



Dr.WEB

Агент для Windows

Руководство пользователя



© «Доктор Веб», 2020. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «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, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «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 ООО «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).

Агент Dr.Web для Windows

Версия 11.5

Руководство пользователя

16.04.2020

ООО «Доктор Веб», Центральный офис в России

Адрес: 125040, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: <https://www.drweb.com/>

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!



Содержание

1. Введение	7
1.1. О чем эта документация	8
1.2. Используемые обозначения и сокращения	8
1.3. Методы обнаружения угроз	9
2. Системные требования	13
3. Установка, изменение и удаление программы	15
3.1. Установка при помощи полного инсталляционного пакета	15
3.2. Установка при помощи персонального инсталляционного пакета	18
3.3. Изменение компонентов программы	22
3.4. Удаление программы	23
4. Начало работы	25
4.1. Проверка антивируса	26
5. Инструменты	28
5.1. Менеджер карантина	28
5.2. Поддержка	29
5.2.1. Создание отчета	30
6. Сканер Dr.Web	34
6.1. Запуск и режимы проверки	34
6.2. Действия при обнаружении угроз	36
6.3. Запуск Сканера с параметрами командной строки	38
6.4. Консольный сканер	38
6.5. Запуск проверки по расписанию	39
7. Настройки	41
8. Основные настройки	42
8.1. Уведомления	42
8.2. Самозащита	45
8.3. Устройства	47
8.4. Дополнительно	49
8.5. Сервер	52
8.6. Сообщения сервера	56
9. Офисный контроль	58
9.1. Настройка модуля Офисный контроль	59
9.1.1. Интернет	60



9.1.2. Время	63
9.1.3. Файлы и папки	64
10. Исключения	66
10.1. Сайты	66
10.2. Файлы и папки	68
10.3. Приложения	71
10.4. Антиспам	74
11. Компоненты защиты	77
11.1. SplDer Guard	77
11.1.1. Настройка SplDer Guard	78
11.2. SplDer Gate	83
11.2.1. Настройка SplDer Gate	84
11.3. SplDer Mail	86
11.3.1. Настройка SplDer Mail	87
11.3.2. Антиспам	91
11.4. Сканер	93
11.5. Брандмауэр	96
11.5.1. Обучение Брандмауэра	96
11.5.2. Настройка Брандмауэра	98
11.6. Dr.Web для Outlook	111
11.6.1. Проверка на вирусы	111
11.6.2. Проверка на спам	114
11.6.3. Регистрация событий	117
11.6.4. Статистика	118
11.7. Превентивная защита	119
12. Статистика	125
13. Сообщения сервера	128
14. Техническая поддержка	129
15. Приложение А. Дополнительные параметры командной строки	130
15.1. Параметры для Сканера и Консольного Сканера	130
15.2. Параметры для инсталляционных пакетов	136
15.3. Коды возврата	139
16. Приложение Б. Угрозы и способы их обезвреживания	141
16.1. Классификация угроз	141



16.2. Действия для обезвреживания угроз

146

17. Приложение В. Принципы именования угроз

147



1. Введение

Агент Dr.Web для Windows предназначен для защиты системной памяти, жестких дисков и съемных носителей компьютеров, работающих под управлением ОС семейства Microsoft® Windows®, от угроз любого типа: вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и всех возможных типов вредоносных объектов из любых внешних источников.

Агент Dr.Web для Windows архитектурно состоит из нескольких модулей, отвечающих за различный функционал. Антивирусное ядро и вирусные базы являются общими для всех компонентов и для различных платформ.

Компоненты продукта постоянно обновляются, а вирусные базы, базы категорий веб-ресурсов и базы правил спам-фильтрации сообщений электронной почты регулярно дополняются новыми сигнатурами угроз. Постоянное обновление обеспечивает актуальный уровень защиты устройств пользователей, а также используемых ими приложений и данных. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре.

Агент Dr.Web для Windows способен обнаруживать и удалять с компьютера различные нежелательные программы: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы, программы взлома. Для обнаружения таких программ и действий над содержащими их файлами применяются стандартные средства антивирусных компонентов 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 и производит антивирусную проверку компьютера.

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

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

SplDer Mail — почтовый антивирусный сторож для рабочих станций, который перехватывает обращения любых почтовых клиентов, работающих на компьютере, к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP (под IMAP4 имеется в виду IMAPv4rev1), обнаруживает и обезвреживает угрозы до получения писем почтовым клиентом с сервера или до отправки письма на почтовый сервер. Почтовый сторож также может осуществлять проверку сообщений на спам с помощью Антиспама Dr.Web.

Dr.Web для Outlook — подключаемый модуль, который проверяет почтовые ящики Microsoft Outlook на наличие угроз и спама.



SplDer Gate — модуль антивирусной проверки HTTP-трафика. При настройках по умолчанию веб-антивирус SplDer Gate автоматически проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих вирусы и другие вредоносные программы. Также по умолчанию включена URL-фильтрация nereкомендуемых сайтов и сайтов, известных как источники распространения вирусов.

Офисный контроль — компонент, который ограничивает доступ к сайтам, файлам и папкам, а также позволяет ограничить время работы в сети Интернет и за компьютером для каждой учетной записи Windows.

Брандмауэр Dr.Web — персональный межсетевой экран, предназначенный для защиты вашего компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети.

Агент Dr.Web — модуль, с помощью которого осуществляется настройка и управление работой компонентов продукта.

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, предназначенная для опытных пользователей.



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

1.2. Используемые обозначения и сокращения

В данном руководстве используются следующие условные обозначения:



Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
<i>Антивирусная сеть</i>	Новый термин или акцент на термине в описаниях.
<i><IP-address></i>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
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 угроз

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

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он основан на поиске в содержимом анализируемого объекта 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 «grcode»). Кроме того, использование технологии Origins



Tracing позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing, добавляется постфикс `.Origin`.

Эмуляция исполнения

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

Эвристический анализ

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

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

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



Поведенческий анализ

Методы поведенческого анализа позволяют анализировать последовательность действий всех процессов в системе. При обнаружении признаков поведения вредоносной программы действия приложения блокируются.

Dr.Web Process Heuristic

Технология поведенческого анализа Dr.Web Process Heuristic защищает от новейших, наиболее опасных вредоносных программ, которые способны избежать обнаружения традиционными сигнатурными и эвристическими механизмами.

Dr.Web Process Heuristic анализирует поведение каждой запущенной программы и на основе актуальных знаний о том, как ведут себя вредоносные программы, делает вывод о ее опасности, после чего принимаются необходимые меры по нейтрализации угрозы.

Данная технология защиты данных позволяет свести к минимуму потери от действий неизвестного вируса при минимальном потреблении ресурсов защищаемой системы.

Dr.Web Process Heuristic контролирует любые попытки изменения системы:

- распознает процессы вредоносных программ, изменяющих нежелательным образом пользовательские файлы (например, попытки шифрования со стороны троянских программ-шифровальщиков), в том числе расположенные в каталогах, доступных по сети;
- препятствует попыткам вредоносных программ внедриться в процессы других приложений;
- защищает от модификаций вредоносными программами критических участков системы;
- выявляет и прекращает вредоносные, подозрительные или ненадежные сценарии и процессы;
- блокирует возможность изменения вредоносными программами загрузочных областей диска с целью невозможности запуска (например, буткитов) на компьютере;
- предотвращает отключение безопасного режима Windows, блокируя изменения реестра;
- не позволяет вредоносным программам изменить правила запуска программ;
- пресекает загрузки новых или неизвестных драйверов без ведома пользователя;
- блокирует автозапуск вредоносных программ, а также определенных приложений, например, анти-антивирусов, не давая им зарегистрироваться в реестре для последующего запуска;
- блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможной установку троянских программ под видом нового виртуального устройства;
- не позволяет вредоносному программному обеспечению нарушить нормальную работу системных служб.



Dr.Web Process Dumper

Комплексный анализатор упакованных угроз Dr.Web Process Dumper значительно повышает уровень детектирования якобы «новых угроз» — известных вирусной базе Dr.Web, но скрытых под новыми упаковщиками, а также исключает необходимость добавления в базы все новых и новых записей об угрозах. Сохранение компактности вирусных баз Dr.Web, в свою очередь, не требует постоянного увеличения системных требований и обеспечивает традиционно малый размер обновлений при неизменно высоком качестве детектирования и лечения.

Dr.Web ShellGuard

Технология Dr.Web ShellGuard защищает компьютер от *эксплойтов* — вредоносных объектов, пытающихся использовать уязвимости с целью получения контроля над атакуемыми приложениями или операционной системой в целом.

Dr.Web ShellGuard защищает распространенные приложения, устанавливаемые на компьютеры под управлением Windows:

- интернет-браузеры (Internet Explorer, Mozilla Firefox, Яндекс.Браузер, Google Chrome, Vivaldi Browser и др.);
- приложения MS Office, включая MS Office 2016;
- системные приложения;
- приложения, использующие java-, flash- и pdf-технологии;
- медиапроигрыватели.

Метод машинного обучения

Применяется для поиска и нейтрализации вредоносных объектов, которых еще нет в вирусных базах. Преимущество этого метода заключается в распознавании вредоносного кода без исполнения, только на основе его характеристик.

Обнаружение угроз строится на классификации вредоносных объектов согласно определенным признакам. С помощью технологии машинного обучения, основанной на методе опорных векторов, происходит классификация и запись в базу фрагментов кода сценарных языков. Затем проверяемые объекты анализируются на основе соответствия признакам вредоносного кода. Технология машинного обучения автоматизирует обновление списка данных признаков и пополнение вирусных баз.

Метод машинного обучения существенно экономит ресурсы операционной системы, так как не требует исполнения кода для выявления угроз, а динамическое машинное обучение классификатора может осуществляться и без постоянного обновления вирусных баз, которое используется при сигнатурном анализе.



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;
- если будет установлен Брандмауэр Dr.Web, необходимо удалить с компьютера другие межсетевые экраны;
- 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 XP с пакетом обновлений SP2 или более поздними; • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10 19H1 или более ранняя; • Windows Server 2003 с пакетом обновлений SP1; • Windows Server 2008 с пакетом обновлений SP2 или более поздними. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10 19H1 или более ранняя;



Компонент	Требование
	• Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016.
Свободная оперативная память	512 МБ и больше.
Разрешение	Рекомендуемое разрешение экрана не менее 800x600.
Поддержка виртуальных и облачных сред	Поддерживается функционирование программы в следующих средах: • VMware; • Hyper-V; • Xen; • KVM.
Прочее	Для обновления вирусных баз Dr.Web и компонентов Dr.Web требуется подключение к серверу централизованной защиты или сети Интернет в Мобильном режиме. Для подключаемого модуля Dr.Web для Outlook необходим установленный клиент Microsoft Outlook из состава MS Office: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 с пакетом обновлений SP2; • Outlook 2013; • Outlook 2016.



Агент Dr.Web 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.

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



3. Установка, изменение и удаление программы

Перед началом установки Агент Dr.Web для Windows ознакомьтесь с [системными требованиями](#), а также рекомендуется выполнить следующие действия:

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



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

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

Установка, изменение и удаление Dr.Web могут быть осуществлены двумя способами:

1. Удаленно — с сервера централизованной защиты через сеть. Производится администратором антивирусной сети, при этом вмешательство пользователя не требуется.
2. Локально — на машине пользователя непосредственно. При этом для установки Dr.Web может использоваться [полный инсталлятор](#) или [персональный инсталляционный пакет](#).

Установка Dr.Web возможна в одном из следующих режимов:

- в режиме командной строки;
- в режиме мастера установки.

3.1. Установка при помощи полного инсталляционного пакета

Установка в режиме командной строки

Для запуска установки Dr.Web в режиме командной строки перейдите в папку, где расположен дистрибутив, после чего введите имя исполняемого файла установки (drweb-11.05.0-xxxxxxx-esuite-agent-full-windows.exe) с необходимыми параметрами.

Полный список параметров командной строки для инсталляционных пакетов приведен в [Приложении А](#).



Установка в режиме мастера установки

1. Запустите инсталляционный пакет, полученный от администратора. Откроется окно Мастера установки Dr.Web.



Если на рабочей станции уже установлены антивирусные программы, то Мастер установки предпримет попытку их удалить. Если попытка окажется неудачной, вам будет необходимо самостоятельно удалить используемое на рабочей станции антивирусное программное обеспечение.

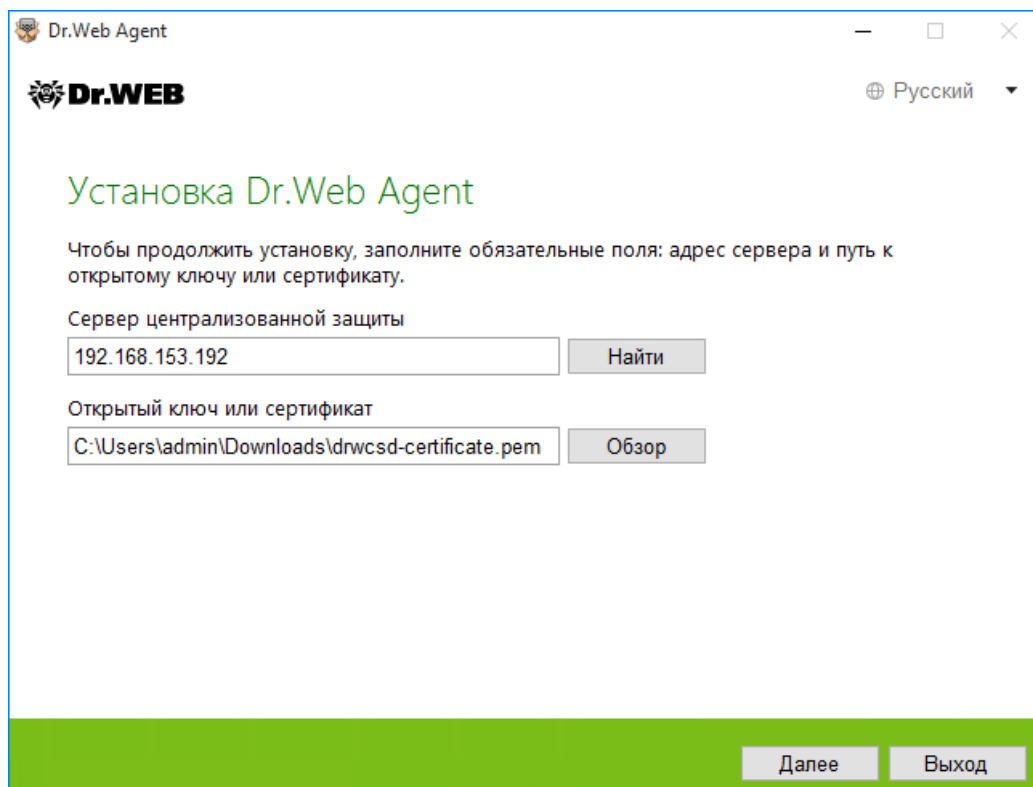


Рисунок 1. Мастер установки

2. В поле **Сервер централизованной защиты** введите сетевой адрес сервера, с которого будет производиться установка Dr.Web, а в поле **Открытый ключ или сертификат** укажите полный путь к открытому ключу шифрования (**drwcsd.pub**) или сертификату с расширением **.pem**, расположенному на вашем компьютере.

Нажмите кнопку **Далее**.

3. Мастер установки проинформирует вас о готовности к установке. Вы можете запустить процесс установки с параметрами по умолчанию, нажав **Установить**.

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

4. Нажмите **Далее**.



5. Если на предыдущем шаге вы нажали кнопку **Установить**, то перейдите к шагу 8. В противном случае откроется окно **Параметры установки**.

На вкладке **Компоненты** будет предоставлен выбор устанавливаемых компонентов Dr.Web.

Активируйте флажки напротив тех компонентов, которые вы хотите установить на ваш компьютер. По умолчанию выбраны все компоненты, кроме Брандмауэра Dr.Web.

6. На вкладке **Путь установки** вы можете задать папку установки, в которую будет установлен Агент Dr.Web для Windows.

По умолчанию это папка DrWeb, расположенная в папке Program Files на системном диске. Для изменения пути установки нажмите кнопку **Обзор** и укажите требуемый путь.

7. На вкладке **Дополнительные опции** вы можете задать дополнительные настройки.

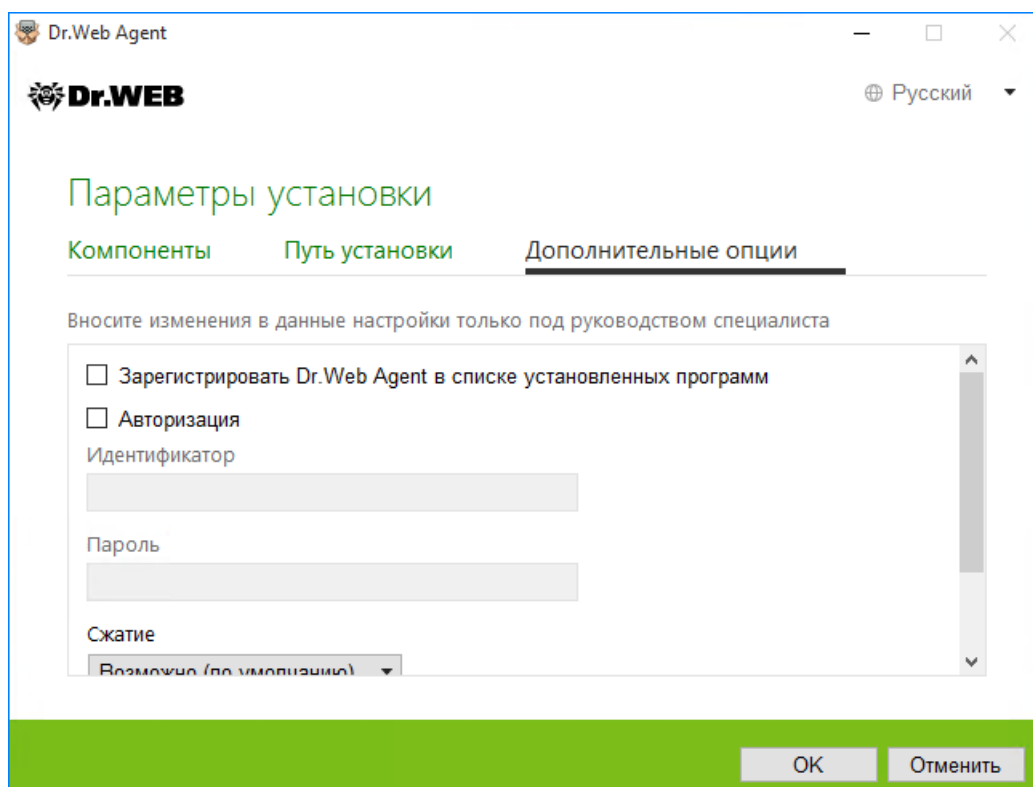


Рисунок 2. Мастер установки, дополнительные настройки

При необходимости установите флажок **Зарегистрировать Dr.Web Agent в списке установленных программ**. Данная опция позволяет, в том числе, осуществлять [удаление](#) программы Dr.Web с помощью Панели управления Windows.

Для авторизации на сервере централизованной защиты вручную активируйте флажок **Авторизация**. Далее необходимо задать параметры авторизации станции:

- **Идентификатор** станции на сервере;
- **Пароль** доступа к серверу.

При этом станция получит доступ без ручного подтверждения администратором на сервере.

В выпадающих списках **Сжатие** и **Шифрование** задайте соответствующие режимы для трафика между сервером и Dr.Web.



Для сохранения внесенных изменений нажмите **ОК**, после чего нажмите кнопку **Установить**.

8. Начнется установка Dr.Web. Вмешательство пользователя не требуется.
9. После завершения установки программа сообщит о необходимости перезагрузить компьютер. Нажмите кнопку **Перезагрузить сейчас**.

3.2. Установка при помощи персонального инсталляционного пакета

Установка в режиме командной строки

Для запуска установки Dr.Web в режиме командной строки перейдите в папку, где расположен дистрибутив, после чего введите имя исполняемого файла установки (drweb_ess_windows_<Station_name>.exe) с необходимыми параметрами.

Полный список параметров командной строки для инсталляционных пакетов приведен в [Приложении А](#).

Установка в режиме мастера установки

1. Запустите инсталляционный пакет, полученный от администратора. Откроется Мастер установки Dr.Web.



Если на рабочей станции уже установлены антивирусные программы, то Мастер установки предпримет попытку их удалить. Если попытка окажется неудачной, вам будет необходимо самостоятельно удалить используемое на рабочей станции антивирусное программное обеспечение.

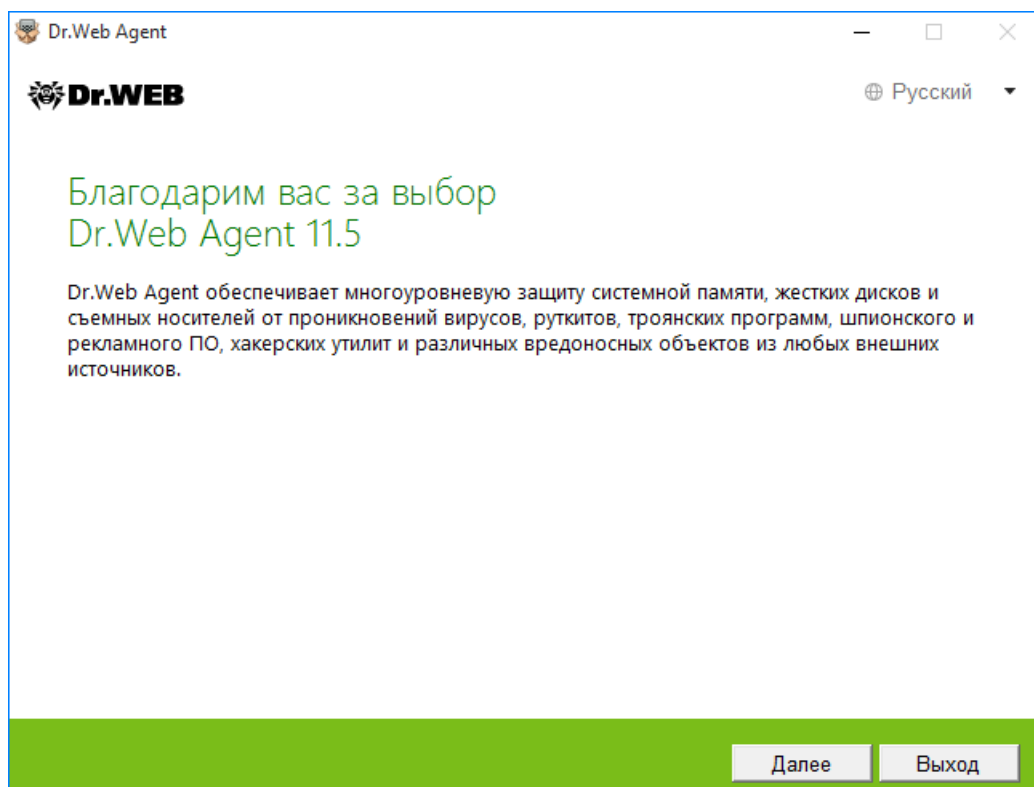


Рисунок 3. Мастер установки

2. Нажмите **Далее**.
3. На следующем шаге мастера укажите путь к открытому ключу шифрования (**drwcsd.pub**) или сертификату с расширением **.pem**, расположенному на вашем компьютере.
4. Вы можете изменить параметры соединения с сервером централизованной защиты. Для этого перейдите по соответствующей ссылке, при этом откроется окно **Параметры соединения**.



Настоятельно рекомендуется ничего не менять без согласования с администратором вашей антивирусной сети.

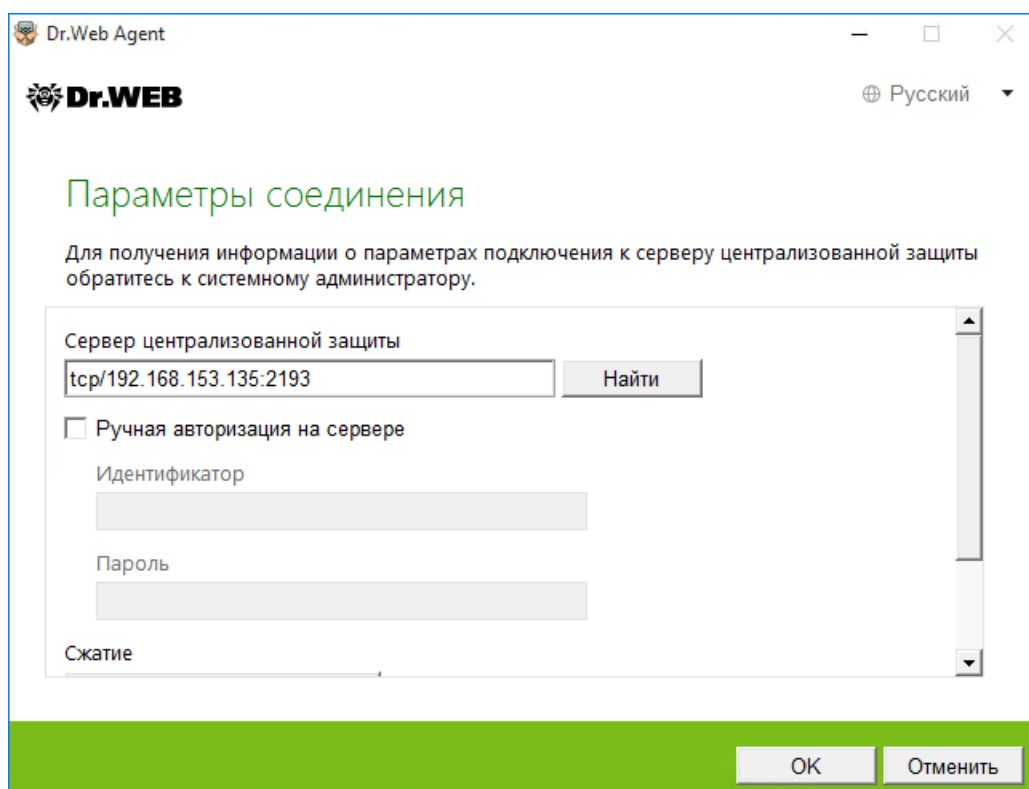


Рисунок 4. Установка параметров соединения с сервером централизованной защиты



Для получения информации о параметрах подключения к серверу централизованной защиты обратитесь к администратору.

