Вы можете изменить реакцию Сканера на обнаружение каждого типа объектов в отдельности. Состав доступных реакций при этом зависит от типа угрозы.

По умолчанию Сканер пытается вылечить файлы, зараженные известным и потенциально излечимым вирусом, остальные наиболее опасные объекты – перемещает в [Карантин](#).

Существуют следующие действия, применяемые к обнаруженным объектам:

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



Действие	Описание
	Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.



При обнаружении вирусов или подозрительного кода внутри составных объектов действия по отношению к угрозам внутри таких объектов выполняются над всем объектом, а не только над зараженной его частью.

Дополнительные возможности

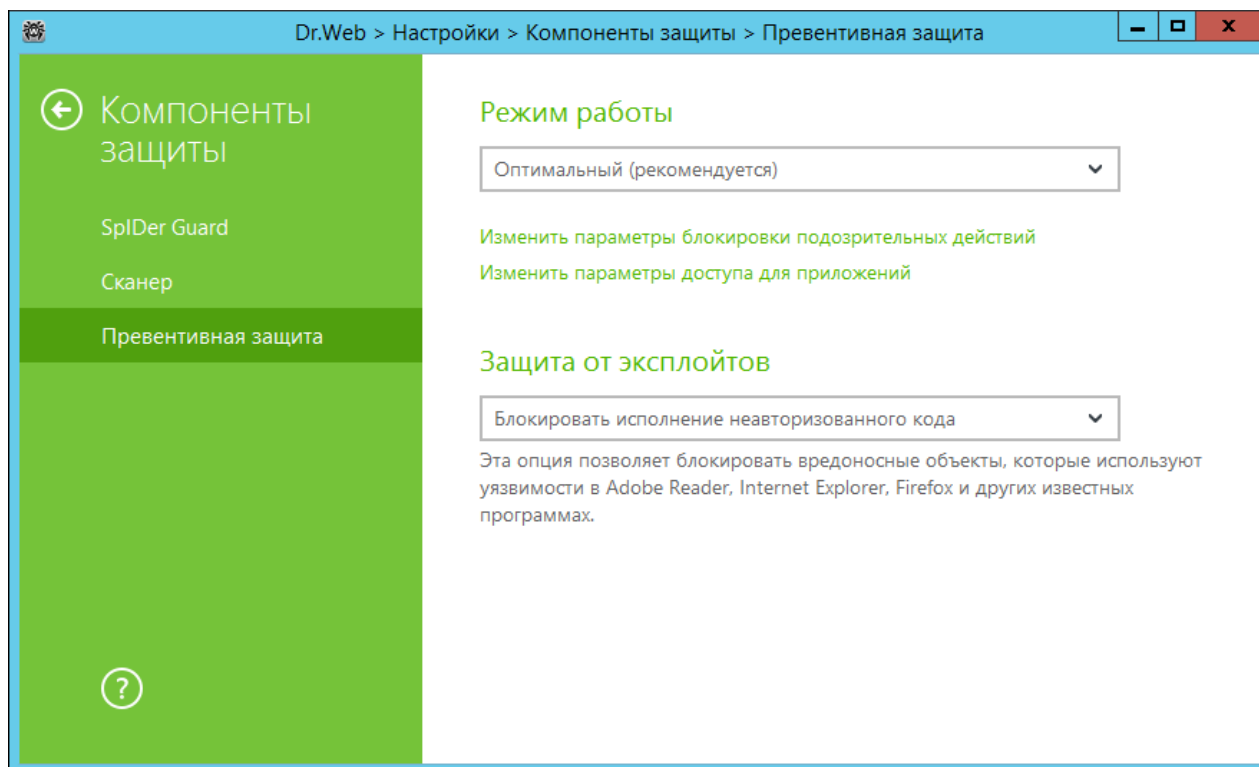
Вы можете отключить проверку установочных пакетов, архивов и почтовых файлов. По умолчанию проверка этих объектов включена.

Вы также можете настроить поведение Сканера после окончания проверки:

1. **Не применять действие.** Сканер выведет таблицу со списком обнаруженных угроз.
2. **Обезвредить обнаруженные угрозы.** Сканер автоматически применит действия к обнаруженным угрозам.
3. **Обезвредить обнаруженные угрозы и выключить компьютер.** Сканер автоматически применит действия к обнаруженным угрозам и после этого выключит компьютер.

