Dr.WEB

Антивирус для Windows

Руководство пользователя

Антивирус Dr.Web для Windows
Версия 12.0
Руководство пользователя
12.01.2022

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, 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

Настоящее руководство содержит подробное описание установки продукта Антивирус для Windows, а также рекомендации по его использованию и решению типичных проблем, связанных с вирусными угрозами. В основном рассматриваются стандартные режимы работы компонентов программы Dr.Web (с настройками по умолчанию).

В Приложениях содержится общая справочная информация, а также дополнительные параметры для настройки программы Dr.Web, предназначенные для опытных пользователей.

1.1. Используемые обозначения и сокращения

Условные обозначения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	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.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

- Dr.Web — Антивирус для Windows;
- FTP — (от англ. File Transfer Protocol) протокол передачи файлов;
- HTTP — (от англ. Hypertext Transfer Protocol) протокол передачи гипертекста;

- IMAP — (от англ. Internet Message Access Protocol) протокол прикладного уровня для доступа к электронной почте;
- IMAPS — (от англ. Internet Message Access Protocol Secure) защищенный протокол прикладного уровня для доступа к электронной почте;
- MTU — (от англ. Maximum Transmission Unit) максимальный размер полезного блока данных;
- NNTP — (от англ. Network News Transfer Protocol) сетевой протокол передачи новостей;
- POP3 — (от англ. Post Office Protocol Version 3) протокол почтового отделения, версия 3;
- POP3S — (от англ. Post Office Protocol Version 3 Secure) защищенный протокол почтового отделения, версия 3;
- SIP — (от англ. Session Initiation Protocol) протокол установления сеанса;
- SMTPS — (от англ. Simple Mail Transfer Protocol Secure) простой защищенный протокол передачи почты;
- SSL — (от англ. Secure Sockets Layer) уровень защищенных сокетов;
- TCP — (от англ. Transmission Control Protocol) протокол управления передачей;
- TLS — (от англ. Transport Layer Security) протокол защиты транспортного уровня;
- UAC — (от англ. User Account Control) контроль учетных записей пользователей;
- UNC — (от англ. Uniform Naming Convention) унифицированное соглашение о названиях;
- URL — (от англ. Uniform Resource Locator) унифицированный локатор ресурса;
- ОС — операционная система;
- ПО — программное обеспечение.

2. О продукте

Антивирус для Windows предназначен для защиты системной памяти, жестких дисков и съемных носителей компьютеров, работающих под управлением ОС семейства Windows, от угроз любого типа: вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и других вредоносных объектов из любых внешних источников.

Антивирус для Windows состоит из нескольких модулей, отвечающих за различную функциональность. Антивирусное ядро и вирусные базы являются общими для всех компонентов и 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.

Антивирус 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 совершения действий над содержащими их файлами применяются стандартные средства антивирусных компонентов Dr.Web.

Информацию о версии продукта, составе компонентов, дате последнего обновления вы можете найти на странице **Поддержка** в разделе О программе.

2.1. Компоненты защиты и модули управления

Антивирус для Windows включает в состав следующие компоненты защиты и модули управления:

Компонент/модуль	Описание
SpIDer Guard	Компонент, который постоянно находится в оперативной памяти. Осуществляет проверку создаваемых файлов и запускаемых процессов, а также обнаруживает проявления вирусной активности.
SpIDer Mail	Компонент, 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.

Компонент/модуль	Описание
Брандмауэр Dr.Web	Персональный межсетевой экран, предназначенный для защиты компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети.
Поведенческий анализ	Компонент, контролирующий доступ приложений к критически важным объектам системы и обеспечивающий целостность запущенных приложений.
Защита от эксплойтов	Компонент, блокирующий вредоносные объекты, которые используют уязвимости в приложениях.
Защита от вымогателей	Компонент, обеспечивающий защиту от вирусов-шифровальщиков.
Сканер	Сканер с графическим интерфейсом, который запускается по запросу пользователя или по расписанию и производит антивирусную проверку компьютера.
Консольный сканер Dr.Web	Версия Сканера с интерфейсом командной строки.
Dr.Web для Microsoft Outlook	Подключаемый модуль, который проверяет почтовые ящики Microsoft Outlook на наличие угроз.
Модуль обновления	Позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов Dr.Web, а также производит их автоматическую установку.
SpIDer Agent	Модуль, с помощью которого осуществляется настройка и управление работой компонентов продукта.

2.2. 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 «gpcode»). Кроме того, использование технологии Origins Tracing позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing, добавляется постфикс `.Origin`.

Эмуляция исполнения

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

Эвристический анализ

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

Эвристический анализатор также использует технологию FLY-CODE — универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические

предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке упакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

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

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, сверяясь с постоянно обновляемым облачным сервисом Dr.Web, 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. К названиям угроз, обнаруженных при помощи Dr.Web Process Heuristic, добавляется префикс `DPH`.

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. К названиям угроз, обнаруженных при помощи Dr.Web Process Dumper, добавляется префикс `DPD`.

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. К названиям угроз, обнаруженных при помощи Dr.Web ShellGuard, добавляется префикс `DPH:Trojan.Exploit`.

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

- интернет-браузеры (Internet Explorer, Mozilla Firefox, Google Chrome и др.);
- приложения MS Office;
- системные приложения;
- приложения, использующие java-, flash- и pdf-технологии;

- медиапроигрыватели.

Анализируя потенциально опасные действия, система защиты благодаря технологии Dr.Web ShellGuard опирается не только на прописанные правила, хранящиеся на компьютере, но и на знания облачного сервиса Dr.Web, в котором собираются:

- данные об алгоритмах программ с вредоносными намерениями;
- информация о заведомо чистых файлах;
- информация о скомпрометированных цифровых подписях известных разработчиков программного обеспечения;
- информация о цифровых подписях рекламных или потенциально опасных программ;
- информация о нежелательных для посещения сайтах;
- алгоритмы защиты тех или иных приложений.

Защита от инжектов

Инжект — способ внедрения вредоносного кода в запущенные на устройстве процессы. Dr.Web постоянно отслеживает поведение всех процессов в системе и предотвращает попытки внедрения, если посчитает их вредоносными. К названиям угроз, обнаруженных при помощи Защиты от инжектов, добавляется префикс `DPH:Trojan.Inject`.

Dr.Web проверяет следующие характеристики приложения, которое запустило процесс:

- является ли приложение новым;
- как оно попало в систему;
- где приложение расположено;
- как оно называется;
- входит ли приложение в список доверенных;
- есть ли у него действительная цифровая подпись от доверенного центра сертификации;
- входит ли оно в черный или белый список приложений, которые находятся на облачном сервисе Dr.Web.

Dr.Web отслеживает состояние запущенного процесса: проверяет, создаются ли удаленные потоки в пространстве процесса, внедряется ли посторонний код в активный процесс.

Антивирус контролирует изменения, которые вносят приложения, запрещает изменять системные и привилегированные процессы. Отдельно Dr.Web следит за тем, чтобы вредоносный код не мог модифицировать память популярных браузеров, например когда вы совершаете покупки в интернете или делаете переводы в онлайн-банках.

Защита от вымогателей

Защита от вымогателей — один из компонентов Превентивной защиты, обеспечивающий защиту файлов пользователей от троянцев-шифровальщиков. Данные вредоносные программы, попадая на компьютер пользователя, блокируют доступ к данным путем шифрования, после чего вымогают деньги за расшифровку. К названиям угроз, обнаруженных при помощи Защиты от вымогателей, добавляется префикс `DPH:Trojan.Encoder`.

Компонент анализирует поведение подозрительного процесса, обращая внимание в частности на поиск файлов, чтение и попытки их модификации.

Также проверяются следующие характеристики приложения:

- является ли приложение новым;
- как оно попало в систему;
- где приложение расположено;
- как оно называется;
- является ли приложение доверенным;
- есть ли у него действительная цифровая подпись от доверенного центра сертификации;
- входит ли оно в черный или белый список приложений, хранящийся на облачном сервисе Dr.Web.

Также проверяется характер модификации файла. При обнаружении признаков поведения вредоносной программы действия приложения блокируются и предотвращаются попытки модификации файлов.

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. Благодаря подключению к облачному сервису обработка больших объемов данных происходит быстрее, а постоянное обучение системы обеспечивает превентивную защиту от новейших угроз. При этом технология может функционировать и без постоянного обращения к облаку.

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.

Облачные технологии обнаружения угроз

Облачные методы обнаружения позволяют проверить любой объект (файл, приложение, расширение для браузера и т. п.) по хеш-сумме. Она представляет собой уникальную последовательность цифр и букв заданной длины. При анализе по хеш-сумме объекты проверяются по существующей базе и затем классифицируются на категории: чистые, подозрительные, вредоносные и т. д. К названиям угроз, обнаруженных при помощи Облачных технологий, добавляется префикс `CLOUD`.

Подобная технология оптимизирует время проверки файлов и экономит ресурсы устройства. Благодаря тому, что анализируется не сам объект, а его уникальная хеш-сумма, решение выносится практически моментально. При отсутствии подключения к серверам Dr.Web файлы проверяются локально, а облачная проверка возобновляется при восстановлении связи.

Таким образом, облачный сервис компании «Доктор Веб» собирает информацию от многочисленных пользователей и оперативно обновляет данные о ранее неизвестных угрозах, тем самым повышая эффективность защиты устройств.

2.3. Системные требования

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

Параметр	**Требование**
Процессор	С поддержкой 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 с пакетом обновлений SP1 или более поздними; • Windows 8; • Windows 8.1; • Windows 10 21H2 или более ранняя. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7 с пакетом обновлений SP1 или более поздними;

Параметр	Требование
	• Windows 8; • Windows 8.1; • Windows 10 21H2 или более ранняя; • Windows 11
Свободная оперативная память	512 МБ и больше
Разрешение экрана	Рекомендуется не менее 1024x768
Поддержка виртуальных и облачных сред	Поддерживается функционирование программы в следующих средах: • VMware; • Hyper-V; • Xen; • KVM
Прочее	Для подключаемого модуля Dr.Web для Microsoft 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; • Outlook 2019; • Outlook 2021

Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой программы Антивирус для Windows на Windows Vista или Windows 7 необходимо убедиться, что система поддерживает алгоритм хеширования SHA-256. Для этого установите все рекомендуемые обновления из Центра обновления Windows. Подробную информацию о необходимых пакетах обновлений вы можете найти на официальном сайте компании «Доктор Веб».

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

Назначение	Направление	Номера портов
Для активации и продления лицензии	исходящий	443
Для обновления (если включена опция обновления по https)	исходящий	443

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

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

Проверка с помощью файла CloudCar

Для проверки работы облачного сервиса Dr.Web Cloud используйте тестовый файл CloudCar, созданный организацией AMTSO (Anti-Malware Testing Standards Organization). Этот файл специально создан для проверки работы облачных сервисов антивирусов и не является вредоносным.

Проверка работы Dr.Web Cloud

1. Убедитесь, что у вас включено использование облачного сервиса Dr.Web Cloud.
2. Загрузите тестовый файл. Для этого перейдите по адресу https://www.amtso.org/feature-settings-check-cloud-lookups/ и нажмите **Launch the Test**.
3. Если у вас установлен и включен компонент SpIDer Guard, при попадании файла на компьютер он автоматически будет перемещен в карантин. Если компонент SpIDer Guard не установлен или отключен, просканируйте загруженный файл. Для этого вызовите контекстное меню нажатием правой кнопки мыши по имени файла и выберите пункт **Проверить с Dr.Web**.
4. Проверьте, что тестовый файл обработан Dr.Web как `CLOUD:AMTSO.Test.Virus`. Префикс `CLOUD` в названии угрозы будет свидетельствовать о корректной работе Dr.Web Cloud.

3. Установка, изменение и удаление программы

Перед началом установки Антивирус для Windows ознакомьтесь с системными требованиями. Также рекомендуется выполнить следующие действия:

- установить все критические обновления, выпущенные компанией Microsoft для вашей версии операционной системы (подробнее об обновлении ОС Windows); если поддержка операционной системы производителем прекращена, рекомендуется перейти на более современную версию операционной системы;
- проверить при помощи системных средств файловую систему и устранить обнаруженные проблемы;
- удалить с компьютера другие антивирусные программы для предотвращения возможной несовместимости их компонентов с компонентами Dr.Web;
- если будет установлен Брандмауэр Dr.Web, необходимо удалить с компьютера другие межсетевые экраны;
- закрыть активные приложения.

> Установка Dr.Web должна выполняться пользователем с правами администратора данного компьютера.
>
> Dr.Web несовместим с продуктами проактивной защиты других производителей.

Установка Dr.Web возможна в одном из следующих режимов:

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

3.1. Установка программы

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

Установка в режиме мастера установки

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

- если у вас имеется установочный файл (`drweb-12.0-av-win.exe`), запустите его;
- если у вас имеется фирменный диск с установочным комплектом, вставьте диск в привод. Если для привода включен режим автозапуска диска, процедура установки запустится автоматически. Если режим автозапуска отключен, запустите на

выполнение файл `autorun.exe`, расположенный на диске. Откроется окно, содержащее меню автозапуска. Нажмите кнопку **Установить**.

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

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

Чтобы установить программу

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

   

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

2. На первом шаге установки вы можете подключиться к облачным сервисам Dr.Web, которые позволят осуществлять проверку данных, используя наиболее свежую информацию об угрозах, которая обновляется на серверах компании «Доктор Веб» в режиме реального времени. Опция включена по умолчанию. Также вы можете указать, требуется ли установка Брандмауэр Dr.Web.

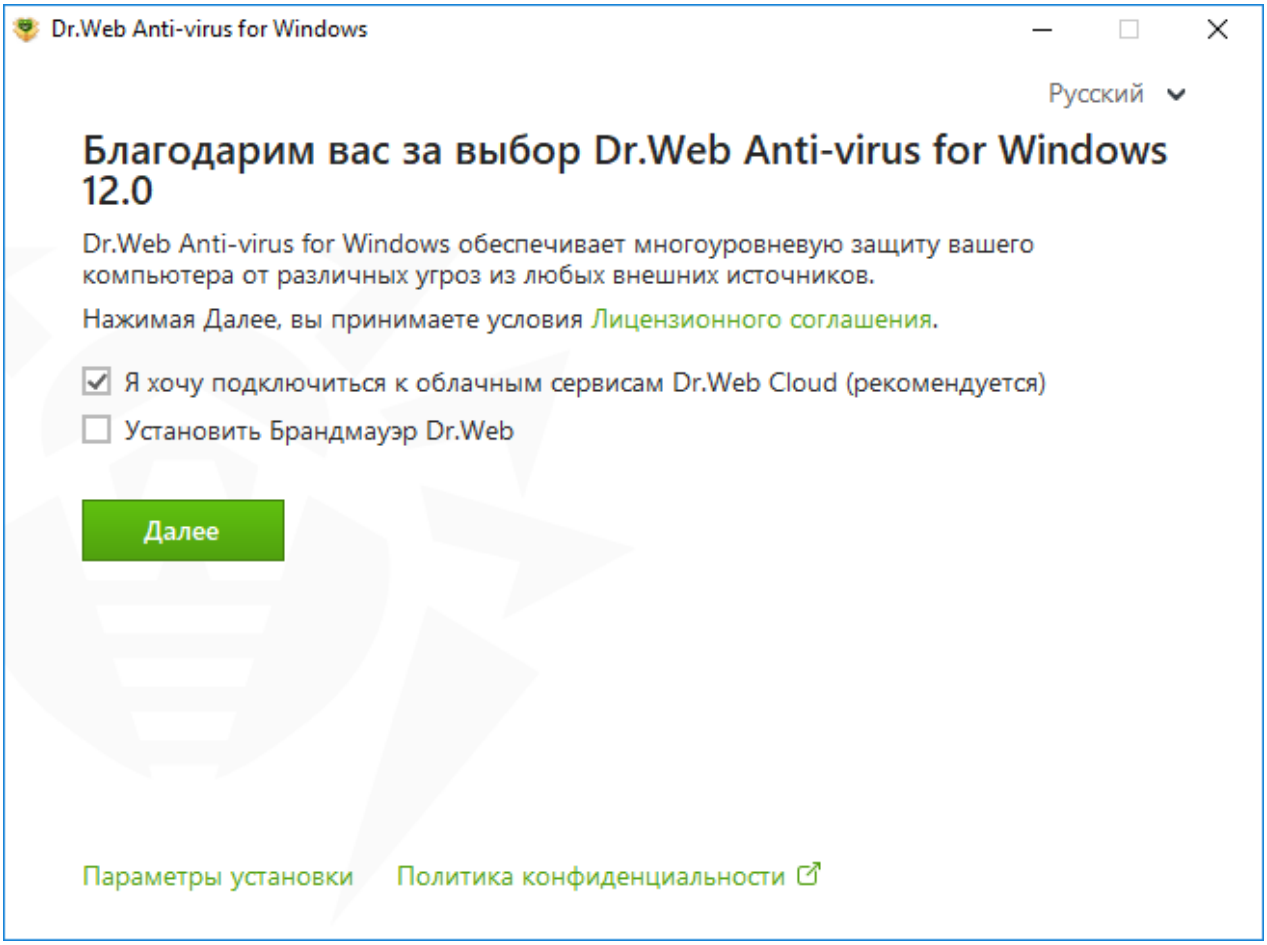

Рисунок 1. Мастер установки

3. Если вы хотите произвести установку с параметрами по умолчанию, перейдите к пункту 4. Чтобы выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры, нажмите ссылку **Параметры установки**.

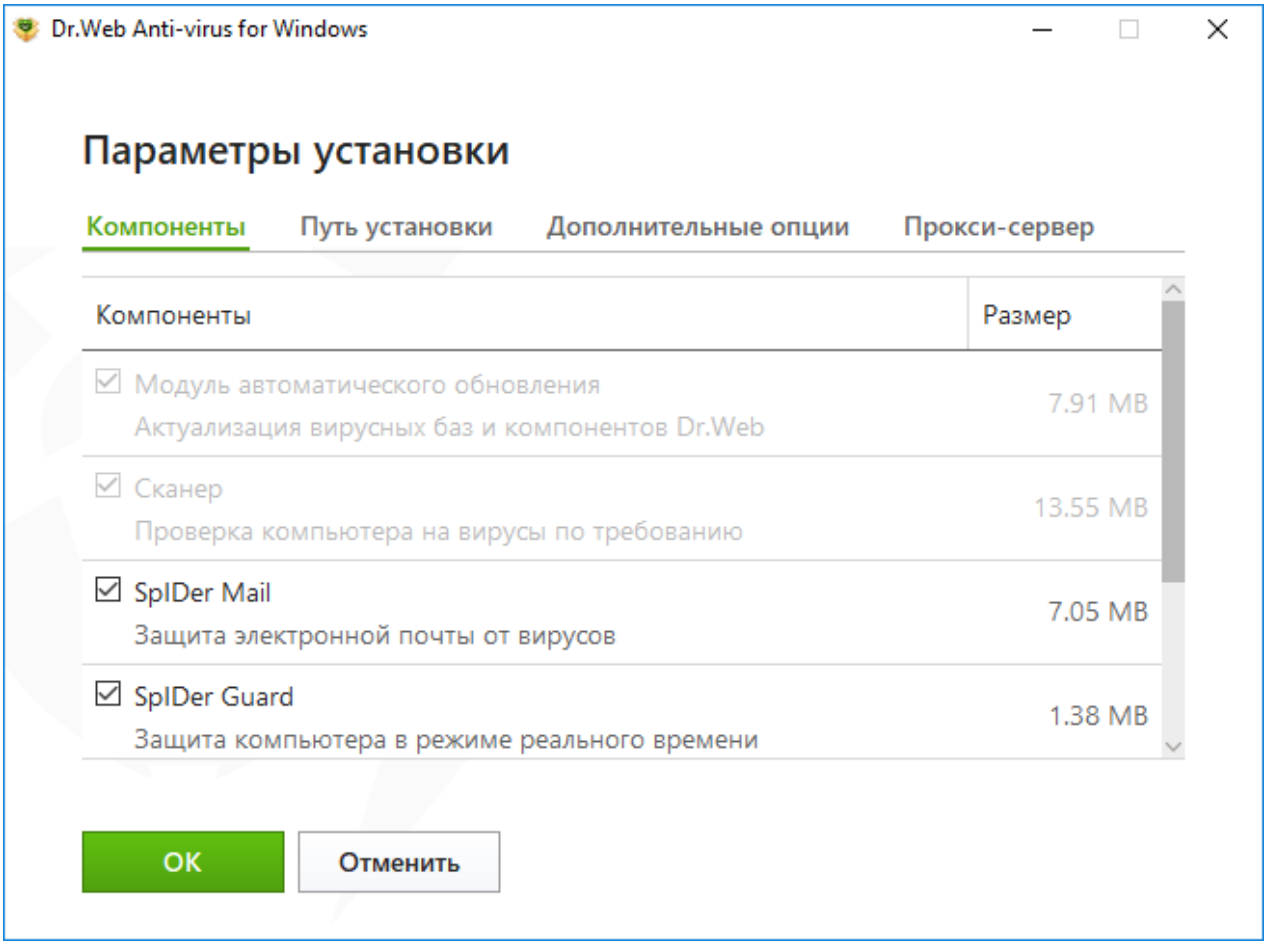

Рисунок 2. Параметры установки

Данная опция предназначена для опытных пользователей.

- На первой вкладке вы можете изменить состав устанавливаемых компонентов. Установите флажки напротив тех компонентов, которые вы хотите установить на ваш компьютер.
- На второй вкладке вы можете изменить путь установки. По умолчанию это папка DrWeb, расположенная в папке `Program Files` на системном диске. Для изменения пути установки нажмите кнопку **Обзор** и укажите необходимый путь.
- На третьей вкладке окна вы можете установить флажок **Загрузить обновления во время установки**, чтобы в процессе установки были загружены актуальные вирусные базы и другие модули антивируса. Вы можете установить флажок **Включить поддержку совместимости со средствами чтения с экрана**, чтобы использовать программы экранного доступа, такие как JAWS и NVDA, для озвучивания элементов интерфейса Dr.Web. Эта функция делает интерфейс программы доступным для людей с ограниченными возможностями. Также вам будет предложено настроить создание ярлыков для запуска программы Dr.Web.
- При необходимости укажите параметры прокси-сервера.