В поле **Сервер централизованной защиты** задайте сетевой адрес сервера, с которого будет производиться установка Dr.Web. Поле заполняется автоматически, указываются данные сервера, на котором был создан установочный файл.

Для варианта ручной авторизации на сервере активируйте соответствующий флажок. Далее необходимо задать параметры авторизации станции:

- **Идентификатор** станции на сервере;
- **Пароль** доступа к серверу.

При этом станция получит доступ без ручного подтверждения администратором на сервере.



При установке Dr.Web при помощи установочного файла, созданного в Центре управления Dr.Web, поля **Идентификатор** и **Пароль** для варианта ручной авторизации заполняются автоматически.

В выпадающих списках **Сжатие** и **Шифрование** задайте соответствующие режимы для трафика между сервером и Dr.Web.

Для сохранения внесенных изменений нажмите **ОК**, после чего нажмите **Далее**.



Если соединение не установлено, проверьте по ссылке сетевые параметры и/или повторите попытку подключения, нажав соответствующую кнопку.

5. При успешном подключении к серверу централизованной защиты откроется окно с сообщением о готовности к установке. Вы можете запустить процесс установки с параметрами по умолчанию, нажав кнопку **Установить**.

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

6. Если на предыдущем шаге вы нажали кнопку **Установить**, то перейдите к шагу 8. В противном случае откроется окно **Параметры установки**.

На вкладке **Компоненты** будет предоставлен выбор устанавливаемых компонентов Dr.Web.

Активируйте флажки напротив тех компонентов, которые вы хотите установить на ваш компьютер. По умолчанию выбраны все компоненты, кроме Брандмауэра Dr.Web.

7. На вкладке **Путь установки** вы можете задать папку установки, в которую будет установлен **Агент Dr.Web для Windows**. По умолчанию это папка DrWeb, расположенная в папке Program Files на системном диске. Для изменения пути установки нажмите кнопку **Обзор** и укажите требуемый путь.

8. На вкладке **Дополнительные опции** вы можете задать дополнительные настройки для установки программы Dr.Web.

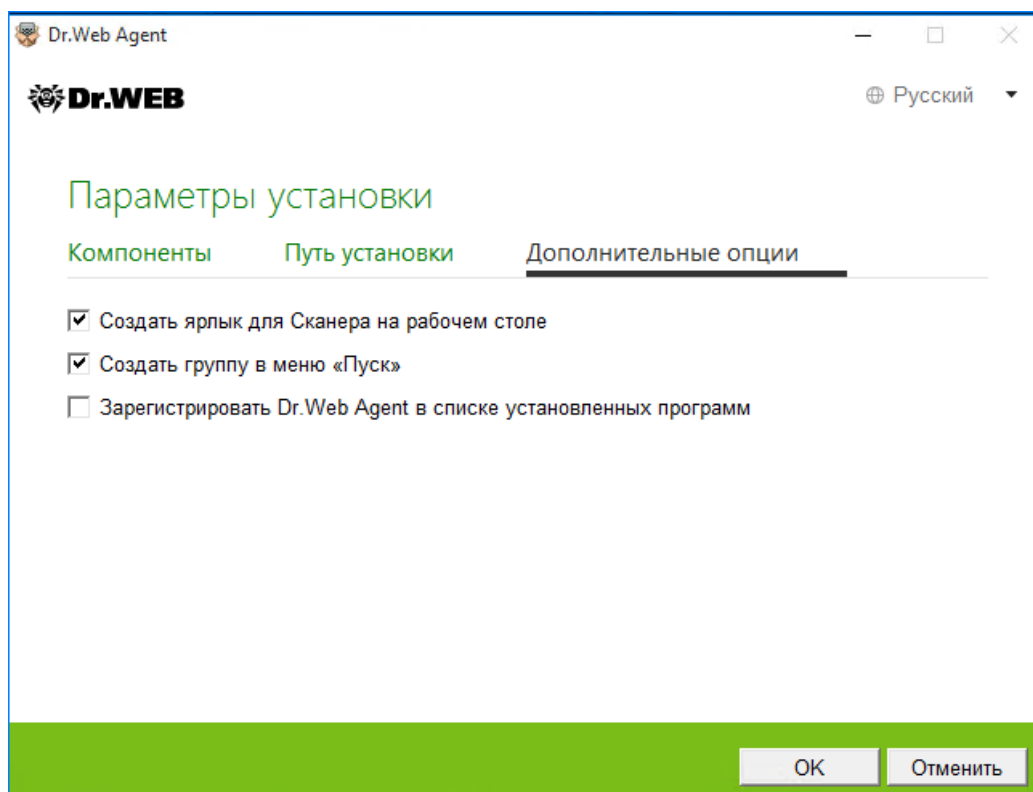


Рисунок 5. Мастер установки, дополнительные настройки



При необходимости активируйте флажок **Зарегистрировать Dr.Web Agent в списке установленных программ**. Данная опция позволяет, в том числе, осуществлять удаление программы Dr.Web с помощью Панели управления Windows.

Для сохранения внесенных изменений нажмите **ОК**, после чего нажмите **Установить**.

9. Начнется установка Dr.Web. Вмешательство пользователя не требуется.
10. После завершения установки мастер сообщит о необходимости перезагрузить компьютер. Нажмите кнопку **Перезагрузить сейчас**.

Ошибка службы BFE при установке программы Dr.Web

Для функционирования некоторых компонентов программы Dr.Web необходимо наличие запущенной службы базового модуля фильтрации (BFE). В случае если данная служба отсутствует или повреждена, установка Dr.Web будет невозможна. Повреждение или отсутствие службы BFE может указывать на наличие угроз безопасности вашего компьютера.

Если попытка установки программы Dr.Web завершилась с ошибкой службы BFE, выполните следующие действия:

1. Просканируйте систему станции при помощи лечащей утилиты CureNet! от компании «Доктор Веб». Вы можете запросить демонстрационную версию утилиты (диагностика без функции лечения) по адресу <https://download.drweb.com/curenet/>.
Ознакомиться с условиями использования и стоимостью полной версии утилиты вы можете по адресу <https://estore.drweb.com/utilities/>.
2. Восстановите службу BFE. Для этого вы можете воспользоваться утилитой для устранения проблем в работе брандмауэра от компании Microsoft (для операционных систем Windows 7 и выше). Скачать утилиту вы можете на сайте: <https://support.microsoft.com/en-us/help/17613/automatically-diagnose-and-fix-problems-with-windows-firewall>.
3. Запустите Мастер установки Dr.Web и произведите установку согласно штатной процедуре, приведенной выше.

Если проблема не устранена, обратитесь в службу технической поддержки компании «Доктор Веб».

3.3. Изменение компонентов программы

1. Чтобы удалить или изменить компоненты Dr.Web, перейдите в раздел Панели управления Windows, посвященный установке и удалению программ.
2. В списке установленных программ выберите строку с названием программы.
3. Нажмите **Изменить**, при этом откроется окно Мастера удаления/изменения компонентов программы.

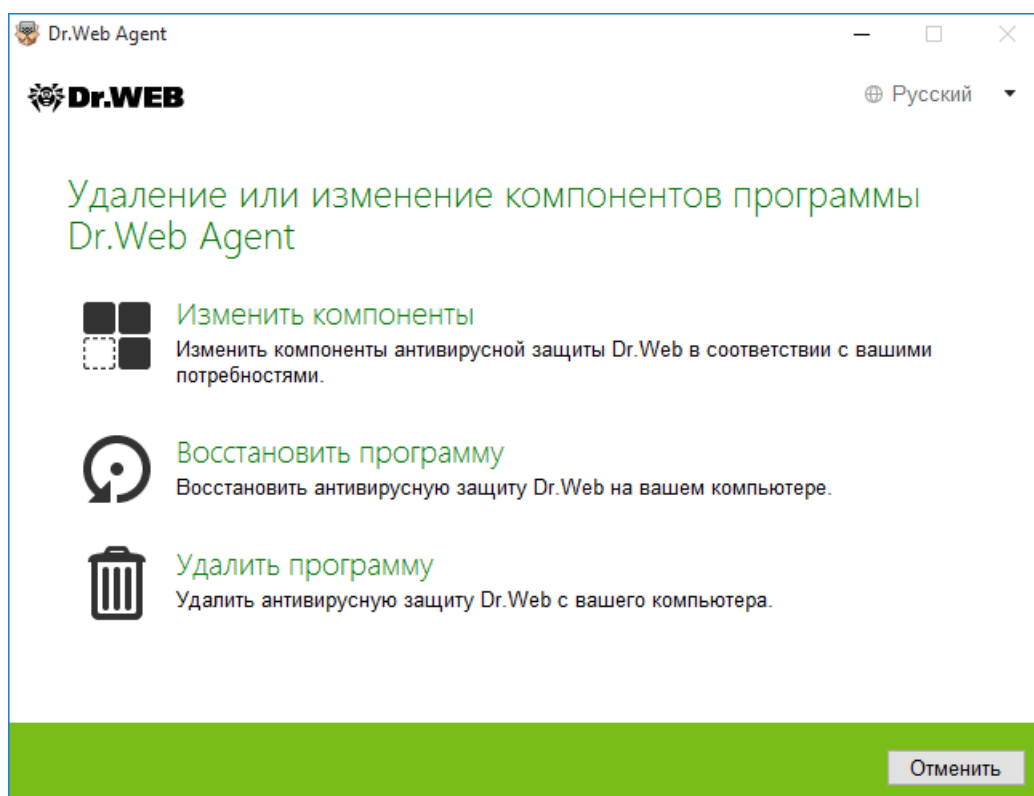


Рисунок 6. Мастер удаления/изменения компонентов

4. Выберите одну из опций:

- **Изменить компоненты.** В открывшемся окне установите флажки напротив компонентов, которые хотите добавить, либо снимите флажки напротив удаляемых компонентов. Определив нужную конфигурацию, нажмите **Применить**.
- **Восстановить программу,** если необходимо восстановить антивирусную защиту на вашем компьютере. Эта функция применяется в том случае, когда некоторые из компонентов программы Dr.Web были повреждены.
- **Удалить программу,** чтобы удалить все установленные компоненты.

3.4. Удаление программы



Для возможности локального удаления Dr.Web, данная опция должна быть разрешена администратором на сервере централизованной защиты.

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



Удаление Dr.Web из Панели управления Windows



Данный метод удаления доступен только в том случае, если с помощью Мастера установки был установлен флажок **Зарегистрировать Dr.Web Agent в списке установленных программ**.

Если Dr.Web был установлен в фоновом режиме, то удаление Dr.Web штатными средствами будет доступно, только если при установке был использован ключ – regagent.

Для удаления программы Агент Dr.Web для Windows запустите компонент удаления программ операционной системы Windows.

1. В открывшемся списке выберите строку с названием программы.
2. Нажмите кнопку **Удалить**.
3. 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 Agent** и **Защищаемые копии файлов**. Нажмите кнопку **Установить**.
4. В следующем окне для подтверждения удаления Dr.Web нажмите кнопку **Удалить**.
5. 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.

Удаление в режиме командной строки

Для удаления Dr.Web в режиме командной строки введите имя исполняемого файла (win-es-agent-setup.exe) с необходимыми параметрами.



Файл win-es-agent-setup.exe размещен в папке C:\ProgramData\Doctor Web\Setup\.

Например, при запуске следующей команды будет проведено удаление Dr.Web в фоновом режиме и проведена перезагрузка:

```
win-es-agent-setup.exe /instMode remove /silent yes
```




4. Начало работы

После установки программы Dr.Web в область уведомлений Windows добавляется значок .



Значок Dr.Web не отображается в области уведомлений, если администратор вашей антивирусной сети установил соответствующую настройку на сервере централизованной защиты.

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

Значок Dr.Web отражает текущее состояние программы:

-  — все компоненты, необходимые для защиты компьютера, запущены и работают правильно, соединение с сервером централизованной защиты установлено;
-  — самозащита Dr.Web или хотя бы один из компонентов отключены, что ослабляет защиту антивируса и компьютера; либо ожидается соединение с сервером, но ещё не установлено. Возможно, сервер отклонил подключение рабочей станции или отказал в доступе к своим ресурсам. Включите самозащиту или отключенный компонент, дождитесь соединения с сервером или обратитесь к администратору вашей антивирусной сети, если соединение не устанавливается;
-  — 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. Если иконка не изменится, обратитесь к администратору вашей антивирусной сети.

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

Для доступа к меню Dr.Web щелкните по значку  в области уведомлений Windows.



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

В меню Dr.Web  сосредоточены основные средства управления и настройки программы.

Инструменты. Открывает меню, предоставляющее доступ к разделам:

- [Менеджер карантина](#);
- [Поддержка](#).

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



Сканер. Быстрый доступ к запуску разных типов проверки.

Сообщения сервера. Открывает окно с просмотра сообщений сервера.

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**. Обратите внимание, что возврат в режим пользователя осуществляется через 15 минут после переключения в режим администратора. Если по истечении этого срока вы продолжаете работать с настройками, то переход в режим пользователя осуществится после закрытия окна настроек.

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

Настройки . Открывает окно с доступом к основным настройкам, настройкам компонентов защиты, а также к модулю Офисный контроль и исключениям.



Изменение настроек и отключение какого-либо компонента невозможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, не дал разрешения на применение этих действий.

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

Если вы забыли пароль к настройкам продукта, обратитесь к администратору вашей антивирусной сети.

Справка . Открывает справку.

4.1. Проверка антивируса

Проверка с помощью файла EICAR

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 «вирусом».



При работе в [оптимальном режиме](#) SplDer 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 SplDer Guard автоматически обрабатывает файл как вредоносную программу и по умолчанию перемещает его в Карантин.



5. Инструменты

Откройте меню Dr.Web  и запустите **Инструменты**. Чтобы были доступны все опции, переключитесь в [режим администратора](#).

Для просмотра списка изолированных файлов и восстановления файлов из карантина, выберите [Менеджер карантина](#).

Если у вас возникли вопросы или неполадки в процессе работы Dr.Web, выберите раздел [Поддержка](#).

5.1. Менеджер карантина

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

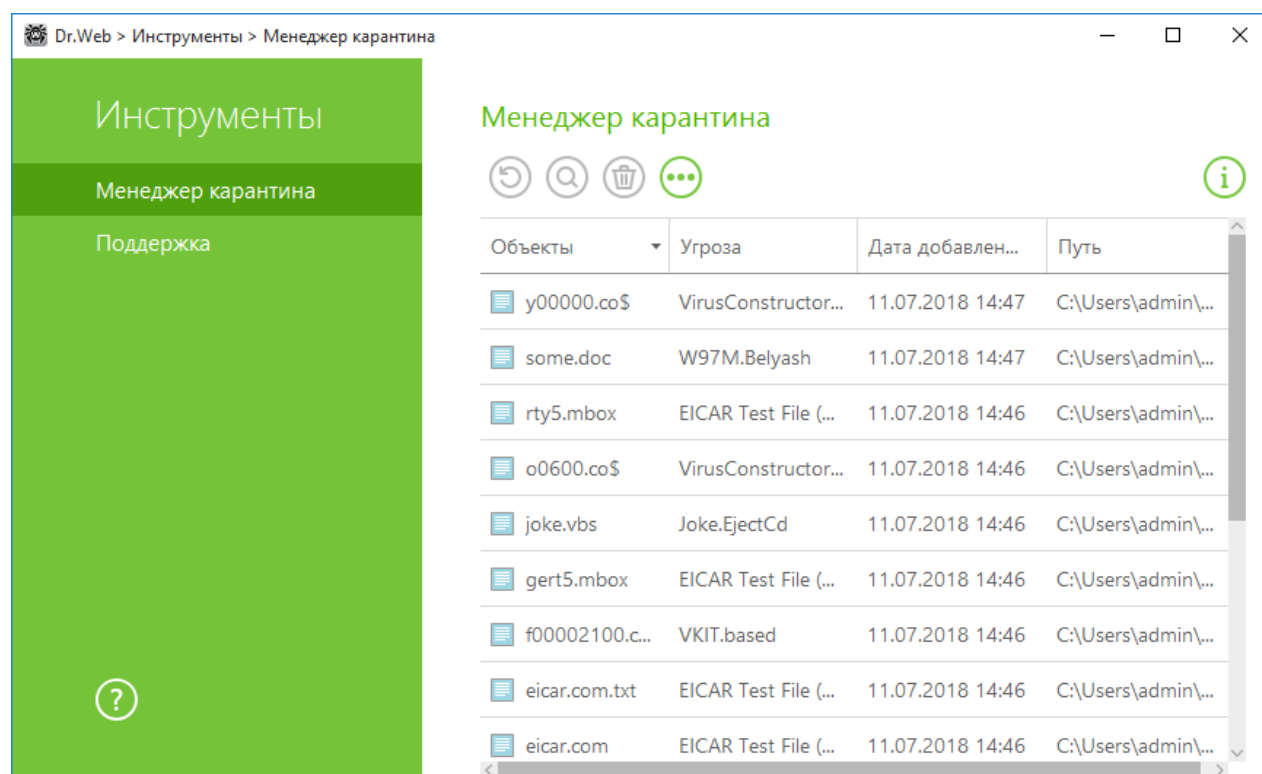


Рисунок 7. Объекты в карантине

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.



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 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.

Резервные копии, перемещенные в карантин, по умолчанию не отображаются в таблице. Чтобы видеть их в списке объектов, нажмите кнопку  и в выпадающем списке выберите пункт **Показывать резервные копии**.

Работа с объектами в карантине

В [режиме администратора](#) для каждого объекта доступны следующие кнопки управления:

- **Восстановить** — переместить один или несколько выбранных объектов под заданным именем в нужную папку;



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

- **Перепроверить** — повторно проверить объект, перемещенный в карантин.
- **Удалить** — удалить один или несколько выбранных объектов из карантина и из системы.

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

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

5.2. Поддержка

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

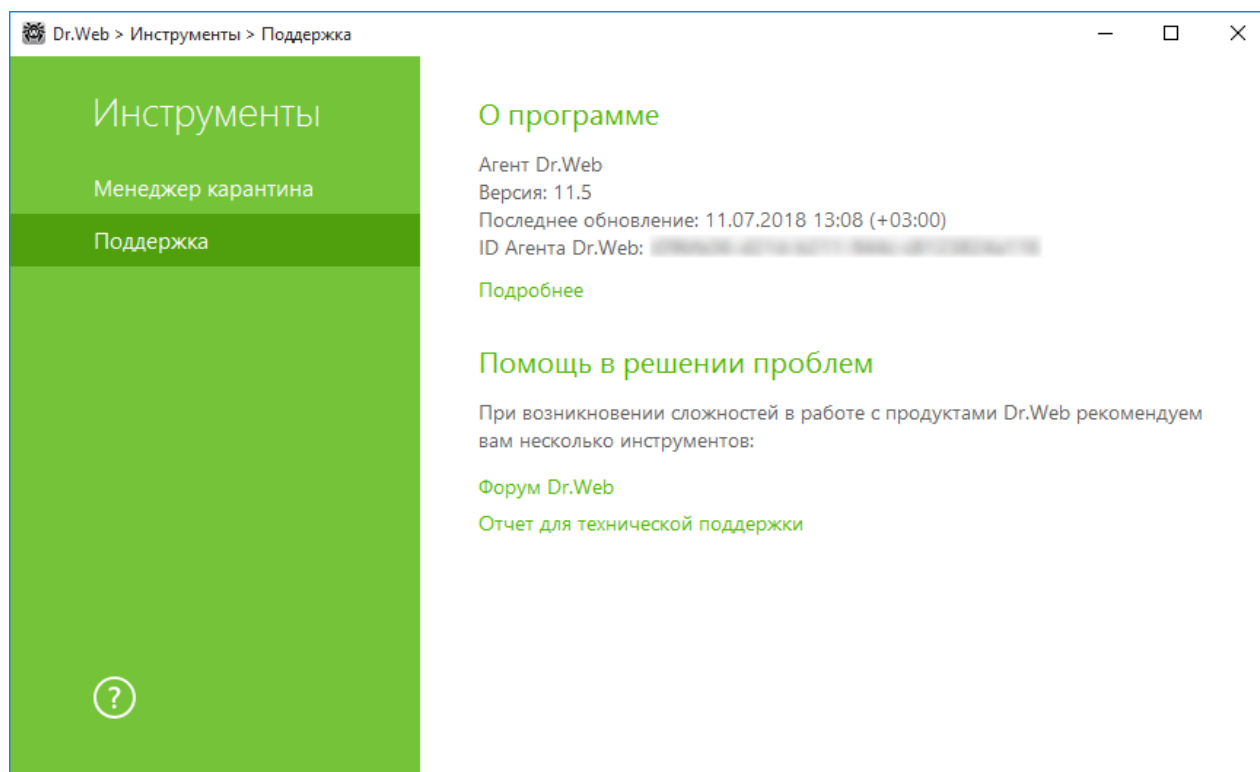


Рисунок 8. Сведения о версии продукта и поддержка

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

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

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

Если проблему не удалось решить после обращения на форум Dr.Web, вы можете заполнить веб-форму вопроса в соответствующей секции раздела <https://support.drweb.com>. К своему запросу вы можете прикрепить отчет для технической поддержки, скриншоты и другую необходимую информацию.

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

5.2.1. Создание отчета

При обращении к администратору вашей антивирусной сети вы можете сформировать отчет о вашей операционной системе и работе Dr.Web.

Чтобы создать отчет

1. Откройте меню .



2. Перейдите в пункт **Инструменты**.
3. Выберите **Поддержка**.

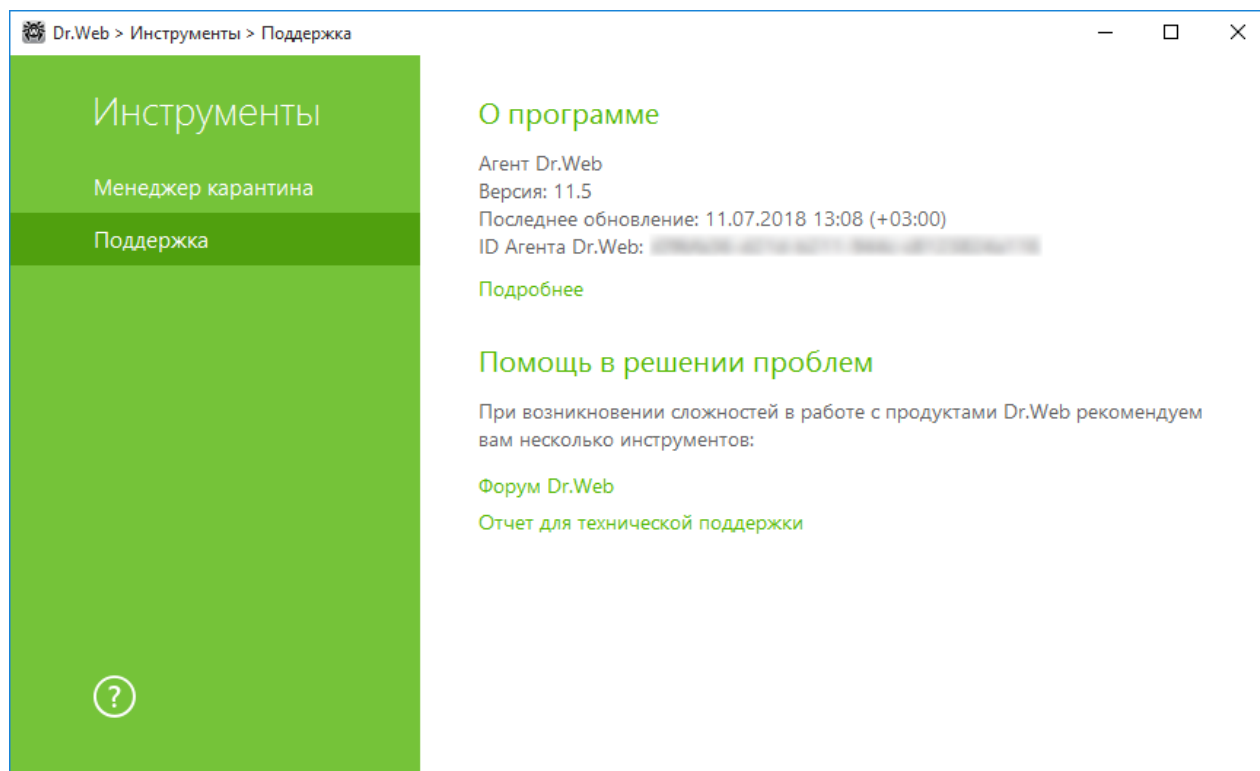


Рисунок 9. Поддержка

4. Нажмите ссылку **Отчет для технической поддержки**.
5. В открывшемся окне нажмите кнопку **Создать отчет**.