12.3. Превентивная защита

В данном разделе вы можете настроить реакцию Dr.Web на действия сторонних приложений, которые могут привести к заражению вашего компьютера, и выбрать уровень защиты от эксплойтов.



При этом вы можете задать отдельный режим защиты для конкретных приложений и общий режим, настройки которого будут применяться ко всем остальным процессам.

Для задания общего режима превентивной защиты, выберите его в списке **Режим работы** или нажмите на опцию **Изменить параметры блокировки подозрительных действий**. В последнем случае откроется окно, где вы сможете подробнее ознакомиться с настройками для каждого из режимов или изменить их. Все изменения в настройках сохраняются в Пользовательском режиме работы. В этом окне вы также можете создать новый профиль для сохранения нужных настроек.

Создание нового профиля

1. Нажмите кнопку .
2. В открывшемся окне укажите название для нового профиля.
3. Просмотрите настройки защиты, заданные по умолчанию и, при необходимости, отредактируйте их.

Для задания настроек превентивной защиты для конкретных приложений, нажмите на опцию **Изменить параметры доступа для приложений**. В открывшемся окне вы можете добавить новое правило для приложения, отредактировать уже созданное правило или удалить ненужное.

Добавление правила

1. Нажмите кнопку .



2. В открывшемся окне нажмите кнопку **Обзор** и укажите путь к исполняемому файлу приложения.
3. Просмотрите настройки защиты, заданные по умолчанию и, при необходимости, отредактируйте их.

Чтобы отредактировать уже созданное правило, выберите его из списка и нажмите кнопку .

Чтобы удалить уже созданное правило, выберите его из списка и нажмите кнопку .

Подробнее с настройками каждого из режимов работы вы можете ознакомиться ниже в разделе Уровень превентивной защиты.

Уровень превентивной защиты

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

Средний уровень защиты можно установить при повышенной опасности заражения. 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.

Параноидальный уровень защиты необходим для полного контроля за доступом к критическим объектам Windows. В данном случае вам также будет доступен интерактивный контроль за загрузкой драйверов и автоматическим запуском программ.

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

Защищаемый объект	Описание
Целостность запущенных приложений	Данная настройка позволяет отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера. Не отслеживается поведение тех процессов, которые добавлены в Исключения .
Целостность файлов пользователей	Данная настройка позволяет отслеживать процессы, которые модифицируют пользовательские файлы по известному алгоритму, свидетельствующему о том, что такие процессы являются угрозой безопасности компьютера. Не отслеживается поведение тех процессов, которые добавлены в Исключения . Для того чтобы защитить свои данные от несанкционированных изменений, вы можете настроить создание защищаемых копий важных файлов.



Защищаемый объект	Описание
HOSTS файл	Файл HOSTS используется операционной системой для упрощения доступа к сети Интернет. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
Низкоуровневый доступ к диску	Данная настройка позволяет запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
Загрузка драйверов	Данная настройка позволяет запрещать приложениям загрузку новых или неизвестных драйверов.
Критические области Windows	Прочие настройки позволяют защищать от модификации ветки реестра (как в системном профиле, так и в профилях всех пользователей). Доступ к Image File Execution Options: • Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Доступ к User Drivers: • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Параметры оболочки Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Нотификаторы Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Автозапуск оболочки Windows: • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Ассоциации исполняемых файлов: • Software\Classes\exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (ключи) Политики ограничения запуска программ (SRP): • Software\Policies\Microsoft\Windows\Safer Плагины Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Автозапуск программ: • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce



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



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

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

Защита от эксплойтов

Эта опция позволяет блокировать вредоносные объекты, которые используют уязвимости в популярных приложениях. В соответствующем выпадающем списке выберите подходящий уровень защиты от эксплойтов.

Уровень защиты	Описание
Блокировать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически заблокирована.
Интерактивный режим	При попытке вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим



Уровень защиты	Описание
	областям операционной системы, Dr.Web выведет соответствующее сообщение. Ознакомьтесь с информацией и выберите нужное действие.
Разрешать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически разрешена.



13. Статистика

Чтобы просмотреть сведения о работе компонентов, откройте меню SpIDer Agent  и перейдите в раздел **Статистика** . На странице **Статистика** доступны отчеты для следующих групп:

- Угрозы
- Обновление

Для записей групп **Угрозы** и **Обновление** доступен подробный отчет. Для записей отчета возможно применение фильтров.