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

4. Нажмите кнопку **Далее**. Обратите внимание, что тем самым вы принимаете условия лицензионного соглашения.
5. В окне **Мастер регистрации** необходимо выбрать одну из следующих опций:
   - если у вас есть ключевой файл и он находится на жестком диске или съемном носителе, выберите **Указать путь к действующему ключевому файлу**. Нажмите кнопку **Обзор** и выберите нужный ключевой файл в открывшемся окне. Подробнее вы можете прочитать в инструкции Активация при помощи ключевого файла;
   - если у вас нет ключевого файла, но вы готовы его получить в процессе установки, выберите **Получить лицензию в процессе установки**. Подробнее вы можете прочитать в инструкции Активация при помощи серийного номера;
   - для продолжения установки без лицензии выберите **Получить лицензию позднее**. Обновления не будут загружаться до тех пор, пока вы не укажете или не получите ключевой файл.

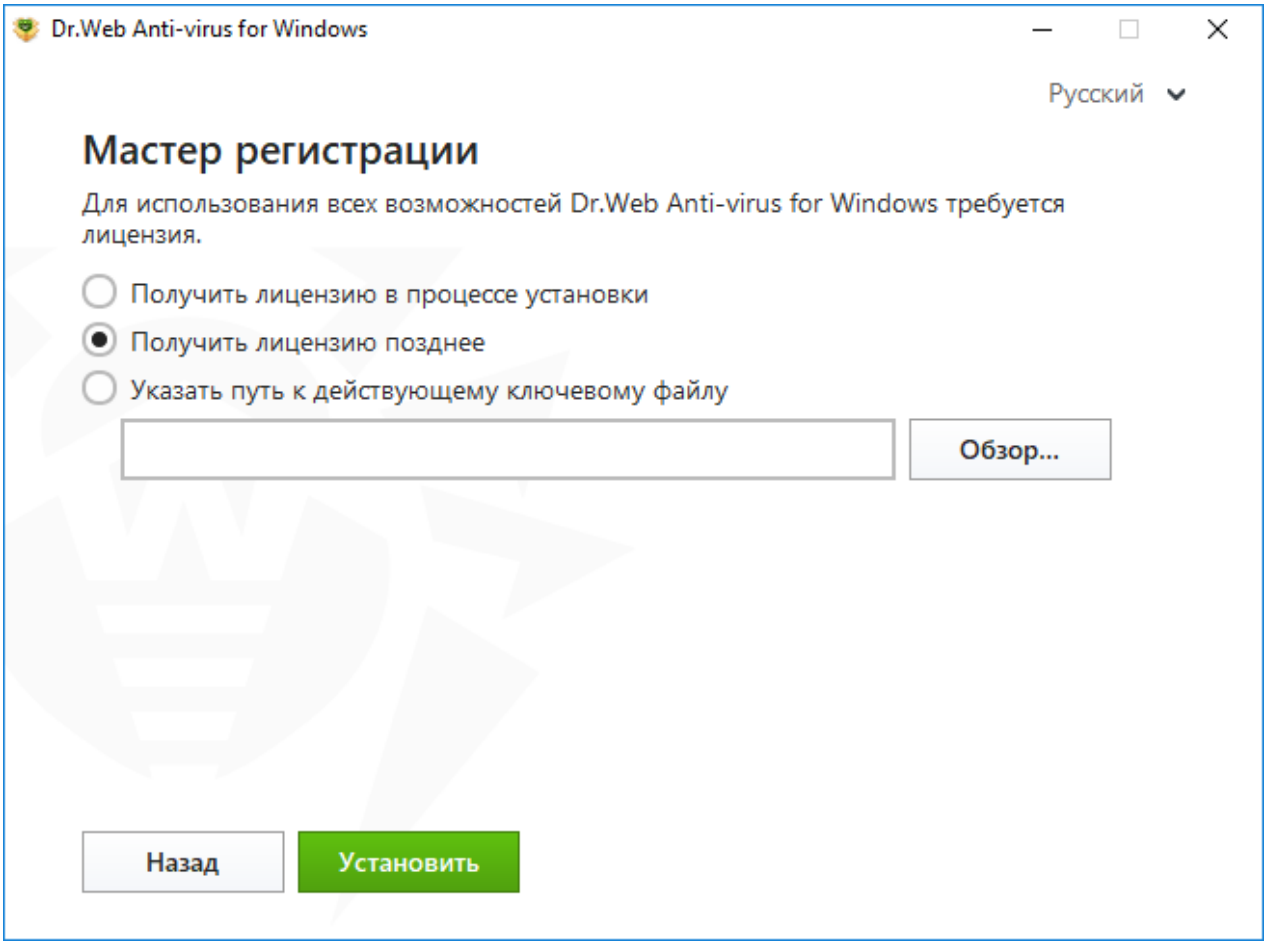

Рисунок 3. Мастер регистрации

Нажмите кнопку **Установить**.

6. Если в процессе установки вы указали или получили действующий ключевой файл и не снимали флажок **Загрузить обновления во время установки**, будет выполнен процесс обновления вирусных баз и других компонентов программы Dr.Web. Обновление проводится автоматически и не требует дополнительных действий.
7. Чтобы завершить установку, перезагрузите компьютер.

Установка в режиме командной строки

Для запуска установки Dr.Web в фоновом режиме введите в командной строке имя исполняемого файла с необходимыми параметрами:

Параметр	Значение
`installFirewall`	Будет установлен Брандмауэр Dr.Web.
`lang`	Язык продукта. Значение параметра — код языка в формате ISO 639-1, например, `/lang ru`.
`reboot`	Автоматическая перезагрузка компьютера после завершения установки. Может принимать значение `yes` или `no`.
`silent`	Установка в фоновом режиме. Может принимать значение `yes` или `no`.
`blockEmulateUserActions`	Включение опции **Запрещать эмуляцию действий пользователя** во время установки. Может принимать значение `yes` или `no`.
`allowUiAccessibility`	Включение опции совместимости со средствами чтения с экрана. Может принимать значение `yes` или `no`.
`importSettings`	Импорт настроек из файла (максимальный размер файла — 20 МБ). Необходимо указать путь к файлу.
`enableDebugLogs`	Ведение журнала отладки. Может принимать значение `yes` или `no`. Журнал ведется для компонентов SpIDer Guard, SpIDer Mail, SpIDer Gate и Сканер, Модуля обновлений и службы Dr.Web. Ведение журнала отключается при перезагрузке компьютера после завершения установки.

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

```
drweb-12.0-av-win.exe /silent yes /reboot yes
```

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 при помощи лечащей утилиты CureIt! от компании «Доктор Веб». Скачать утилиту вы можете на сайте: https://free.drweb.com/download+cureit+free/.
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).
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».

3.2. Изменение компонентов программы

Изменение компонентов программы осуществляется через Мастер удаления/изменения компонентов. Вы можете открыть Мастер удаления/изменения компонентов двумя способами:

- при наличии установочного файла запустите его;
- из Панели управления Windows:
  1. Выберите (в зависимости от операционной системы):

Операционная система	**Последовательность действий**			
Windows XP	Меню «Пуск»	**Пуск → Панель управления → Установка и удаление программ**		
	Классическое меню «Пуск»	**Пуск → Настройка → Панель управления → Установка и удаление программ**		
Windows Vista	Меню «Пуск»	**Пуск → Панель управления**	Классический вид	**Программы и компоненты**

Операционная система	Последовательность действий			
			Домашняя страница	**Программы** → **Программы и компоненты**
	Классическое меню «Пуск»	**Пуск** → **Настройка** → **Панель управления** → **Программы и компоненты**		
Windows 7	**Пуск** → **Панель управления**	Мелкие/крупные значки: **Программы и компоненты**		
		Категория: **Программы** → **Удаление программ**		
Windows 8, Windows 8.1, Windows 10, Windows 11	**Панель управления**	Мелкие/крупные значки: **Программы и компоненты**		
		Категория: **Программы** → **Удаление программ**		

2. В списке установленных программ выберите строку **Dr.Web Anti-virus for Windows**.
3. Нажмите кнопку **Изменить**.

Чтобы удалить или добавить компоненты

1. В окне Мастера удаления/изменения компонентов нажмите **Изменить компоненты**:

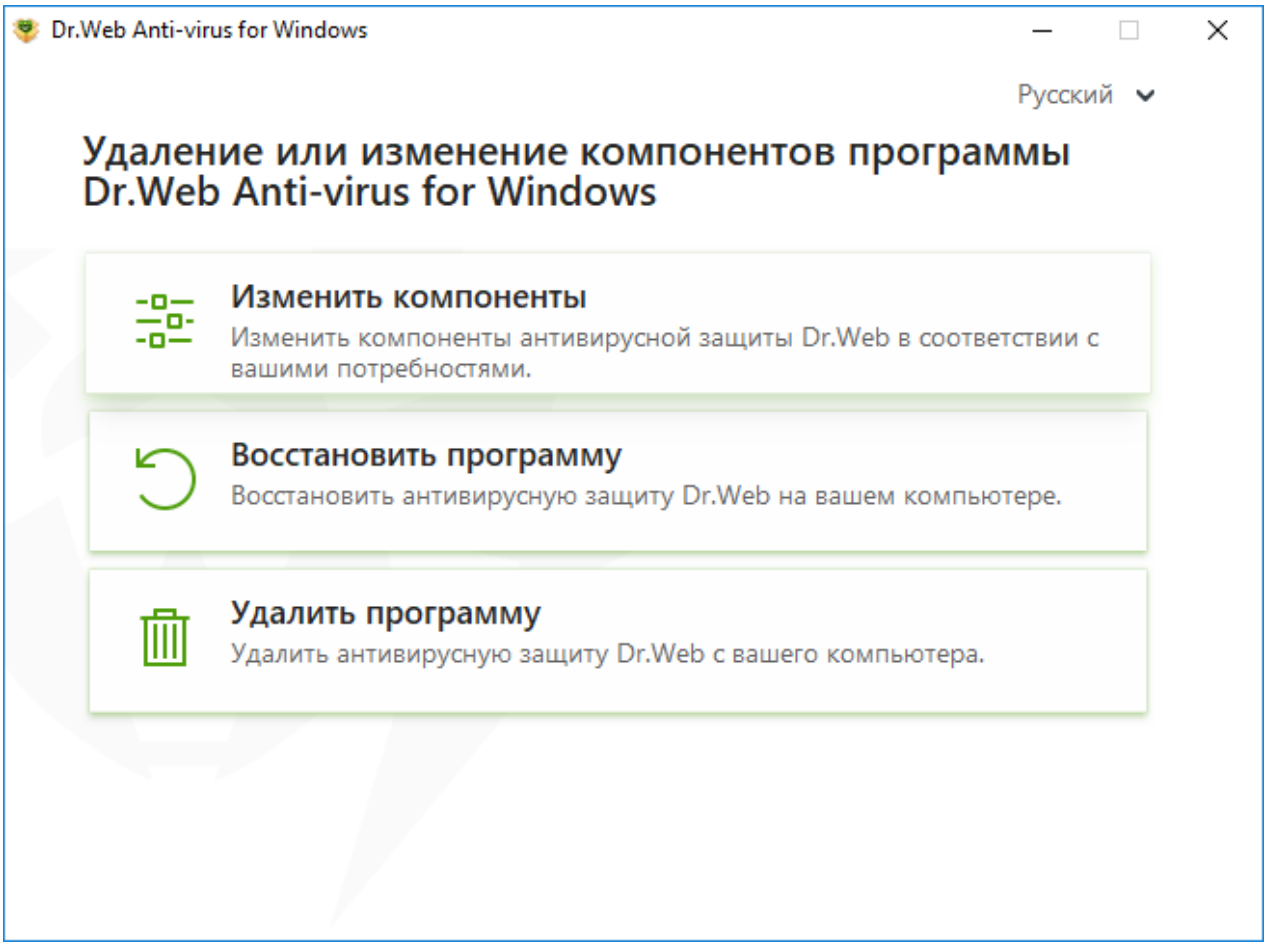

Рисунок 4. Мастер удаления/изменения компонентов

2. В открывшемся окне установите флажки напротив компонентов, которые хотите добавить, либо снимите флажки напротив удаляемых компонентов.
3. Нажмите **Применить**.
4. В открывшемся окне **Отключение Самозащиты** введите изображенный код подтверждения.
5. Нажмите кнопку **Применить**.

В окне Мастера удаления/изменения компонентов программы также доступны следующие опции:

- **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.

3.3. Удаление и переустановка программы

Удаление Dr.Web

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

При наличии установочного файла вы можете пропустить шаги 1–3. Запустите установочный файл и перейдите к шагу 4.

1. Для удаления программы Антивирус для Windows из Панели управления Windows выберите (в зависимости от операционной системы):

Операционная система	**Последовательность действий**			
Windows XP	Меню «Пуск»	**Пуск → Панель управления → Установка и удаление программ**		
	Классическое меню «Пуск»	**Пуск → Настройка → Панель управления → Установка и удаление программ**		
Windows Vista	Меню «Пуск»	**Пуск → Панель управления**	Классический вид	**Программы и компоненты**
			Домашняя страница	**Программы → Программы и компоненты**
	Классическое меню «Пуск»	**Пуск → Настройка → Панель управления → Программы и компоненты**		
Windows 7	**Пуск → Панель управления**	Мелкие/крупные значки:		

Операционная система	Последовательность действий			
		Программы и компоненты		
		Категория: **Программы** → **Удаление программ**		
Windows 8, Windows 8.1, Windows 10, Windows 11	**Панель управления**	Мелкие/крупные значки: **Программы и компоненты**		
		Категория: **Программы** → **Удаление программ**		

2. В открывшемся списке выберите строку с названием программы.
3. Нажмите кнопку **Удалить**.
4. В окне **Сохраняемые параметры** установите флажки напротив того, что следует сохранить после удаления программы. Сохраненные объекты и настройки могут использоваться программой при повторной установке. По умолчанию выбраны все опции — **Карантин**, **Настройки Dr.Web Anti-virus for Windows** и **Защищаемые копии файлов**. Нажмите кнопку **Далее**.
5. Откроется окно **Отключение Самозащиты**, в котором необходимо ввести изображенный код подтверждения, после чего нажать кнопку **Удалить программу**.
6. Изменения вступят в силу после перезагрузки компьютера. Процесс перезагрузки можно отложить, нажав кнопку **Перезагрузить позже**. Нажмите кнопку **Перезагрузить сейчас** для немедленного завершения процедуры удаления или изменения состава компонентов Dr.Web.

Переустановка Dr.Web

1. Загрузите актуальный дистрибутив программы с официального сайта компании «Доктор Веб». Для этого необходимо ввести действительный серийный номер в соответствующее поле.
2. Удалите продукт, как описано выше.
3. Перезагрузите компьютер.
4. Заново установите программу, используя загруженный дистрибутив (`drweb-12.0-av-win.exe`). На этапе установки введите действующий серийный номер или укажите путь к ключевому файлу.
5. Перезагрузите компьютер.

4. Лицензирование

Права пользователя на использование Dr.Web регулируются лицензией, приобретенной на сайте компании «Доктор Веб» или у партнеров. Лицензия позволяет полноценно использовать все возможности продукта на протяжении всего срока действия. Лицензия регулирует права пользователя, установленные в соответствии с Лицензионным соглашением, условия которого пользователь принимает во время установки программы.

Каждой лицензии сопоставлен уникальный *серийный номер*, а на локальном компьютере пользователя с лицензией связывается специальный файл, регулирующий работу Dr.Web в соответствии с параметрами лицензии. Этот файл называется лицензионным *ключевым файлом*. Подробнее о ключевом файле см. в разделе Ключевой файл.

Способы активации лицензии

Активировать коммерческую лицензию вы можете одним из следующих способов:

- во время установки продукта при помощи Мастера регистрации;
- в любой момент работы продукта при помощи Мастера регистрации, который входит в состав Менеджера лицензий;
- на официальном сайте компании «Доктор Веб» по адресу https://products.drweb.com/register/.

Активация лицензии в Мастере регистрации возможна при помощи серийного номера или ключевого файла. Пользователи Windows XP могут активировать лицензию только при помощи ключевого файла.

Подробнее об активации лицензии см. в разделе Как активировать лицензию.

Если у вас остались вопросы по лицензированию, ознакомьтесь со списком наиболее частых вопросов на сайте компании «Доктор Веб».

Возможные вопросы

Как я могу перенести лицензию на другой компьютер?

Вы можете перенести вашу коммерческую лицензию на другой компьютер при помощи ключевого файла или серийного номера. Если вы хотите перенести лицензию на компьютер, на котором используется Windows XP, вы можете это сделать только при помощи ключевого файла.

Чтобы перенести лицензию на другой компьютер

- при помощи серийного номера:
  1. Скопируйте серийный номер с компьютера, с которого вы хотите перенести лицензию.
  2. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
  3. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию. Для этого воспользуйтесь Мастером регистрации во время установки продукта или после установки во время работы продукта (см. Активация при помощи серийного номера).
- при помощи ключевого файла:
  1. Скопируйте ключевой файл с компьютера, с которого вы хотите перенести лицензию. По умолчанию ключевой файл хранится в папке установки Dr.Web и имеет расширение `.key`.
  2. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
  3. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию. Для этого воспользуйтесь Мастером регистрации во время установки продукта или после установки во время работы продукта (см. Активация при помощи ключевого файла).

Я забыл регистрационный email. Как я могу его восстановить?

Если вы забыли адрес электронной почты, который вы указывали во время регистрации, вам необходимо обратиться в службу технической поддержки компании «Доктор Веб» по адресу https://support.drweb.com.

Если вы сделаете запрос с адреса, отличающегося от того, на который зарегистрирована ваша лицензия, специалист технической поддержки может попросить предоставить: фото- или скан-копию лицензионного сертификата, чек об оплате лицензии, письмо интернет-магазина и другие подтверждающие документы.

Как я могу изменить регистрационный email?

Если вам необходимо изменить адрес электронной почты, который вы указывали при регистрации, воспользуйтесь специальным сервисом замены электронной почты по адресу https://products.drweb.com/register/change_email.

Почему в моем продукте отсутствует часть компонентов?

- При установке продукта были установлены не все входящие в лицензию компоненты.

  Чтобы включить недостающие компоненты

  1. Перейдите в раздел Панели управления Windows, посвященный установке и удалению программ.
  2. В списке установленных программ выберите строку с названием программы.
  3. Нажмите кнопку **Изменить**, при этом откроется окно Мастера удаления/изменения компонентов программы.
  4. Выберите опцию **Изменить компоненты**.
  5. Выберите из списка компонентов те компоненты, которые вы хотите включить, и нажмите кнопку **Применить**.

  Либо запустите установочный файл `drweb-12.0-av-win.exe` и в открывшемся окне выберите опцию **Изменить компоненты**. Перейдите к шагу 5.

- Установлен продукт, не соответствующий приобретенной лицензии.

  Чтобы установить другой продукт Dr.Web, соответствующий активированной лицензии

  1. Скачайте актуальную версию Dr.Web с официального сайта: https://download.drweb.com/.
  2. Укажите серийный номер продукта и регистрационный email, после чего нажмите **Скачать**.
  3. Выберите необходимую версию продукта, после чего загрузите пакет с дистрибутивом.
  4. Удалите установленный у вас продукт, руководствуясь инструкциями по удалению в разделе Удаление и переустановка программы.
  5. Установите скачанный продукт, используя скачанный дистрибутив.

4.1. Как активировать лицензию

Чтобы использовать все функции и компоненты программы, необходимо активировать лицензию. Активация лицензии возможна при помощи ключевого файла или серийного номера. Пользователи Windows XP могут активировать лицензию только при помощи ключевого файла.

Если ключевого файла нет, но есть серийный номер, его необходимо зарегистрировать на сайте компании «Доктор Веб». После завершения процесса регистрации вам будет

предоставлена ссылка для скачивания ключевого файла. Используйте этот ключевой файл для активации лицензии.

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

Активация при помощи серийного номера

Если у вас есть серийный номер, вы можете:

- активировать лицензию во время установки продукта при помощи Мастера регистрации:

1. Запустите установку продукта. На 5 шаге установки выберите пункт **Получить лицензию в процессе установки**. Нажмите **Установить**.

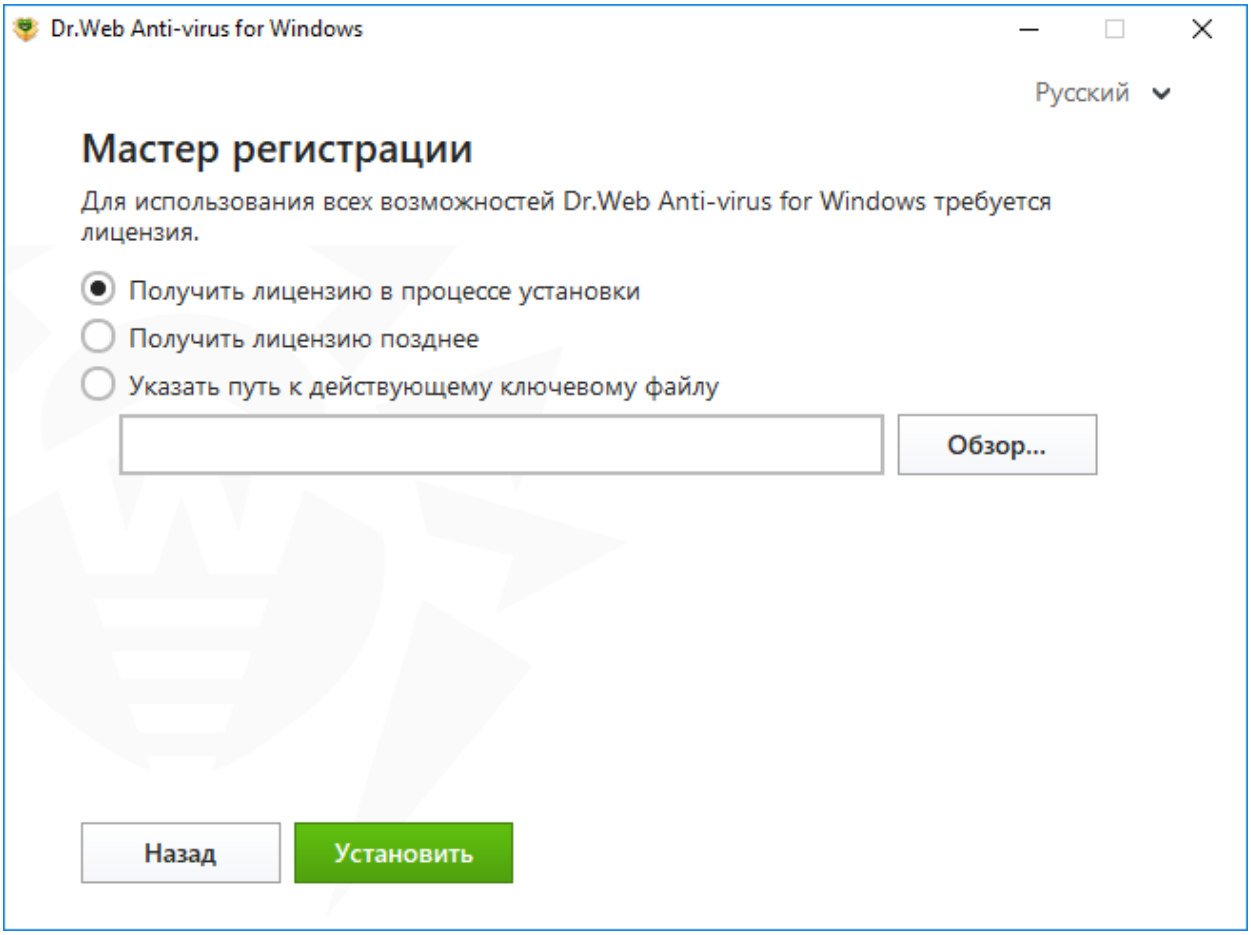

Рисунок 5. Установка. Мастер регистрации

2. Начнется установка продукта. В конце этапа Получение лицензии откроется окно Мастера регистрации. Введите серийный номер и нажмите **Активировать**. Если

серийный номер еще не был зарегистрирован, откроется окно, где вам необходимо указать свои регистрационные данные.