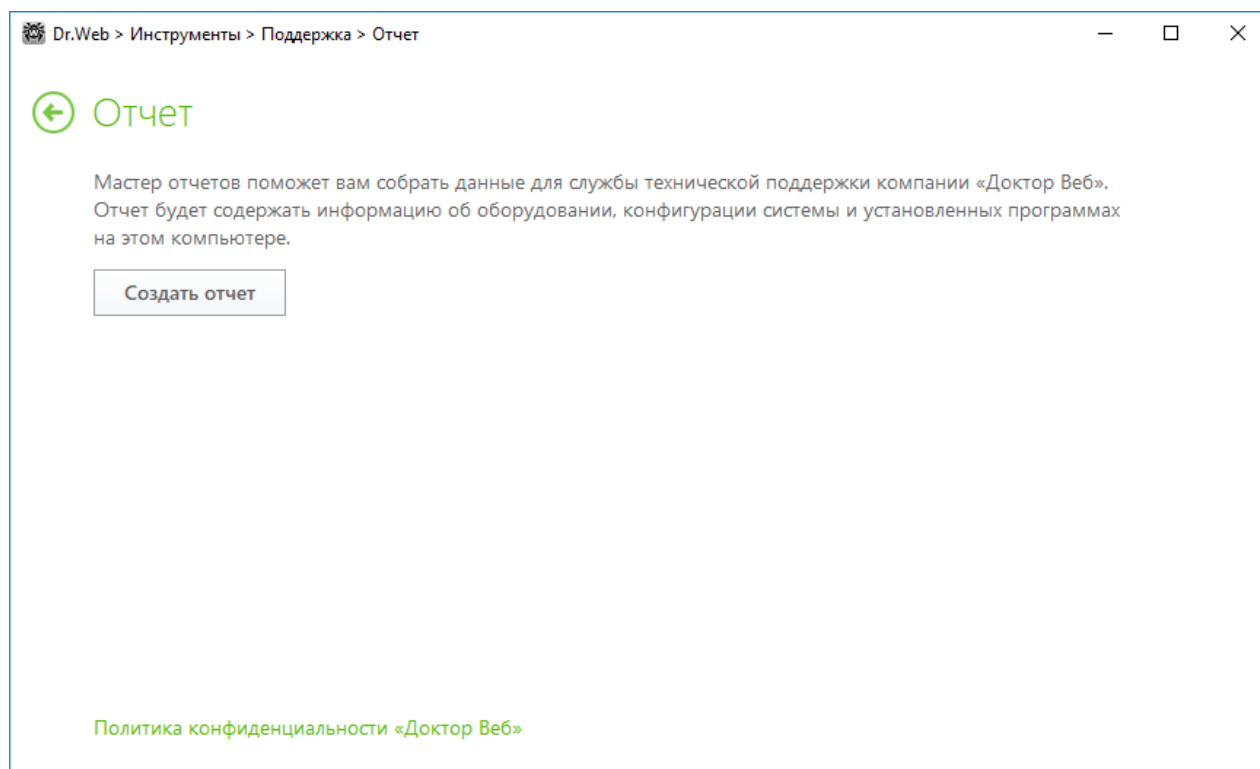


Рисунок 10. Создание отчета

Отчет будет собран автоматически и сохранен в виде архива в папке Doctor Web, расположенной 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`



6. 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.

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.

6.1. Запуск и режимы проверки



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

Запуск Сканера Dr.Web

1. В [меню](#)  выберите пункт **Сканер**. Откроется меню быстрого доступа к запуску разных типов проверки.

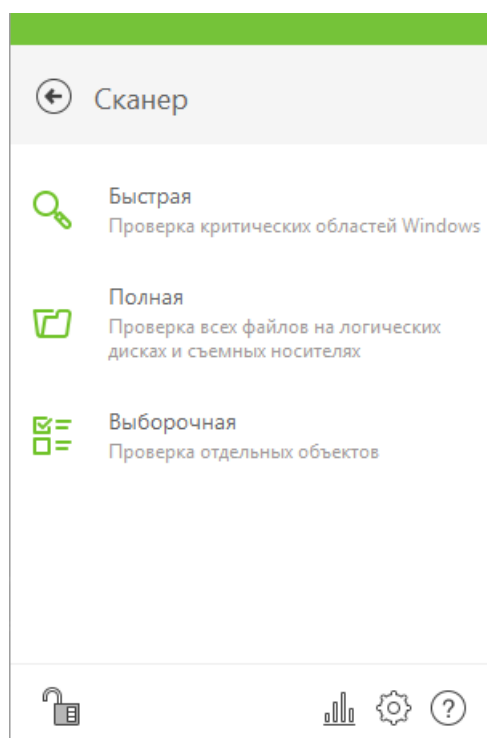


Рисунок 11. Выбор режима проверки сканера

2. Выберите необходимый режим проверки:

- пункт **Выборочная**, чтобы проверить только указанные вами объекты. Откроется окно выбора файлов для проверки Сканером Dr.Web;
- пункт **Быстрая**, чтобы проверить только критические области Windows;
- пункт **Полная**, чтобы проверить все файлы.

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**.

Из этого окна вы можете вернуться в окно выбора режима сканирования.



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

6.2. 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 выберите все угрозы и нажмите кнопку **Обезвредить**, и Сканер Dr.Web применит оптимальные действия по умолчанию для всех обнаруженных угроз.



По нажатию кнопки **Обезвредить** действия применяются к выбранным объектам в таблице. Необходимо вручную выбрать конкретные объекты или группы объектов, для которых требуется применить действия по нажатию кнопки **Обезвредить**. Для этого используйте флажки рядом с названиями объектов или выпадающее меню в заголовке таблицы.

Выбор действия

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

Существуют следующие ограничения:

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

Подробный отчет о работе программы сохраняется в 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	В этом столбце указано рекомендованное действие для найденной угрозы. Нажмите на стрелочку на этой кнопке, чтобы задать действие для выбранной угрозы.



Название столбца	Описание
	Вы можете применить указанное на кнопке действие отдельно, без нейтрализации остальных угроз. Для этого нажмите на эту кнопку.
Путь	В этом столбце указан полный путь к соответствующему файлу.



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

6.3. Запуск Сканера с параметрами командной строки

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

Синтаксис команды запуска следующий:

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

Список объектов проверки может быть пуст или содержать несколько элементов, разделенных пробелами. Если путь к объектам проверки не указан, поиск осуществляется в папке установки Dr.Web.

Наиболее распространенные следующие варианты указания объектов 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 и загрузочные секторы всех дисков, а также провести проверку на наличие руткитов.

Параметры — ключи командной строки, которые задают настройки программы. Если они отсутствуют, 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.

6.4. Консольный сканер

В состав компонентов Dr.Web также 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.

Чтобы запустить Консольный сканер, воспользуйтесь следующей командой:

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

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](#).

Коды возврата:

- 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

6.5. 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.



Если в состав установленных компонентов входит Брандмауэр, то после установки программы Dr.Web и первой перезагрузки служба системного расписания будет заблокирована Брандмауэром. Компонент **Назначенные задания** будет



функционировать только после повторной перезагрузки, т. к. необходимое правило уже будет создано к этому моменту.



7. Настройки

Для доступа к настройкам откройте меню Dr.Web  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 к администратору вашей антивирусной сети.



8. Основные настройки

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

Чтобы получить доступ к основным настройкам Dr.Web, откройте меню , запустите **Настройки**  в [режиме администратора](#) и выберите раздел **Основные**.



Изменение основных настроек возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.

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

Чтобы настроить вывод уведомлений на экран, выберите раздел [Уведомления](#).

Чтобы настроить дополнительные параметры безопасности, выберите раздел [Самозащита](#).

Чтобы ограничить доступ к определенным классам устройств или шин, выберите раздел [Устройства](#).

Чтобы изменить язык интерфейса, а также параметры журнала и карантина, выберите [Дополнительно](#).

Чтобы настроить параметры подключения к серверу централизованной защиты, выберите [Сервер](#).

8.1. Уведомления

В данном разделе вы можете настроить параметры получения уведомлений о работе Агент Dr.Web для Windows.

Уведомления, которые выводятся на экран

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

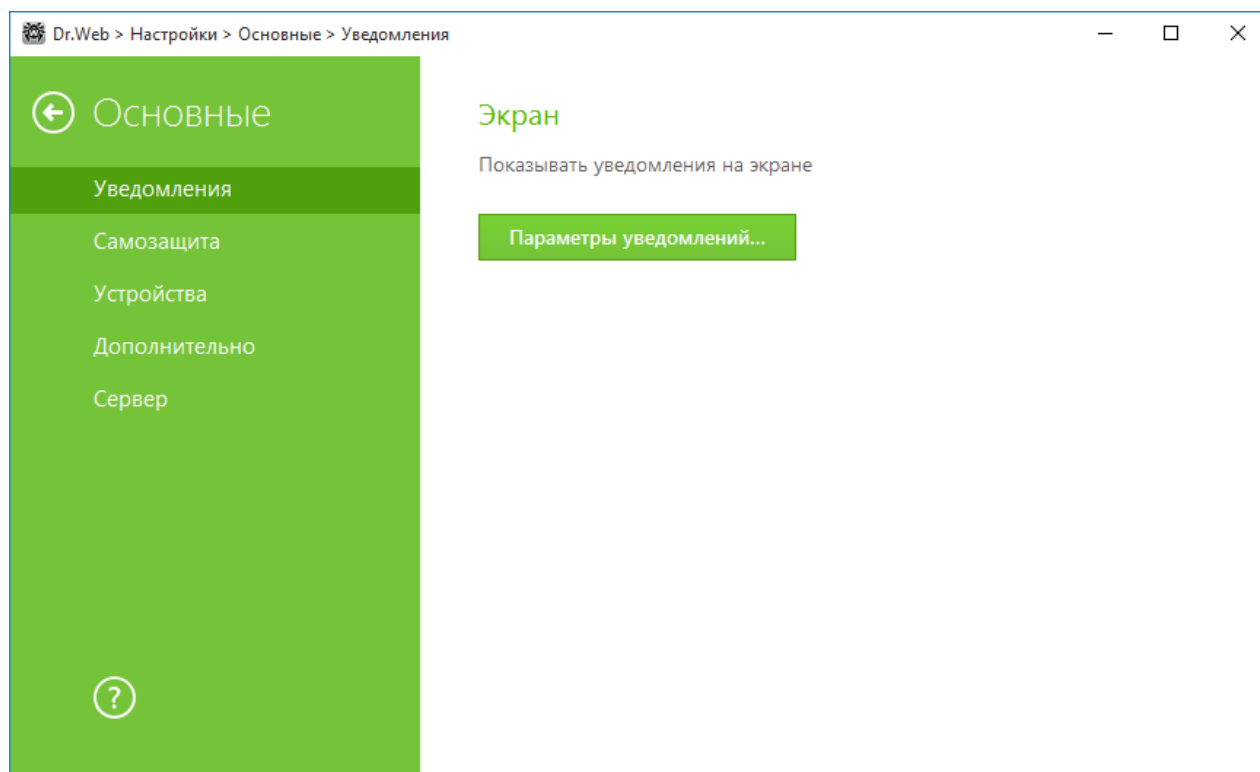


Рисунок 12. Настройки уведомлений

Параметры уведомлений

1. Нажмите кнопку **Параметры уведомлений**.
2. Выберите уведомления, которые вы хотите получать. Чтобы отображать уведомления, установите флажки напротив нужных типов уведомлений. Если вы не хотите получать уведомления о событии, снимите флажки.

Тип уведомления	Описание
Обнаружена угроза	Уведомления об угрозах, обнаруженных SplDer Guard и SplDer Gate. По умолчанию уведомления включены.
Критичные уведомления	Критичные уведомления о следующих событиях: • обнаружены соединения, ожидающие ответа Брандмауэра; • ваши имя пользователя и пароль уже используются для подключения к серверу централизованной защиты. По умолчанию уведомления включены.
Важные уведомления	Важные уведомления о следующих событиях: • истекает время работы за компьютером; • заблокировано устройство;



Тип уведомления	Описание
	• заблокирована попытка изменения системных даты и времени; • попытка доступа к защищаемому объекту заблокирована Превентивной защитой; • вирусные базы устарели (при работе в Мобильном режиме). По умолчанию уведомления включены.
Малозначительные уведомления	Малозначительные уведомления о следующих событиях: • успешное обновление; • ошибка обновления; • истекает время работы в Интернет; • URL был заблокирован модулем Офисный контроль; • URL был заблокирован SplDer Gate; • попытка доступа к защищаемому объекту заблокирована модулем Офисный контроль; • администратором антивирусной сети запущен процесс проверки вашего компьютера; • процесс проверки вашего компьютера запущен по расписанию; • проверка вашего компьютера завершена. По умолчанию уведомления выключены.

3. При необходимости задайте дополнительные параметры отображения экраных оповещений:

Флажок	Описание
Не показывать уведомления в полноэкранном режиме	Уведомления при работе с приложениями в полноэкранном режиме (просмотр фильмов, графики и т. д.). Снимите этот флажок, чтобы получать уведомления всегда.
Отображать уведомления Брандмауэра на отдельном экране в полноэкранном режиме	Отображение уведомлений от Брандмауэра на отдельном рабочем столе во время работы приложений в полноэкранном режиме (игры, видео). Снимите этот флажок, чтобы уведомления выводились на том же рабочем столе, на котором запущено приложение в полноэкранном режиме.



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;
- сообщение, отправленное администратором сервера централизованной защиты.

8.2. Самозащита

В данном разделе вы можете настроить параметры защиты самого Dr.Web от несанкционированного воздействия, например, от программ, вредоносное действие которых направлено на антивирусные программы, а также от случайного повреждения.

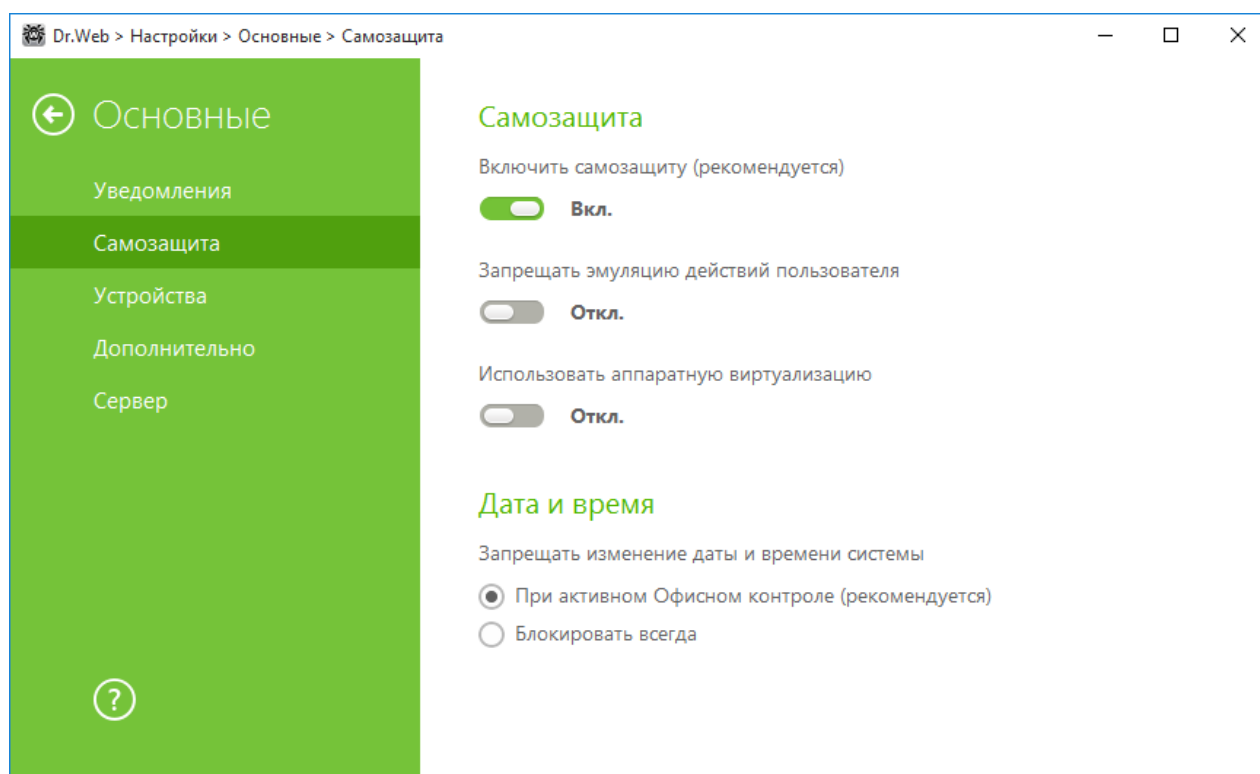


Рисунок 13. Параметры защиты Dr.Web

Самозащита

Настройка **Включить самозащиту (рекомендуется)** позволяет защитить файлы и процессы 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 сторонними программными средствами. В том числе будет запрещено исполнение скриптов, эмулирующих работу клавиатуры и мыши в окнах Dr.Web (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

Некоторые вредоносные программы намеренно изменяют системные дату и время. В этом случае обновления вирусных баз антивирусной программы не происходит по установленному расписанию, лицензия может определяться как просроченная, и компоненты защиты будут отключены.

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



8.3. Устройства

В данном разделе вы можете ограничить доступ к определенным устройствам или шинам устройств и настроить черный и белый списки.



Настройки доступа к устройствам применяются для всех учетных записей Windows.

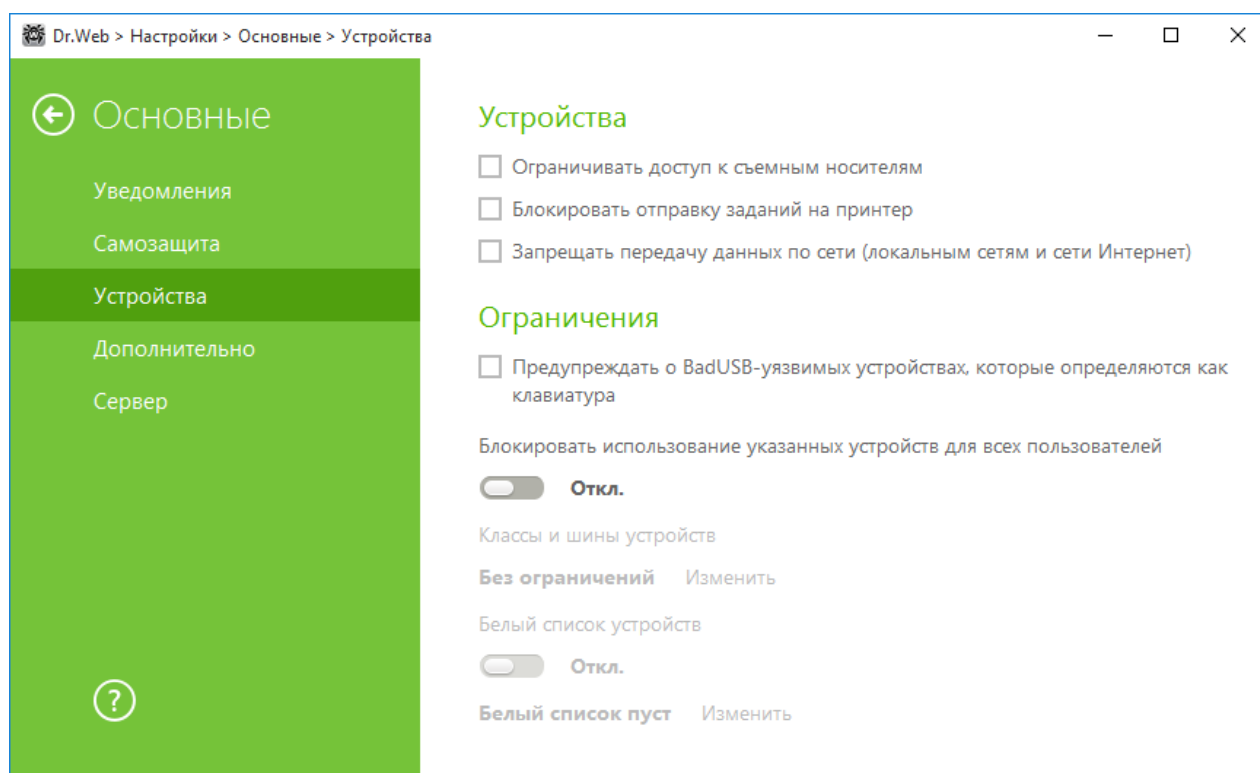


Рисунок 14. Настройки блокировки устройств

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 и шины устройств

Эта функция позволяет как заблокировать один или несколько классов устройств на всех шинах, так и заблокировать все устройства, подключенные к одной или нескольким шинам. Под классами устройств понимаются устройства, выполняющие одинаковые функции (например, устройства для печати). Под шинами — подсистемы передачи данных между функциональными блоками компьютера (например, шина USB).

Чтобы заблокировать доступ к выбранным классам и шинам устройств, включите соответствующую опцию. Сформируйте список таких объектов, нажав кнопку **Изменить**. В открывшемся окне вы можете выбрать классы или шины устройств, доступ к которым хотите заблокировать.

Формирование списка заблокированных классов устройств

1. Чтобы полностью заблокировать класс устройств, в столбце **Блокируемые классы**, нажмите кнопку .
2. В открывшемся списке выберите необходимые классы и нажмите **ОК**. Выбранные классы устройств будут заблокированы на всех шинах. В списке выбора классов устройств отображаются только незаблокированные классы.
3. Чтобы разблокировать класс устройств, в окне **Классы и шины устройств** выберите нужный класс и нажмите кнопку .

Формирование списка заблокированных шин устройств

1. Чтобы заблокировать шину полностью или некоторые устройства на шине, в столбце **Блокируемые шины** нажмите кнопку .
2. В открывшемся окне выберите необходимые классы устройств. Для блокировки всей шины выберите все классы из списка. Нажмите **ОК**.
3. Чтобы разблокировать шину, в окне **Классы и шины устройств** выберите нужную шину и нажмите кнопку .
4. Чтобы отредактировать список заблокированных классов на конкретной шине, нажмите кнопку .



При активации блокировки уже подключенного устройства требуется либо подключить устройство заново, либо перезагрузить компьютер. Блокировка работает только для устройств, подключенных после активации функции.

Белый список устройств

Если вы ограничили доступ к каким-либо классам или шинам устройств, 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.

Добавление устройства в белый список

1. Включите опцию **Белый список устройств** (опция становится активна, если заданы ограничения).
2. Для формирования списка устройств нажмите **Изменить**.
3. Убедитесь, что устройство подключено к компьютеру.
4. Нажмите кнопку . В открывшемся окне нажмите кнопку **Обзор** и выберите нужное устройство. Воспользуйтесь фильтром, чтобы в таблице отображались только подключенные или только отключенные устройства. Нажмите кнопку **ОК**.
5. 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 .
6. Чтобы сохранить изменения, нажмите **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите **Отменить**. Вы вернётесь к белому списку устройств.
7. Для того чтобы отредактировать набор правил для устройства, выберите его в списке и нажмите .
8. Чтобы удалить набор правил для устройства, выберите его в списке и нажмите .

8.4. Дополнительно

В данном разделе задаются язык программы, 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.

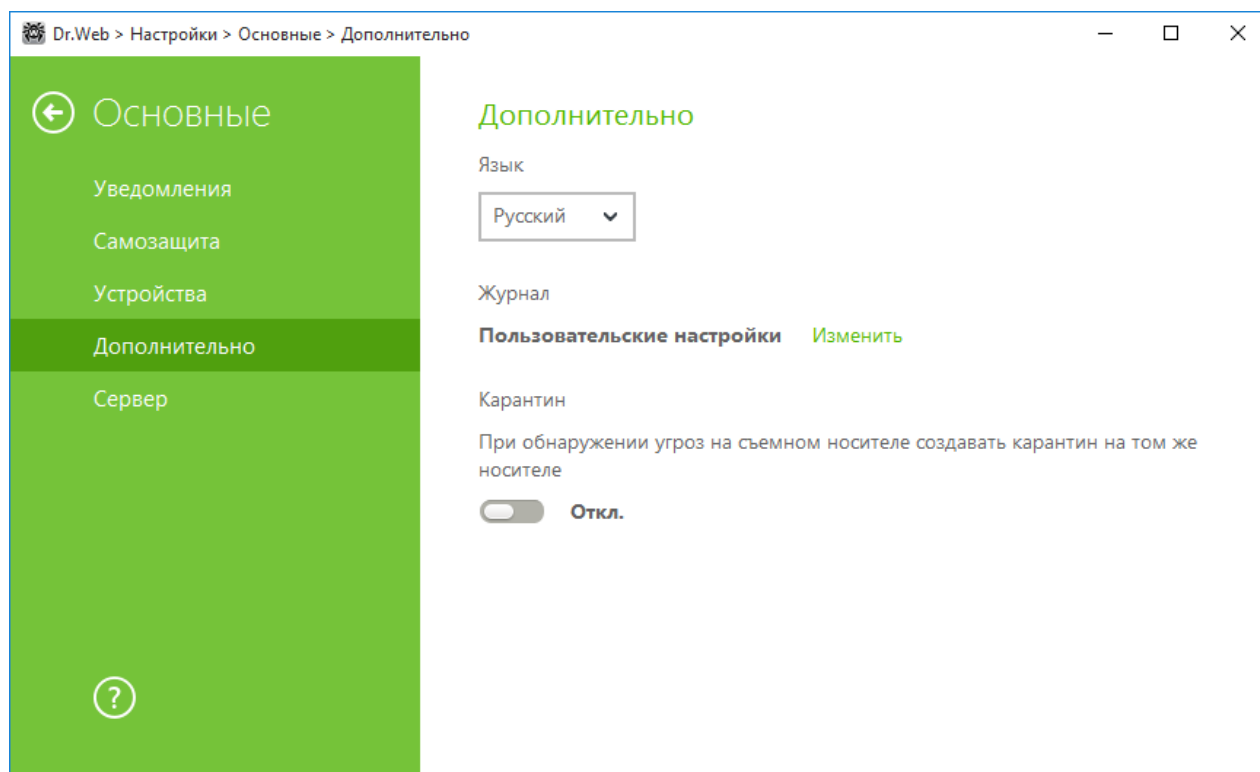


Рисунок 15. Дополнительные настройки

Настройки Журнала

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



Изменение настроек ведения журнала невозможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, не дал разрешения на применение этих действий.