Подробный отчет

Чтобы просмотреть подробный отчет о событиях работы Dr.Web, выберите нужное событие и нажмите кнопку . Повторное нажатие этой кнопки скроет подробные данные о событии.

С помощью кнопки  вы можете удалить, скопировать, экспортировать отдельные события или весь отчет целиком, а также очистить отчет.

Для отбора событий можно воспользоваться фильтрами.

Фильтры

Чтобы посмотреть в списке только те события, которые соответствуют определенным параметрам, воспользуйтесь фильтрами. Для всех отчетов имеются предустановленные фильтры, которые доступны в выпадающем списке вверху страницы каждой группы.

Вы можете создавать собственные фильтры событий. Чтобы создать новый фильтр, нажмите кнопку  и выберите пункт **Создать** в выпадающем списке. В открывшемся окне укажите необходимые критерии фильтрации. Обратите внимание, что в поле **Компонент** вы можете задать сразу несколько компонентов.

События можно отфильтровать по кодам. Для этого укажите их в поле **Код (например: 100-103, -102, 403)** в соответствии со следующими правилами:

- коды нужно указывать через запятую;
- можно указывать диапазон кодов (например, 100-103);
- символ «-» перед кодом исключает его из диапазона.

Таким образом, запись вида «100-103, -102, 403» означает, что необходимо показать все события с «100» по «103», но исключить из фильтра код «-102» и показать событие «403».

Созданные пользователем фильтры можно изменить или удалить.



Приложения

Приложение А. Дополнительные параметры командной строки

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

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

Ключи перечислены в алфавитном порядке.

Параметры для Сканера и Консольного сканера

/AA – автоматически применять действия к обнаруженным угрозам. (Только для Сканера).

/AC – проверять инсталляционные пакеты. По умолчанию опция включена.

/AFS – использовать прямой слеш при указании вложенности внутри архива. По умолчанию опция отключена.

/AR – проверять архивы. По умолчанию опция включена.

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

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

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

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

/ARX:<размер> – максимальный размер проверяемых объектов в архивах, в килобайтах. По умолчанию – без ограничений.

/BI – вывести информацию о вирусных базах. По умолчанию опция включена.



/CUSTOM – запустить Сканер на странице выборочной проверки. Если при этом заданы дополнительные параметры (например, объекты для проверки или параметры /TM, /TB), то будет запущена выборочная проверка указанных объектов. (Только для Сканера).

/CL – использовать облачный сервис Dr.Web. По умолчанию опция включена. (Только для Консольного Сканера).

/DCT – не отображать расчетное время проверки. (Только для Консольного Сканера).

/DR – рекурсивно проверять папки (проверять подпапки). По умолчанию опция включена.

/E: <количество_потоков> – провести проверку в указанное количество потоков.

/FAST – произвести быструю проверку системы. Если при этом заданы дополнительные параметры (например, объекты для проверки или параметры /TM, /TB), то указанные объекты также будут проверены. (Только для Сканера).

/FL: <имя_файла> – проверять пути, указанные в файле.

/FM: <маска> – проверять файлы по маске. По умолчанию проверке подвергаются все файлы.

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

/FULL – произвести полную проверку всех жестких дисков и съемных носителей (включая загрузочные секторы). Если при этом заданы дополнительные параметры (например, объекты для проверки или параметры /TM, /TB), то будет произведена быстрая проверка и проверка указанных объектов. (Только для Сканера).

/FX: <маска> – не проверять файлы, соответствующие маске. (Только для Консольного Сканера).

/GO – режим работы Сканера, при котором вопросы, подразумевающие ожидание ответа от пользователя, пропускаются; решения, требующие выбора, принимаются автоматически. Этот режим полезно использовать для автоматической проверки файлов, например, при ежедневной или еженедельной проверке жесткого диска. В командной строке необходимо указать объект для проверки. Вместе с параметром /GO также можно использовать параметры /LITE, /FAST, /FULL. В этом режиме при переходе на работу от батареи проверка прекращается.

/H или /? – вывести на экран краткую справку о работе с программой. (Только для Консольного Сканера).

/HA – производить эвристический анализ файлов и поиск в них неизвестных угроз. По умолчанию опция включена.