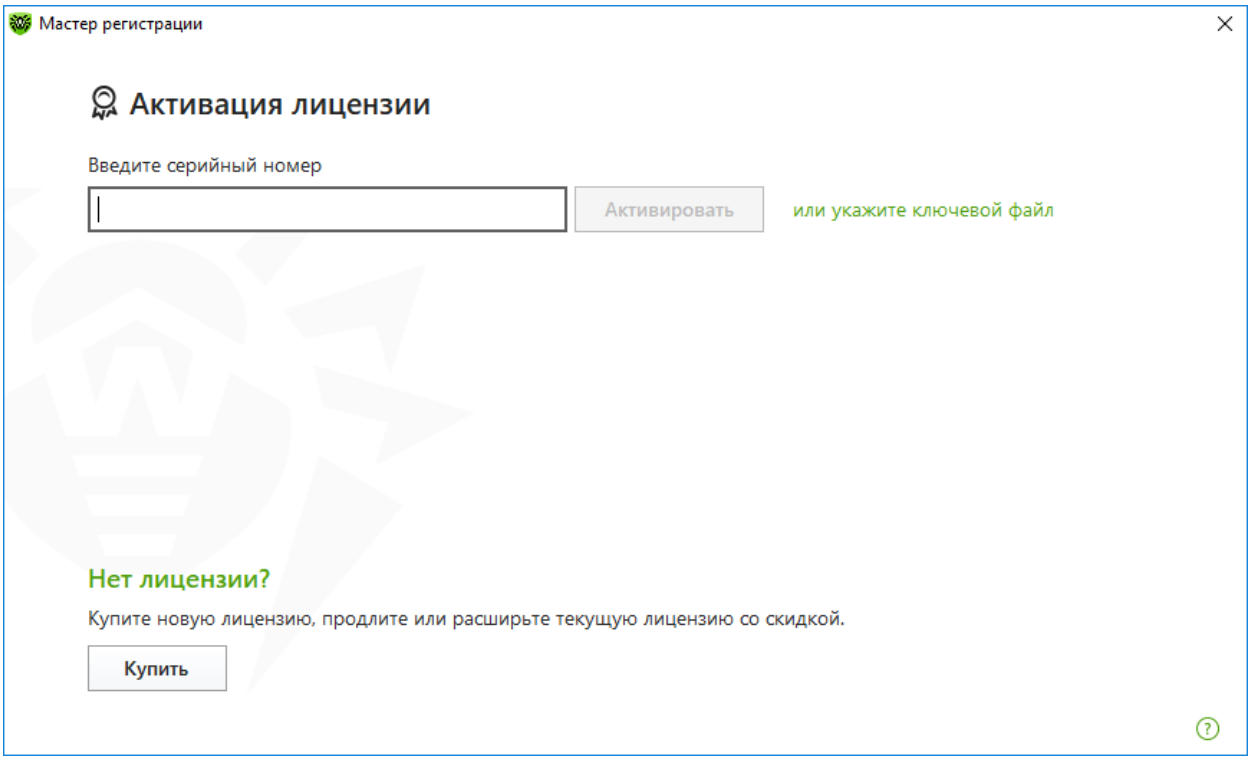

Рисунок 6. Мастер регистрации. Активация лицензии

3. Продолжите установку продукта, следуя инструкциям Мастера установки.

Если активация лицензии завершилась неудачно, выводится сообщение об ошибке. Проверьте подключение к интернету либо нажмите кнопку **Повторить** для исправления неверно введенных данных.

- активировать лицензию в любое время работы продукта при помощи Мастера регистрации, который входит в состав Менеджера лицензии:

1. В меню Dr.Web выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать или купить новую лицензию**.

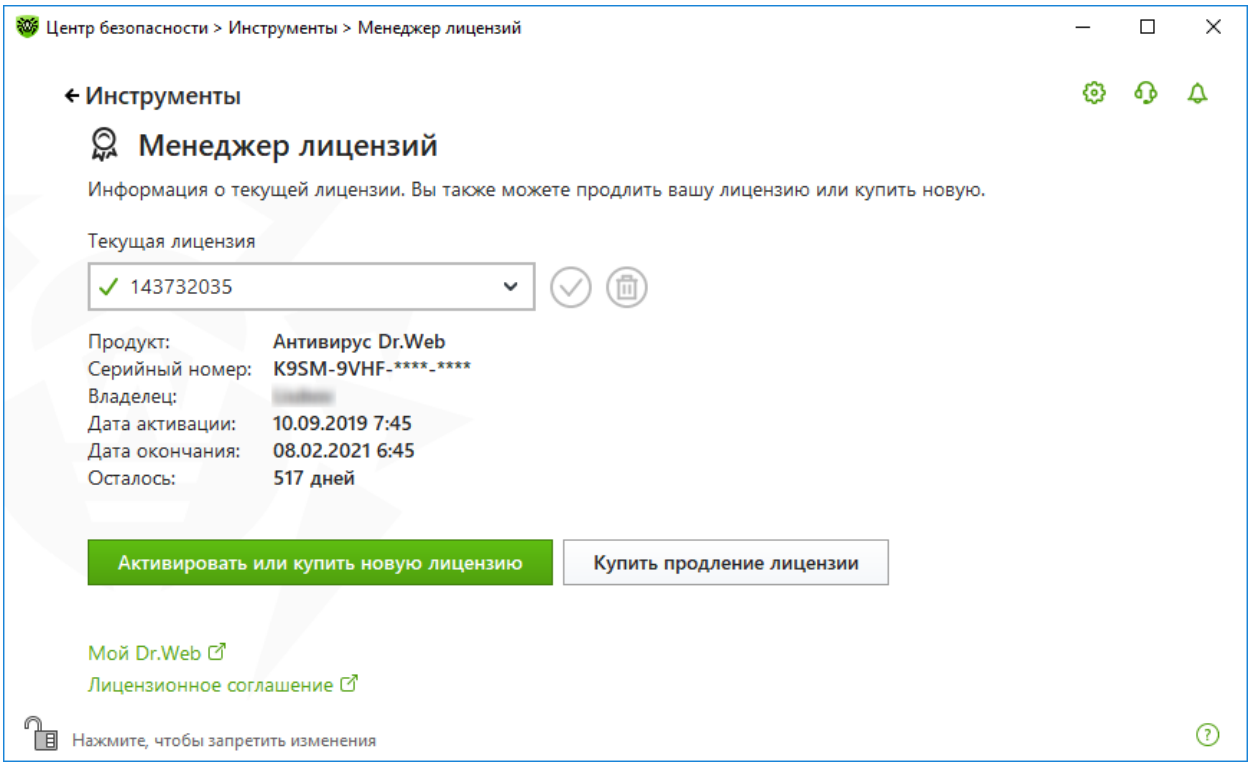

Рисунок 7. Менеджер лицензий

2. Откроется окно Мастера регистрации. Введите серийный номер и нажмите **Активировать**. Если серийный номер еще не был зарегистрирован, откроется окно, где вам необходимо указать свои регистрационные данные.

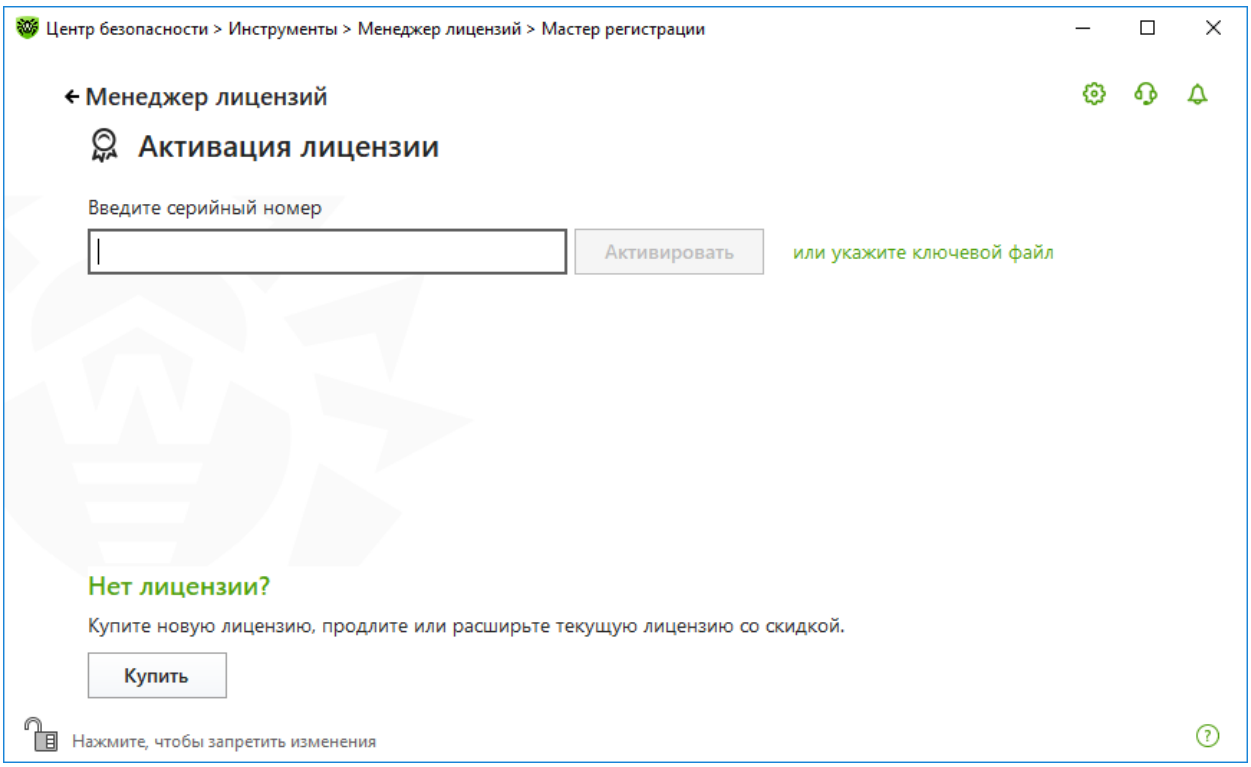

Рисунок 8. Мастер регистрации. Активация лицензии

Если активация лицензии завершилась неудачно, выводится сообщение об ошибке. Проверьте подключение к интернету либо нажмите кнопку **Повторить** для исправления неверно введенных данных.

- зарегистрировать серийный номер на сайте компании «Доктор Веб» и получить ключевой файл, с помощью которого вы сможете актировать лицензию.

Активация при помощи ключевого файла

Если у вас есть ключевой файл, вы можете активировать лицензию:

- во время установки продукта при помощи Мастера регистрации:

  1. Запустите установку продукта. На 5 шаге установки выберите пункт **Указать путь к действующему ключевому файлу**. Нажмите **Установить**.

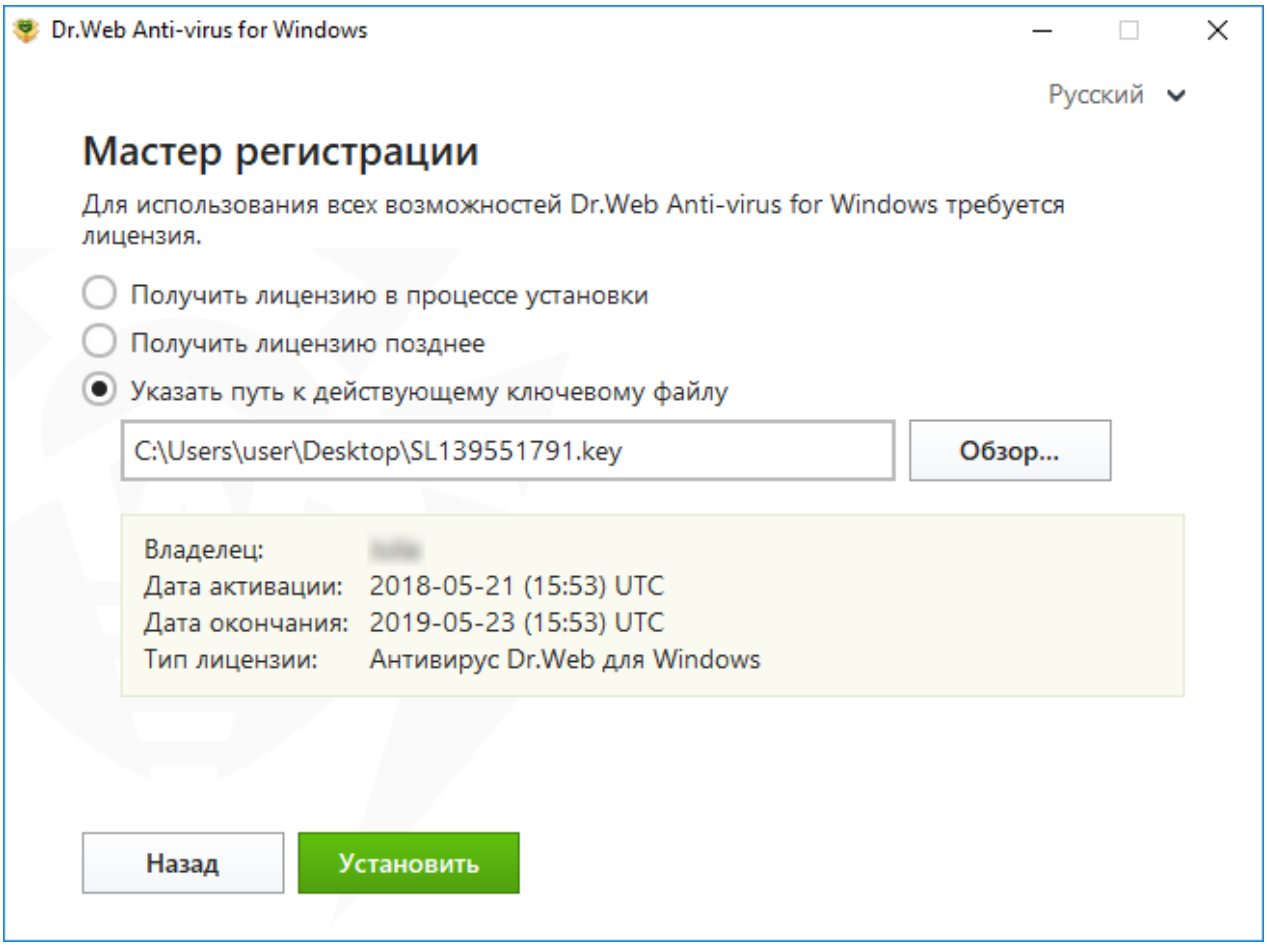

Рисунок 9. Установка. Мастер регистрации

  2. Продолжите установку продукта, следуя инструкциям Мастера установки.

- в любое время работы продукта при помощи Мастера регистрации, который входит в состав Менеджера лицензии:

  1. В меню Dr.Web выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать или купить новую лицензию**.

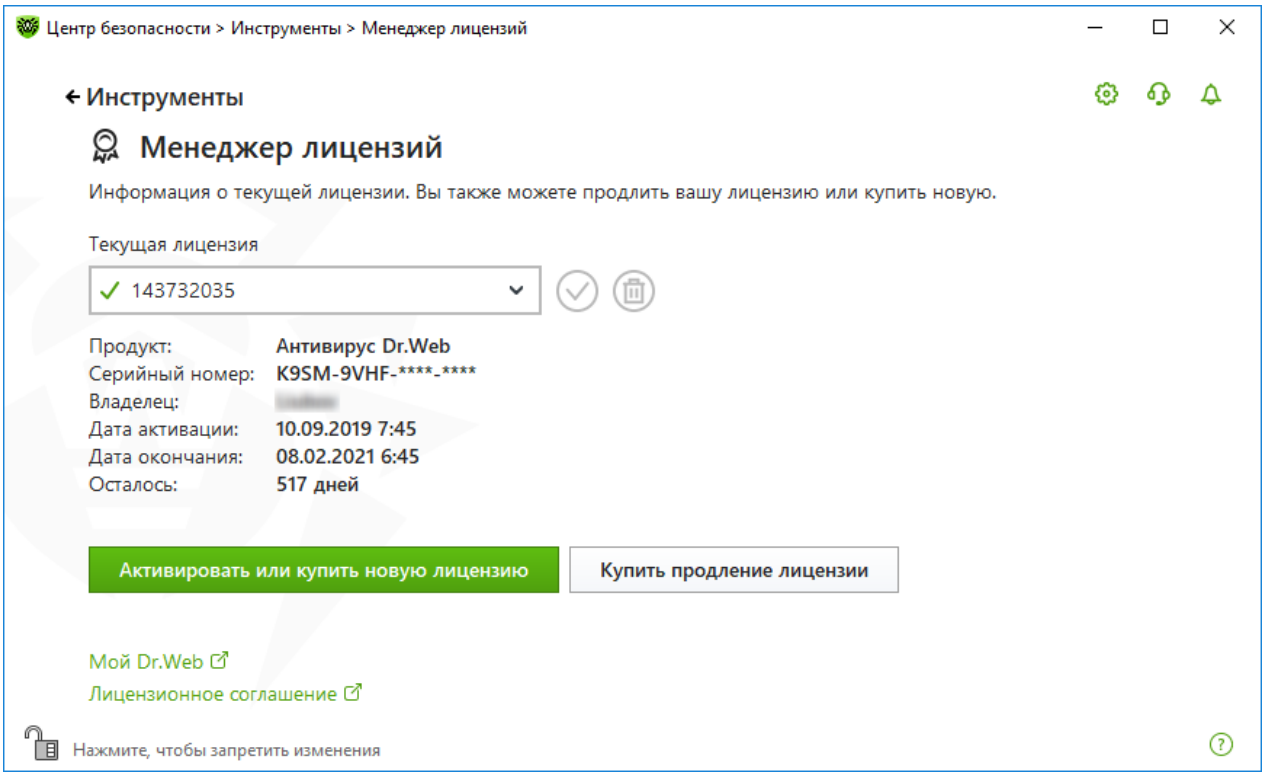

Рисунок 10. Менеджер лицензий

2. Откроется окно Мастера регистрации. Нажмите ссылку **или укажите ключевой файл**. В открывшемся окне укажите путь к ключевому файлу.

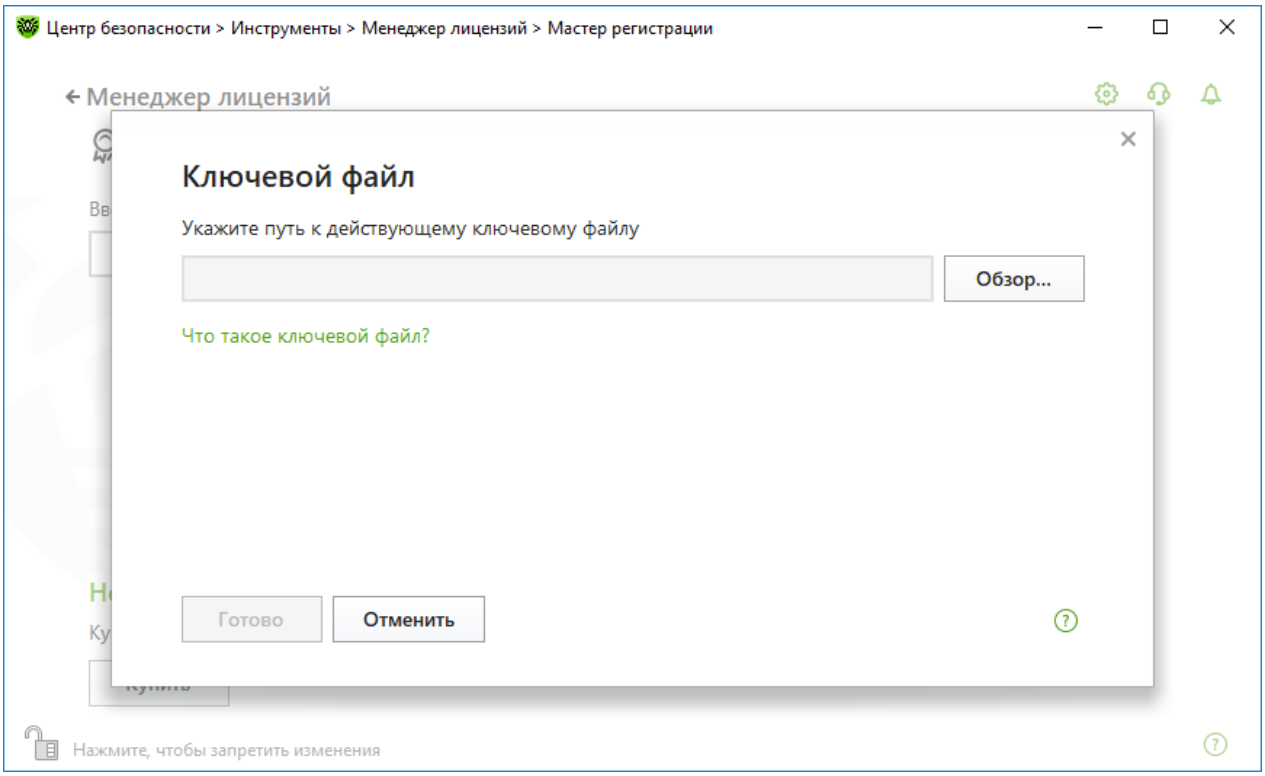

Рисунок 11. Мастер регистрации. Активация лицензии

Активации лицензии на Windows XP

Пользователи Windows XP могут активировать лицензию только при помощи ключевого файла. Если ключевого файла нет, но есть серийный номер, его необходимо зарегистрировать на сайте компании «Доктор Веб». После завершения процесса регистрации вам будет предоставлена ссылка для скачивания ключевого файла. Используйте этот ключевой файл для активации лицензии.

Повторная активация

Повторная активация лицензии может потребоваться в случае утраты ключевого файла.