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ (для компонента SplDer 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 Dr.Web журнал ведется в стандартном режиме, фиксирующем следующую информацию:

Компонент	Информация
SplDer Guard	Проведение обновлений, запуск и остановка сторожа SplDer 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 SplDer Guard проверяет наиболее часто. При необходимости вы можете добавить такие объекты в список исключений, что может снизить нагрузку на компьютер.
SplDer Mail	Проведение обновлений, запуск и остановка почтового сторожа SplDer Mail, вирусные события, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов. Рекомендуется использовать этот режим для проверки настроек перехвата соединений с почтовыми серверами.
SplDer Gate	Проведение обновлений, запуск и остановка веб-антивируса SplDer Gate, вирусные события, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов. Рекомендуется использовать этот режим для получения более детальной информации о проверенных объектах и работе веб-антивируса.
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.
Брандмауэр	В стандартном режиме Брандмауэр не ведет файл журнала. При включении режима ведения подробного журнала собираются данные о сетевых пакетах (рсар-логи).
Обновление Dr.Web	Список обновленных файлов Dr.Web и статусы их загрузки, информация о работе вспомогательных скриптов, дата и время проведения обновления, информация о перезапуске компонентов Dr.Web после обновления.
Служба Dr.Web	Информация о компонентах Dr.Web, изменение настроек компонентов, включение и выключение компонентов, события превентивной защиты, подключение к серверу централизованной защиты.

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 приведет 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 администратора вашей антивирусной сети.

1. Чтобы включить режим ведения подробного журнала для одного из компонентов Dr.Web, установите соответствующий флажок.
2. 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.

8.5. Сервер

В данном разделе вы можете просматривать и редактировать параметры взаимодействия Dr.Web с сервером централизованной защиты, а также задать настройки для Мобильного режима работы Dr.Web. Администратор вашей антивирусной сети может запретить вам изменять параметры взаимодействия с сервером, в этом случае кнопки и флажки будут не доступны для управления.

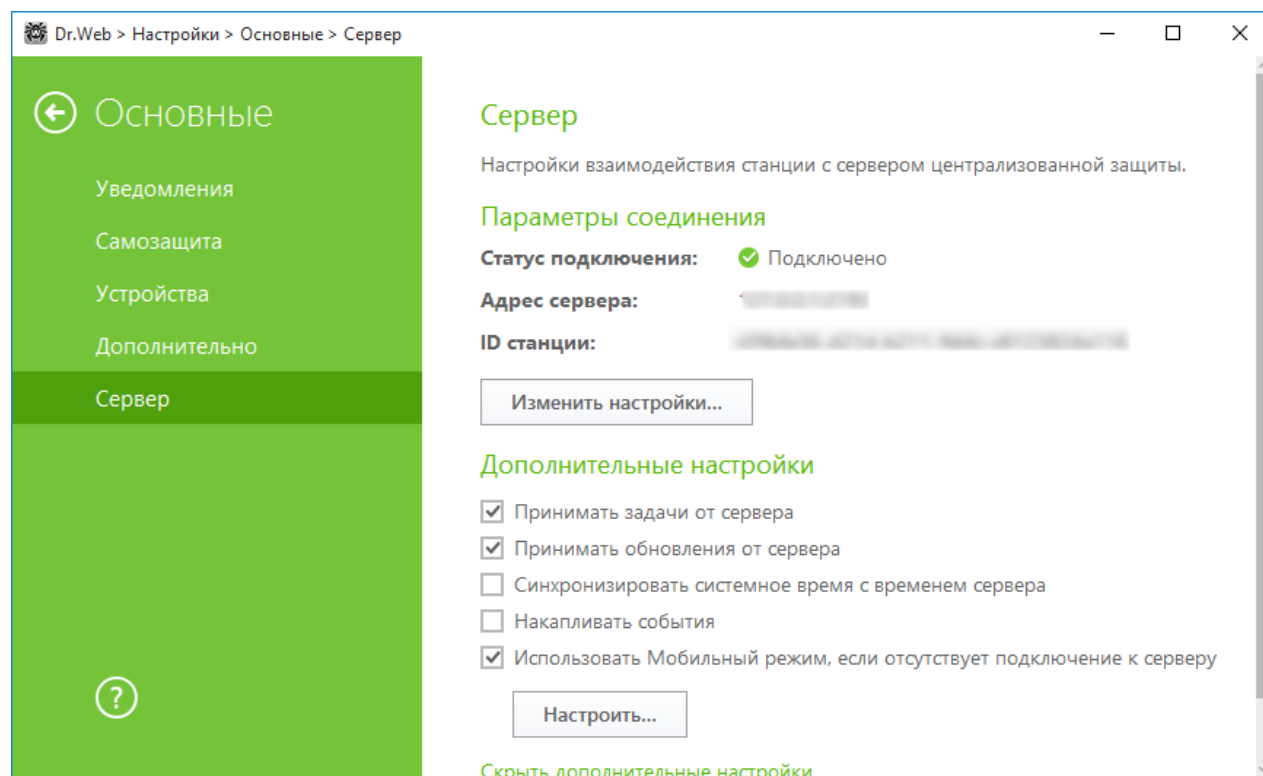


Рисунок 16. Настройки подключения к серверу

Параметры соединения

В группе **Параметры соединения** отображаются:

- **Статус подключения** — статус подключения станции к серверу централизованной защиты;
- **Адрес сервера** — адрес сервера централизованной защиты, к которому подключена станция;
- **ID станции** — идентификатор станции для подключения к серверу.

Вы можете просматривать и управлять настройками соединения с сервером, если администратор сети предоставил вам такие права.



Настройки подключения к серверу централизованной защиты можно менять только согласованно с администратором антивирусной сети, иначе ваш компьютер будет отключен от антивирусной сети.

Для изменения настроек подключения к текущему серверу или добавления другого сервера нажмите **Изменить настройки**. Откроется окно **Настройки подключения сервера**.

Настройки подключения

В таблице выводится список всех серверов, к которым может быть подключена станция. Вы можете удалять серверы из таблицы и добавлять новые. Для удаления строки нажмите кнопку



. Для настройки соединения с другим сервером нажмите кнопку . В открывшемся окне необходимо указать адрес сервера централизованной защиты, предоставленный администратором.

Добавление сертификата

Необходимым условием подключения станции к серверу централизованной защиты является наличие действующего сертификата. Сертификат может быть уникальный для каждого конкретного сервера или подходить к нескольким серверам. Можно добавить несколько сертификатов для подключения к нескольким серверам.

По умолчанию указан сертификат, использованный при установке программы, если на сервере не проводилась плановая замена ключей шифрования. Если замена ключей производилась, будет указан последний из сгенерированных сертификатов. Чтобы просмотреть список доступных сертификатов или добавить другой сертификат, перейдите по ссылке **Список сертификатов**.

Чтобы добавить новый сертификат, нажмите кнопку  и в открывшемся окне выберите необходимый файл.

Чтобы удалить неиспользуемый сертификат, нажмите кнопку .

Параметры подключения станции

Чтобы изменить параметры подключения станции:

1. В окне **Параметры подключения станции** укажите идентификатор станции и пароль для подключения к серверу. Эти данные предоставляются администратором сервера.
2. Нажмите **ОК** для сохранения изменений.

Чтобы сбросить параметры подключения и подключиться как новичок к серверу централизованной защиты:

1. В окне **Параметры подключения станции** нажмите **Сбросить параметры и подключиться как новичок**.
2. В открывшемся окне подтвердите, что вы хотите сбросить параметры подключения станции и подключиться как новичок. Обратите внимание, что это действие необратимо.
3. После подтверждения регистрации станции на сервере централизованной защиты Dr.Web получит новые идентификатор станции и пароль. Они будут использоваться для подключения к серверу.



Дополнительные настройки

В группе **Дополнительные настройки** вы можете выбрать следующие опции:

- **Принимать задачи от сервера** — для периодического получения заданий от администратора.
- **Принимать обновления от сервера** — для получения регулярных обновлений компонентов Dr.Web и вирусных баз с сервера централизованной защиты. Обновления происходят в соответствии с настройками, заданными на сервере.
- **Синхронизировать системное время с временем сервера** — для синхронизации системного времени на вашем компьютере со временем на сервере централизованной защиты. В данном режиме Dr.Web периодически устанавливает системное время на вашем компьютере в соответствии с временем на сервере.
- **Накапливать события** — для сохранения данных о произошедших событиях для последующей отправки на сервер централизованной защиты. При включении опции информация на сервер не передается. Если флажок не установлен, а соединения с сервером нет, то важная информация (например, об обнаруженных угрозах и статистике) будет утрачена.
- **Использовать Мобильный режим, если отсутствует подключение к серверу** — для своевременного получения обновлений вирусных баз.

Если ваш компьютер долгое время не будет иметь связи с сервером централизованной защиты, для своевременного получения обновлений с серверов компании «Доктор Веб» рекомендуется установить мобильный режим работы Dr.Web. Для этого установите флажок **Использовать Мобильный режим, если отсутствует подключение к серверу**.



Флажок **Использовать Мобильный режим, если отсутствует подключение к серверу** будет доступен при условии, что на сервере централизованной защиты в правах станции разрешено **Изменение конфигурации Агента Dr.Web**.

В Мобильном режиме Dr.Web пытается подключиться к серверу централизованной защиты, делает три попытки, и, если не удалось, выполняет обновление вирусных баз с серверов компании «Доктор Веб». Попытки обнаружения сервера централизованной защиты идут непрерывно с интервалом около минуты.

Чтобы задать настройки Мобильного режима работы, нажмите кнопку **Настроить**. Откроется окно **Мобильный режим**.

В выпадающем списке **Периодичность обновлений** вы можете выбрать периодичность, с которой будет производиться проверка на наличие обновлений на серверах компании «Доктор Веб».



При выборе в списке **Периодичность обновлений** опции **Вручную** автоматические обновления происходить не будут. Вы сможете запустить



обновление в меню Dr.Web.

При использовании прокси-сервера установите соответствующий флажок. В этом случае станут активными поля:

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.

По окончании редактирования нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для выхода из окна без сохранения изменений. Чтобы отредактировать настройки подключения к прокси-серверу, еще раз нажмите кнопку **Изменить**.



В Мобильном режиме производится обновление только вирусных баз.

Если снять флажок **Использовать Мобильный режим, если отсутствует подключение к серверу** до возобновления связи с сервером централизованной защиты, то вирусные базы перестанут обновляться, но поиск сервера продолжится.

Все изменения, которые задаются для станции на сервере централизованной защиты, вступят в силу, как только связь Dr.Web с сервером возобновится.

8.6. Сообщения сервера

Для удобства работы с оповещениями на сервере централизованной защиты у администратора сети есть возможность включить отправку сообщений на станцию. В этом случае в окне **Основные** появится раздел **Сообщения сервера**.

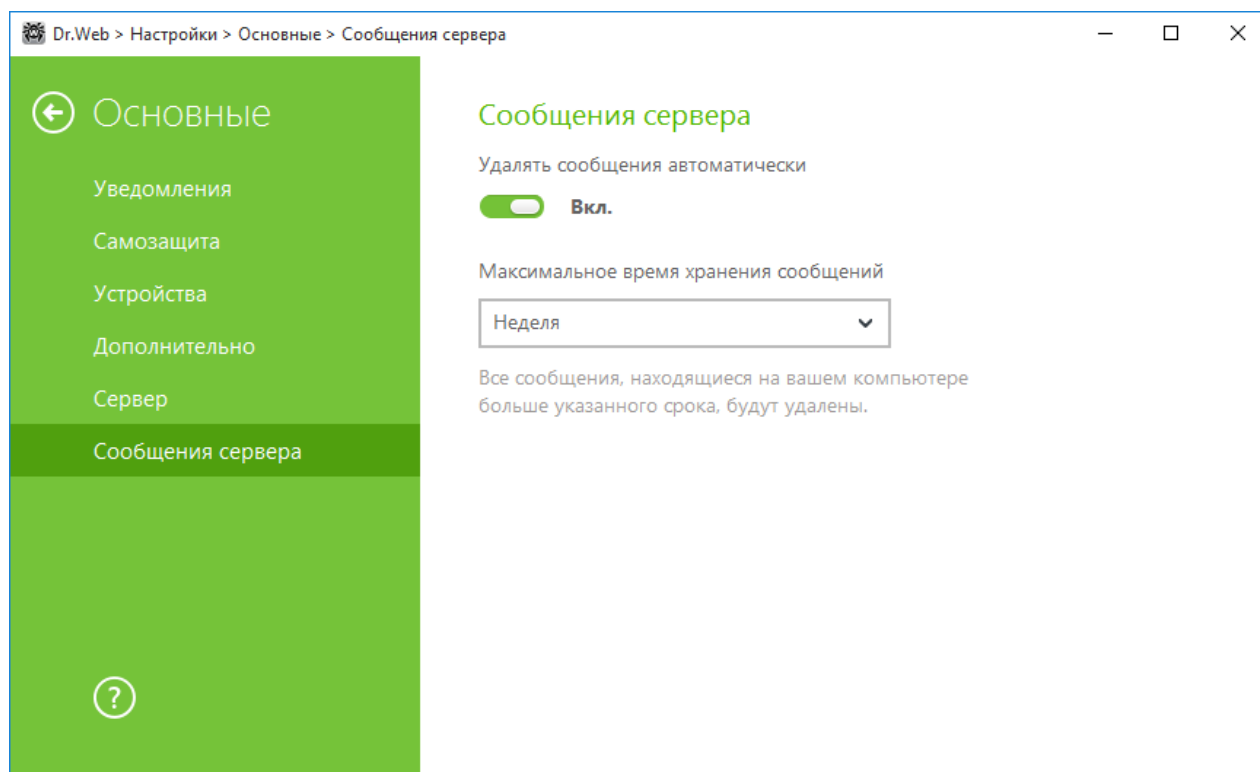


Рисунок 17. Настройки автоматического удаления сообщений сервера

Вы можете задать настройки автоматического удаления сообщений. Для этого включите опцию **Удалять сообщения автоматически** и в пункте **Максимальное время хранения сообщений** в выпадающем списке выберите необходимый период времени. Сообщения будут удаляться по истечении этого срока.



9. Офисный контроль

С помощью модуля Офисный контроль осуществляется управление доступом пользователей к сайтам, файлам и папкам, а также контролируется время работы в сети Интернет и за компьютером для каждой учетной записи Windows.

Чтобы настроить Офисный контроль, откройте меню Dr.Web , запустите **Настройки**  в [режиме администратора](#) и выберите раздел **Офисный контроль**.

Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность и конфиденциальность важных данных и защитить файлы от заражения. Существует возможность защиты как отдельных файлов, так и папок целиком, расположенных как на локальных дисках, так и на съемных носителях информации.

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



9.1. Настройка модуля Офисный контроль



Изменение настроек компонента возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.

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

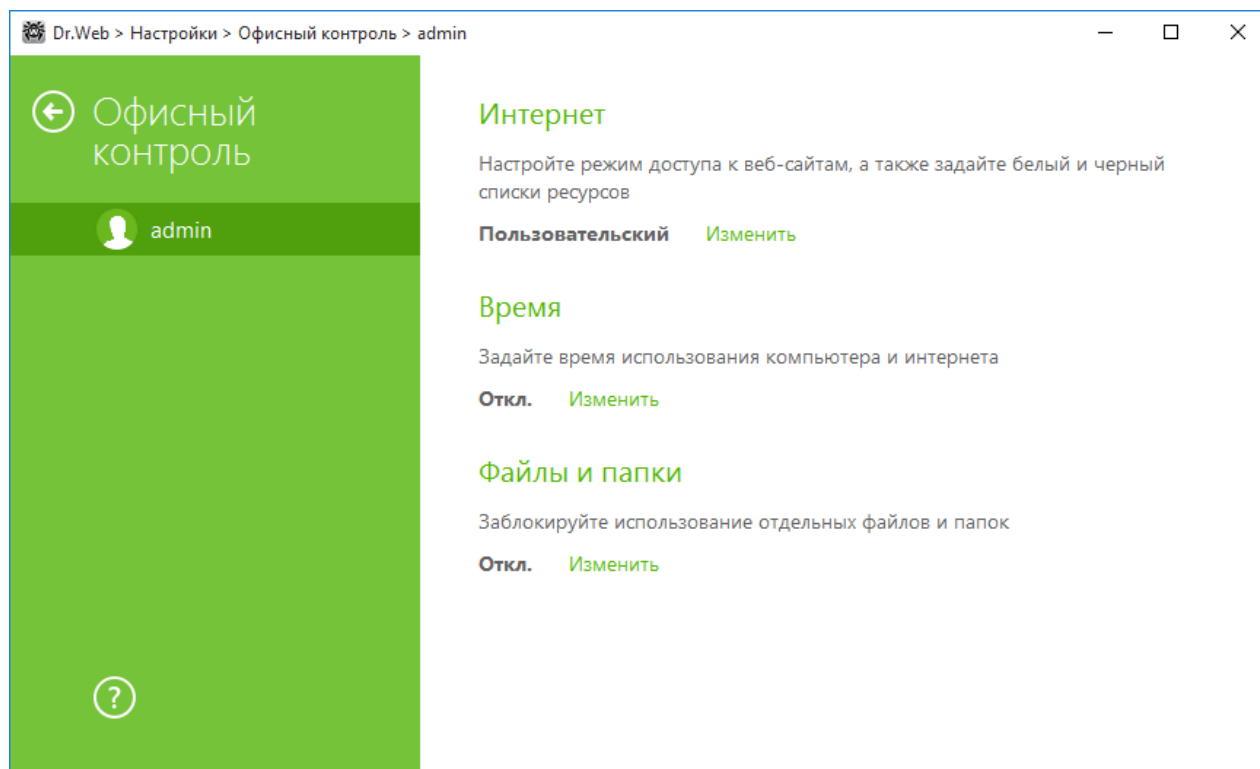


Рисунок 18. Настройки модуля Офисный контроль

Настройка параметров модуля Офисный контроль для разных пользователей

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



Новые пользователи отображаются в списке только после того, как выполнят первый вход в свою учетную запись.



Вы можете [настроить](#) вывод уведомлений о действиях модуля Офисный контроль



на экран.

9.1.1. Интернет

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

Блокировать по категориям

Один и тот же сайт может быть отнесен сразу к нескольким различным категориям. В этом случае модуль Офисный контроль блокирует доступ к сайту, если он попадает хотя бы в одну из категорий, включенных для запрета доступа.

В этом режиме вы можете указать категории тех ресурсов, доступ к которым вы хотите ограничить:

Категория	Описание
Сайты для взрослых	Сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.
Насилие	Сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
Оружие	Сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
Азартные игры	Сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.
Наркотики	Сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
Онлайн-игры	Сайты, на которых размещены игры, использующие постоянное соединение с интернетом.
Терроризм	Сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
Нецензурная лексика	Сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
Чаты	Сайты для обмена сообщениями в режиме реального времени.
Электронная почта	Сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика.



Категория	Описание
Социальные сети	Социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств.
Анонимайзеры	Сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам.
Пулы для добычи криптовалют	Сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют.

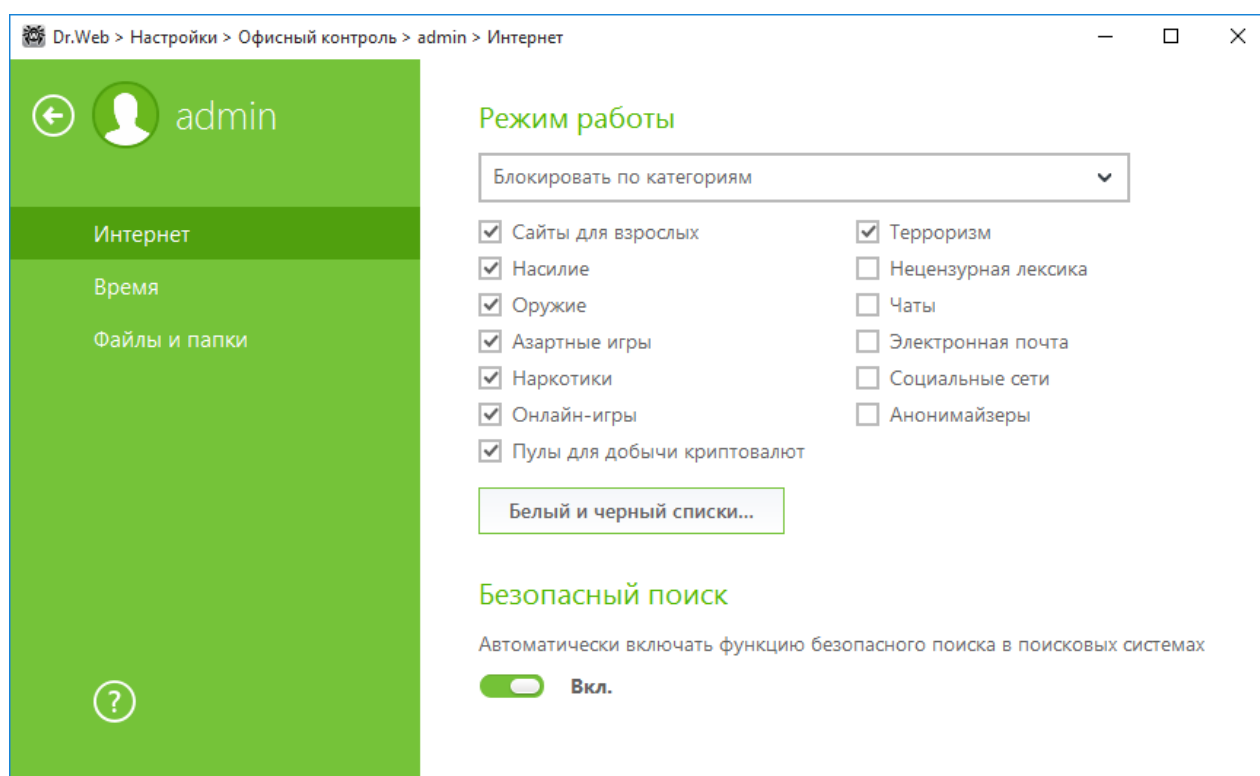


Рисунок 19. Настройка доступа в Интернет по категориям сайтов

Для запрета доступа к ресурсам требуемой категории установите соответствующий флажок.

Также в этом режиме вы можете самостоятельно указывать сайты, доступ к которым будет запрещаться или разрешаться вне зависимости от других ограничений:

- Чтобы заблокировать доступ к сайту, не относящемуся ни к одной из указанных категорий, его следует включить в пользовательский черный список.
- Чтобы принудительно разрешить доступ к сайту, несмотря на то что он относится к какой-либо из нежелательных категорий, его следует включить в пользовательский белый список.



Блокировать всё, кроме сайтов из белого списка

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

Безопасный поиск

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

Для активации функции **Безопасный поиск** установите переключатель в состояние **Вкл.**

Белый и черный списки сайтов

В этом окне задаются списки сайтов, доступ к которым разрешается или блокируется вне зависимости от остальных настроек модуля Офисный контроль.

Для работы с белым и черным списками нажмите кнопку **Белый и черный списки**.