/KEY: <ключевой_файл> – указать путь к ключевому файлу. Параметр необходим в том случае, если ключевой файл находится не в той же папке, что и сканер. По умолчанию используется drweb32.key или другой подходящий из папки C:\Program Files\DrWeb\.

/LITE – произвести стартовую проверку системы, при которой проверяются оперативная память и загрузочные секторы всех дисков, а также провести проверку на наличие руткитов. (Только для Сканера).

/LN – проверять файлы, на которые указывают ярлыки. По умолчанию опция отключена.

/LS – проверять под учетной записью LocalSystem. По умолчанию опция отключена.

/MA – проверять почтовые файлы. По умолчанию опция включена.

/MC: <число_попыток> – установить максимальное число попыток вылечить файл. По умолчанию – без ограничений.

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

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

/NOREBOOT – отменяет перезагрузку и выключение после проверки. (Только для Сканера).

/NT – проверять NTFS-потоки. По умолчанию опция включена.

/OK – выводить полный список проверяемых объектов, сопровождая незараженные пометкой *Ok*. По умолчанию опция отключена.

/P: <приоритет> – приоритет запущенной задачи проверки в общей очереди задач на проверку:

0 – низший.

L – низкий.

N – обычный. Приоритет по умолчанию.

H – высокий.

M – максимальный.

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

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



/QL: <имя_логического_диска> – вывести список всех файлов, помещённых в карантин на указанном логическом диске. (Только для Консольного Сканера).

/QNA – выводить пути в двойных кавычках.

/QR[:[d]][:p]] – удалить файлы с указанного диска *<d>* (*имя_логического_диска*), находящиеся в карантине дольше *<p>* (*количество*) дней. Если *<d>* и *<p>* не указаны, то будут удалены все файлы, находящиеся в карантине, со всех логических дисков. (Только для Консольного Сканера).

/QUIT – закрыть Сканер после проверки (вне зависимости от того, были ли применены действия к обнаруженным угрозам). (Только для Сканера).

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

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

/RK – проверка на наличие руткитов. По умолчанию опция отключена.

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

/RPC: <сек> – тайм-аут соединения с Scanning Engine, в секундах. По умолчанию – 30 секунд. (Только для Консольного Сканера).

/RPCD – использовать динамический идентификатор RPC. (Только для Консольного Сканера).

/RPCE – использовать динамический целевой адрес RPC. (Только для Консольного Сканера).

/RPCE: <целевой_адрес> – использовать указанный целевой адрес RPC. (Только для Консольного Сканера).

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

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

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

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

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

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



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

/SST – выводить время проверки объекта. По умолчанию опция отключена.

/ST – запуск Сканера в фоновом режиме. Если не задан параметр /GO, то графический режим отображается только при обнаружении угроз. В этом режиме при переходе на работу от батареи проверка прекращается.

/TB – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.

/TM – выполнять поиск угроз в оперативной памяти (включая системную область Windows).

/TR – проверять системные точки восстановления.

/W: <сек> – максимальное время проверки, в секундах. По умолчанию – без ограничений.

/WCL – вывод, совместимый с drwebwcl. (Только для Консольного Сканера).

/X:S[:R] – по окончании проверки перевести машину в указанный режим: выключение/перезагрузка/ждущий режим/спящий режим.

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

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



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

`/AC` –режим явно отключается,

`/AC`, `/AC+` –режим явно включается.

Такая возможность может быть полезна в случае, если режим включен/отключен по умолчанию или по выполненным ранее установкам в конфигурационном файле. Список ключей, допускающих применение модификаторов:

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

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

Для ключей `/ARC`, `/ARL`, `/ARS`, `/ART`, `/ARX`, `/NI[:X]`, `/PAL`, `/RPC`, `/W` значение параметра «0» означает, что параметр используется без ограничений.

Пример использования ключей при запуске Консольного сканера:

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

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



Параметры для Модуля обновления

Общие параметры:

Параметр	Описание
-h [--help]	Вывести на экран краткую справку о работе с программой.
-v [--verbosity] arg	Уровень детализации отчета: error (стандартный), info (расширенный), debug (отладочный).
-d [--data-dir] arg	Каталог, в котором размещены репозиторий и настройки.
--log-dir arg	Каталог, в котором будет сохранен отчет.
--log-file 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, exes – выполнить, keyupdate – обновить ключ, download – скачать.
-z [--zone] arg	Список зон, который будет использоваться вместо заданных в конфигурационном файле.