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

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

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

Возможные вопросы

Как я могу перенести лицензию на другой компьютер?

Вы можете перенести вашу коммерческую лицензию на другой компьютер при помощи ключевого файла или серийного номера. Если вы хотите перенести лицензию на компьютер, на котором используется Windows XP, вы можете это сделать только при помощи ключевого файла.

Чтобы перенести лицензию на другой компьютер

- при помощи серийного номера:
  1. Скопируйте серийный номер с компьютера, с которого вы хотите перенести лицензию.

2. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
3. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию. Для этого воспользуйтесь Мастером регистрации во время установки продукта или после установки во время работы продукта (см. Активация при помощи серийного номера).

- при помощи ключевого файла:
  1. Скопируйте ключевой файл с компьютера, с которого вы хотите перенести лицензию. По умолчанию ключевой файл хранится в папке установки Dr.Web и имеет расширение `.key`.
  2. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
  3. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию. Для этого воспользуйтесь Мастером регистрации во время установки продукта или после установки во время работы продукта (см. Активация при помощи ключевого файла).

4.2. Продление лицензии

Чтобы продлить текущую лицензию при помощи Менеджера лицензий

1. Откройте меню Dr.Web и выберите пункт **Лицензия**.
2. В окне Менеджера лицензий нажмите кнопку **Купить продление лицензии**. Откроется страница сайта компании «Доктор Веб», на которой вы можете оформить продление лицензии с возможностью получения скидки.

Dr.Web поддерживает обновление на лету, при котором не требуется переустанавливать Dr.Web или прерывать его работу. Чтобы обновить лицензию на использование Dr.Web, вам необходимо активировать новую лицензию.

Чтобы активировать лицензию

1. Откройте окно Менеджера лицензий, выбрав пункт **Лицензия** в меню Dr.Web. Нажмите кнопку **Активировать или купить новую лицензию**.
2. В открывшемся окне введите серийный номер или нажмите ссылку **или укажите ключевой файл** и укажите путь к ключевому файлу. Пользователи Windows XP могут активировать лицензию только при помощи ключевого файла.

Подробная инструкция по активации лицензии доступна в разделе Как активировать лицензию.

Если срок действия лицензии, которую вы хотите продлить, закончился, Dr.Web начнет использовать новую лицензию.

Если срок действия лицензии, которую вы хотите продлить, еще не закончился, то количество оставшихся дней будет автоматически добавлено к новой лицензии. При этом старая лицензия будет заблокирована, и вам придет соответствующее уведомление на адрес электронной почты, который вы указывали при регистрации. Рекомендуется также удалить старую лицензию при помощи Менеджера лицензий.

Если у вас остались вопросы по продлению лицензии, ознакомьтесь со списком наиболее частых вопросов на сайте компании «Доктор Веб».

Возможные вопросы

После продления лицензии я получил письмо, что мой ключевой файл будет заблокирован через 30 дней.

Если срок действия лицензии, которую вы продлили, еще не закончился, то количество оставшихся дней автоматически добавляется к новой лицензии. При этом лицензия, на основе которой было сделано продление, блокируется. При использовании заблокированной лицензии компоненты Dr.Web не работают, и не происходит обновление.

Рекомендуется удалить старую лицензию из продукта. Для этого:

1. В режиме администратора в меню Dr.Web выберите пункт **Лицензия**. Откроется окно Менеджера лицензий.
2. В выпадающем списке выберите лицензию, на основе которой было сделано продление и нажмите кнопку .

4.3. Ключевой файл

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

Ключевой файл имеет расширение `.key` и содержит следующую информацию:

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

При работе программы ключевой файл по умолчанию должен находиться в папке установки Dr.Web. Программа регулярно проверяет наличие и корректность

ключевого файла. Во избежание порчи ключа не модифицируйте ключевой файл.

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

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

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

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

Если при установке Dr.Web вы не получили ключевой файл и не указали путь к нему, используется временный ключевой файл. Такой ключевой файл обеспечивает полную функциональность компонентов программы Dr.Web. Однако в меню Dr.Web будет отсутствовать пункт **Обновление**. Обновления не будут загружаться до тех пор, пока вы не активируете лицензию или пробную версию либо с помощью Мастера регистрации не укажете путь к действительному ключевому файлу.

Рекомендуется сохранять ключевой файл до истечения срока действия лицензии.

5. Меню программы

После установки программы Dr.Web в область уведомлений Windows добавляется значок, который также отражает состояние программы. Чтобы открыть меню Dr.Web, нажмите значок. Если программа не запущена, в меню **Пуск** раскройте группу **Dr.Web** и выберите пункт **Центр безопасности**.

В меню Dr.Web вы можете увидеть статус защиты, а также получить доступ к основным средствам управления и настройкам программы.

Для доступа к параметрам компонентов и для перехода к онлайн-сервису Мой Dr.Web необходимо ввести пароль, если в настройках вы включили опцию **Защищать настройки Dr.Web паролем**.

Если вы забыли пароль к настройкам продукта, обратитесь в службу технической поддержки.

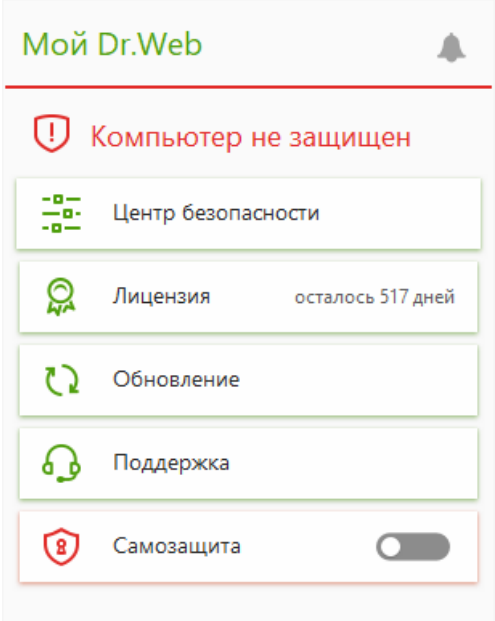

Рисунок 12. Меню программы

Пункты меню программы

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

Статус защиты компьютера. При всех работающих компонентах программы отображается статус **Компьютер защищен**. При отключении одного или нескольких компонентов защиты статус меняется на **Компьютер не защищен**.

Центр безопасности. Открывает окно с доступом к основным настройкам, параметрам компонентов защиты и исключениям.

Лицензия. Информация о количестве дней, оставшихся до окончания действия лицензии. Открывает Менеджер лицензий.

Обновление. Информация об актуальности вирусных баз и времени последнего обновления. Запускает обновление компонентов программы и вирусных баз.

Поддержка. Открывает окно поддержки.

Самозащита (появляется при отключении Самозащиты). С помощью переключателя вы можете снова включить Самозащиту.

Кнопка **Лента уведомлений** . Открывает окно Лента уведомлений.

Возможные состояния программы

Значок Dr.Web отражает текущее состояние программы:

Значок Dr.Web	Описание
	Все компоненты, необходимые для защиты компьютера, запущены и работают правильно.
	Самозащита или хотя бы один из компонентов отключены либо вирусные базы устарели, что ослабляет защиту антивируса и компьютера. Включите Самозащиту или отключенный компонент.
	Ожидается запуск компонентов после старта операционной системы, дождитесь запуска компонентов программы; либо в процессе запуска одного из ключевых компонентов Dr.Web возникла ошибка, компьютер находится под угрозой заражения. Проверьте наличие действительного ключевого файла и при необходимости установите его.
	В данный момент Сканер проводит проверку.

6. Центр безопасности

Окно **Центр безопасности** предоставляет доступ ко всем компонентам, инструментам, статистике и настройкам программы.

Чтобы перейти к окну Центр безопасности

1. Откройте меню Dr.Web .
2. Выберите пункт **Центр безопасности**.

Чтобы перейти к окну Центр безопасности из меню Пуск

1. В меню **Пуск** раскройте группу **Dr.Web**.
2. Нажмите **Центр безопасности**.

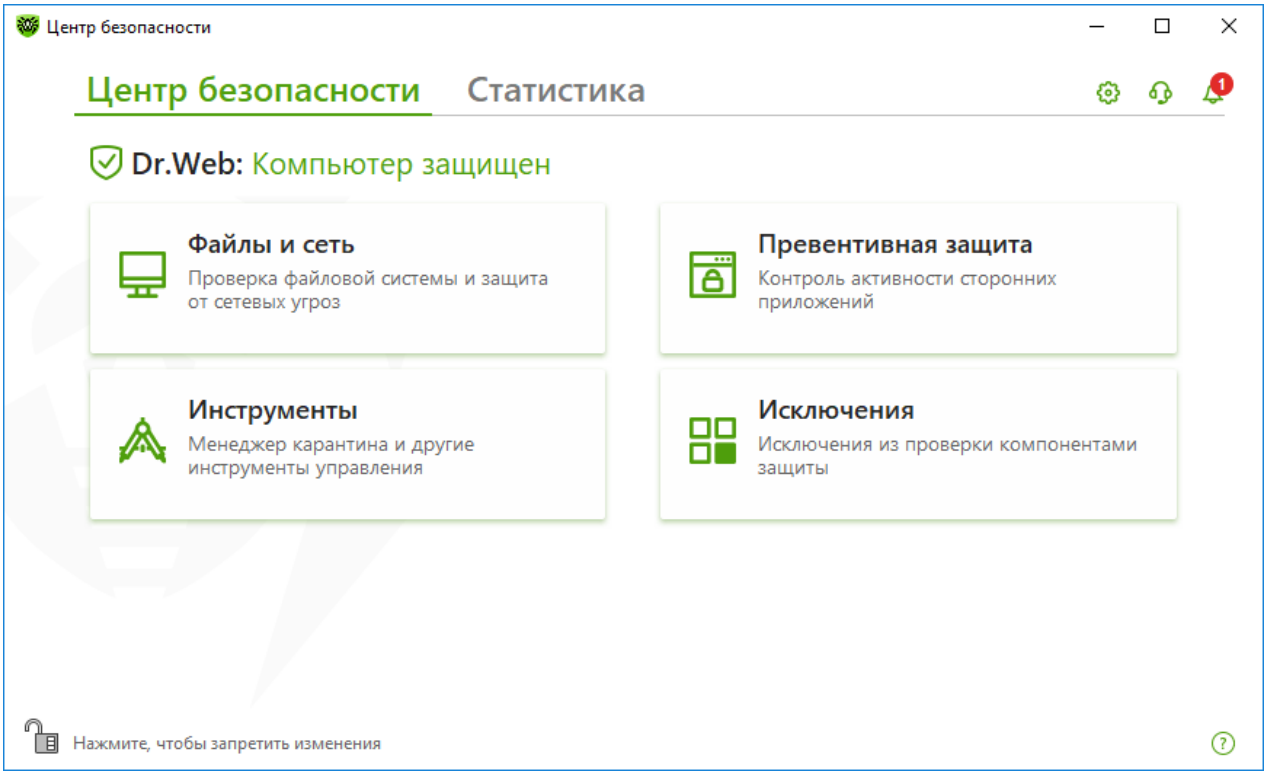

Рисунок 13. Окно Центр безопасности

Группы настроек

Из основного окна предоставляется доступ к следующим группам настроек:

- Основная вкладка **Центр безопасности** — доступ ко всем компонентам защиты и инструментам:
  - Файлы и сеть;
  - Превентивная защита;

  - Инструменты;
  - Исключения;
- Вкладка Статистика — статистика по основным событиям работы программы;
- Кнопка в верхней части окна — доступ к настройкам программы;
- Кнопка в верхней части окна — доступ к окну **Поддержка**, где вы можете собрать отчет для службы технической поддержки и просмотреть информацию о версии продукта и дате последнего обновления компонентов и вирусных баз;
- Кнопка в верхней части окна — доступ к окну **Лента уведомлений**, где вы можете посмотреть важные уведомления о событиях работы программы.

Режим администратора

Для доступа ко всем группам настроек необходимо переключить Dr.Web в режим администратора, нажав на замок в нижней части окна. Когда Dr.Web работает в режиме администратора, замок «открыт».

В любом режиме есть полный доступ к группе настроек **Инструменты**. Также, не переключая Dr.Web в режим администратора, вы можете включить любой из компонентов защиты и запустить Сканер. Выключение компонентов защиты, переход к параметрам компонентов и настройкам программы возможны только в режиме администратора.

Статусы защиты

В верхней части окна отображается статус защищенности системы.

- **Компьютер защищен** — все компоненты включены и работают, Самозащита включена, лицензия действует. Отображается зеленым цветом.
- **Компьютер не защищен** — отображается, если какой-либо из компонентов защиты отключен. Отображается красным цветом. Плитка отключенного компонента также выделена красным.
- **Лицензия истекает** — начинает отображаться за 7 дней до окончания действия лицензии. Отображается желтым цветом. Для продления лицензии необходимо перейти в Менеджер лицензий.

7. Обновление баз и программных модулей

Для обнаружения вредоносных объектов продукты Dr.Web используют вирусные базы, в которых содержится информация обо всех известных вредоносных программах. Регулярное обновление позволяет обнаруживать ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев излечивать ранее неизлечимые зараженные файлы. Помимо вирусных баз обновляются также программные модули Dr.Web и справка продукта.

Для обновления Dr.Web необходимо иметь доступ к интернету либо к зеркалу обновлений (локальной или сетевой папке), либо к антивирусной сети, в которой хотя бы на одном из компьютеров настроено зеркало обновлений. Настройка источника обновлений и других параметров производится в группе настроек **Общие** → **Обновление**. Подробная инструкция по настройке параметров обновления программы Dr.Web доступна в разделе Настройки обновления.

Проверка актуальности обновлений

Чтобы проверить актуальность вирусных баз и компонентов, откройте меню Dr.Web. В случае актуальности обновлений в меню пункт **Обновление** будет выделен зеленым цветом:

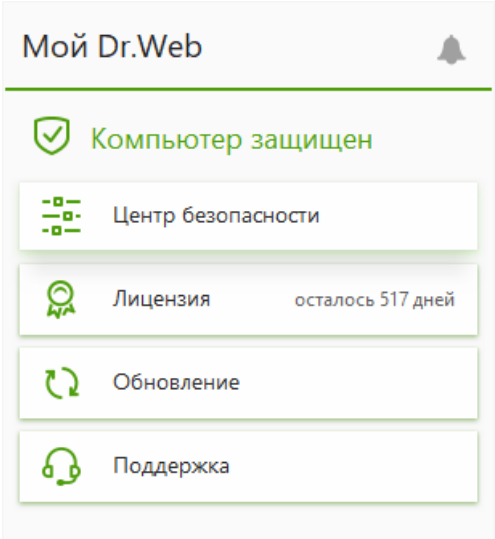

Рисунок 14. Меню Dr.Web

При необходимости обновления в меню появится пункт **Требуется обновление**, выделенный красным цветом:

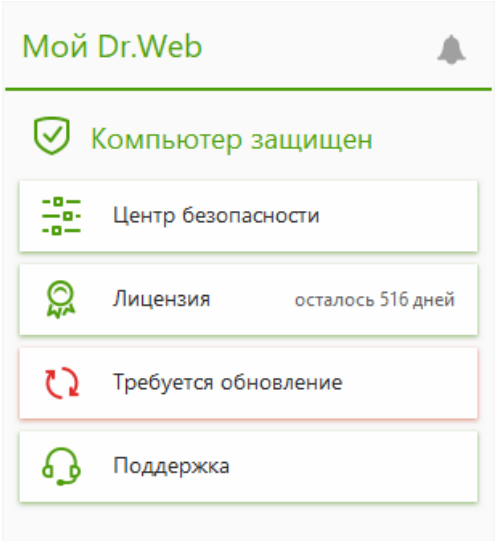

Рисунок 15. Необходимость обновления

Запуск процесса обновления

При обновлении Dr.Web загрузит все обновленные файлы, соответствующие вашей версии Dr.Web, а также новую версию Dr.Web при ее наличии.

При обновлении исполняемых файлов, драйверов и библиотек может потребоваться перезагрузка компьютера. В этом случае будет показано соответствующее предупреждение. Вы можете задать любое удобное время перезагрузки либо выбрать время следующего напоминания.

Чтобы запустить обновления из меню Dr.Web

1. Откройте меню Dr.Web и выберите пункт **Обновление**. В зависимости от актуальности вирусных баз и компонентов цветовая индикация этого пункта может варьироваться.
2. Откроется информация об актуальности обновлений, а также дата последнего обновления. Нажмите кнопку **Обновить**, чтобы запустить процесс обновления.

Чтобы запустить обновления из командной строки

1. Перейдите в папку установки Dr.Web (`%PROGRAMFILES%\Common Files\Doctor Web\Updater`).
2. Запустите `drwupsrv.exe`. Список параметров запуска вы можете найти в Приложении А.

Отчеты и журнал статистики

Чтобы посмотреть историю обновлений во вкладке Статистика

1. Откройте меню Dr.Web  .
2. Выберите пункт **Центр безопасности**.
3. Перейдите во вкладку **Статистика**.
4. Нажмите плитку **Подробный отчет**.

Отчеты обновления также записываются в файл `dwupdater.log` в папке `%allusersprofile%\Doctor Web\Logs\`.

Как настроить обновление баз и компонентов без доступа к интернету?

Если компьютер подключен к локальной сети, вы можете настроить обновление вирусных баз и компонентов с зеркала обновлений, созданного на другом компьютере с установленным продуктом Dr.Web (Security Space, Антивирус для Windows или Антивирус для серверов Windows). Компьютер, на котором создано зеркало обновлений, должен быть подключен к интернету. Версия продукта должна совпадать.

Подробнее о том, как настроить зеркало обновлений

Вы можете настроить обновление с зеркала обновлений двумя способами:

Чтобы настроить получение обновлений при подключении к антивирусной сети

1. Разрешите удаленное управление продуктом Dr.Web в разделе настроек Антивирусная сеть.

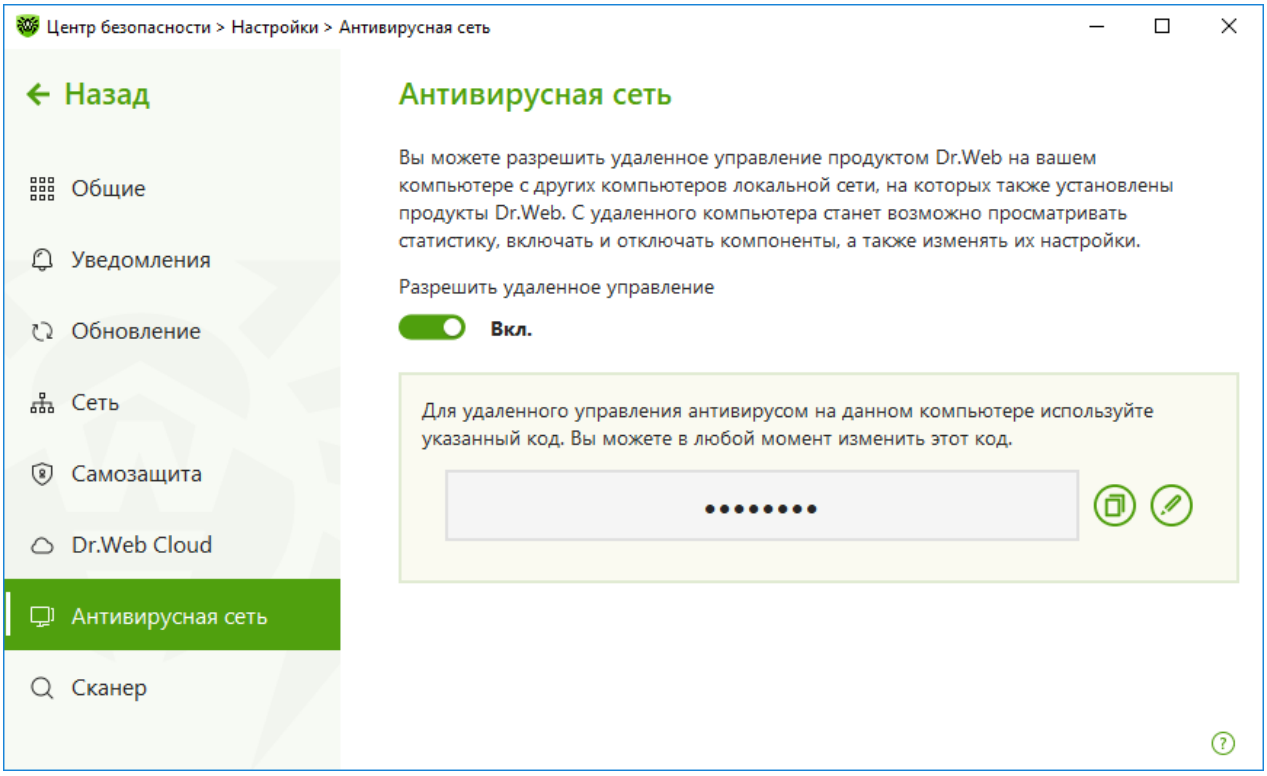

Рисунок 16. Включение удаленного доступа

2. Перейдите в окно **Настройки** → **Обновление**.
3. В пункте **Источник обновлений** нажмите **Изменить** и в выпадающем списке выберите **Антивирусная сеть**.