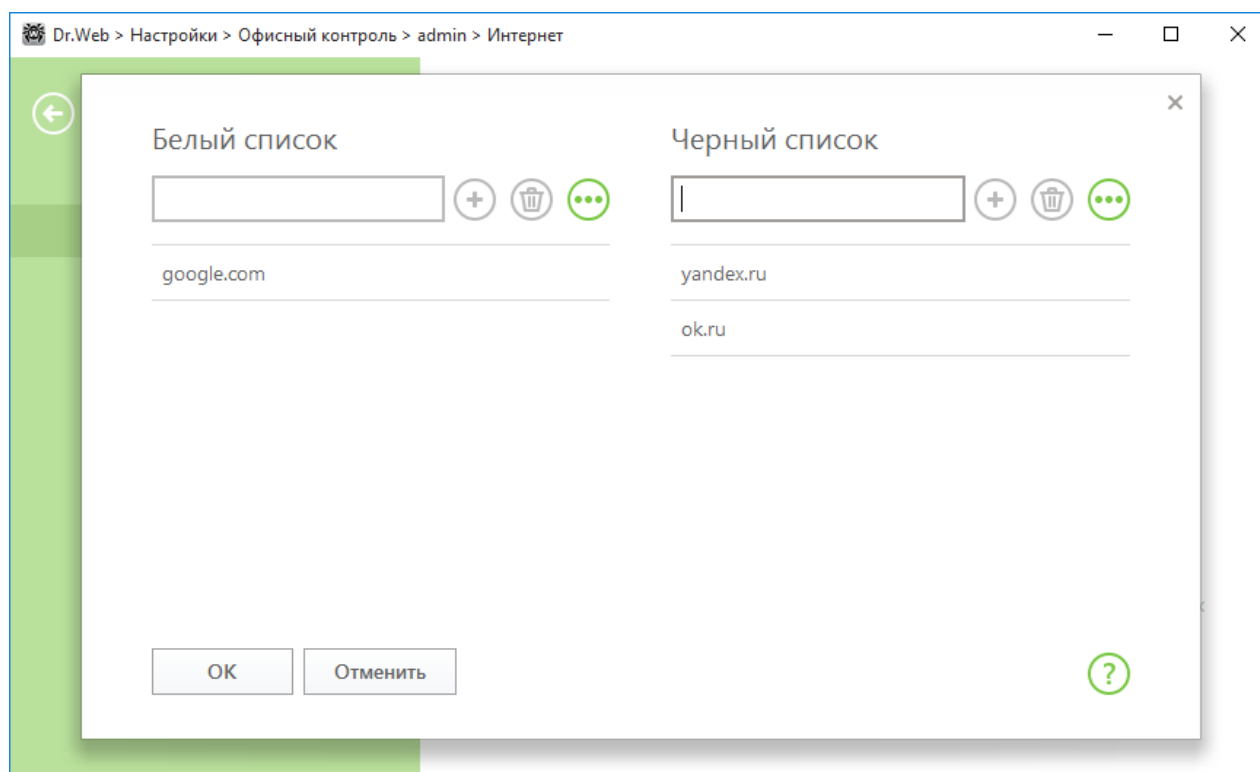


Рисунок 20. Формирование белого и черного списков

По умолчанию списки пусты. При необходимости вы можете добавить адреса сайтов в белый или черный список.



Формирование списка доменных адресов

1. Введите доменное имя или часть доменного имени сайта в поле **Белый список** или **Черный список**, в зависимости от того, хотите ли вы разрешить или запретить доступ к нему соответственно:
 - чтобы добавить в список определенный сайт, введите его адрес (например, `www.example.com`). Доступ ко всем ресурсам, расположенным на этом сайте, будет определяться данной записью;
 - чтобы разрешить доступ к тем сайтам, в адресе которых содержится определенный текст, введите в поле этот текст. Пример: если вы введете текст `example`, то доступ к адресам `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru` и т. п. будет определяться данной записью;
 - чтобы разрешить доступ к определенному домену, укажите имя домена с символом «.». В таком случае доступ ко всем ресурсам, находящимся в этом домене, будет определяться данной записью. Если при указании домена используется символ «/», то та часть подстроки, что стоит слева от символа «/», будет считаться доменным именем, а части справа от символа — частью разрешенного на данном домене адреса. Пример: если вы введете текст `example.com/test`, то будут обрабатываться такие адреса как `example.com/test11`, `template.example.com/test22` и т. п.;
 - чтобы добавить в исключения определенные сайты, введите определяющую их маску в поле ввода. Маски добавляются в формате: `mask://...`

Маска задает общую часть имени объекта, при этом:

□ символ «*» заменяет любую, возможно пустую, последовательность символов;

□ символ «?» заменяет любой, в том числе пустой, но только один символ.

Примеры:

□ `mask://*.ru/` или `.ru` — будут открываться все сайты в зоне `.ru`;

□ `mask://mail` — будут открываться все сайты, в которых содержится слово "mail";

□ `mask://????.ru/` или `.ru` — будут открываться все сайты зоны `.ru`, имена которых состоят из трех или менее знаков.

Введенная строка при добавлении в список может быть преобразована к универсальному виду. Например: адрес `http://www.example.com` будет преобразован в запись `www.example.com`.

2. Нажмите кнопку , чтобы добавить адрес в список.
3. Чтобы удалить адрес из списка, выберите его в списке и нажмите кнопку .
4. При необходимости повторите шаги 1 и 2 для добавления других ресурсов.

9.1.2. Время

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



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

Вы можете назначить ограничение по времени работы для пользователей, используя таблицу с временными квадратами.

Ограничение времени доступа в режиме таблицы

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

Вы можете также создавать разные настройки для одного пользователя, сохраняя их в профили. Данная опция будет удобна, если вам понадобится периодически менять настройки на другие predetermined значения (например, задавать разные ограничения во время учебного года и школьных каникул).

Создание и изменение профиля настроек

Вы можете изменить пользовательский профиль настроек или создать новый.

1. Для создания нового профиля нажмите кнопку  и задайте имя профиля. Нажмите **ОК**.
2. Для изменения пользовательского профиля выберите его из списка.
3. После этого внесите необходимые изменения в таблицу.

При выборе профиля **Без ограничений** и внесении изменений в таблицу профиль будет автоматически заменен на пользовательский.

9.1.3. Файлы и папки

По умолчанию ограничения на доступ к файлам и папкам отсутствуют. Чтобы настроить ограничения, включите соответствующую опцию и нажмите кнопку **Объекты**.

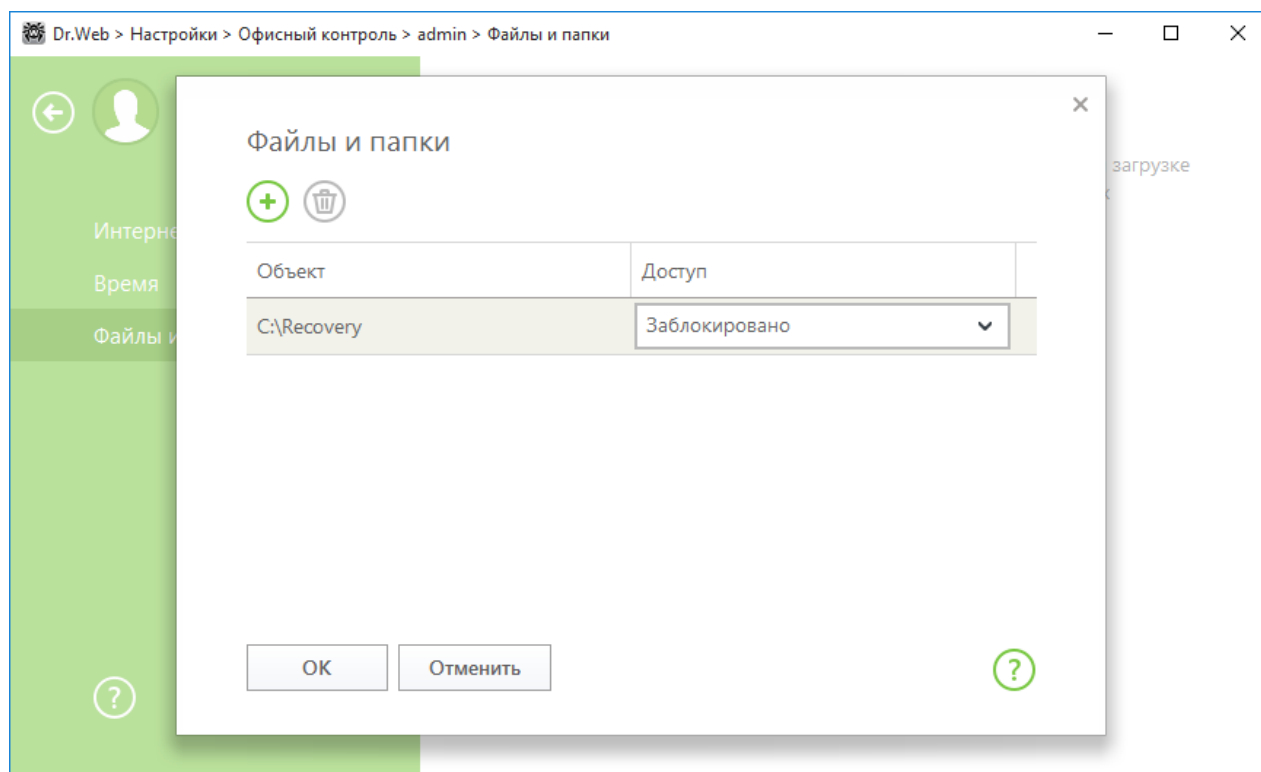


Рисунок 21. Управление доступом к файлам и папкам

Для того чтобы добавить объект в список, нажмите кнопку и выберите нужный файл или папку. По умолчанию, добавленный объект будет доступен пользователю только для чтения.

Для того чтобы полностью заблокировать доступ к выбранному объекту, нажмите на установленное ограничение и в выпадающем списке выберите **Заблокировано**.

Для того чтобы удалить объект, выберите его в списке и нажмите кнопку .

Обратите внимание, что ограничение доступа не гарантируется при загрузке компьютера со съемных носителей или обращении к заданным объектам из других операционных систем, установленных на компьютере.



10. Исключения

В данном разделе вы можете настроить исключения из проверок компонентами SplDer Guard, SplDer Gate, SplDer Mail и Сканер, а также добавить адреса отправителей в черный или белый список, чтобы письма от них не проверялись на спам.

Чтобы настроить исключения, откройте меню , запустите **Настройки**  в [режиме администратора](#) и выберите раздел **Исключения**.



Обратите внимание, что изменения в этом разделе могут быть заблокированы со стороны администратора вашей антивирусной сети.

Для настройки доступа к сайтам, которые не рекомендуются к посещению компанией «Доктор Веб», выберите раздел [Веб-сайты](#).

Для исключения определенных файлов и папок из проверки выберите раздел [Файлы и папки](#).

Для исключения определенных процессов из проверки компонентами Dr.Web выберите раздел [Приложения](#).

Для настройки проверки писем на спам компонентом SplDer Mail выберите раздел [Антиспам](#).

10.1. Сайты

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

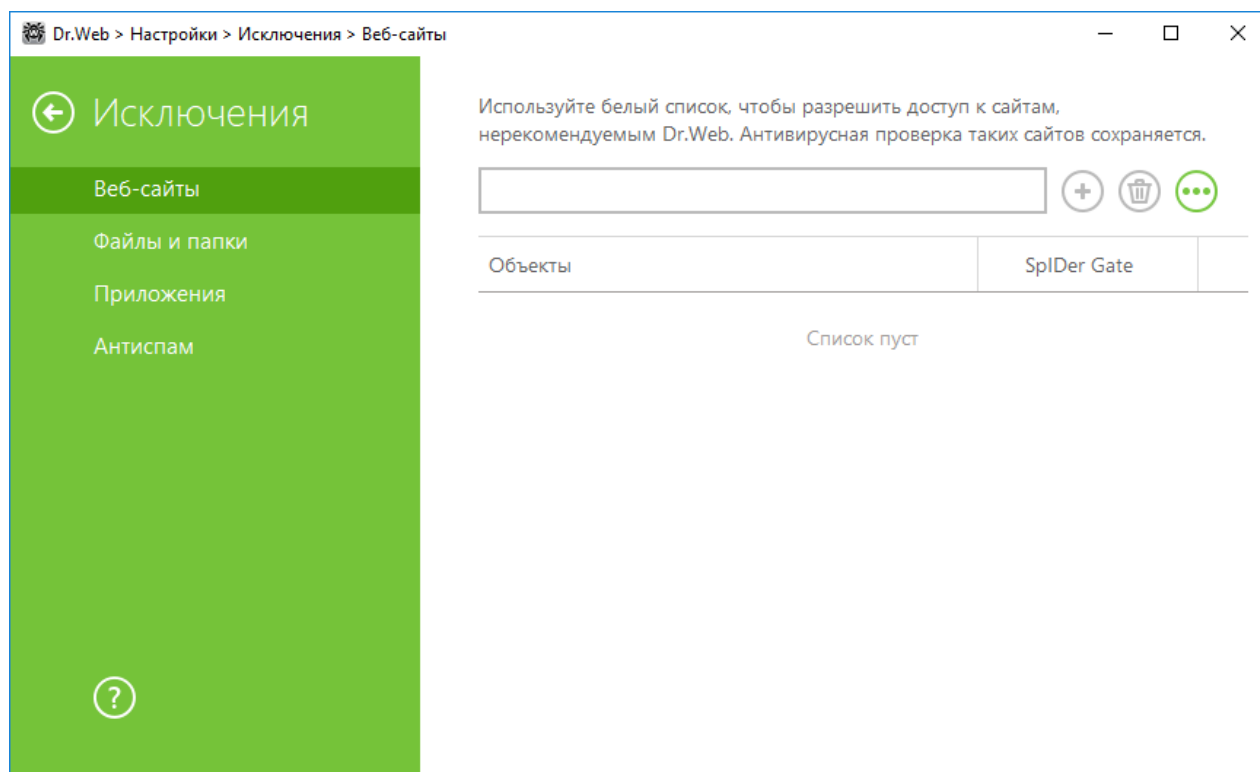


Рисунок 22. Добавление сайтов в исключения

Формирование списка доменных адресов

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

Маска задает общую часть имени объекта, при этом:

- символ «*» заменяет любую, возможно пустую, последовательность символов;



□ символ «?» заменяет любой, в том числе пустой, но только один символ.

Примеры:

□ `mask:/*.*.ru` — будут открываться все сайты в зоне .ru;

□ `mask://mail` — будут открываться все сайты, в которых содержится слово "mail";

□ `mask://???.ru` — будут открываться все сайты зоны .ru, имена которых состоят из трех или менее знаков.

Введенная строка при добавлении в список может быть преобразована к универсальному виду. Например: адрес `http://www.example.com` будет преобразован в запись `www.example.com`.

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

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.

10.2. Файлы и папки

В этом разделе задается список папок и файлов, которые исключаются из проверки компонентами SplDer 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.

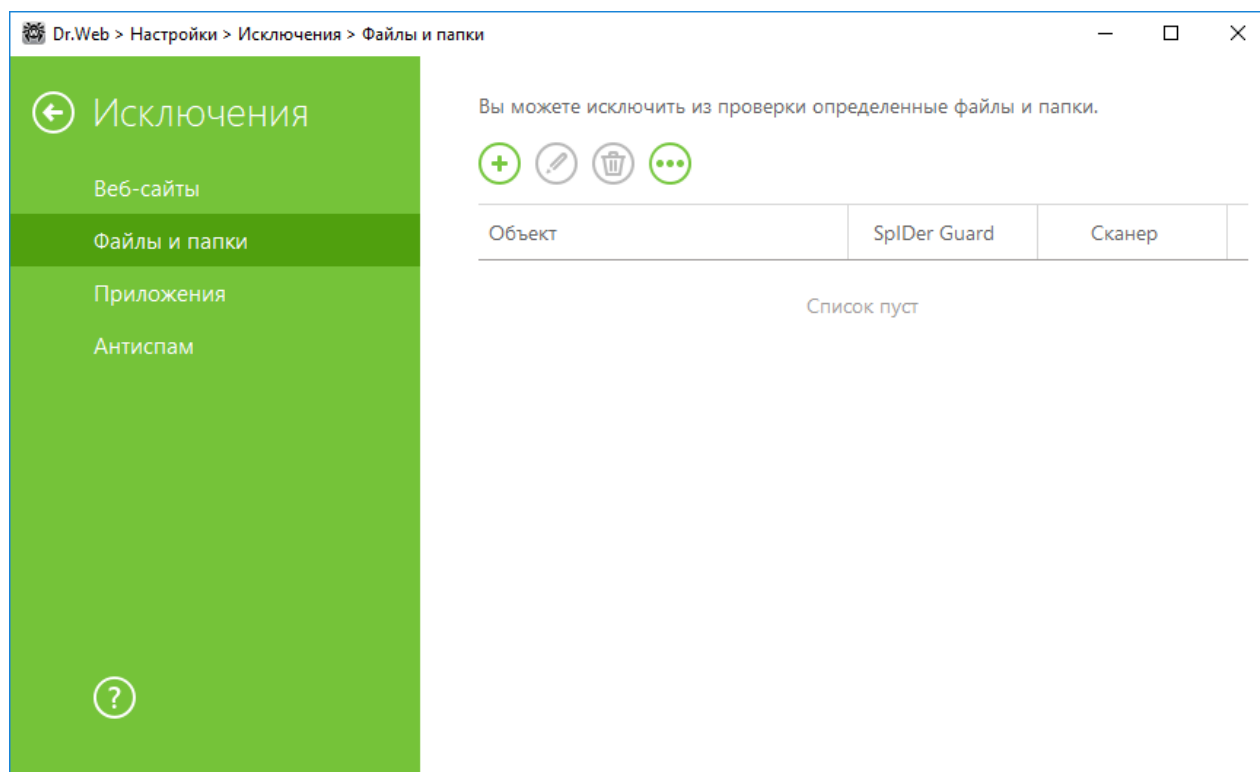


Рисунок 23. Исключения файлов и папок из проверки

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. Например:
 - `C:\folder\file.txt` — исключает из проверки файл `file.txt` в папке `C:\folder`.
 - `C:\folder` — исключает из проверки все подпапки и файлы в папке `C:\folder`.
 - чтобы исключить из проверки файл с определенным именем, введите имя файла, включая расширение, в поле ввода. Указывать путь к файлу при этом не требуется. Например:
 - `file.txt` — исключает из проверки все файлы с именем `file` и расширением `.txt` во всех папках.
 - `file` — исключает из проверки все файлы с именем `file` без расширения во всех папках.
 - чтобы исключить из проверки файлы или папки определенного вида, введите определяющую их маску в поле ввода.

Маска задает общую часть имени объекта, при этом:



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

Примеры:

- отчет*.doc — маска, задающая все документы Microsoft Word, название которых начинается с подстроки «отчет», например, файлы отчет-февраль.doc, отчет121209.doc и т.д.;
- *.exe — маска, задающая все исполняемые файлы с расширением EXE, например, setup.exe, iTunes.exe и т. д.;
- photo????09.jpg — маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных символа, например, photo121209.jpg, photомама09.jpg или photo----09.jpg.
- 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.
- C:\folder** — исключает из проверки все подпапки и файлы в папке C:\folder. В подпапках файлы будут проверяться.
- C:\folder* — исключает из проверки все файлы в папке C:\folder и всех подпапках на любом уровне 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.

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 .

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.

10.3. Приложения

В этом разделе задается список программ и процессов, которые исключаются из проверки SplDer Guard, SplDer Gate и SplDer Mail.

По умолчанию список пуст.

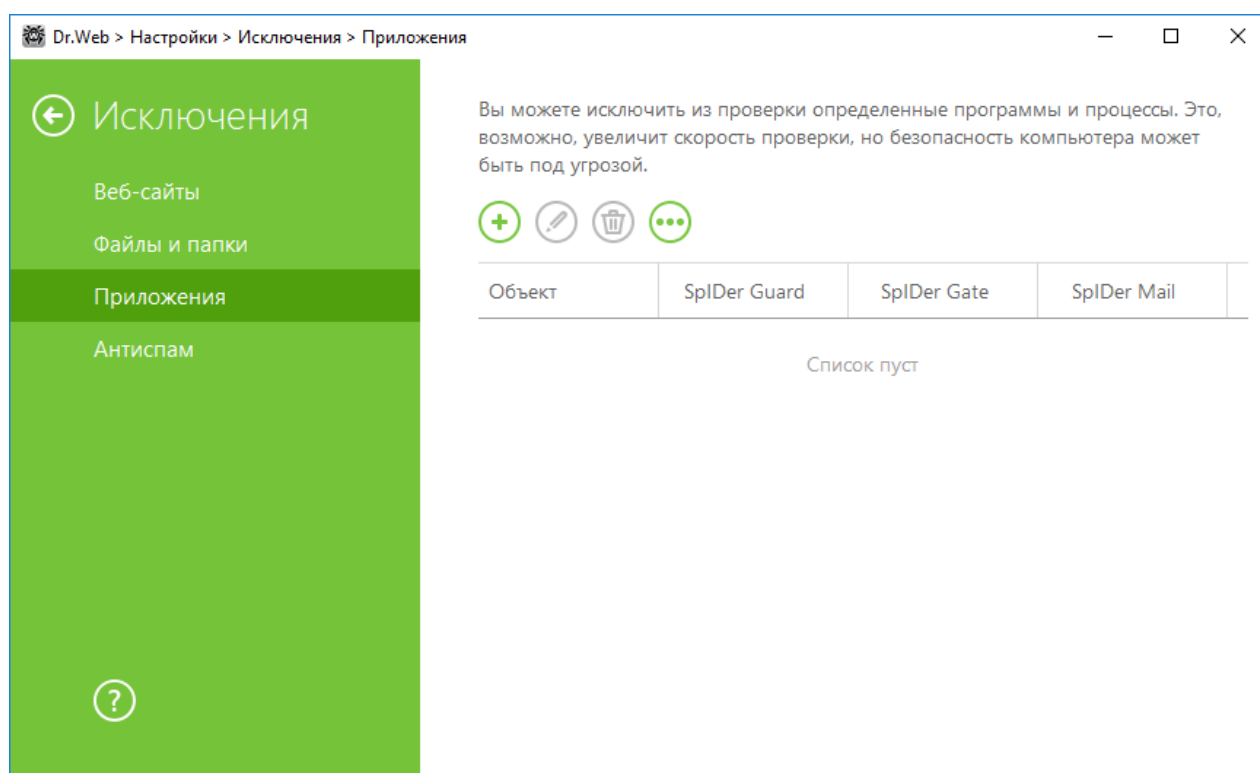


Рисунок 24. Список исключаемых приложений

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. Например:

`C:\Program Files\folder\example.exe`

- 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

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\*.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.
- вы можете исключить из проверки приложение по имени переменной, если в настройках системных переменных задано имя и значение этой переменной. Например:
- `%EXAMPLE_PATH%\example.exe` — исключает из проверки приложение по имени системной переменной. Имя системной переменной и ее 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`.

2. В окне настройки укажите, какие компоненты не должны проводить проверку выбранного приложения. Для объектов, исключаемых из проверки компонентами SplDer Gate и SplDer Mail, укажите дополнительные условия.



Параметр	Описание
Независимо от наличия цифровой подписи приложения	Выберите эту настройку, если приложение должно быть исключено из проверки вне зависимости от наличия у него действительной цифровой подписи.
При наличии действительной цифровой подписи приложения	Выберите эту настройку, если приложение должно быть исключено из проверки только при наличии действительной цифровой подписи приложения. В противном случае приложение будет проверено компонентами.
Любой трафик	Выберите эту настройку, чтобы исключить из проверки и зашифрованный, и незашифрованный трафик приложения.
Зашифрованный трафик	Выберите эту настройку, чтобы исключить из проверки только зашифрованный трафик приложения.
По всем IP-адресам и портам	Выберите эту настройку, чтобы исключить из проверки трафик, передаваемый на любые IP-адреса и порты.
По указанным IP-адресам и портам	Выберите эту настройку, чтобы указать IP-адреса или порты для исключения из проверки переданного с них трафика. Трафик, переданный с остальных IP-адресов или портов, будет проверен (если не исключен другими настройками).
Задание адресов и портов	Для тонкой настройки исключений используйте следующие рекомендации: • чтобы исключить из проверки определенный домен по определенному порту, укажите, например, <code>site.com:80</code>; • для исключения из проверки трафика по нестандартному порту (например, 1111) необходимо указать: <code>*:1111</code>; • для исключения из проверки трафика от домена по любому порту укажите: <code>site:*</code>.

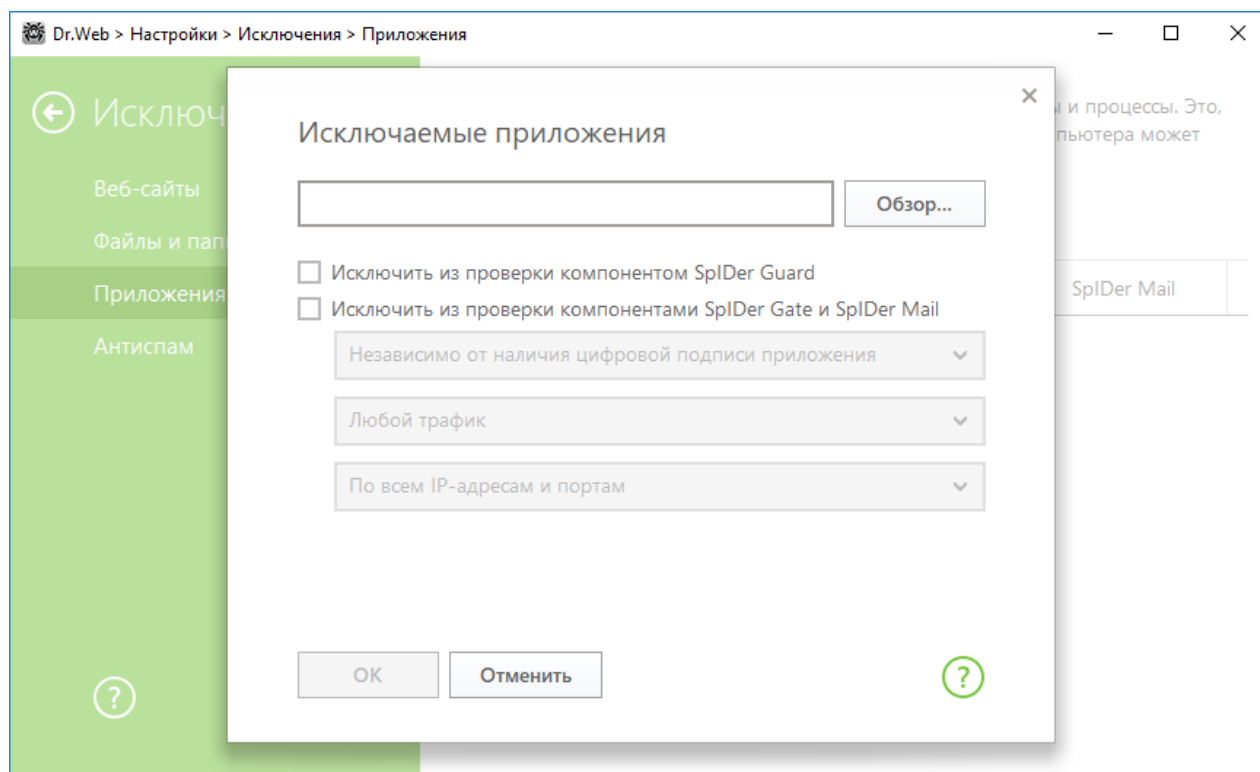


Рисунок 25. Добавление приложений в исключения

3. Нажмите кнопку **ОК**. Выбранное приложение появится в списке.
4. При необходимости повторите действия для добавления других программ.