Параметры команды инициализации (init):

Параметр	Описание
-s [--version] arg	Номер версии.
-p [--product] arg	Название продукта.
-a [--path] arg	Путь, по которому будет установлен продукт. Этот каталог будет использоваться по умолчанию в качестве каталога для всех компонентов, включенных в продукт. Модуль обновления будет проверять наличие ключевого файла именно в этом каталоге.
-n [--component] arg	Имя компонента и каталог установки в формате <name>, <install path>.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.



Параметр	Описание
-g [--proxy] arg	Прокси-сервер для обновления в формате <i><адрес>: <порт></i> .
-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: <i><name>, <target revision></i> .
-x [--selfrestart] arg (=yes)	Перезапуск после обновления модуля обновления. По умолчанию значение <i>yes</i> . Если указано значение <i>no</i> , то выводится предупреждение о необходимости перезапуска.
--geo-update	Получить список IP-адресов <i>update.drweb.com</i> перед обновлением.
--type arg (=normal)	Может быть одним из следующих: • <i>reset-all</i> – принудительное обновление всех компонентов; • <i>reset-failed</i> – сбросить все изменения для поврежденных компонентов; • <i>normal-failed</i> – попытаться обновить компоненты, включая поврежденные, до последней либо до указанной версии; • <i>update-revision</i> – обновить компоненты в пределах текущей ревизии; • <i>normal</i> – обновить все компоненты.
-g [--proxy] arg	Прокси-сервер для обновления в формате <i><адрес>: <порт></i> .
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
--param arg	Передать дополнительные параметры в скрипт. Формат: <i><имя>: <значение></i> .
-l [--progress-to-console]	Вывести на консоль информацию о загрузке и выполнении 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.



Параметр	Описание
-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 <i><адрес>: <порт></i> .
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-s [--version] arg	Имя версии
-p [--product] arg	Название продукта, который необходимо скачать.

Коды возврата

Возможные значения кода возврата и соответствующие им события следующие:

Код возврата	Событие
0	Вирусов или подозрений на вирусы не обнаружено.
1	Обнаружены известные вирусы.
2	Обнаружены модификации известных вирусов.
4	Обнаружены подозрительные на вирус объекты.
8	В архиве, контейнере или почтовом ящике обнаружены известные вирусы.
16	В архиве, контейнере или почтовом ящике обнаружены модификации известных вирусов.



Код возврата	Событие
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

Под термином «угроза» в данной классификации следует понимать любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они могут нанести вред пользователю.

В продуктах и документации компании «Доктор Веб» угрозы принято разделять на два типа в соответствии с уровнем опасности:

- **значительные угрозы** – классические компьютерные угрозы, которые сами по себе способны выполнять различные деструктивные и незаконные действия в системе (удаление и кража важной информации, нарушение работы сети и т.д.). Этот тип компьютерных угроз состоит из программ, которые традиционно называют вредоносными (вирусы, черви и троянские программы);
- **незначительные угрозы** – компьютерные угрозы, которые считаются менее опасными по сравнению со значительными угрозами, но могут быть использованы третьими лицами для совершения вредоносных действий. Помимо этого, само присутствие



незначительных угроз в системе является несомненным свидетельством низкого уровня ее защищенности. Специалисты в области информационной безопасности иногда называют этот тип компьютерных угроз «серым» программным обеспечением или потенциально нежелательными программами. К незначительным угрозам относятся рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

Значительные угрозы

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Большая часть вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы делят по типу файлов, которые они инфицируют:

- **файловые вирусы** инфицируют файлы операционной системы (обычно, исполняемые файлы и динамические библиотеки) и активизируются при обращении к зараженному файлу;
- **макро-вирусы** инфицируют файлы документов, используемые приложениями Microsoft® Office или другими программами, допускающими наличие макрокоманд, написанных, чаще всего на языке Visual Basic. Макрокоманды – это встроенные программы (макросы), написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в Microsoft® Word макросы могут запускаться при открытии, закрытии или сохранении документа);
- **скрипт-вирусы** пишутся на языках сценариев (скриптов) и в большинстве случаев заражают другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях;
- **загрузочные вирусы** заражают загрузочные сектора дисков и разделов, а также главные загрузочные сектора жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- **шифрованные вирусы** шифруют свой код при каждом новом заражении, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры;



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

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

Компьютерные черви

В последнее время вредоносные программы типа «компьютерный червь» стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты) и рассылает свои функциональные копии на другие компьютеры. Для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). 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).