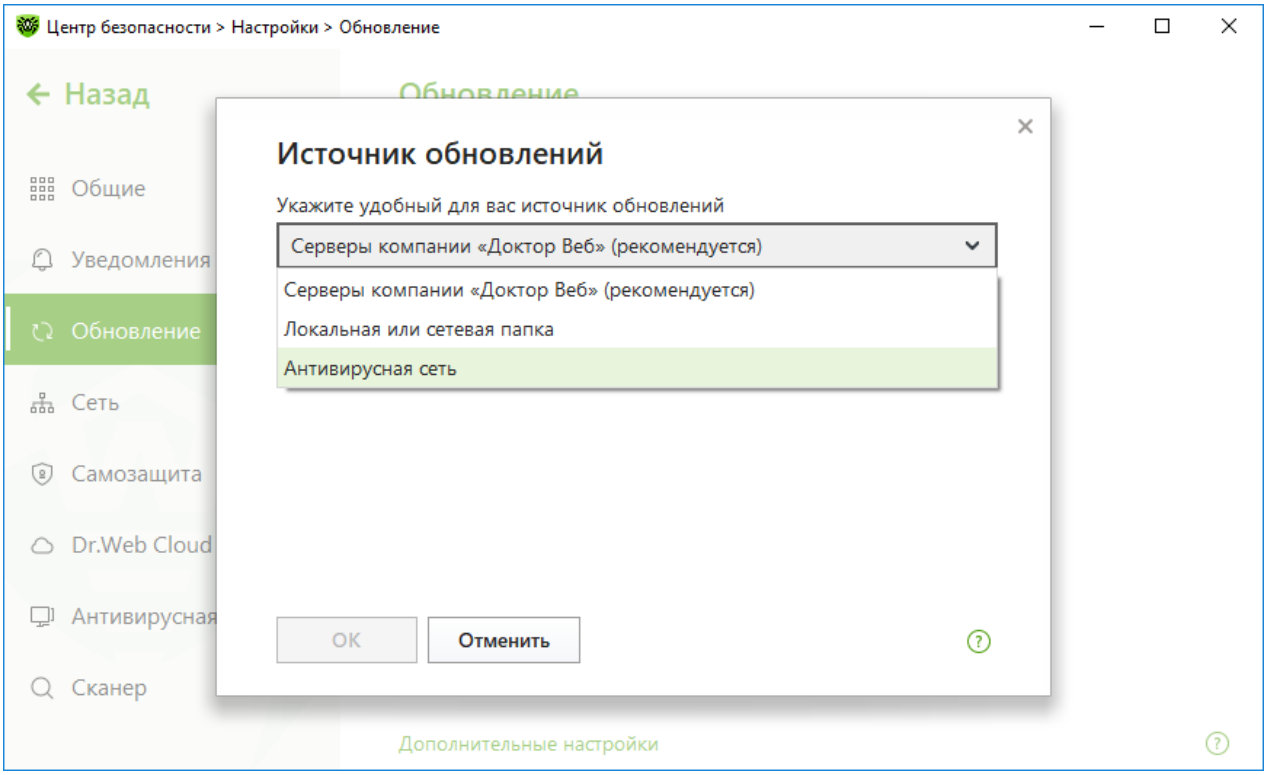

Рисунок 17. Выбор источника обновлений

4. Выберите необходимый компьютер, с которого будет производиться обновление вирусных баз и компонентов программы.
5. Нажмите **ОК**.

Чтобы настроить получение обновлений из локальной или сетевой папки

1. Перейдите в окно **Настройки** → **Обновление**.
2. В пункте **Источник обновлений** нажмите **Изменить** и в выпадающем списке выберите **Локальная или сетевая папка**.

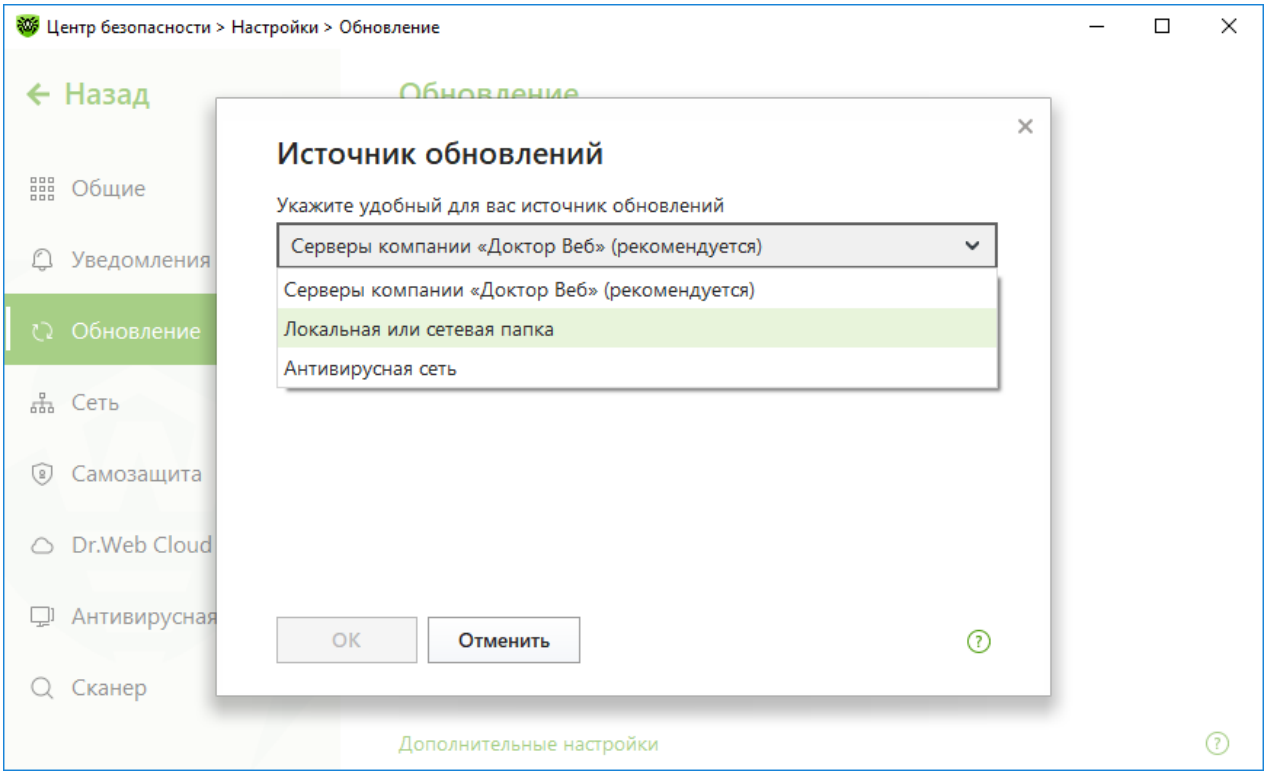

Рисунок 18. Выбор источника обновлений

3. В строке **Путь к зеркалу обновлений** укажите папку, содержащую файлы созданного зеркала обновлений. Для этого нажмите кнопку **Обзор** и выберите нужную папку или введите путь вручную в формате UNC.
4. При необходимости укажите **Логин** и **Пароль** к папке, к которой осуществляется подключение. **Логин** — это имя пользователя учетной записи на компьютере, где лежит сетевая папка. Логин должен включать название компьютера в локальной сети и полный путь к папке. **Пароль** — это пароль этой учетной записи.
5. Нажмите **ОК**.

8. Лента уведомлений

В этом окне собраны важные уведомления о событиях работы программы. Уведомления в этом разделе дублируют некоторые из всплывающих на экране уведомлений.

Чтобы перейти к ленте уведомлений из Меню программы

1. Откройте меню Dr.Web.
2. Нажмите кнопку. Над значком отображается количество сохраненных уведомлений.
3. Откроется окно с уведомлениями о событиях.

Чтобы перейти к ленте уведомлений из Центра безопасности

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В верхней части окна программы нажмите.
3. Откроется окно с уведомлениями о событиях.

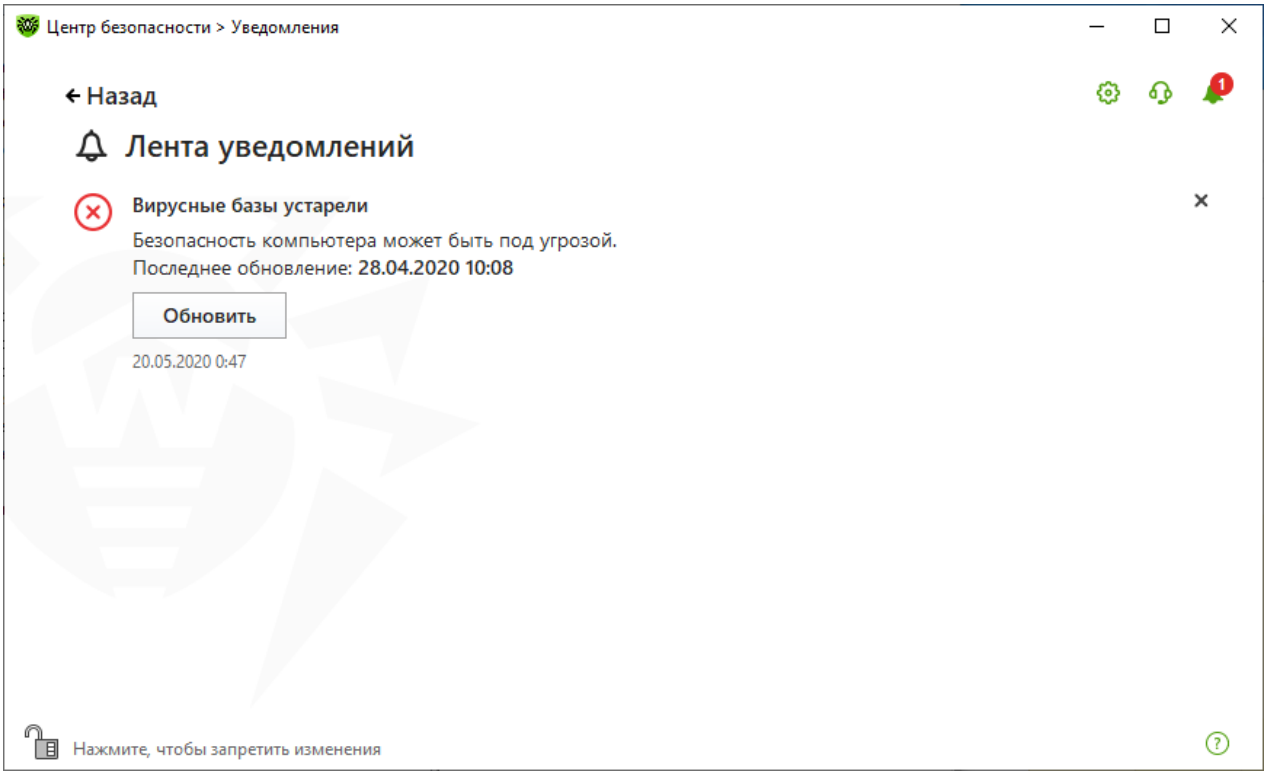

Рисунок 19. Окно ленты уведомлений

Срок хранения уведомлений

Срок хранения уведомлений составляет две недели. При устранении проблем уведомления о них также удаляются.

Типы уведомлений

Критические уведомления	
Лицензия	• Действующая лицензия не найдена. • Текущая лицензия заблокирована.
Угрозы	• Обнаружена угроза. • Требуется перезагрузка для обезвреживания угроз. • Вирусные базы устарели.
Важные уведомления	
Лицензия	• Срок действия лицензии истекает. • Текущая лицензия заблокирована.
Обновление	• Требуется перезагрузка, чтобы обновления вступили в силу.
Маловажные информационные уведомления	
Новая версия	• Доступна новая версия продукта.

Настройки отображения

Настройки отображения уведомлений в ленте дублируют настройки всплывающих уведомлений. Если вы хотите изменить настройки отображения так, чтобы определенные уведомления не отображались в ленте, в окне **Параметры уведомлений** необходимо снять флажок в столбце **Экран** напротив необходимого пункта (см. раздел Настройки уведомлений).

9. Настройки программы

Чтобы перейти к изменению настроек программы

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите .
4. Откроется окно с настройками программы.

> Если в общих настройках вы установили флажок **Защищать настройки Dr.Web паролем**, для доступа к основным настройкам Dr.Web запрашивается пароль.

В этом разделе:

- Общие — защита настроек паролем, выбор языка программы, а также импорт и экспорт настроек.
- Уведомления — настройка вывода уведомлений на экран или получение их по почте.
- Обновление — изменение источника или периодичности обновлений и создание зеркала обновлений.
- Сеть — настройка использования прокси-сервера и проверки данных, передаваемых по безопасным протоколам.
- Самозащита — настройка дополнительных параметров безопасности.
- Dr.Web Cloud — настройка доступа к облачным сервисам компании «Доктор Веб».
- Антивирусная сеть — настройка удаленного доступа к Dr.Web, установленному на вашем компьютере.
- Параметры проверки файлов — настройка параметров работы Сканера.

9.1. Общие настройки

К общим настройкам относятся следующие:

- защита настроек программы паролем;
- выбор языка программы;
- управление настройками программы (импорт, экспорт, восстановление настроек по умолчанию);
- настройки ведения журнала работы;
- настройки карантина;
- настройки автоматического удаления записей статистики.

Чтобы открыть общие настройки

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Общие**.

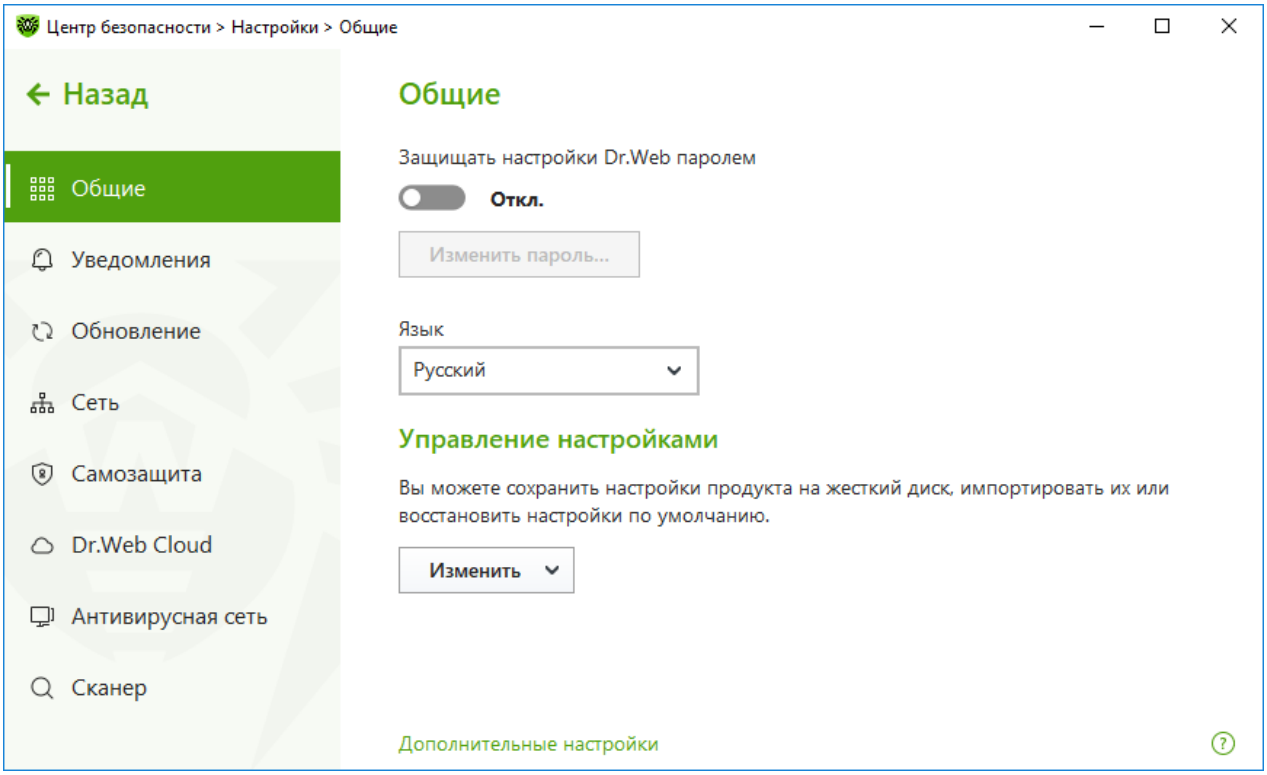

Рисунок 20. Общие настройки

9.1.1. Защита настроек программы паролем

Вы можете ограничить доступ к настройкам Dr.Web на вашем компьютере при помощи пароля. Пароль будет запрашиваться каждый раз при обращении к настройкам Dr.Web.

Чтобы задать пароль

1. В окне изменения общих настроек включите опцию **Защищать настройки Dr.Web паролем** при помощи соответствующего переключателя .

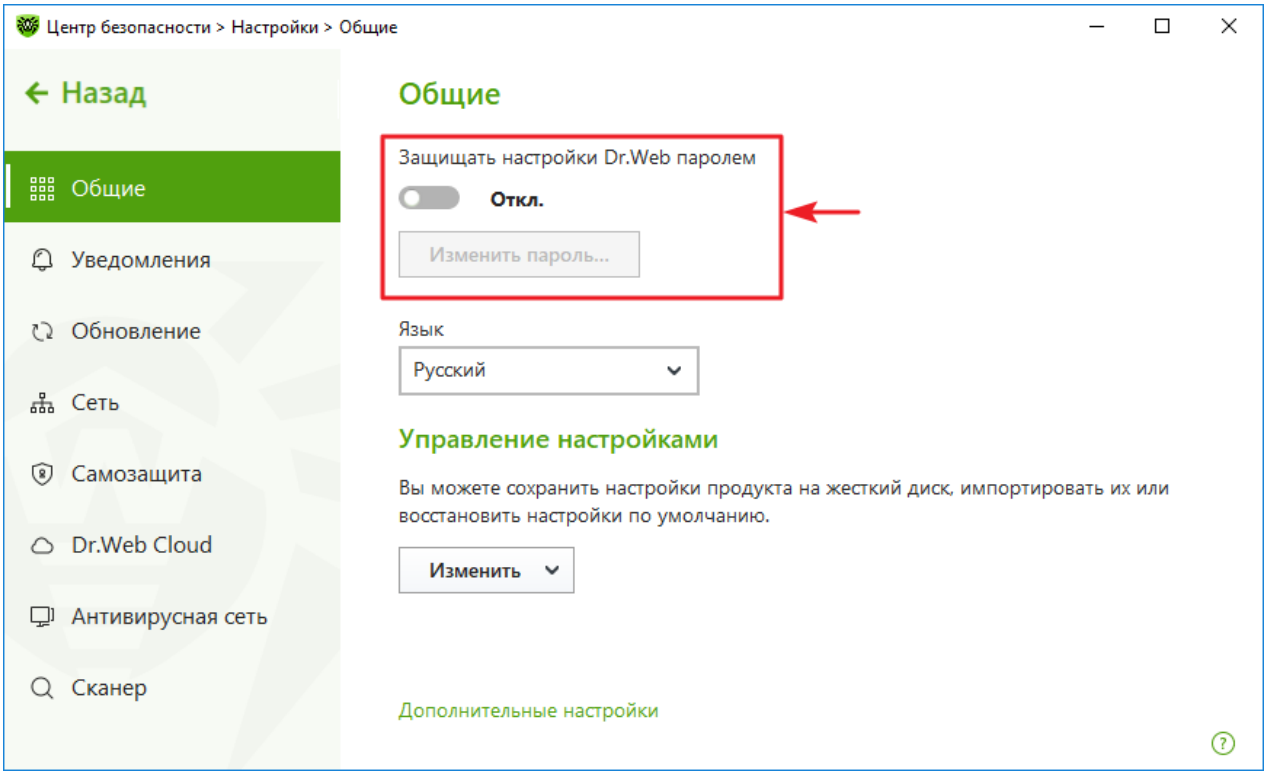

Рисунок 21. Защита настроек паролем

2. В открывшемся окне задайте пароль и подтвердите его ввод.
3. Нажмите кнопку **ОК**.

Если вы забыли пароль к настройкам продукта, необходимо переустановить программу Dr.Web без сохранения текущих настроек.

9.1.2. Выбор языка программы

При необходимости вы можете переключить язык интерфейса программы. Список языков пополняется автоматически и содержит все доступные на текущий момент локализации графического интерфейса Dr.Web. Для этого в выпадающем списке **Язык** выберите необходимый язык.

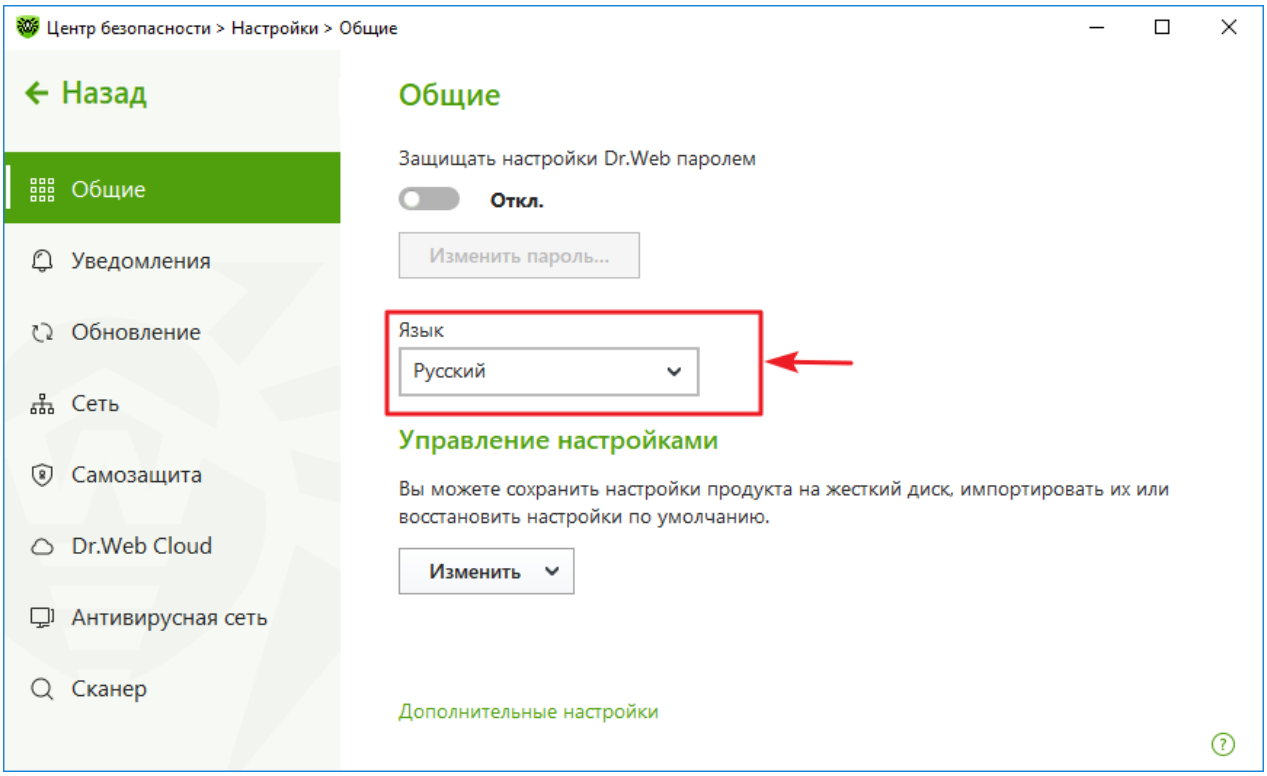

Рисунок 22. Выбор языка программы

9.1.3. Управление настройками Dr.Web

Для управления настройками выберите одно из следующих значений в выпадающем списке группы настроек **Управление настройками**:

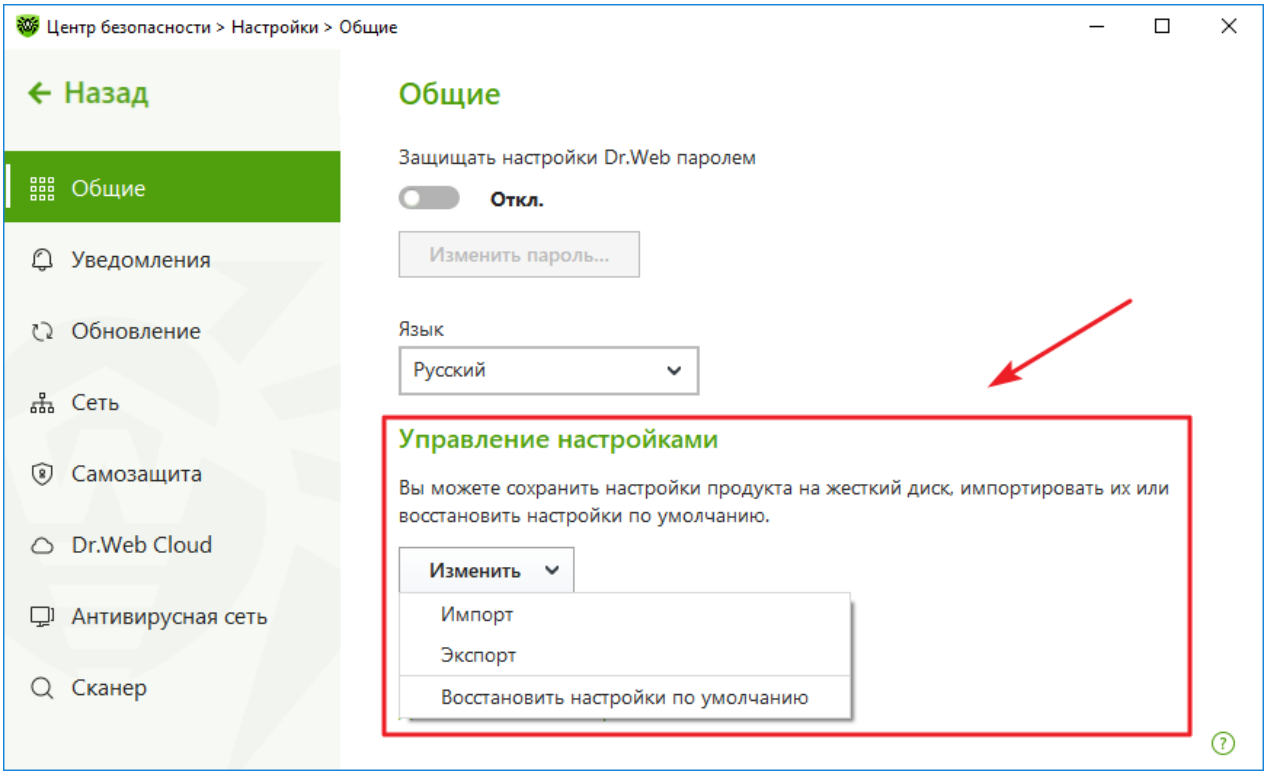

Рисунок 23. Управление настройками

- **Восстановить настройки по умолчанию**, чтобы сбросить пользовательские настройки до настроек по умолчанию.
- **Импорт**, если вы уже настроили работу антивируса на другом компьютере и хотите использовать те же настройки.
- **Экспорт**, если вы хотите использовать свои настройки на других компьютерах. Затем воспользуйтесь функцией импорта настроек на другом компьютере.