Работа с объектами в списке

Чтобы отредактировать исключение, выберите нужный элемент в списке и нажмите . Чтобы удалить приложение из списка исключений, выберите соответствующий элемент в списке и нажмите .

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.

10.4. Антиспам

В этом окне задаются списки отправителей, письма которых будут исключены из проверки на спам. Компонент SplDer Mail пропускает или расценивает такие письма как спам без проведения анализа.



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

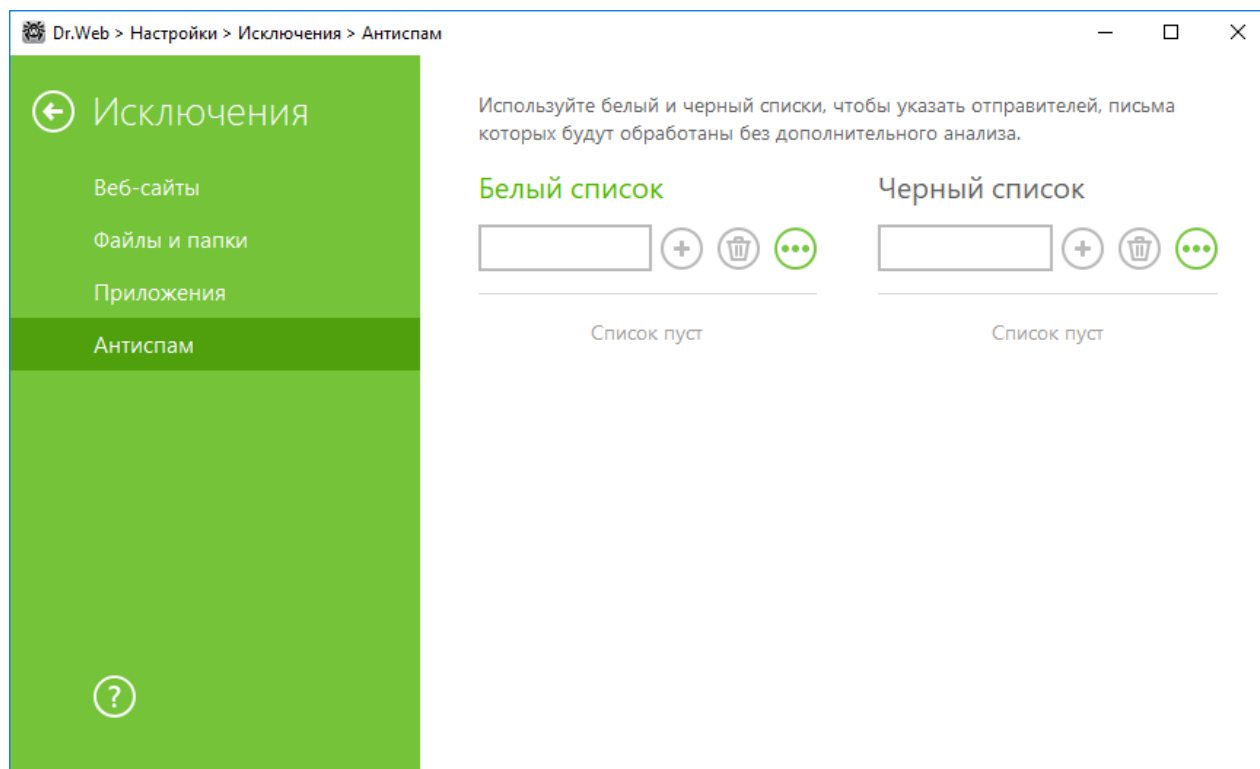


Рисунок 26. Добавление почтовых адресов в исключения

Задание списков антиспама

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



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

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. Компоненты защиты

Компоненты защиты обеспечивают сканирование системы, проверку писем на наличие угроз и спам, контроль сетевых соединений и HTTP-трафика.

Чтобы настроить компоненты защиты, откройте меню , запустите **Настройки**  в [режиме администратора](#) и выберите раздел **Компоненты защиты**.



Настройки компонентов защиты доступны только при запуске с [правами администратора](#).

Чтобы настроить проверку открываемых файлов или запускаемых процессов, выберите [SplDer Guard](#).

Чтобы настроить проверку HTTP-трафика, выберите [SplDer Gate](#).

Чтобы настроить проверку почты на наличие угроз, выберите [SplDer Mail](#).

Для контроля за подключениями и передачу данных по сети Интернет, а также для и блокировки подозрительных соединений на уровне пакетов и приложений, выберите [Брандмауэр](#).

Для изменения общих параметров проверки файлов и различных объектов, реакции на обнаружение зараженных или подозрительных файлов и вредоносных программ, выберите [Сканер](#).

Для контроля за поведением сторонних приложений выберите раздел [Превентивная защита](#).

11.1. SplDer Guard

SplDer 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 SplDer Guard применяет к ним действия согласно установленным настройкам.

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



проникновения на ваш компьютер вредоносных объектов, распространяемых посредством электронной почты, [используйте](#) почтовый сторож SplDer Mail.

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



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

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

11.1.1. Настройка SplDer Guard



Изменение настроек компонента возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.

Для доступа к настройкам сторожа SplDer 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.

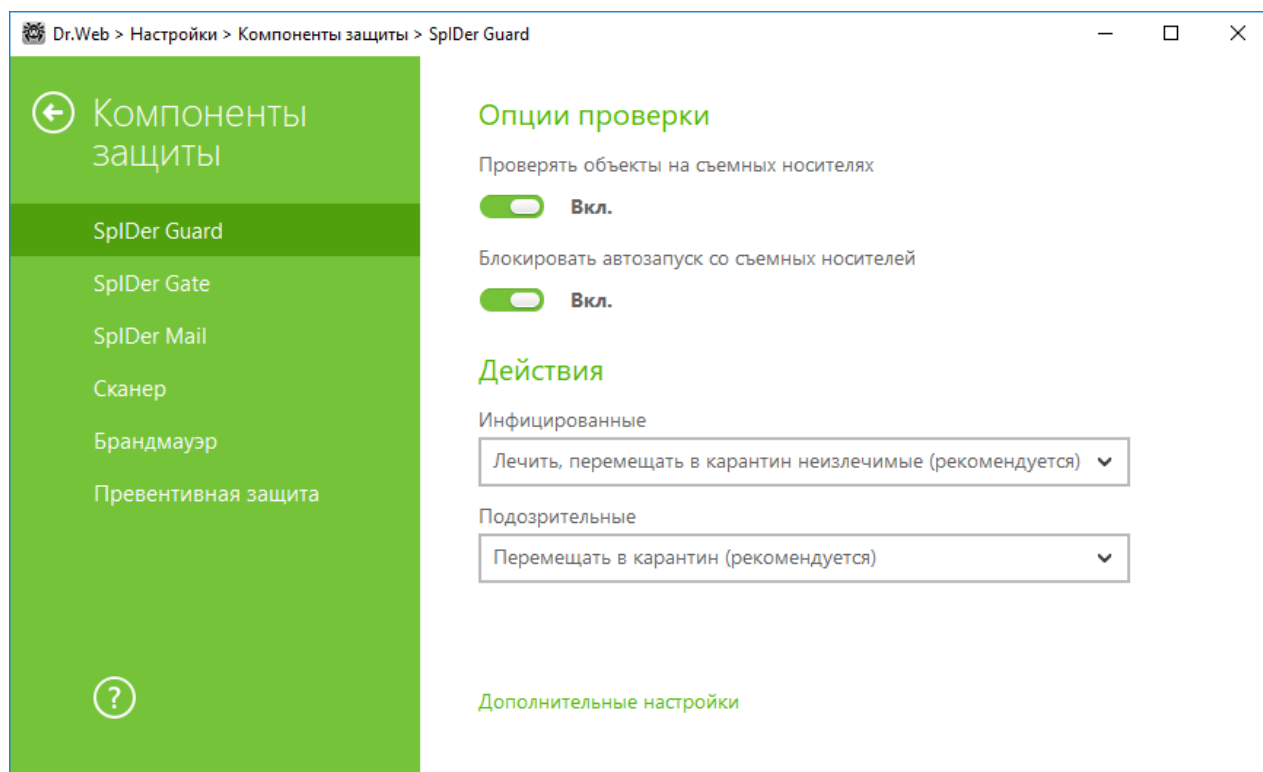


Рисунок 27. Настройка SplDer Guard

Опции проверки

SplDer Guard по умолчанию проверяет открываемые, изменяемые и запускаемые файлы на съемных носителях информации (CD/DVD-диски, флеш-накопители и т. д.), а также блокирует автоматический запуск их активного содержимого. Использование этих настроек помогает предотвратить заражение вашего компьютера через съемные носители. При отключении этих опций объекты на съемных носителях проверяться не будут.



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

Действия

В этом разделе задается реакция сторожа SplDer 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 SplDer Guard на обнаружение каждого типа объектов в отдельности. Состав доступных реакций при этом зависит от типа угрозы.

По умолчанию сторож SplDer 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 SplDer 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 (архивов, файлов электронной почты или файловых контейнеров).
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 (архивов, файлов электронной почты или файловых контейнеров).
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.
Сообщать	Выводить оповещение и пропустить объект без выполнения каких-либо действий.



Действие	Описание
	Данное действие возможно только для подозрительных объектов и вредоносных программ.



Сторож SplDer 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 SplDer 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 SplDer 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 SplDer Guard автоматически обрабатывает файл как вредоносную программу и по умолчанию перемещает его в Карантин.

Уточнения и рекомендации

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 SplDer 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 SplDer Guard неминуемо обнаруживает вредоносный объект.

Дополнительные настройки

Эта группа настроек позволяет задать параметры проверки на лету, которые будут применяться вне зависимости от выбранного режима работы сторожа SplDer 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);
- проверку скриптов, выполняемых Windows Script Host и Power Shell (для Windows 10).

Эвристический анализ

По умолчанию SplDer 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 Антивирус позволяет в фоновом режиме проводить проверку вашей операционной системы на наличие сложных угроз и при необходимости проводить лечение активного заражения.



При включении данной настройки Антируткит Dr.Web будет постоянно находиться в памяти. В отличие от проверки файлов на лету, проводимой сторожем SplDer Guard, поиск руткитов (вредоносных программ, предназначенных для сокрытия изменений в операционной системе, таких как работа определенных процессов, модификация ключей реестра, папок или файлов) 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 SplDer Guard не влияет на фоновую проверку. Если настройка включена, фоновая проверка осуществляется независимо от того, включен или выключен SplDer Guard.

11.2. SplDer Gate

SplDer Gate — модуль антивирусной проверки HTTP-трафика. При настройках по умолчанию SplDer Gate автоматически проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы. Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, т. е. работающие с сетью Интернет.

С помощью [изменения настроек](#) SplDer Gate вы можете отключить проверку входящего трафика или добавить к проверке и исходящий трафик, а также сформировать список тех приложений, HTTP-трафик которых будет проверяться в любом случае и в полном объеме. Также существует возможность исключения из проверки трафика отдельных приложений.

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

SplDer Gate не поддерживает проверку безопасных соединений, то есть не проверяет данные, передаваемые по криптографическим протоколам.



Программа постоянно находится в оперативной памяти компьютера и автоматически перезапускается при загрузке Windows.

11.2.1. Настройка SplDer Gate



Изменение настроек компонента возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.

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

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

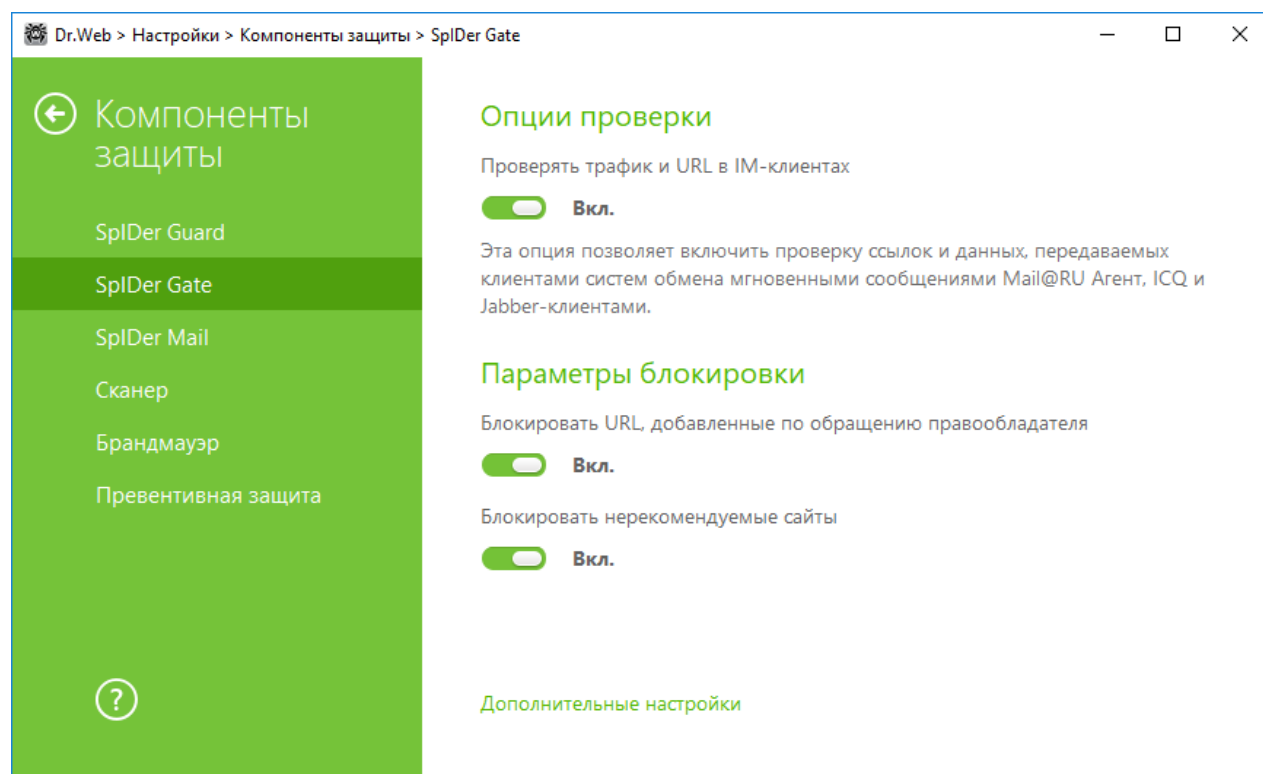


Рисунок 28. Настройка SplDer Gate

Проверка трафика IM-клиентов

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



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

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

Параметры блокировки

В группе **Параметры блокировки** вы можете установить автоматическую блокировку доступа к URL, добавленных по обращению правообладателя (для этого включите соответствующую опцию), а также к nereкомендованным сайтам, известным как неблагонадежные (для этого включите опцию **Блокировать nereкомендуемые сайты**). В разделе **Исключения** вы можете [указать сайты](#), доступ к которым должен быть разрешен, несмотря на установленные ограничения.



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

Блокировка программ

Веб-антивирус SpliDer Gate может блокировать следующие вредоносные программы:

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

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

Блокировка объектов

SpliDer Gate может блокировать непроверенные или поврежденные объекты. По умолчанию эти опции выключены.



Дополнительные настройки

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

Также вы можете настроить **Приоритет проверки** — распределение ресурсов в зависимости от приоритетности проверки трафика. При меньшем приоритете проверки скорость работы с сетью Интернет уменьшается, поскольку веб-антивирусу SplDer Gate приходится дольше ждать загрузки данных и проверять больший объем информации. При увеличении приоритета проверка производится чаще, что позволяет сторожу отдавать данные быстрее, тем самым повышая скорость работы с сетью. Однако при более частых проверках повышается нагрузка на процессор.

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

11.3. SplDer Mail

Почтовый сторож SplDer Mail по умолчанию включается в состав устанавливаемых компонентов, постоянно находится в памяти и автоматически запускается при загрузке операционной системы.

SplDer Mail не поддерживает проверку зашифрованного почтового трафика.

Обработка писем

Почтовый сторож SplDer Mail получает все входящие письма вместо почтового клиента и подвергает их антивирусной проверке с максимальной степенью подробности. При отсутствии вирусов или подозрительных объектов оно передается почтовой программе «прозрачным» образом — так, как если бы оно поступило непосредственно с сервера. Аналогично исходящие письма проверяются до отправки на сервер.

[Реакция](#) почтового сторожа SplDer Mail на обнаружение инфицированных и подозрительных входящих писем, а также писем, не прошедших проверки (например, писем с чрезмерно сложной структурой), по умолчанию следующая:

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



Инфицированные или подозрительные исходящие письма не передаются на сервер, пользователь извещается об отказе в отправке сообщения (как правило, почтовая программа при этом сохраняет письмо).

Настройки почтового сторожа SplDer Mail по умолчанию являются оптимальными для начинающего пользователя, обеспечивая максимальный уровень защиты при наименьшем вмешательстве пользователя. При этом, однако, блокируется ряд возможностей почтовых программ (например, направление письма по многим адресам может быть воспринято как массовая рассылка, полученный спам не распознается), а также утрачивается возможность получения полезной информации из автоматически уничтоженных писем (из незараженной текстовой части). Более опытные пользователи могут [изменить](#) параметры проверки почты и настройки реакции почтового сторожа SplDer Mail на различные события.

Проверка писем другими средствами

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

- далеко не все форматы почтовых ящиков популярных программ поддерживаются Сканером Dr.Web; при использовании почтового сторожа SplDer Mail зараженные письма даже не попадают в почтовые ящики;
- Сканер Dr.Web проверяет почтовые ящики, но только по запросу пользователя, а не в момент получения почты, причем данное действие является трудоемким и занимает значительное время.

Таким образом, при настройках всех компонентов Dr.Web по умолчанию почтовый сторож SplDer Mail первым обнаруживает и не допускает на компьютер вирусы и подозрительные объекты, распространяющиеся по электронной почте. Его работа является весьма экономичной с точки зрения расхода вычислительных ресурсов; остальные компоненты могут не использоваться для проверки почтовых файлов.

11.3.1. Настройка SplDer Mail



Изменение настроек компонента возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.

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

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

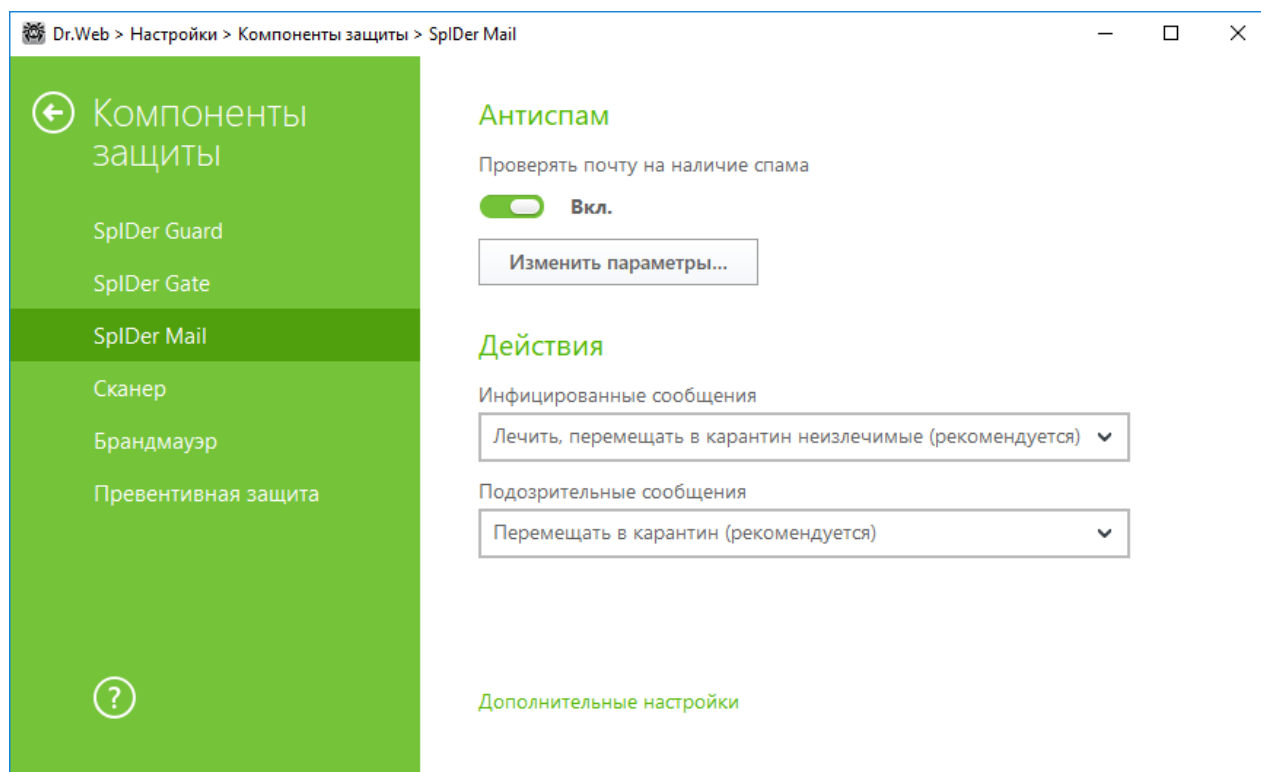


Рисунок 29. Настройка SplDer Mail

Антиспам

По умолчанию SplDer Mail проверяет письма на наличие спама. Вы можете отключить эту опцию с помощью соответствующего переключателя или изменить параметры проверки, нажав кнопку **Изменить параметры**. Технологии антиспам-фильтра и настраиваемые параметры подробно описаны в разделе [Антиспам](#).

Действия

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

Реакции почтового сторожа SplDer Mail аналогичны соответствующим реакциям Сканера Dr.Web.

Вы можете предписать почтовому сторожу SplDer Mail следующие реакции:

Действие	Описание
Лечить, перемещать	Восстановить состояние письма до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин.



Действие	Описание
в карантин неизлечимые	Данное действие возможно только для инфицированных писем, зараженных известным излечимым вирусом, за исключением троянских программ, которые при обнаружении удаляются. Лечение файлов в архивах невозможно вне зависимости от типа вируса.
Лечить, удалять неизлечимые	Восстановить состояние письма до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален.
Удалять	Удалить письмо. В этом случае электронное письмо не пересылается получателю, вместо этого почтовой программе передается сообщение о совершенной операции.
Перемещать в карантин	Переместить письмо в специальную папку Карантина . В этом случае письмо не пересылается получателю, вместо этого почтовой программе передается сообщение о совершенной операции.
Игнорировать	Передать письмо без выполнения каких-либо действий над ним.

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

Вы можете увеличить надежность антивирусной защиты по сравнению с уровнем, предусмотренным по умолчанию, выбрав в списке **Непроверенные** пункт **Перемещать в карантин**. Файлы с перемещенными письмами в этом случае рекомендуется впоследствии проверять Сканером Dr.Web.



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

Действия над письмами

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

Настройка	Описание
Добавлять заголовок 'X-Antivirus' к сообщениям	Установлена по умолчанию. При использовании данной настройки в заголовок всех писем, обработанных почтовым сторожем SplDer Mail, добавляется информация о проверке электронного сообщения и версии Dr.Web. Вы не можете изменить формат добавляемого заголовка.



Настройка	Описание
Удалять модифицированные письма на сервере	При использовании данной настройки входящие письма, удаленные или перемещенные в карантин почтовым сторожем SplDer Mail, удаляются с почтового сервера независимо от настроек почтовой программы.

Оптимизация проверки

Вы можете задать условие, при выполнении которого сложноустроенные письма, проверка которых является чрезмерно трудоемкой, признаются непроверенными. Для этого включите опцию **Тайм-аут проверки письма** и задайте максимальное время, в течение которого письмо проверяется. По истечении указанного времени почтовый сторож SplDer Mail прекратит проверку письма. По умолчанию задано значение 250 секунд.