В компании «Доктор Веб» червей делят по способу (среде) распространения:

- **сетевые черви** распространяются посредством различных сетевых протоколов и протоколов обмена файлами;
- **почтовые черви** распространяются посредством почтовых протоколов (POP3, SMTP и т.д.).

Троянские программы

Этот тип вредоносных программ не способен к саморепликации. Троянские программы производят какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т.д.), либо делают возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловые сервера, записываются на носители информации или пересылаются в виде вложений в



сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- **бэкдоры** – это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы, они прописывают себя в реестре, модифицируя ключи;
- **дропперы** – это файлы-носители, которые содержат в своем теле вредоносные программы. При запуске дроппера он копирует на диск пользователя вредоносные файлы, не оповещая пользователя, и запускает их;
- **клавиатурные перехватчики (кейлоггеры)** используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действия является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т.д.);
- **кликеры** переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DoS-атак);
- **прокси-трояны** предоставляют злоумышленнику анонимный выход в сеть Интернет через компьютер жертвы;
- **руткиты** предназначены 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 принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (User Mode Rootkits (UMR)), и руткиты, работающие в режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет обнаружение и обезвреживание) (Kernel Mode Rootkits (KMR)).

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Незначительные угрозы

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (файерволах, брандмауэрах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут



пользоваться администраторы для проверки надежности своих сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

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 веб-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, использующие доступ к сети Интернет с разрешения пользователя для того, чтобы попасть на определенные сайты. Обычно имеют подписанный сертификат и уведомляют о всех своих действиях.

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-сервера и т.д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типом компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать в карантин, а также отправлять на анализ специалистам антивирусной лаборатории компании «Доктор Веб».



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 антивирусную лабораторию «Доктор Веб».
3. **Удаление** – эффективное действие для борьбы с компьютерными угрозами. Оно применимо для любого типа вредоносных объектов. Следует отметить, что иногда удаление будет применено к некоторым файлам, для которых было выбрано лечение. Это происходит в случае, когда весь файл целиком состоит из вредоносного кода и не содержит никакой полезной информации. Так, например, под лечением компьютерного червя подразумевается удаление всех его функциональных копий.
4. **Блокировка, переименование** – это также действия, позволяющие обезвредить вредоносные программы, при которых, однако, в файловой системе остаются их полноценные копии. В первом случае блокируются любые попытки обращения от и к вредоносному объекту. Во втором случае, расширение файла изменяется, что делает его неработоспособным.



Приложение В. Принципы именования угроз

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

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

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

Основные префиксы

Префиксы операционной системы

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

- Win – 16-разрядные программы ОС Windows 3.1;
- Win95 – 32-разрядные программы ОС Windows 95, ОС Windows 98, ОС Windows Me;
- WinNT – 32-разрядные программы ОС Windows NT, ОС Windows 2000, ОС Windows XP, ОС Windows Vista;
- Win32 – 32-разрядные программы различных сред ОС Windows 95, ОС Windows 98, ОС Windows Me и ОС Windows NT, ОС Windows 2000, ОС Windows XP, ОС Windows Vista;
- Win32.NET – программы в ОС Microsoft .NET Framework;
- OS2 – программы ОС OS/2;
- Unix – программы различных UNIX-систем;
- Linux – программы ОС Linux;
- FreeBSD – программы ОС FreeBSD;
- SunOS – программы ОС SunOS (Solaris);
- Symbian – программы ОС Symbian OS (мобильная ОС).



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

Вирусы, поражающие файлы MS Office

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

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

Префиксы языка разработки

Группа префиксов HLL применяется для именования вирусов, написанных на языках программирования высокого уровня, таких как C, C++, Pascal, Basic и другие. Используются модификаторы, указывающие на базовый алгоритм функционирования, в частности:

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

К группе префиксов языка разработки можно также отнести:

- Java – вирусы для среды виртуальной машины Java.

Троянские программы

Trojan – общее название для различных Троянских программ (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.