9.1.4. Ведение журнала работы Dr.Web

Вы можете включить ведение подробного журнала о работе одного или нескольких компонентов или сервисов Dr.Web.

Чтобы изменить настройки ведения журнала

1. Нажмите ссылку **Дополнительные настройки**.
2. В разделе настроек **Журнал** нажмите кнопку **Изменить**.

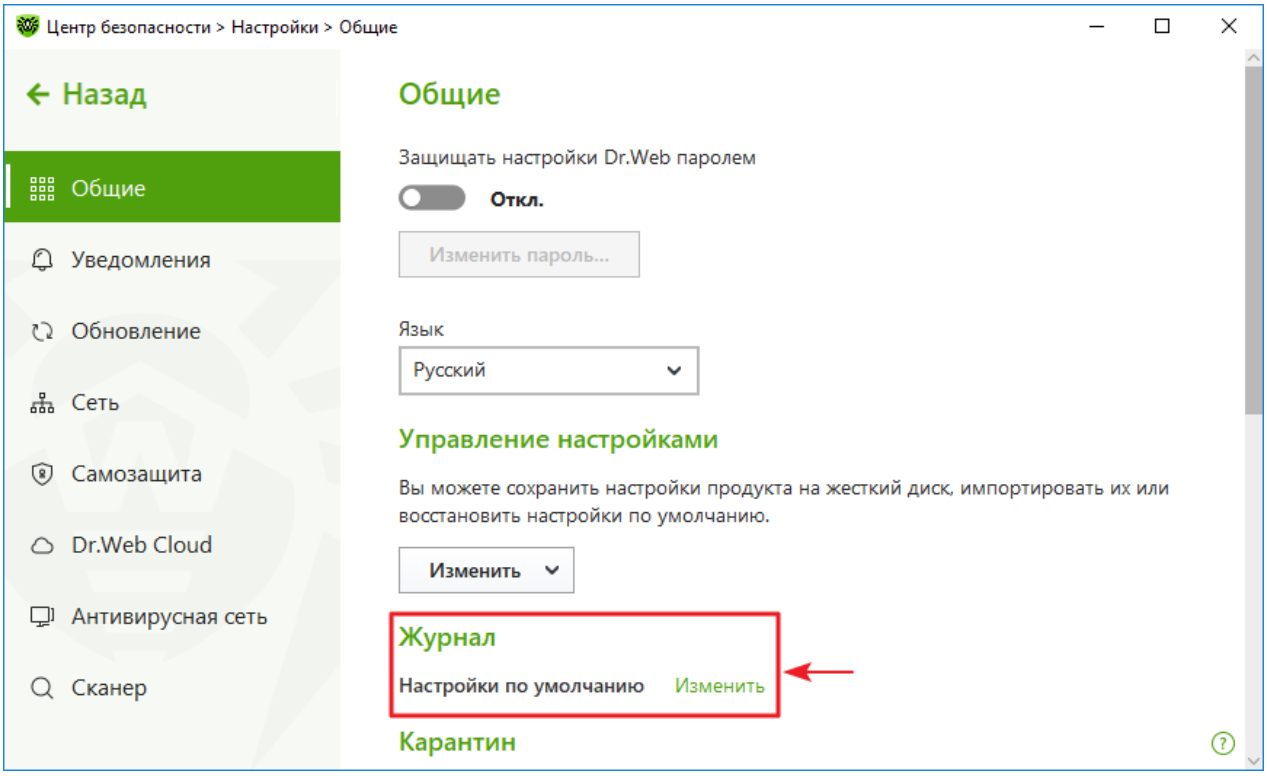

Рисунок 24. Общие настройки. Журнал

Откроется окно настроек ведения подробного журнала:

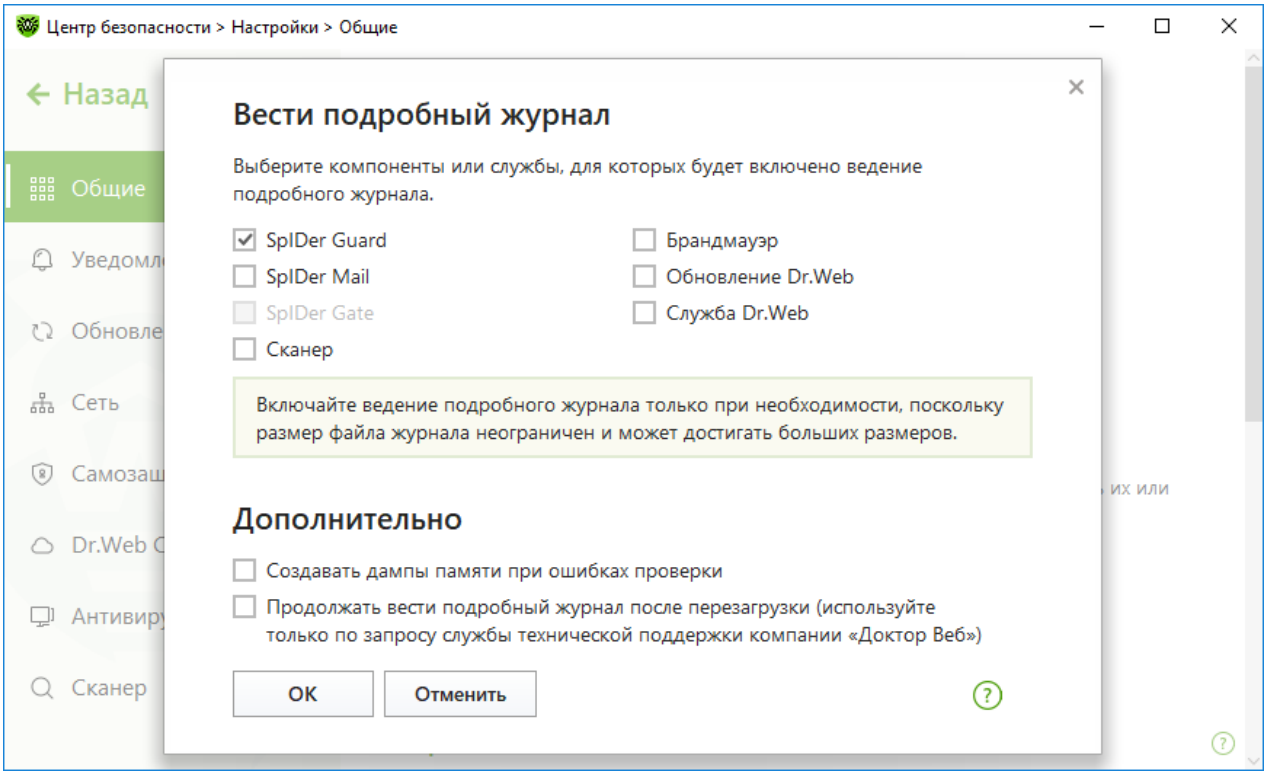

Рисунок 25. Настройки ведения журнала работы

3. Выберите компоненты, для которых будет включено ведение подробного журнала. По умолчанию для всех компонентов Dr.Web журнал ведется в стандартном режиме, фиксирующем следующую информацию:

Компонент	Информация
SplDer Guard	Проведение обновлений, запуск и остановка 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 монитор файловой системы SplDer Guard проверяет наиболее часто. При необходимости добавьте такие объекты в список исключений, что может снизить нагрузку на компьютер.
SplDer Mail	Проведение обновлений, запуск и остановка почтового антивируса 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.
Сканер	Обновление версий сканирующих модулей и информации о вирусных базах, запуск и остановка Сканера, обнаруженные угрозы, а также данные об именах упаковщиков и содержимом проверяемых архивов.
Брандмауэр	Информация о приходящих в сервис запросах и решения по ним, информация о неизвестных соединениях с причиной запроса, а также информация об ошибках. При включении режима ведения подробного журнала собираются данные о сетевых пакетах (pcap-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 антивирусной сети.

Создание дампов памяти

Настройка **Создавать дампы памяти при ошибках проверки** позволяет сохранять полезную информацию о работе некоторых компонентов Dr.Web, что даст возможность специалистам компании «Доктор Веб» в дальнейшем провести более полный анализ проблемы и предложить ее решение. Рекомендуется включать данную настройку по просьбе сотрудников технической поддержки компании «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 включении подробных журналов 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 службы технической поддержки компании «Доктор Веб».

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

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

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

9.1.5. Настройки карантина

Чтобы чрезмерно не загружать диск, вы можете задать настройки хранения объектов в карантине, такие как время хранения объектов и создание папки карантина на съемном носителе.

Чтобы изменить настройки хранения обнаруженных угроз

1. В окне изменения общих настроек нажмите ссылку **Дополнительные настройки**.
2. В разделе настроек **Карантин** включите или отключите необходимую опцию при помощи переключателя .

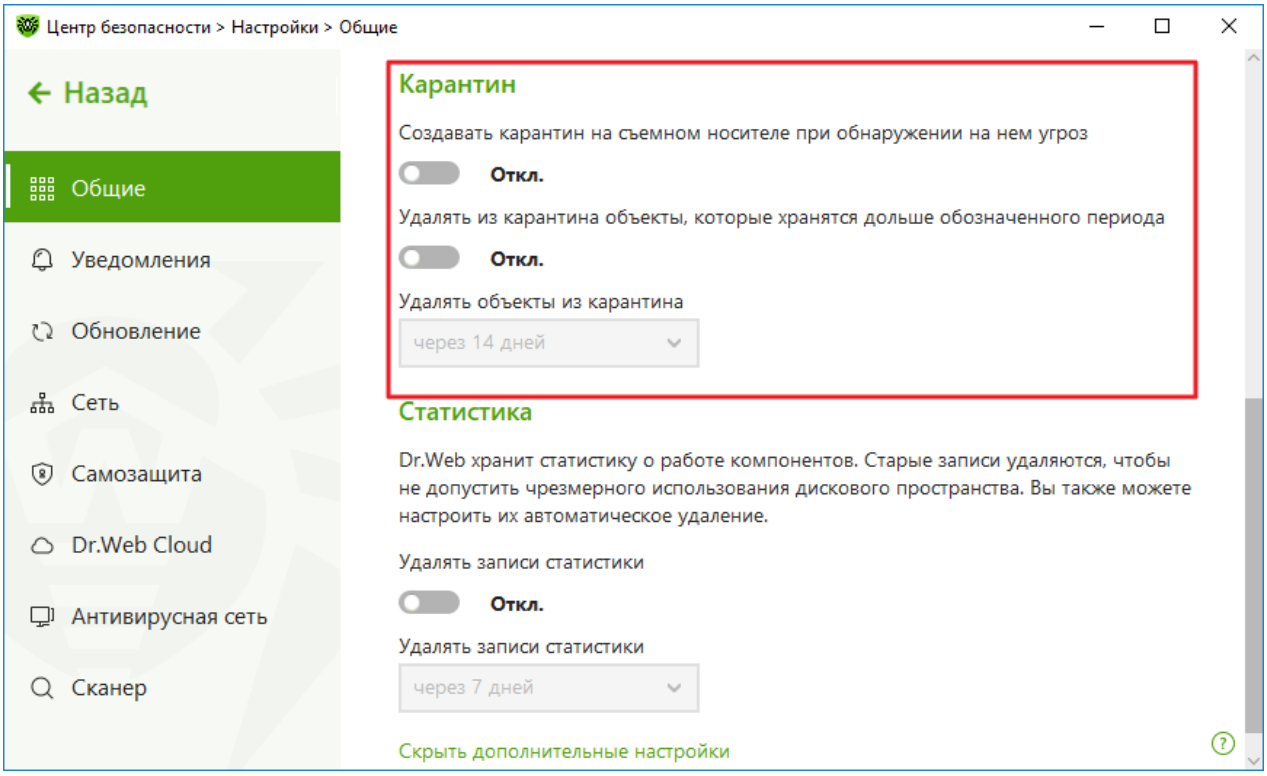

Рисунок 26. Настройки карантина

3. При включении автоматического удаления объектов из карантина в выпадающем меню выберите время. Объекты, хранящиеся дольше указанного срока, будут удаляться.

Создание карантина на съемном носителе

Опция **Создавать карантин на съемном носителе при обнаружении на нем угроз** позволяет при обнаружении угрозы на съемном носителе создавать папку карантина на том же носителе и помещать в эту папку угрозы без предварительного шифрования. На съемном носителе папка карантина создается, только если возможна запись на носитель. Использование отдельных папок и отказ от шифрования на съемных носителях позволяет предотвратить возможную потерю данных.

Если опция отключена, обнаруженные на съемных носителях угрозы помещаются в карантин на локальном диске.

Автоматическое удаление объектов из карантина

Чтобы избежать чрезмерного использования места на диске, включите автоматическое удаление объектов из карантина.

9.1.6. Автоматическое удаление записей статистики

По умолчанию Dr.Web хранит оптимальное количество записей статистики, чтобы избежать чрезмерного использования места на диске. В дополнение к этому вы можете включить автоматическое удаление записей, хранящихся дольше указанного срока.

Чтобы включить или отключить автоматическое удаление записей статистики

1. В окне изменения общих настроек нажмите ссылку **Дополнительные настройки**.
2. В разделе настроек **Статистика** включите или отключите автоудаление записей статистики при помощи переключателя .

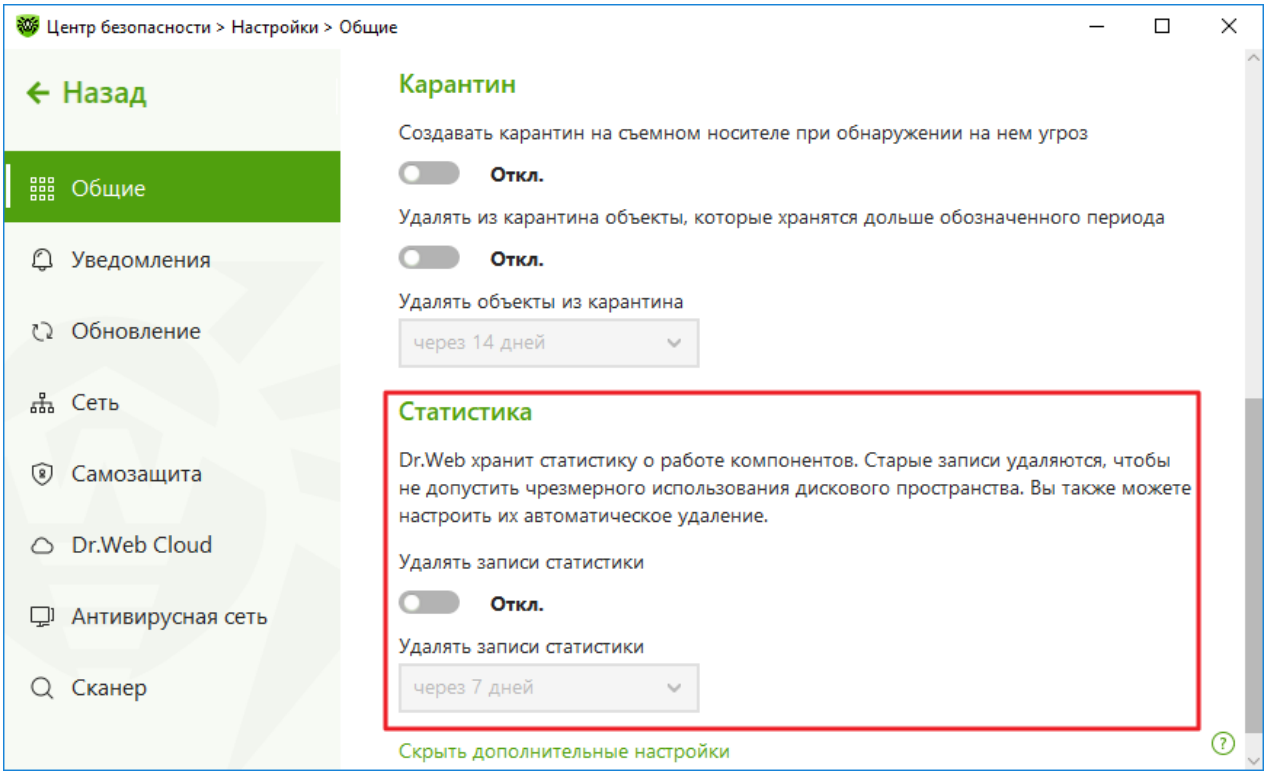

Рисунок 27. Настройки статистики

3. При включении автоудаления записей статистики в выпадающем меню выберите время. Записи, хранящиеся дольше указанного срока, будут удаляться.

9.2. Настройки уведомлений

Вы можете настроить параметры получения уведомлений о критичных и важных событиях работы Dr.Web.

В этом разделе:

- Настройка параметров уведомлений
- Настройка вывода уведомлений на экран

- Настройка отправки уведомлений по почте

При необходимости настройте параметры получения уведомлений о критичных и важных событиях работы Dr.Web.

Чтобы открыть настройки уведомлений

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Уведомления**.

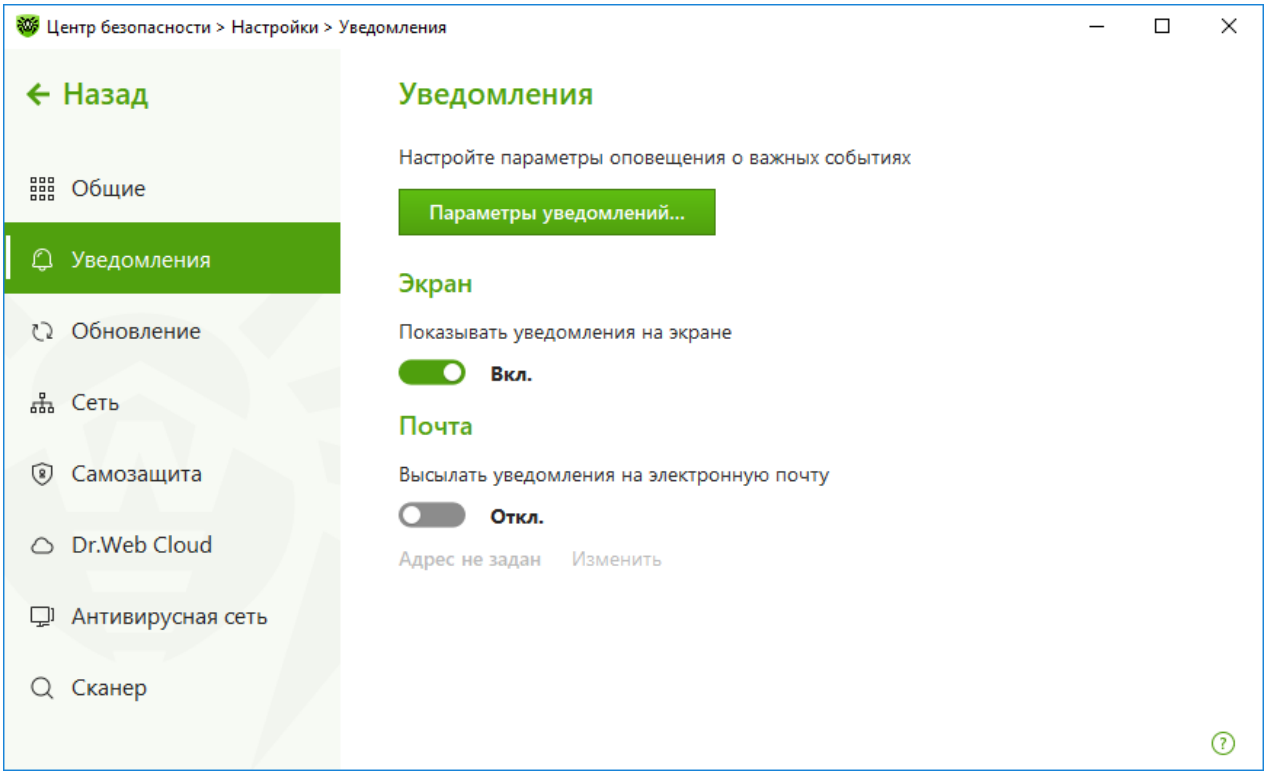

Рисунок 28. Настройки уведомлений

Чтобы настроить параметры уведомлений

1. Нажмите кнопку **Параметры уведомлений**.
2. Выберите уведомления, которые вы хотите получать.
   - Чтобы уведомления отображались на экране, установите соответствующий флажок в столбце **Экран**.
   - Чтобы получать оповещения по почте, установите соответствующий флажок в столбце **Почта**.