Проверка архивов

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

- **Максимальный размер файла при распаковке.** Если распакованный архив превысит указанный размер, то почтовый сторож SplDer Mail не будет распаковывать и проверять его. По умолчанию задано значение 30720 КБ;
- **Максимальный коэффициент сжатия архива.** Если коэффициент сжатия превышает указанный, то почтовый сторож SplDer Mail не будет распаковывать и проверять его. По умолчанию задано значение 0;
- **Максимальный уровень вложенности в архив.** Если уровень вложенности превышает заданное значение, то почтовый сторож SplDer Mail проверит архив только до указанного уровня. По умолчанию задано значение 64.

Для включения одного или нескольких параметров оптимизации установите соответствующие флажки.



Ограничения для параметра отсутствуют, если задано значение 0.

Дополнительные настройки

Эта группа настроек задает дополнительные параметры проверки электронной почты:

- использование эвристического анализа — в данном режиме используются специальные механизмы, позволяющие выявить в электронной почте подозрительные объекты, с большой вероятностью зараженные еще неизвестными вирусами. Чтобы



отключить эвристический анализ, снимите флажок **Использовать эвристический анализ (рекомендуется)**;

- проверка инсталляционных пакетов. Эта настройка по умолчанию выключена.

11.3.2. Антиспам

Технологии антиспам-фильтра Dr.Web состоят из нескольких тысяч правил, которые условно можно разбить на несколько групп:

- **эвристический анализ** — чрезвычайно сложная высокоинтеллектуальная технология эмпирического разбора всех частей письма: поля заголовка, тела, содержания вложения;
- **фильтрация противодействия** — состоит в распознавании уловок, используемых спамерами для обхода антиспам-фильтров;
- **анализ на основе HTML-сигнатур** — сообщения, в состав которых входит HTML-код, сравниваются с образцами библиотеки HTML-сигнатур антиспама. Такое сравнение, в сочетании с данными о размерах изображений, обычно используемых отправителями спама, защищает пользователей от спам-сообщений, содержащих ссылки на веб-страницы;
- **семантический анализ** — сравнение слов и выражений сообщения со словами и идиомами, типичными для спама, производится по специальному словарю. Анализ подвергается как видимые, так и визуально скрытые специальными техническими уловками слова, выражения и символы;
- **анти-скамминг технология** — к числу скамминг- и фарминг-сообщений относятся т. н. «нигерийские письма», сообщения о выигрышах в лотерею, казино, поддельные письма банков. Для их фильтрации применяется специальный модуль;
- **фильтрация технического спама** — так называемые bounce-сообщения возникают как реакция на вирусы или как проявление вирусной активности. Специальный модуль антиспама определяет такие сообщения как нежелательные.

Вы можете настроить следующие параметры работы Антиспама:

Настройка	Описание
Разрешить текст на кириллице	Установлена по умолчанию. Данная настройка указывает почтовому сторожу SplDer Mail без предварительного анализа не причислять к спаму письма, написанные в соответствии с установленной кириллической кодировкой. Если этот флажок снят, то такие письма с большой вероятностью будут отмечены фильтром как спам.
Разрешить текст на азиатских языках	Установлена по умолчанию. Данная настройка указывает почтовому сторожу SplDer Mail без предварительного анализа не причислять к спаму письма, написанные в соответствии с наиболее распространенными кодировками азиатских языков. Если этот флажок снят, то такие



Настройка	Описание
	письма с большой вероятностью будут отмечены фильтром как спам.
Добавлять префикс к теме писем, содержащих спам	Установлена по умолчанию. В начало темы спам-писем добавляется подстрока «[SPAM]». Данная настройка указывает почтовому сторожу SplDer Mail добавлять указанный префикс к темам писем, распознаваемых как спам. Добавление префикса поможет вам создать правила для фильтрации почтовых сообщений, помеченных как спам, в тех почтовых клиентах (например, MS Outlook Express), в которых невозможно настроить фильтры по заголовкам писем.

Обработка писем спам-фильтром

Почтовый сторож SplDer Mail добавляет ко всем проверенным письмам следующие заголовки:

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

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



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

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



Спам-фильтром обрабатываются почтовые сообщения, составленные в соответствии со стандартом MIME RFC 822.



Исправление ошибок распознавания

1. При обнаружении ошибки в работе спам-фильтра, создайте новое письмо и приложите к нему неправильно распознанное сообщение. Письма, отправленные в тексте письма, анализироваться не будут.
2. Отправьте письмо с вложением администратору вашей антивирусной сети.

11.4. Сканер



Изменение настроек компонента возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.

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.

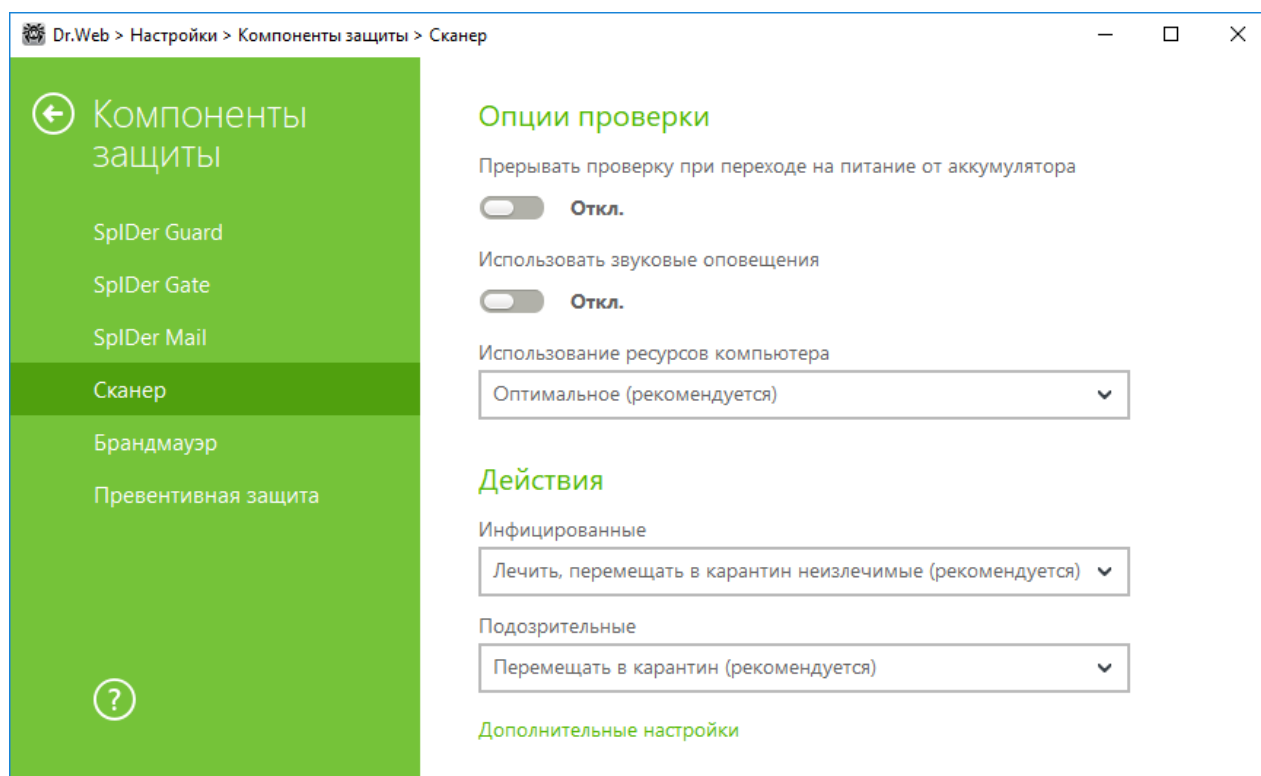


Рисунок 30. Настройка Сканера

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 (архивов, файлов электронной почты или файловых контейнеров).
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



Действие	Описание
	файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).
Удалить	Удалить объект. Для загрузочных секторов никаких действий производиться не будет.
Перемещать в карантин	Переместить объект в специальную папку Карантина . Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропустить объект без выполнения каких-либо действий и не выводить оповещения. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.
Сообщить	Выводить оповещение и пропустить объект без выполнения каких-либо действий. Данное действие возможно только для подозрительных объектов и вредоносных программ.



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

Дополнительные настройки

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.



11.5. Брандмауэр

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

Брандмауэр предоставляет вам следующие преимущества:

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

11.5.1. Обучение Брандмауэра

После установки Брандмауэра некоторое время в процессе вашей работы за компьютером производится обучение программы. Режим обучения актуален для следующих режимов работы Брандмауэра (подробнее о режимах работы Брандмауэра см. раздел [Настройка брандмауэра](#)):

- **Разрешать соединения для доверенных приложений** (установлен по умолчанию);
- **Интерактивный режим**.

В режиме **Разрешать соединения для доверенных приложений** при обнаружении попытки системы или приложений подключиться к сети Брандмауэр проверяет, являются ли эти приложения доверенными и заданы ли для них правила фильтрации. Если правила отсутствуют, Dr.Web выводит соответствующее предупреждение, где вы можете задать правило. Для доверенных приложений правила при этом не создаются. Подключение к сети для таких приложений разрешено.

К доверенным приложениям относятся: системные или имеющие сертификат Microsoft приложения, а также приложения из списка доверенных приложений Dr.Web.

В режиме **Интерактивный режим** при обнаружении попытки системы или приложений подключиться к сети Брандмауэр проверяет, заданы ли для этих программ правила фильтрации. Если правила отсутствуют, то выводится соответствующее предупреждение, где вы можете задать правило. В дальнейшем подобные подключения будут обрабатываться по этому правилу.



При работе под ограниченной учетной записью (Гость) Брандмауэр Dr.Web не выдает пользователю предупреждения о попытках доступа к сети. Предупреждения



будут выдаваться под учетной записью с правами администратора, если такая сессия активна одновременно с гостевой.

Правила для приложений

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

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

2. Примите решение о подходящей для данного случая операции и выберите соответствующее действие в нижней части окна:
 - чтобы однократно блокировать данное подключение, выберите действие **Запретить однократно**;
 - чтобы однократно позволить приложению данное подключение, выберите действие **Разрешить однократно**;
 - чтобы перейти к форме создания правила фильтрации, выберите действие **Создать правило**. Откроется окно, в котором вы можете либо выбрать предустановленное правило, либо вручную [создать правило для приложений](#).
3. Нажмите кнопку **ОК**. Брандмауэр выполнит указанную вами операцию, и окно оповещения будет закрыто.



В некоторых случаях операционная система Windows не позволяет однозначно идентифицировать службу, работающую как системный процесс. При обнаружении попытки подключения со стороны системного процесса, обратите внимание на порт, указанный в сведениях о соединении. Если вы используете приложение, которое может обращаться к указанному порту, разрешите данное подключение.



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

Правила для родительских процессов

1. При обнаружении попытки подключения к сети со стороны приложения, запущенного неизвестной для Брандмауэра программой, ознакомьтесь с информацией об исполняемом файле родительской программы.
2. Когда вы примете решение о подходящей для данного случая операции, выполните одно из следующих действий:
 - чтобы однократно блокировать подключение приложения к сети, нажмите кнопку **Запретить**;
 - чтобы однократно позволить приложению подключиться к сети, нажмите кнопку **Разрешить**;
 - чтобы создать правило, нажмите **Создать правило** и в открывшемся окне задайте необходимые [настройки для родительского процесса](#).
3. Нажмите кнопку **ОК**. Брандмауэр выполнит указанную вами операцию, и окно оповещения будет закрыто.

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

11.5.2. Настройка Брандмауэра

В этом разделе вы можете настроить следующие параметры работы Брандмауэра:

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



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

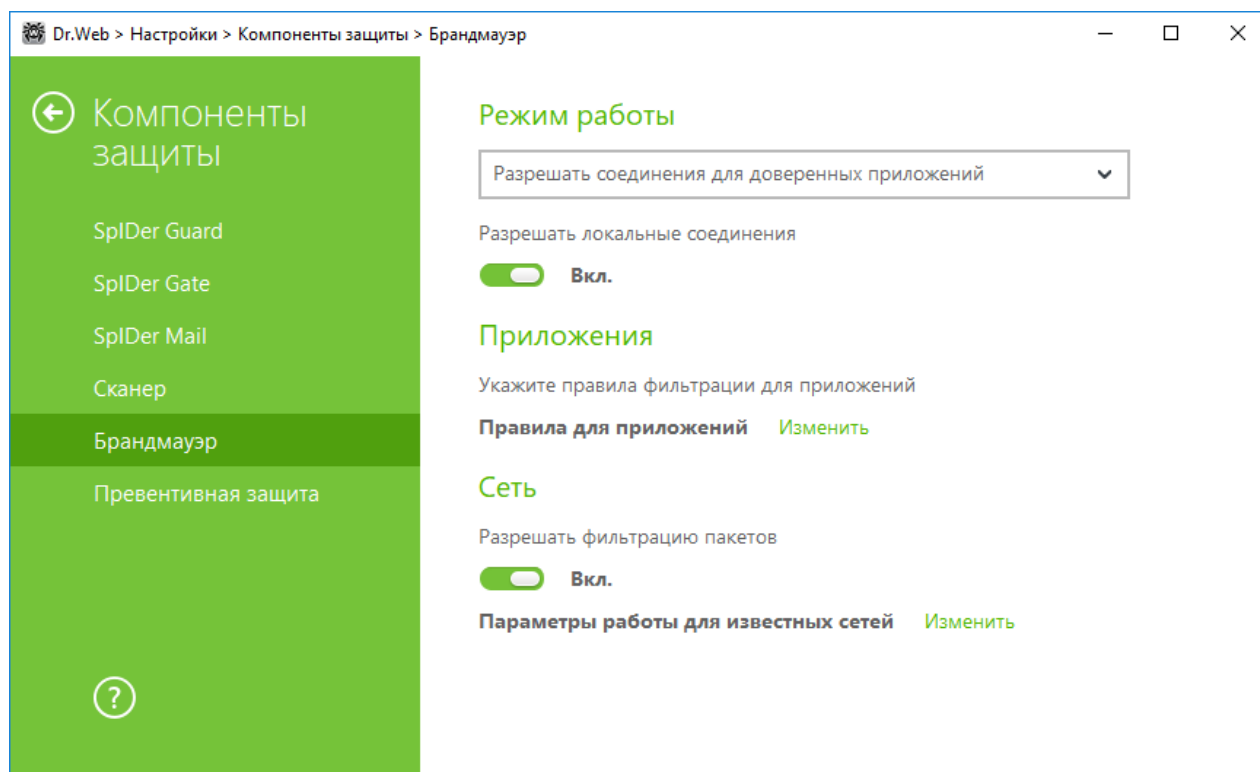


Рисунок 31. Основные настройки Брандмауэра

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

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

Настройка **Разрешать локальные соединения** позволяет всем приложениям беспрепятственно устанавливать локальные соединения (с интерфейса или на интерфейс 127.0.0.1 (localhost)) на вашем компьютере. Эта опция применяется после проверки соединений на соответствие заданным правилам. Отключите эту опцию, чтобы применять правила фильтрации вне зависимости от того, происходит ли соединение по сети или в рамках вашего компьютера.

Выбор режима работы

Выберите один из следующих режимов работы:

- **Разрешать соединения для доверенных приложений** — режим, при котором всем доверенным приложениям предоставляется доступ к сетевым ресурсам (используется по умолчанию), для всех остальных приложений выдается предупреждение, где вы можете задать правило (см. раздел [Обучение Брандмауэра](#));
- **Разрешать неизвестные соединения** — режим, при котором всем неизвестным приложениям предоставляется доступ к сетевым ресурсам;
- **Интерактивный режим** — [режим обучения](#), при котором пользователю предоставляется полный контроль над реакцией Брандмауэра;



- **Блокировать неизвестные соединения** — режим, при котором все неизвестные подключения автоматически блокируются. Известные соединения обрабатываются Брандмауэром согласно заданным правилам фильтрации.

Разрешать соединения для доверенных приложений

Этот режим используется по умолчанию.

В этом режиме всем доверенным приложениям разрешается доступ к сетевым ресурсам, включая Интернет. К доверенным приложениям относятся: системные или имеющие сертификат Microsoft приложения, а также приложения из списка доверенных приложений Dr.Web. Правила для таких приложений не отображаются в списке правил. Для других приложений Брандмауэр предоставляет вам возможность вручную запрещать или разрешать неизвестное соединение, а также создавать для него правило.

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

Разрешать неизвестные соединения

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

Интерактивный режим

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

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

Блокировать неизвестные соединения

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

При обнаружении попытки со стороны операционной системы или пользовательского приложения получить доступ к сетевым ресурсам Брандмауэр проверяет, заданы ли для этих



программ правила фильтрации. Если правила фильтрации отсутствуют, то Брандмауэр автоматически блокирует доступ к сети и не выводит никаких сообщений. Если правила фильтрации для данного подключения заданы, то выполняются указанные в них действия.

Параметры для приложений



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

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

В данном разделе вы можете формировать наборы правил фильтрации, создавая новые, редактируя существующие или удаляя ненужные правила. Приложение однозначно идентифицируется полным путем к исполняемому файлу. Для указания ядра операционной системы Microsoft Windows (процесс system, для которого нет соответствующего исполняемого файла) используется имя `SYSTEM`.



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

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

Правила для приложений

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

Для доступа к этому окну в настройках Брандмауэра в пункте **Правила для приложений** нажмите **Изменить** и в появившемся окне нажмите кнопку  или выберите приложение и нажмите кнопку .

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



Запуск других приложений

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

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

Доступ к сетевым ресурсам

1. Выберите режим доступа к сетевым ресурсам:

- **Разрешать все** — все соединения приложения будут разрешены;
- **Блокировать все** — все соединения приложения запрещены;
- **Не задано**. В этом случае на это приложение будут распространяться настройки выбранного [режима работы](#) Брандмауэра.
- **Пользовательский** — в этом режиме вы можете создать набор правил, разрешающих или запрещающих те или иные соединения приложения.

2. Если был выбран **Пользовательский** режим доступа к сетевым ресурсам, то ниже отобразится таблица с информацией о наборе правил для данного приложения.

Параметр	Описание
Включено	Состояние правила.
Действие	Указывает на действие, выполняемое Брандмауэром при попытке программы подключиться к сети Интернет: • Блокировать пакеты — блокировать попытку подключения; • Разрешать пакеты — разрешить подключение.
Имя правила	Название правила.
Тип соединения	Направление соединения: • Входящее — правило применяется, если соединение инициируется из сети к программе на вашем компьютере; • Исходящее — правило применяется, если соединение инициируется программой на вашем компьютере; • Любое — правило применяется вне зависимости от направления соединения.
Описание	Пользовательское описание правила.



3. При необходимости отредактируйте предустановленный или создайте новый набор правил для приложения.
4. Если вы выбрали создание нового или редактирование существующего правила, [настройте его параметры](#) в отобразившемся окне.
5. По окончании редактирования набора правил нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для отказа от изменений. Изменения, внесенные в набор правил, сохраняются при переключении на другой режим.

Установите флажок **Запрашивать подтверждение при изменении объекта (рекомендуется)**, если вы хотите, чтобы при изменении или обновлении приложений доступ к сетевым ресурсам для приложения запрашивался заново.

Настройка параметров правила

Правила фильтрации регулируют сетевое взаимодействие программы с конкретными хостами сети.

Создание и редактирование правила

Для добавления нового правила в окне **Редактирование набора правил** нажмите кнопку . Для редактирования существующего правила выберите необходимое правило и нажмите кнопку . При этом в пункте **Доступ к сетевым ресурсам** должен быть выбран режим **Пользовательский**.

Задайте следующие параметры правила:

Параметр	Описание
Общее	
Имя правила	Имя создаваемого/редактируемого правила.
Описание	Краткое описание правила.
Действие	Указывает на действие, выполняемое Брандмауэром при попытке программы подключиться к сети Интернет: • Блокировать пакеты — блокировать попытку подключения; • Разрешать пакеты — разрешить подключение.
Состояние	Состояние правила: • Включено — правило применяется; • Отключено — правило временно не применяется.



Параметр	Описание
Тип соединения	Направление соединения: • Входящее — правило применяется, если соединение инициируется из сети к программе на вашем компьютере; • Исходящее — правило применяется, если соединение инициируется программой на вашем компьютере; • Любое — правило применяется вне зависимости от направления соединения.
Ведение журнала	Режим ведения журнала: • Включено — регистрировать события; • Отключено — не сохранять информацию о правиле.
Настройки правила	
Протокол	Протоколы сетевого и транспортного уровня, по которым осуществляется подключение. Поддерживаются следующие протоколы сетевого уровня: • IPv4; • IPv6; • IP all — протокол IP любой версии. Поддерживаются следующие протоколы транспортного уровня: • TCP; • UDP; • TCP & UDP — протокол TCP или UDP; • RAW.
Локальный адрес/Удаленный адрес	IP-адрес удаленного хоста, участвующего в подключении. Вы можете указывать как конкретный адрес (Равен), так и диапазон адресов (В диапазоне), а также маску конкретной подсети (Маска) или маски всех подсетей, в которых ваш компьютер имеет сетевой адрес (MY_NETWORK). Чтобы задать правило для всех хостов, выберите вариант Любой.



Параметр	Описание
Локальный порт/Удаленный порт	Порт, по которому осуществляется подключение. Вы можете указывать как конкретный порт (Равен), так и диапазон портов (В диапазоне). Чтобы задать правило для всех портов, выберите вариант Любой.

Параметры для сетей

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

Данный вид фильтрации предоставляет вам общие механизмы контроля, в отличие от [фильтрации на уровне приложений](#).

Фильтр пакетов

В окне **Сеть** вы можете задать набор правил фильтрации пакетов, передающихся через определенный интерфейс.

Для доступа к этому окну в окне настроек Брандмауэра в пункте **Параметры работы для известных сетей** нажмите **Изменить**. Найдите в списке интересующий вас интерфейс и сопоставьте ему соответствующий набор правил. Если подходящий набор правил отсутствует в списке, создайте его.

Брандмауэр поставляется со следующими предустановленными наборами правил:

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

Для удобства использования и быстрого переключения между режимами фильтрации вы можете [задать дополнительные наборы правил](#).

Для того чтобы увидеть все доступные интерфейсы или добавить в таблицу новый интерфейс, нажмите кнопку . В открывшемся окне вы можете указать, какие интерфейсы должны всегда отображаться в таблице. Активные интерфейсы будут отображаться в таблице автоматически.

Неактивные сетевые интерфейсы можно удалить из отображаемой таблицы, нажав кнопку .



Настройки пакетного фильтра

Для управления существующими наборами правил и добавления новых перейдите в окно **Настройки пакетного фильтра**, нажав кнопку **Наборы правил**.

На этой странице вы можете:

- **формировать** наборы правил фильтрации, создавая новые, редактируя существующие или удаляя ненужные правила;
- **задавать** дополнительные параметры фильтрации.

Формирование набора правил

Для формирования набора правил выполните одно из следующих действий:

- чтобы создать набор правил для сетевого интерфейса, нажмите ;
- чтобы отредактировать существующий набор правил, выберите его в списке и нажмите ;
- чтобы добавить копию существующего набора правил, нажмите . Копия добавляется под выбранным набором;
- чтобы удалить выбранный набор правил, нажмите .

Дополнительные настройки

Чтобы задать дополнительные настройки фильтрации пакетов, в окне **Настройки пакетного фильтра** установите следующие флажки:

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



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

Нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для выхода из окна без сохранения изменений.

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



Для каждого правила в списке предоставляется следующая краткая информация:

Параметр	Описание
Включено	Состояние правила.
Действие	Указывает на действие, выполняемое Брандмауэром при обработке пакета: • Блокировать пакеты — блокировать пакет; • Разрешать пакеты — передать пакет.
Имя правила	Имя правила.
Направление	Направление соединения: •  — правило применяется, если пакет принимается из сети; •  — правило применяется, если пакет отправляется с вашего компьютера; •  — правило применяется вне зависимости от направления соединения.
Ведение журнала	Режим регистрации событий. Указывает на то, какая информация должна быть занесена в журнал: • Только заголовки — заносить в журнал только заголовки пакетов; • Весь пакет — заносить в журнал пакеты целиком; • Отключено — не сохранять информацию о пакете.
Описание	Краткое описание правила.

Редактирование и создание набора правил

1. При необходимости задайте имя или измените имя набора правил.
2. Создайте правила фильтрации, используя следующие опции:
 - чтобы добавить новое правило, нажмите . Правило добавляется в начало списка;
 - чтобы отредактировать выбранное правило, нажмите ;
 - чтобы добавить копию выбранного правила, нажмите кнопку . Копия добавляется перед выбранным правилом;
 - чтобы удалить выбранное правило, нажмите .
3. Если вы выбрали создание нового или редактирование существующего правила, [настройте его параметры](#).
4. Используйте стрелочки справа от списка, чтобы определить порядок выполнения правил. Правила выполняются последовательно, согласно очередности в списке.
5. По окончании редактирования списка нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для отказа от изменений.



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

Добавление или редактирование правила фильтрации

1. В окне редактирования набора правил для пакетного фильтра нажмите кнопку или кнопку . Откроется окно создания или редактирования правила пакетной фильтрации.
2. Задайте следующие параметры правила:

Параметр	Описание
Имя правила	Имя создаваемого/редактируемого правила.
Описание	Краткое описание правила.
Действие	Указывает на действие, выполняемое Брандмауэром при обработке пакета: • Блокировать пакеты — блокировать пакет; • Разрешать пакеты — передать пакет.
Направление	Направление соединения: • Входящее — правило применяется, если пакет принимается из сети; • Исходящее — правило применяется, если пакет отправляется с вашего компьютера; • Любое — правило применяется вне зависимости от направления соединения.
Ведение журнала	Режим регистрации событий. Указывает на то, какая информация должна быть занесена в журнал: • Весь пакет — заносить в журнал пакеты целиком; • Только заголовки — заносить в журнал только заголовки пакетов; • Отключено — не сохранять информацию о пакете.