   Если вы не хотите получать уведомления о событии, снимите флажки.

Тип уведомления	Описание
Обнаружена угроза	Уведомления об угрозах, обнаруженных SpIDer Guard. По умолчанию уведомления включены.
Критичные уведомления	Критичные уведомления о следующих событиях: • Обнаружены соединения, ожидающие ответа Брандмауэра. По умолчанию уведомления включены.
Важные уведомления	Важные уведомления о следующих событиях: • Вирусные базы устарели. • Заблокирована попытка изменения системных даты и времени. • Доступ к защищаемому объекту заблокирован Поведенческим анализом. • Доступ к защищаемому объекту заблокирован Защитой от эксплойтов. • Доступ к защищаемому объекту заблокирован Защитой от вымогателей. • Информация об обновлениях и поддержке продукта. По умолчанию уведомления включены.
Малозначительные уведомления	Малозначительные уведомления о следующих событиях: • Успешное обновление. • Ошибка обновления. По умолчанию уведомления выключены.
Лицензия	Уведомления о следующих событиях: • Срок действия лицензии истекает. • Действующая лицензия не найдена. • Текущая лицензия заблокирована.

3. При необходимости задайте дополнительные параметры отображения экранных оповещений:

Флажок	Описание
Не показывать уведомления в полноэкранном режиме	Отображение уведомлений 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).

Флажок	Описание
	Снимите этот флажок, чтобы уведомления выводились на том же рабочем столе, на котором запущено приложение в полноэкранном режиме.

4. Если вы выбрали одно или несколько почтовых уведомлений, настройте отправку почты с вашего компьютера.

> 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;
> - автоматическая перезагрузка;
> - запрос на разрешение процессу модификации объекта;
> - подключена новая клавиатура.

Уведомления, которые выводятся на экран

В окне настроек уведомлений включите соответствующую опцию, чтобы получать уведомления в виде всплывающего окна над значком Dr.Web в области уведомлений Windows.

Уведомления по почте

Чтобы получать уведомления о событиях по почте

1. В окне настроек уведомлений включите опцию **Высылать уведомления на электронную почту**.
2. В появившемся окне введите адрес электронной почты, на который вы хотите получать уведомления. Использование этого адреса необходимо будет подтвердить на шаге 7.

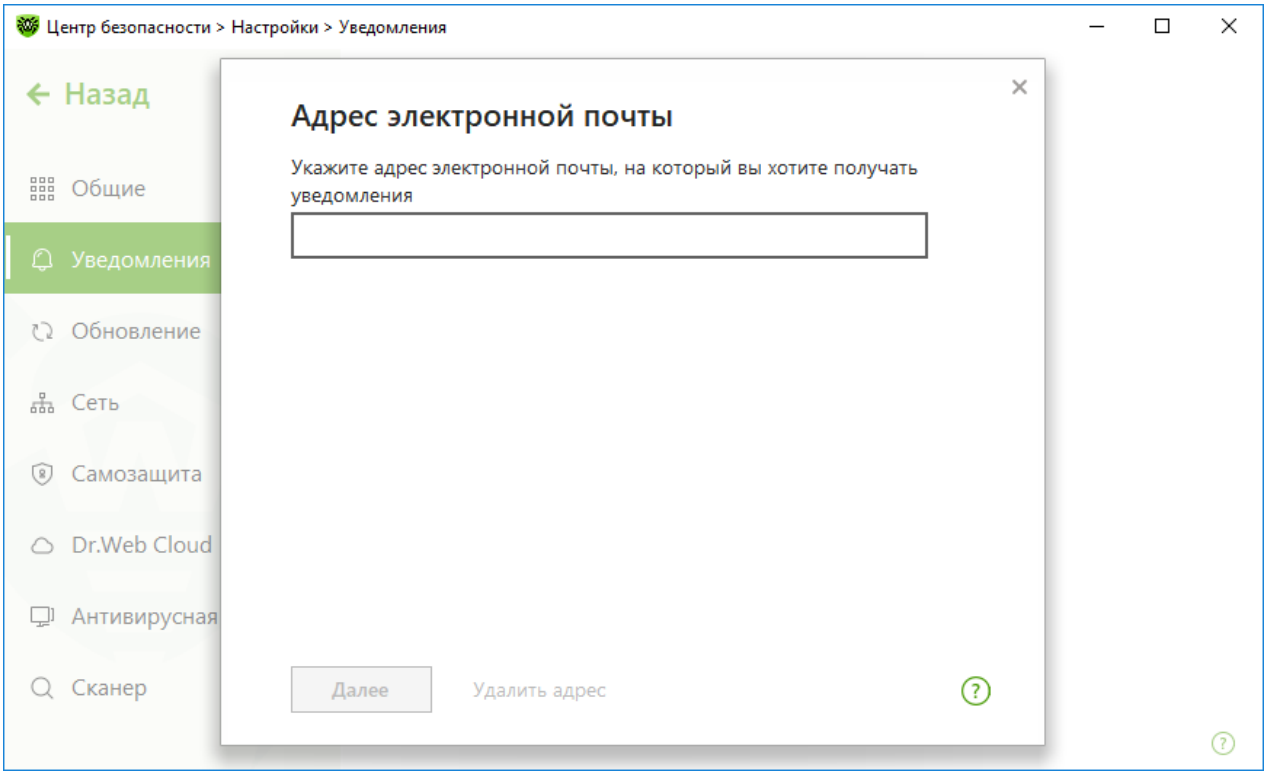

Рисунок 29. Указание адреса для почтовых уведомлений

3. Нажмите **Далее**.
4. В открывшемся окне укажите данные учетной записи, с которой будут отправляться уведомления.
   - Если список почтовых серверов содержит необходимый сервер, выберите его, а затем укажите логин и пароль от вашей учетной записи.
   - Если список почтовых серверов не содержит необходимого сервера, выберите **Указать вручную** и в открывшемся окне заполните необходимые поля:

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

5. Нажмите ссылку **Отправить тестовое сообщение**, чтобы проверить, что учетная запись указана верно. Сообщение придет на тот адрес, с которого должны отправляться уведомления (настроенный на шаге 4).
6. Нажмите **Далее**.
7. Введите код подтверждения, который придет на электронный адрес, указанный для получения уведомлений на шаге 2. Если код не придет в течение 10 минут, нажмите кнопку **Отправить код повторно**. Если вы не введете код подтверждения, уведомления на этот адрес отправляться не будут.

Чтобы изменить адрес электронной почты и другие параметры, в окне настроек уведомлений (см. рисунок Настройки уведомлений) нажмите **Изменить** и повторите все действия, начиная с шага 2.

9.3. Настройки обновления

Настройте период получения обновлений и источник обновлений для вирусных баз и компонентов. Также вы можете создать зеркало обновлений для получения обновлений на другом компьютере.

Вы можете настроить следующие параметры обновления Dr.Web:

- периодичность обновлений;
- источник обновлений;
- обновляемые компоненты;
- зеркало обновлений.

Чтобы открыть настройки обновления

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Обновление**.

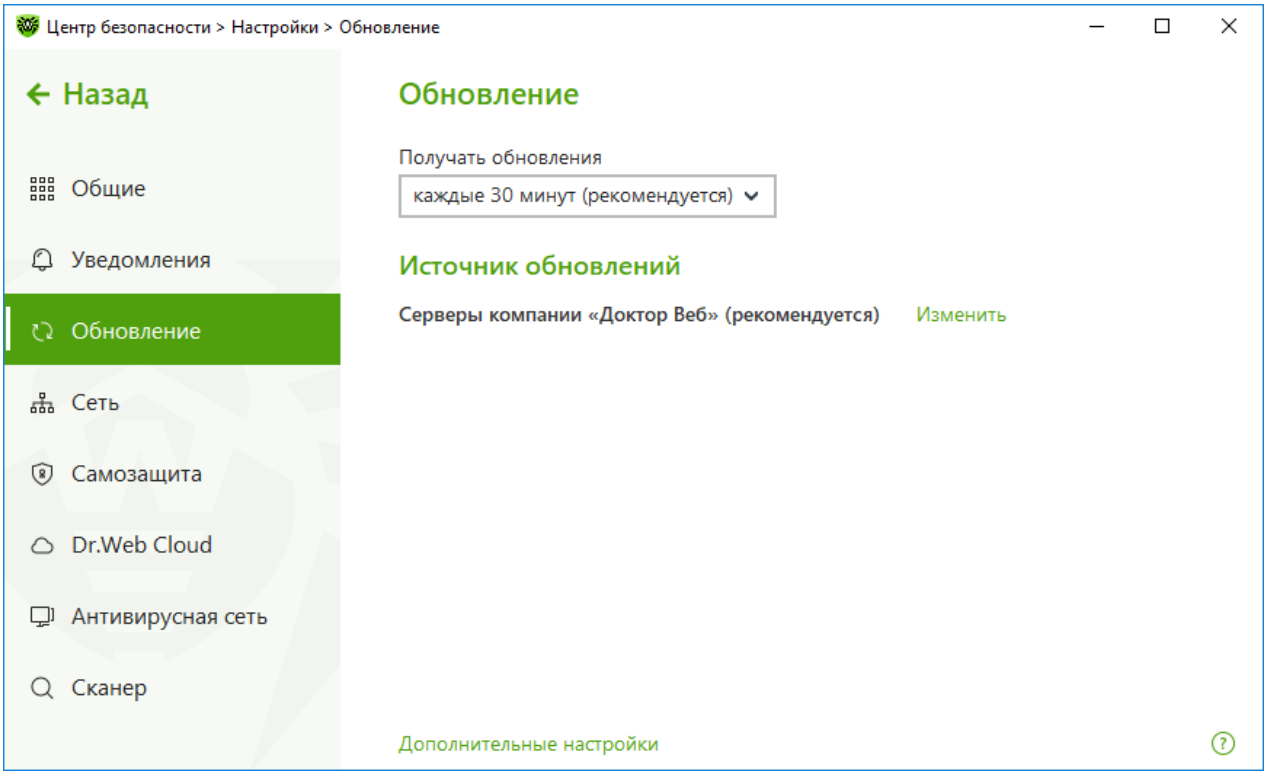

Рисунок 30. Настройки обновления

Периодичность обновлений

По умолчанию установлено оптимальное значение (30 минут), которое позволяет поддерживать информацию об угрозах в актуальном состоянии. Чтобы изменить периодичность обновлений, выберите необходимое значение в выпадающем меню.

Автоматическое обновление проводится в фоновом режиме. Вы также можете выбрать из выпадающего списка значение **Вручную**. В этом случае вам необходимо будет вручную запускать обновление Dr.Web.

Настройка источника обновлений

По умолчанию в качестве источника обновления указано значение **Серверы компании «Доктор Веб» (рекомендуется)**.

Чтобы настроить удобный для вас источник обновлений

1. В окне настройки обновления (см. рисунок Настройки обновления) в разделе **Источник обновлений** нажмите ссылку **Изменить**. Откроется окно настройки источника обновлений.

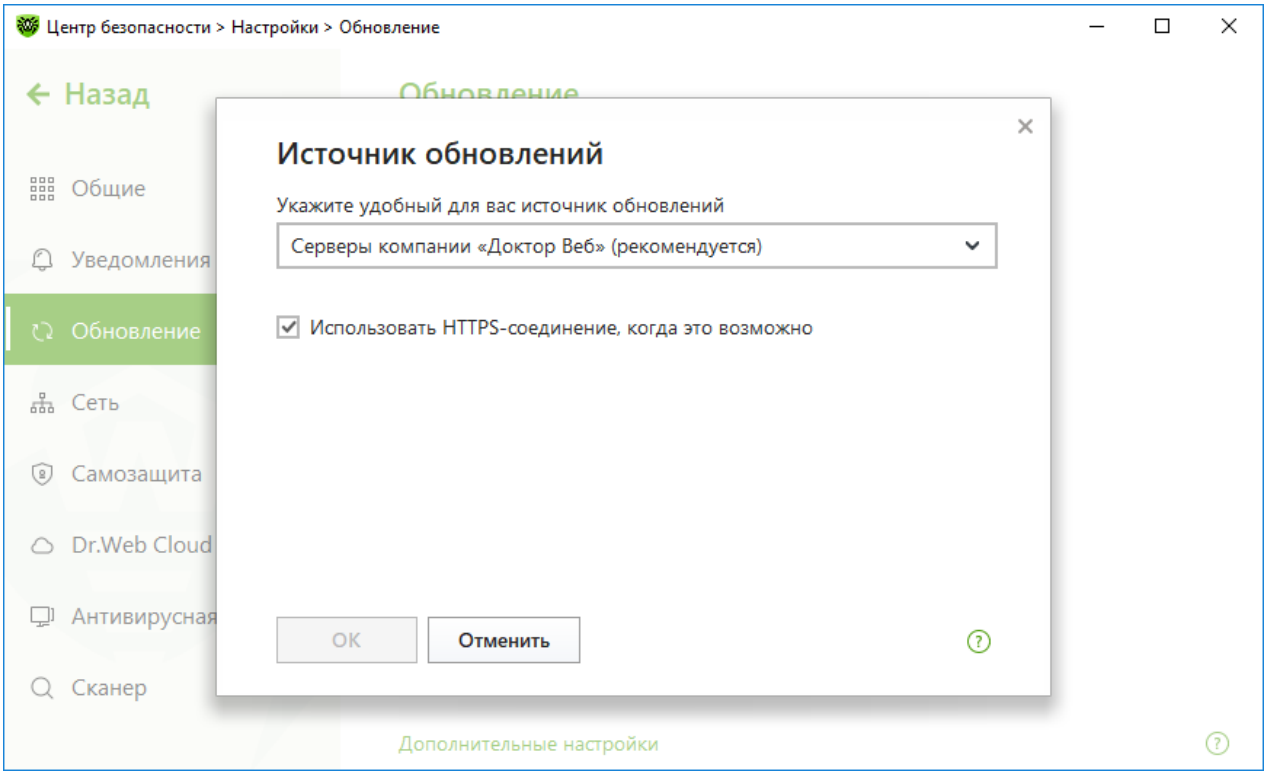

Рисунок 31. Настройка источника обновлений

2. Выберите удобный для вас источник обновлений из выпадающего списка.
   - **Серверы компании «Доктор Веб» (рекомендуется)**. Обновление будет происходить с серверов компании «Доктор Веб» через интернет. Если вы хотите загружать обновления по безопасному протоколу при такой возможности, включите опцию **Использовать HTTPS-соединение, когда это возможно**.
   - **Локальная или сетевая папка**. Обновление будет происходить из локальной или сетевой папки, в которую скопированы обновления. Укажите путь к папке (нажав кнопку **Обзор** или введя путь вручную в формате UNC), а также имя пользователя и пароль, если это необходимо.
   - **Антивирусная сеть**. Обновление будет происходить через локальную сеть с компьютера, на котором установлен продукт Dr.Web и создано зеркало обновлений. Выберите компьютер, который будет использоваться в качестве источника обновлений.
3. Нажмите **ОК**, чтобы сохранить изменения.

Если на компьютере уже установлен продукт Dr.Web версии 12.0, не допускается в качестве источника обновлений указывать компьютер с более ранней версией продукта, поскольку это приведет к критическим ошибкам в работе системы.

Дополнительные настройки

Для перехода к дополнительным настройкам в окне **Обновление** (см. рисунок Настройки обновления) нажмите ссылку **Дополнительные настройки**.

Настройка обновляемых компонентов

Вы можете выбрать один из следующих вариантов загрузки обновлений компонентов Dr.Web:

- **Все (рекомендуется)**, при котором загружаются обновления как вирусных баз Dr.Web, так и антивирусного ядра и других программных компонентов Dr.Web;
- **Только вирусные базы**, при котором загружаются только обновления вирусных баз Dr.Web и антивирусного ядра; другие компоненты Dr.Web не обновляются.

Создание зеркала обновлений

Зеркало обновлений — это папка, в которую копируются обновления. Зеркало обновлений может быть использовано как источник обновлений Dr.Web для компьютеров в локальной сети, которые не подключены к интернету.

Чтобы настроить ваш компьютер в качестве зеркала обновлений

1. В окне настройки обновления (см. рисунок Настройки обновления) нажмите ссылку **Дополнительные настройки** и включите использование зеркала обновлений при помощи переключателя. Откроется окно настройки зеркала обновлений.

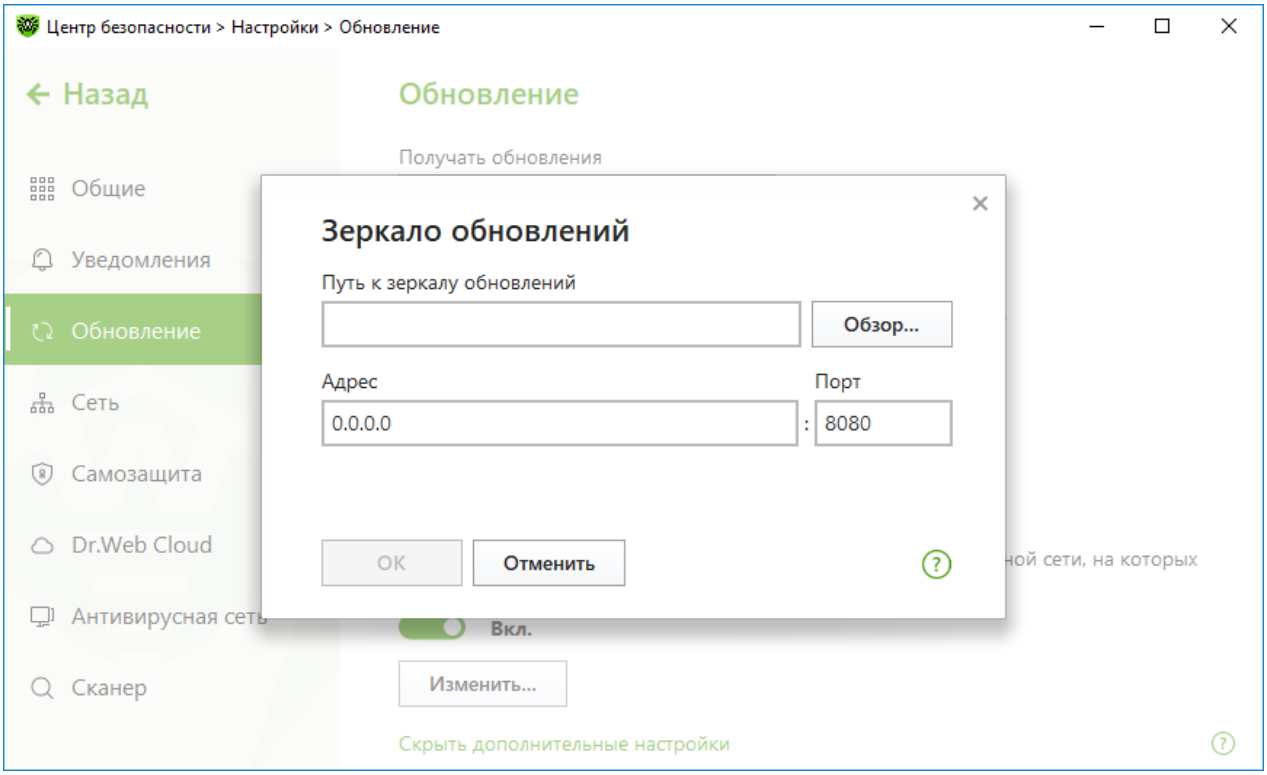

Рисунок 32. Настройка зеркало обновлений

2. Нажмите **Обзор** и выберите папку, в которую будут копироваться обновления. Рекомендуется выбрать пустую папку или создать новую папку. Если указана непустая папка, все ее содержимое будет удалено. Также вы можете указать путь к папке вручную в формате UNC.
3. Если ваш компьютер входит в несколько подсетей, вы можете указать адрес, который будет доступен только для одной из подсетей. Также вы можете указать порт, на котором HTTP-сервер будет принимать запросы на соединение.
   - В поле **Адрес** указывается имя хоста или IP-адрес в форматах IPv4 или IPv6.
   - В поле **Порт** указывается любой свободный порт.
4. Нажмите **OK**, чтобы сохранить изменения.

Периодичность загрузки обновлений на зеркало будет совпадать с выбранным значением выпадающего меню **Получать обновления**.

9.4. Сеть

Вы можете настроить параметры соединения с прокси-сервером, включить проверку данных, передаваемых по криптографическим протоколам, а также экспортировать сертификат Dr.Web для последующего импорта в другие программы.

В этом разделе:

- Настройка соединения с прокси-сервером
- Проверка данных, передаваемых по криптографическим протоколам

- Экспорт сертификата Dr.Web

Чтобы открыть настройки сети

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Сеть**.