3. При необходимости добавьте критерий фильтрации, например, транспортный или сетевой протокол, нажав кнопку **Добавить критерий**. Откроется окно **Добавить критерий фильтрации**:

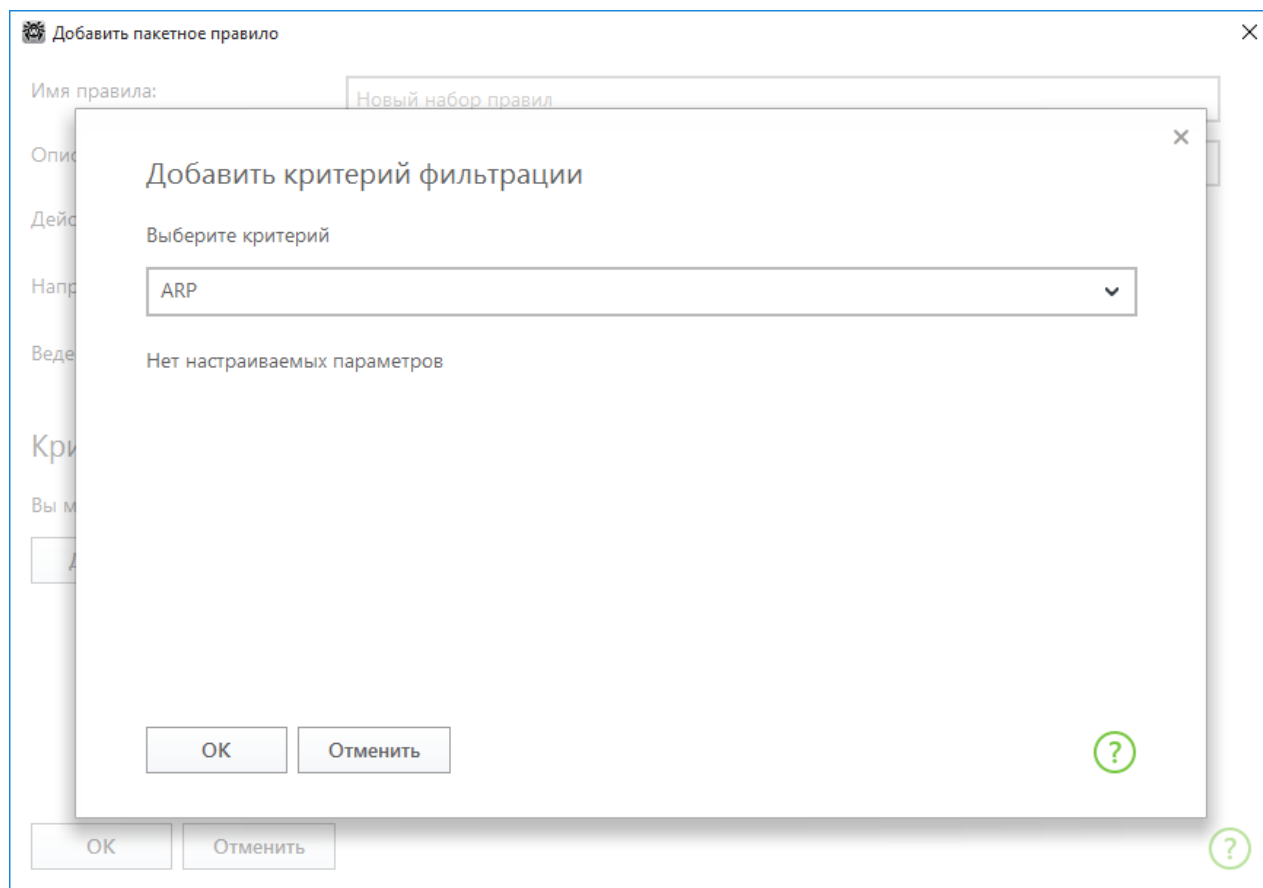


Рисунок 32. Добавление критерия фильтрации

Выберите нужный критерий в выпадающем списке. В этом же окне вы можете настроить параметры для выбранного критерия. Вы можете добавить любое необходимое количество критериев. При этом, чтобы действие из правила было применено к пакету, пакет должен соответствовать всем критериям правила.

Для некоторых заголовков доступны дополнительные критерии фильтрации. Все добавленные критерии отображаются в окне редактирования пакетного правила и доступны для редактирования.

4. По окончании редактирования нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для выхода из окна без сохранения изменений.



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



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

11.6. Dr.Web для Outlook

Основные функции компонента

Подключаемый модуль Dr.Web для Outlook выполняет следующие функции:

- антивирусная проверка вложенных файлов входящих почтовых сообщений;
- проверка почтовых сообщений на спам;
- обнаружение и нейтрализацию вредоносного программного обеспечения;
- использование эвристического анализатора для дополнительной защиты от неизвестных вирусов.

Настройка модуля Dr.Web для Outlook

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



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

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

- [Журнал](#) — позволяет настроить регистрацию событий программы;
- [Проверка вложений](#) — позволяет настроить проверку электронной почты и определить действия программы для обнаруженных вредоносных объектов;
- [Спам-фильтр](#) — позволяет определить действия программы для спам-сообщений, а также создать белый и черный списки электронных адресов;
- [Статистика](#) — показывает данные об объектах, проверенных и обработанных программой.

11.6.1. Проверка на вирусы

Dr.Web для Outlook использует различные [методы обнаружения вирусов](#). К найденным вредоносным объектам применяются определяемые пользователем действия: программа



может лечить инфицированные объекты, удалять их или перемещать в [Карантин](#) для их изоляции и безопасного хранения.

Программа Dr.Web для Outlook обнаруживает следующие вредоносные объекты:

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

Действия

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

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



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

Для ОС Windows Vista и более поздних версий при нажатии кнопки **Проверка вложений**:

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

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



Для задания действий над обнаруженными вредоносными объектами служат следующие настройки:

- выпадающий список **Инфицированные** задает реакцию на обнаружение объектов, зараженных известными и (предположительно) излечимыми вирусами;
- выпадающий список **Невылеченные** задает реакцию на обнаружение объектов, зараженных известным неизлечимым вирусом, а также когда предпринятая попытка излечения не принесла успеха;
- выпадающий список **Подозрительные** задает реакцию на обнаружение объектов, предположительно зараженных вирусом (срабатывание эвристического анализатора);
- раздел **Вредоносные программы** задает реакцию на обнаружение следующего нежелательного ПО:
 - ☐ рекламные программы;
 - ☐ программы дозвона;
 - ☐ программы-шутки;
 - ☐ программы взлома;
 - ☐ потенциально опасные;
- выпадающий список **При ошибке проверки** позволяет настроить действия программы в случае, если проверка вложения невозможна, например, если оно представляет собой поврежденный или защищенный паролем файл;
- флажок **Проверять архивы** позволяет включить или отключить проверку вложенных файлов, представляющих собой архивы. Установите этот флажок для включения проверки, снимите — для отключения.

Состав доступных реакций зависит от типа вирусного события.

Предусмотрены следующие действия над обнаруженными объектами:

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



11.6.2. Проверка на спам

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

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



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

Для ОС Windows Vista и более поздних версий при нажатии кнопки **Спам-фильтр**:

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

Настройка спам-фильтра

Для настройки параметров спам-фильтра:

- Установите флажок **Проверять почту на спам** для активации спам-фильтра.
- Если вы хотите добавлять специальный текст в заголовок сообщения, распознанного как спам, установите флажок **Добавлять префикс в тему письма**. Добавляемый текст можно ввести в текстовом поле справа от флажка. По умолчанию добавляется префикс *****SPAM*****.
- Проверенные сообщения могут отмечаться как прочитанные в свойствах письма. Для этого необходимо установить флажок **Отметить письмо как прочитанное**. По умолчанию флажок **Отметить письмо как прочитанное** установлен.
- Также вы можете настроить [белые и черные списки](#) для фильтрации писем.



Если некоторые письма были неправильно распознаны, следует отправить их администратору вашей антивирусной сети.

Белый и черный списки

Белый и черный списки электронных адресов служат для фильтрации сообщений.



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

Чтобы добавить адрес в белый или черный список:

1. Нажмите кнопку **Добавить**.
2. Введите электронный адрес в соответствующее поле.
3. Нажмите кнопку **ОК** в окне **Редактировать список**.

Чтобы изменить адреса в списке:

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

Чтобы удалить адрес из списка:

1. Выберите адрес в списке.
2. Нажмите кнопку **Удалить**.

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

Белый список

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

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

Например, допускаются следующие варианты:

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



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

Символ «@» обязателен.

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

Черный список

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

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

Например, допускаются следующие варианты:

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



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

Символ «@» обязателен.

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



Например, чтобы пометить как спам все письма от отправителей с названием почтового ящика «ivanov», введите `ivanov@*`;

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

11.6.3. Регистрация событий

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

- журнале регистрации событий операционной системы (Event Log);
- текстовом журнале отладки.

Журнал операционной системы

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

- сообщения о запуске и остановке программы;
- параметры модулей программы: сканера, ядра, вирусных баз (информация заносится при запуске программы и при обновлении модулей);
- сообщения об обнаружении вирусов.

Чтобы просмотреть журнал регистрации событий операционной системы:

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

Текстовый журнал отладки

В текстовый журнал отладки заносится следующая информация:

- сообщения об обнаружении вирусов;
- сообщения об ошибках записи или чтения файлов, ошибках анализа архивов или файлов, защищенных паролем;
- параметры модулей программы: сканера, ядра, вирусных баз;
- сообщения об экстренных остановках ядра программы.



Настройка регистрации событий

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



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

3. Нажмите кнопку **ОК** для сохранения изменений.



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

Для операционной системы Windows Vista и более поздних версий при нажатии кнопки **Журнал**:

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

Просмотр журнала событий программы

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

11.6.4. Статистика

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

Объекты разделяются на следующие категории:

- **Проверено** — общее количество проверенных писем;
- **Инфицированных** — количество писем, содержащие вирусы;
- **Подозрительных** — количество писем, предположительно зараженных вирусом (срабатывание эвристического анализатора);



- **Вылечено** — количество объектов, успешно вылеченных программой;
- **Непроверенных** — количество объектов, проверка которых невозможна или при проверке возникли ошибки;
- **Чистых** — количество писем, не содержащих вредоносных объектов.

Затем указывается количество объектов, к которым были применены действия:

- **Перемещено** — количество объектов, перемещенных в Карантин;
- **Удалено** — количество объектов, удаленных из системы;
- **Пропущено** — количество объектов, пропущенных без изменений;
- **Спам-писем** — количество писем, распознанных как спам.

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



Статистическая информация накапливается в рамках одной сессии. После перезагрузки компьютера, или при рестарте Агент Dr.Web для Windows, статистика обнуляется.

11.7. 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.

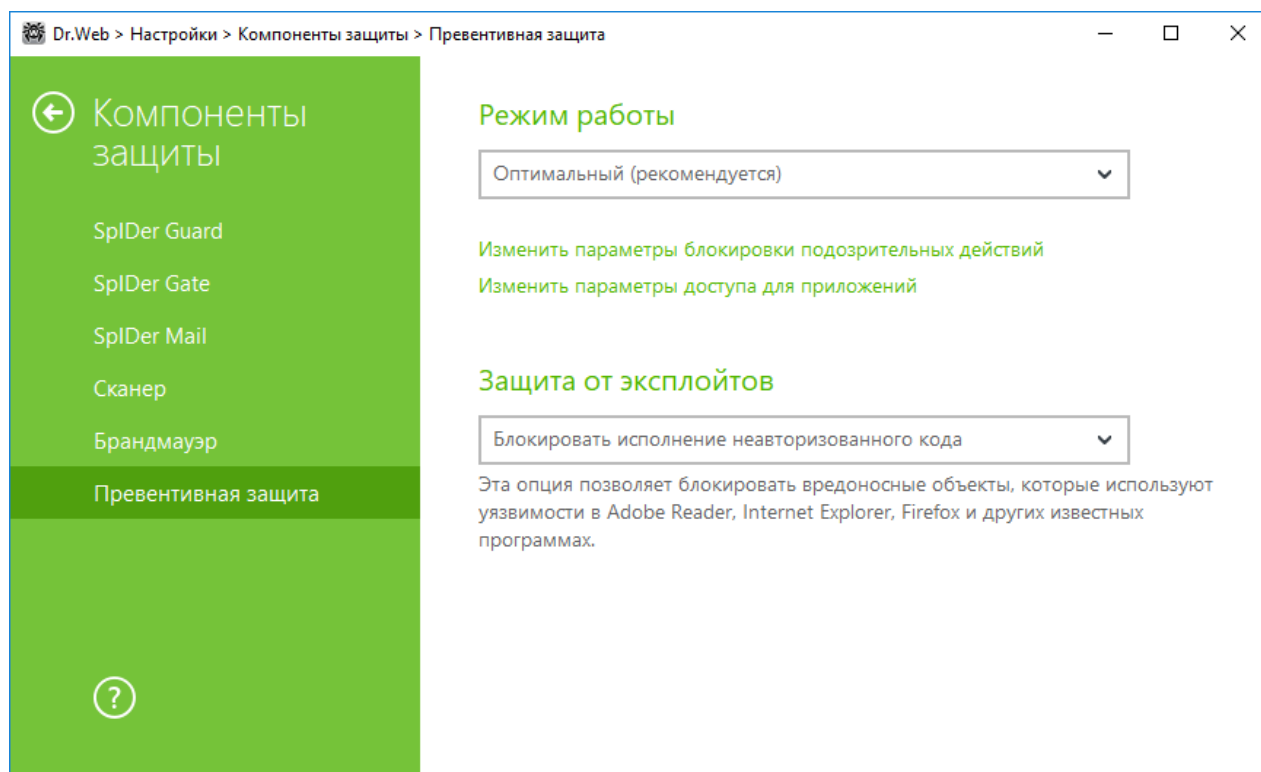


Рисунок 33. Настройка Превентивной защиты

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 на .

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

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

Уровень превентивной защиты

В режиме работы **Оптимальный**, 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 приложениям, действия которых также однозначно определяются, как попытка вредоносного воздействия на операционную систему.



Блокируются только действия приложений, которые не являются доверенными.

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 .
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, Applnit_DLLs, LoadApplnit_DLLs, Load, Run, IconServiceLib Ассоциации исполняемых файлов: • Software\Classes\exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи)



Защищаемый объект	Описание
	• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, Inkfile (ключи) Политики ограничения запуска программ (SRP): • Software\Policies\Microsoft\Windows\Safer Плагины Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Автозапуск программ: • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce 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.



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 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.



12. Статистика

В данном окне собрана статистика по важным событиям в работе компонентов защиты.

Чтобы просмотреть сведения о работе компонентов, откройте меню  в [режиме администратора](#) и перейдите в раздел **Статистика** . На странице **Статистика** доступны отчеты для следующих групп:

- Угрозы
- Обновление
- Офисный контроль

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

В группе **Офисный контроль** отражается статистика заблокированных URL для каждой учетной записи.

В отчете фиксируются следующие сведения:

- Частота посещений;
- Действие;
- URL.

Для записей отчета имеются предустановленные фильтры, которые доступны в выпадающем списке вверху страницы.

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

Сетевая активность

Если установлен Брандмауэр Dr.Web, вам доступен отчет по сетевой активности.

Вы можете увидеть данные по активным приложениям, журналу приложений, журналу пакетного фильтра. Для этого выберите нужный объект в выпадающем списке.

Для каждого активного приложения в отчете отображается:

- направление передачи данных;
- протокол работы;
- локальный адрес;
- удаленный адрес;
- размер отправленного пакета данных;
- размер полученного пакета данных.



В журнале приложений вы увидите:

- время начала работы приложения;
- имя приложения;
- имя правила обработки приложения;
- направление передачи данных;
- действие;
- целевой адрес.

В журнале пакетного фильтра отображаются следующие данные:

- время начала обработки пакета данных;
- направление передачи пакета данных;
- имя правила обработки;
- интерфейс;
- содержимое пакета.

С помощью кнопки  вы можете экспортировать записи журналов или очистить журналы от записей.

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.



13. Сообщения сервера

У администратора сети есть возможность настроить отправку серверных сообщений на любую из станций. Эта функция удобна при работе администратора сети на одной из станций для получения оповещений с сервера.

Все полученные сообщения выводятся списком в верхней части окна. Чтобы посмотреть в списке только те сообщения, которые соответствуют определенным параметрам, воспользуйтесь фильтрами. Имеются предустановленные фильтры, которые доступны в выпадающем списке.

Вы можете создавать собственные фильтры сообщений. Чтобы создать новый фильтр, нажмите кнопку  и выберите пункт **Создать** в выпадающем списке. В открывшемся окне укажите необходимые критерии фильтрации.

Фильтровать сообщения можно по следующим категориям:

- Станции;
- Репозитории;
- Лицензии;
- Администраторы;
- Другое.

Созданные пользователем фильтры можно изменить или удалить.

С помощью кнопки  вы можете удалить, скопировать, экспортировать выделенные сообщения, а также удалить все сообщения.



14. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу <https://download.drweb.com/doc/>;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу <https://forum.drweb.com/>.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела <https://support.drweb.com/>;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу <https://company.drweb.com/contacts/offices/>.



15. Приложение А. Дополнительные параметры командной строки

Параметры командной строки используются для задания параметров программам, которые могут быть запущены путем открытия на выполнение исполняемого файла. Это относится к Сканеру Dr.Web и Консольному сканеру. 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.

15.1. Параметры для Сканера и Консольного Сканера

Ключ	Описание
/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.



Ключ	Описание
/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, /TV), то будет запущена выборочная проверка указанных объектов. (Только для 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, /TV), 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, /TV), 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



Ключ	Описание
	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/удаленных 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.



Ключ	Описание
/OK	Выводить полный список проверяемых объектов, сопровождая незараженные пометкой Ok. По умолчанию опция отключена
/P: <приоритет>	Приоритет запущенной задачи проверки в общей очереди задач на проверку: O — низший. L — низкий. N — обычный. Приоритет по умолчанию. H — высокий. M — максимальный.
/PAL: <уровень_вложенности>	Максимальный уровень вложенности упаковщиков исполняемого файла. Если уровень вложенности превышает указанный, проверка будет производиться только до указанного уровня вложенности. По умолчанию — 1000.
/QL	Вывести список всех файлов, помещенных в карантин на всех дисках. (Только для Консольного Сканера).
/QL: <имя_логического_диска>	Вывести список всех файлов, помещенных в карантин на указанном логическом диске. (Только для Консольного Сканера).
/QNA	выводить пути в двойных кавычках.
/QR[:[d]][:p]]	Удалить файлы с указанного диска <d> (имя_логического_диска), находящие в карантине дольше <p> (количество) дней. Если <d> и <p> не указаны, то будут удалены все файлы, находящиеся в карантине, со всех логических дисков. (Только для Консольного Сканера).
/QUIT	Закрыть Сканер после проверки (вне зависимости от того, были ли применены действия к обнаруженным угрозам). (Только для Сканера).
/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.



Ключ	Описание
/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, np, 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.



Ключ	Описание
/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)):

Действие	Описание
/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)



Действие	Описание
/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.

15.2. Параметры для инсталляционных пакетов

/compression <режим> — режим сжатия трафика с сервером централизованной защиты. Параметр <режим> может принимать следующие значения:

- yes — использовать сжатие.
- no — не использовать сжатие.
- possible — сжатие возможно. Окончательное решение принимается в зависимости от настроек на стороне сервера.

Если ключ не задан, по умолчанию используется значение possible.

/encryption <режим> — режим шифрования трафика с сервером централизованной защиты. Параметр <режим> может принимать следующие значения:



- `yes` — использовать шифрование.
- `no` — не использовать шифрование.
- `possible` — шифрование возможно. Окончательное решение принимается в зависимости от настроек на стороне сервера.

Если ключ не задан, по умолчанию используется значение `possible`.

`/excludeFeatures <компоненты>` — список компонентов, которые будут исключены при установке. При задании нескольких компонентов используйте знак `,` в качестве разделителя. Доступные компоненты:

- `scanner` — Сканер Dr.Web,
- `spider-mail` — SplDer Mail,
- `spider-g3` — SplDer Guard,
- `outlook-plugin` — Dr.Web для Microsoft Outlook,
- `firewall` — Брандмауэр Dr.Web,
- `spider-gate` — SplDer Gate,
- `parental-control` — Офисный контроль,
- `antispam-outlook` — Антиспам Dr.Web для компонента Dr.Web для Microsoft Outlook,
- `antispam-spidermail` — Антиспам Dr.Web для компонента SplDer Mail.

Для компонентов, не указанных напрямую, сохраняется статус установки, заданный для них по умолчанию.

`/id <идентификатор_станции>` — идентификатор станции, на которую устанавливается Агент Dr.Web.

Задается вместе с паролем (ключ `/pwd`) для ручной авторизации на сервере. Если параметры авторизации не заданы, решение об авторизации принимается на стороне сервера.

`/includeFeatures <компоненты>` — список компонентов, которые необходимо установить. При задании нескольких компонентов используйте знак `,` в качестве разделителя. Доступные компоненты:

- `scanner` — Сканер Dr.Web,
- `spider-mail` — SplDer Mail,
- `spider-g3` — SplDer Guard,
- `outlook-plugin` — Dr.Web для Microsoft Outlook,
- `firewall` — Брандмауэр Dr.Web,
- `spider-gate` — SplDer Gate,
- `parental-control` — Офисный контроль,
- `antispam-outlook` — Антиспам Dr.Web для компонента Dr.Web для Microsoft Outlook,
- `antispam-spidermail` — Антиспам Dr.Web для компонента SplDer Mail.



Для компонентов, не указанных напрямую, сохраняется статус установки, заданный для них по умолчанию.

`/installdir <папка>` — папка установки.

Если ключ не задан, по умолчанию установка осуществляется в каталог Program Files\DrWeb на системном диске.

`/instMode <режим>` — режим запуска инсталлятора. Параметр `<режим>` может принимать следующее значение:

- `remove` — удалить установленный продукт.

Если ключ не задан, по умолчанию инсталлятор автоматически определяет режим запуска.

`/lang <код_языка>` — язык инсталлятора и устанавливаемого продукта. Задается в формате ISO-639-1 для кода языка.

Если ключ не задан, по умолчанию используется системный язык.

`/pubkey <путь>` — полный путь к файлу сертификата или открытого ключа сервера.

Если сертификат или открытый ключ не задан, по умолчанию при запуске локальной установки инсталлятор автоматически подхватывает сертификат (с расширением `.pem`) или открытый ключ (`drwcsd.pub`) из папки своего запуска. В случае размещения сертификата или открытого ключа в папке, отличной от папки инсталлятора, необходимо вручную задать полный путь до сертификата или открытого ключа.

При запуске инсталляционного пакета, созданного в Центре Управления, сертификат или открытый ключ входит в состав инсталляционного пакета, и дополнительное указание не требуется.

`/pwd <пароль>` — пароль Агента Dr.Web для доступа к серверу.

Задается вместе с идентификатором станции (ключ `/id`) для ручной авторизации на сервер. Если параметры авторизации не заданы, решение об авторизации принимается на стороне сервера.

`/regagent <режим>` — определяет, будет ли зарегистрирован Агент Dr.Web в списке установленных программ. Параметр `<режим>` может принимать следующие значения:

- `yes` — зарегистрировать Агент Dr.Web в списке установленных программ.
- `no` — не регистрировать Агент Dr.Web в списке установленных программ.

Если ключ не задан, по умолчанию используется значение `no`.

`/retry <количество>` — количество попыток поиска сервера посредством отправки multicast-запросов. При отсутствии ответа от сервера по истечении заданного количества попыток, считается, что сервер не найден.



Если ключ не задан, по умолчанию осуществляется 3 попытки поиска сервера.

`/server [<протокол>]/<адрес_сервера>[:<порт>]` — адрес сервера, с которого будет осуществляться установка Агента Dr.Web и к которому после установки подключится Агент Dr.Web.

Если ключ не задан, по умолчанию осуществляется поиск сервера посредством отправки multicast-запросов.

`/silent <режим>` — определяет, будет ли инсталлятор запущен в фоновом режиме.

Параметр `<режим>` может принимать следующие значения:

- `yes` — запускать инсталлятор в фоновом режиме.
- `no` — запускать инсталлятор в графическом режиме.

Если ключ не задан, по умолчанию установка Агента Dr.Web осуществляется в графическом режиме.

`/timeout <время>` — предельное время ожидания каждого ответа при поиске сервера.

Задается в секундах. Прием ответных сообщений продолжается, пока время ожидания ответа не превышает значение тайм-аута.

Если ключ не задан, по умолчанию используется значение 3 секунды.

15.3. 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.
32	В архиве, контейнере или почтовом ящике обнаружены подозрительные на вирус объекты.
64	Успешно выполнено лечение хотя бы одного зараженного вирусом объекта.



Код возврата	Событие
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.



16. 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».

16.1. 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 пишутся 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».



16.2. 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.



17. 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 <https://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;
- HLLQ — 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 дозвола (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.