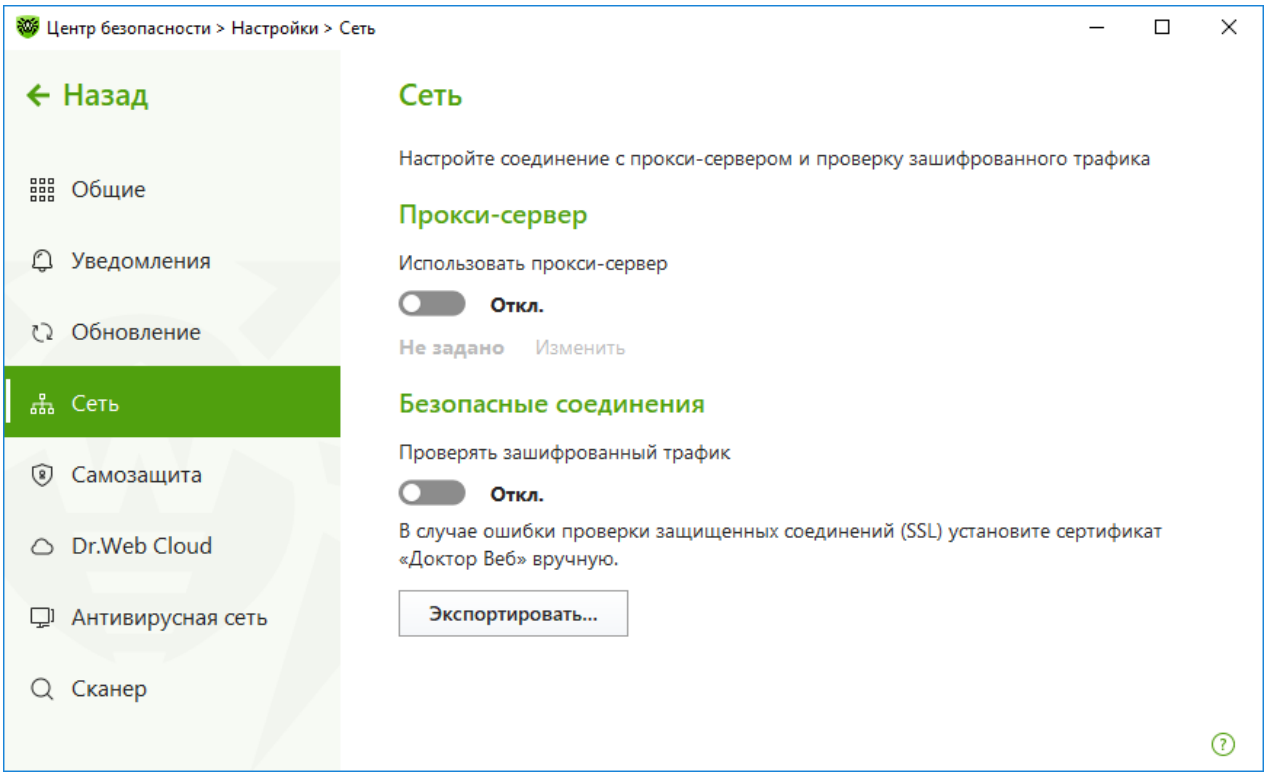

Рисунок 33. Подключение к прокси-серверу и проверка зашифрованного трафика

Использование прокси-сервера

Вы можете включить режим использования прокси-сервера и задать настройки подключения к нему. Для этого:

1. Включите опцию **Использовать прокси-сервер** при помощи переключателя .
2. Нажмите ссылку **Изменить**, чтобы задать настройки подключения к прокси-серверу:

Настройка	Описание
Адрес	Укажите адрес прокси-сервера.
Порт	Укажите порт прокси-сервера.

Настройка	Описание
Логин	Укажите имя учетной записи для подключения к прокси-серверу.
Пароль	Укажите пароль учетной записи, используемой для подключения к прокси-серверу.
Тип авторизации	Выберите тип авторизации, требуемый для подключения к прокси-серверу.

Безопасные соединения

Чтобы Dr.Web проверял данные, передаваемые по криптографическим протоколам SSL, TLS или STARTTLS, включите опцию **Проверять зашифрованный трафик**. SpIDer Mail будет проверять данные, передаваемые по протоколам POP3S, SMTPS, IMAPS.

Если приложение, использующее для своей работы шифрованные соединения, не обращается к хранилищу сертификатов системы Windows, то необходимо экспортировать сертификат безопасности компании «Доктор Веб» и импортировать вручную в каждое приложение.

Срок действия сертификата безопасности — 1 год. При необходимости импортируйте сертификат каждый год заново.

Что такое сертификат безопасности

Сертификат безопасности — это электронный документ, подтверждающий, что сертифицированная программа прошла проверку в одном из центров сертификации. Также сертификаты безопасности называются SSL-сертификатами, поскольку для работы используется SSL-протокол (Secure Socket Layer — англ. Уровень защищенных сокетов). Он обеспечивает защищенное шифрованием взаимодействие между веб-узлами, например, компьютером пользователя и веб-сервером.

Установка (импорт) в программу, работающую с интернетом, сертификата безопасности какого-либо веб-узла гарантирует, что связь с ним будет осуществляться в защищенном режиме с проверкой подлинности. В таком случае злоумышленникам будет крайне трудно осуществить перехват данных.

Импорт сертификата Dr.Web может потребоваться для работы следующих программ:

- браузер Opera;
- браузер Firefox;
- почтовый клиент Mozilla Thunderbird;
- почтовый клиент The Bat! и др.

Чтобы экспортировать и импортировать сертификат безопасности Dr.Web

1. Включите опцию **Проверять зашифрованный трафик** при помощи переключателя, если кнопка **Экспорт** не активна. При этом будет сгенерирован сертификат безопасности Dr.Web.
2. Нажмите кнопку **Экспорт**.
3. Выберите папку, в которую вы хотите сохранить сертификат. Нажмите **ОК**.
4. Импортируйте сертификат в нужное приложение. Подробнее о том, как импортировать сертификат, см. в справочных материалах к необходимому приложению.

9.5. Самозащита

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.

В этом разделе:

- Включение и отключение самозащиты
- Запрет изменения даты и времени системы

Чтобы перейти к настройкам Самозащиты

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите.
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Самозащита**.

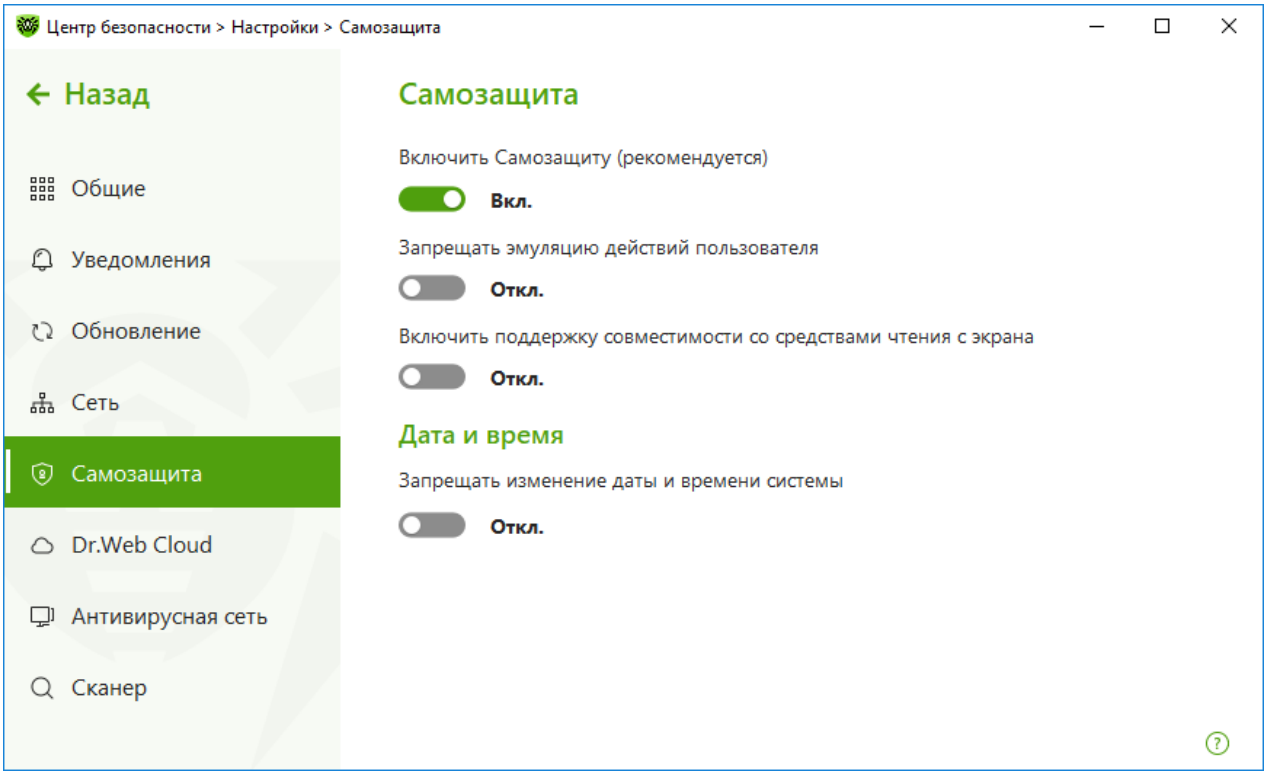

Рисунок 34. Параметры защиты Dr.Web

Настройки Самозащиты

Настройка **Включить Самозащиту (рекомендуется)** позволяет защитить файлы и процессы Dr.Web от несанкционированного доступа. Самозащита включена по умолчанию. Отключать Самозащиту не рекомендуется.

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

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 **Включить поддержку совместимости со средствами чтения с экрана** позволяет использовать программы экранного доступа, такие как JAWS и NVDA, для озвучивания элементов интерфейса Dr.Web. Эта функция делает интерфейс программы доступным для людей с ограниченными возможностями.

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. Вы можете настроить получение уведомлений в том случае, если осуществлялась попытка изменить системное время.

9.6. Dr.Web Cloud

Вы можете подключиться к облачному сервису компании «Доктор Веб» и программе улучшения качества работы продуктов Dr.Web. Облачный сервис собирает информацию о последних угрозах на станциях пользователей, благодаря чему постоянно обновляются вирусные базы и эффективно устраняются новейшие угрозы. Кроме того, обработка данных на облачном сервисе происходит быстрее, чем локально на компьютере пользователя.

В этом разделе:

- Облачный сервис
- Программа улучшения качества ПО

Чтобы включить или отключить Dr.Web Cloud

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите.
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Dr.Web Cloud**.
5. Включите или отключите Dr.Web Cloud при помощи переключателя.

Рисунок 35. Подключение к Dr.Web Cloud

Облачный сервис

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

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

Программа улучшения качества ПО

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

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

9.7. Удаленный доступ к Dr.Web

Чтобы разрешить или запретить удаленное управление продуктом Dr.Web

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите.
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Антивирусная сеть**.
5. Разрешите или запретите удаленное управление продуктом Dr.Web при помощи переключателя.

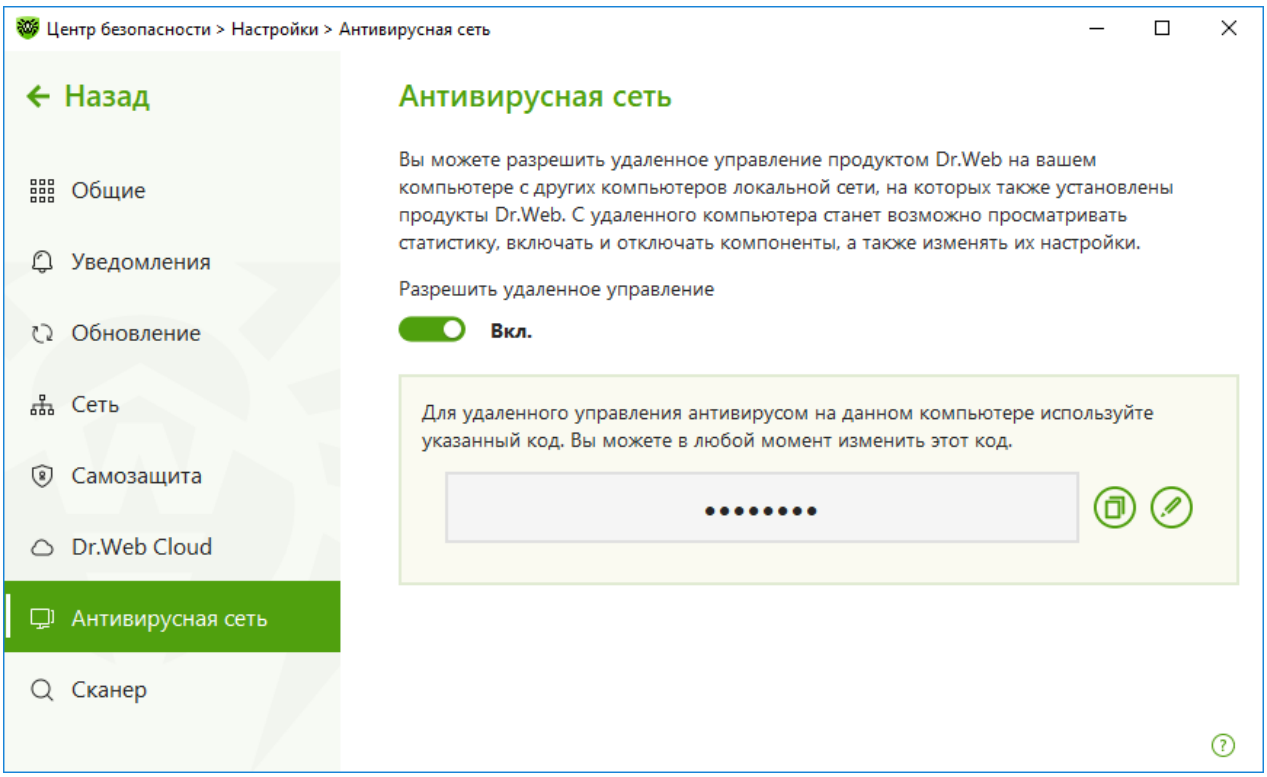

Рисунок 36. Включение удаленного управления антивирусом

Вы можете разрешить доступ к Антивирусу Dr.Web на своем компьютере. Для этого включите опцию **Разрешить удаленное управление** и задайте код, который необходимо будет ввести для удаленного управления вашим антивирусом.

Если вы используете ключ для Dr.Web Security Space, вы можете скачать соответствующую документацию на сайте компании https://download.drweb.com/doc, чтобы ознакомиться с работой компонента Антивирусная сеть.

Удаленное управление позволяет просматривать статистику, включать и отключать модули, а также изменять их настройки. Компоненты Карантин и Сканер недоступны.

9.8. Параметры проверки файлов

Вы можете задать настройки работы сканера, а также изменить действия по умолчанию при обнаружении вредоносных объектов. Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

Чтобы перейти к параметрам проверки файлов

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Сканер**.

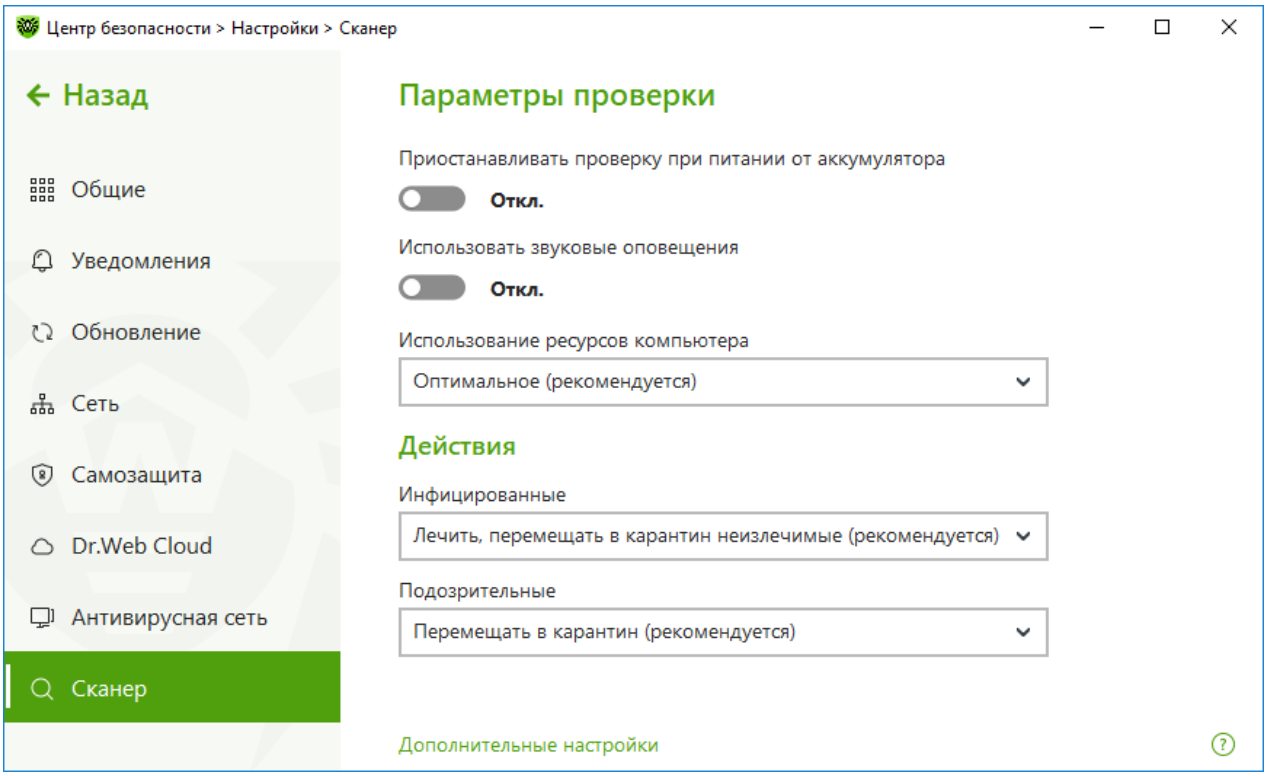

Рисунок 37. Настройка Сканера

Параметры проверки

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

- **Приостанавливать проверку при питании от аккумулятора**. Включите эту опцию, чтобы при переходе на питание от аккумулятора проверка была приостановлена. По умолчанию опция отключена.

- **Использовать звуковые оповещения**. Включите эту опцию, чтобы Сканер Dr.Web сопровождал обнаружение и обезвреживание каждой угрозы 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 этой группе настроек 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.

По умолчанию Сканер пытается вылечить файлы, зараженные известным и потенциально излечимым вирусом, остальные наиболее опасные объекты — перемещает в Карантин. Вы можете изменить реакцию Сканера на обнаружение каждого типа объектов в отдельности. Состав доступных реакций при этом зависит от типа угрозы. Действия, установленные по умолчанию, являются оптимальными и отмечены как рекомендуемые.

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).
Удалить	Удалить объект.

Действие	Описание
	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.

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 возможности

Для перехода к дополнительным настройкам в окне **Параметры проверки** (см. рисунок Настройки сканера) нажмите ссылку **Дополнительные настройки**.

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

Вы также можете настроить поведение Сканера после окончания проверки:

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

10. Файлы и сеть

Данная группа настроек предоставляет доступ к параметрам основных компонентов защиты и к Сканеру.

Чтобы перейти в группу настроек Файлы и сеть

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Файлы и сеть**.

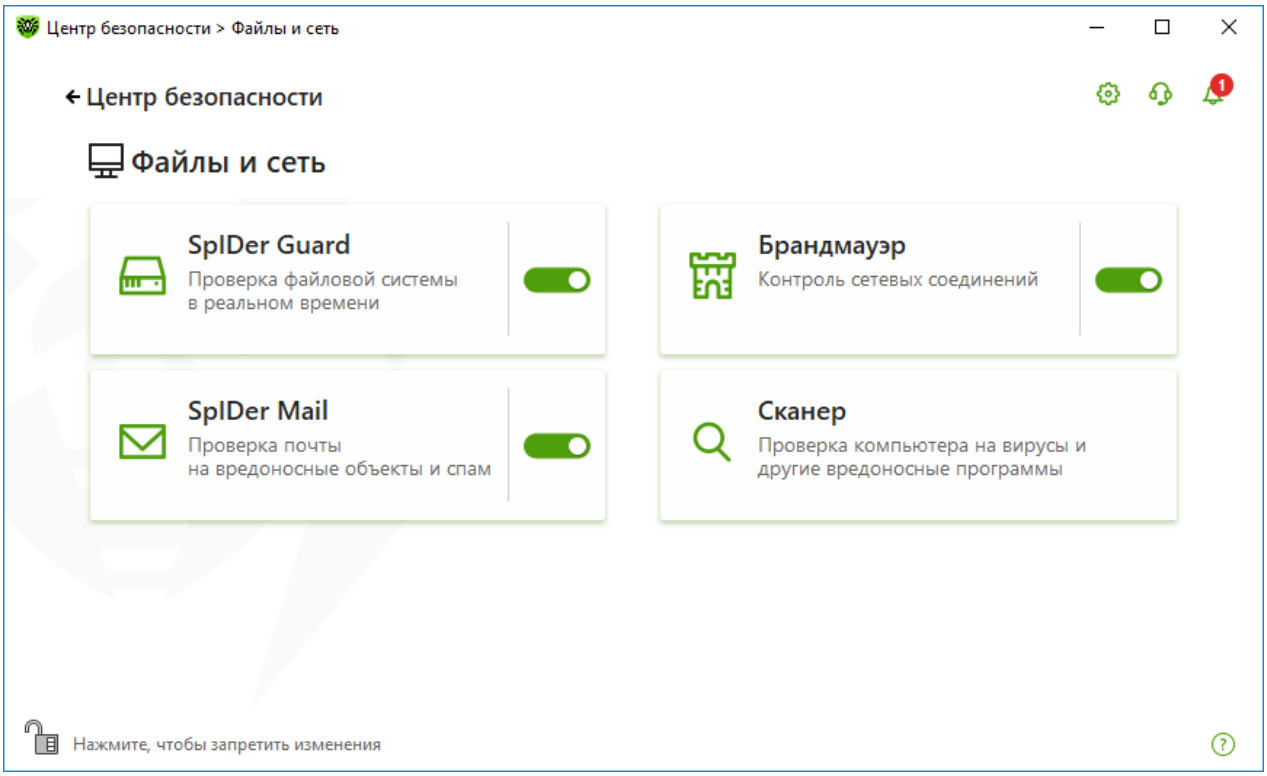

Рисунок 38. Окно Файлы и сеть

Включение и отключение компонентов защиты

Включите или отключите необходимый компонент при помощи переключателя .

Чтобы перейти к параметрам компонентов

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку необходимого компонента.

В этом разделе:

- Монитор файловой системы SpIDer Guard — компонент, проверяющий файлы во время их открытия, запуска или изменения, а также запускаемые процессы в режиме реального времени.
- Почтовый антивирус SpIDer Mail — компонент, проверяющий электронные письма на наличие вредоносных объектов и спама.
- Брандмауэр — компонент, контролирующий подключения и передачу данных по сети, а также блокирующий подозрительные соединения на уровне пакетов и приложений.
- Сканер — компонент, проверяющий объекты по запросу или по расписанию.
- Dr.Web для Microsoft Outlook — модуль Dr.Web для Microsoft Outlook.

Чтобы *отключить* какой-либо из компонентов, Dr.Web должен работать в режиме администратора. Для этого нажмите на замок  в нижней части окна программы.

10.1. Постоянная защита файловой системы

Монитор файловой системы SpIDer Guard защищает компьютер в режиме реального времени и предотвращает его заражение. SpIDer Guard запускается при загрузке операционной системы и проверяет файлы во время их открытия, запуска или изменения, а также отслеживает действия запущенных процессов.

Чтобы включить или отключить монитор файловой системы

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Файлы и сеть**.
3. Включите или отключите монитор файловой системы SpIDer Guard при помощи переключателя .

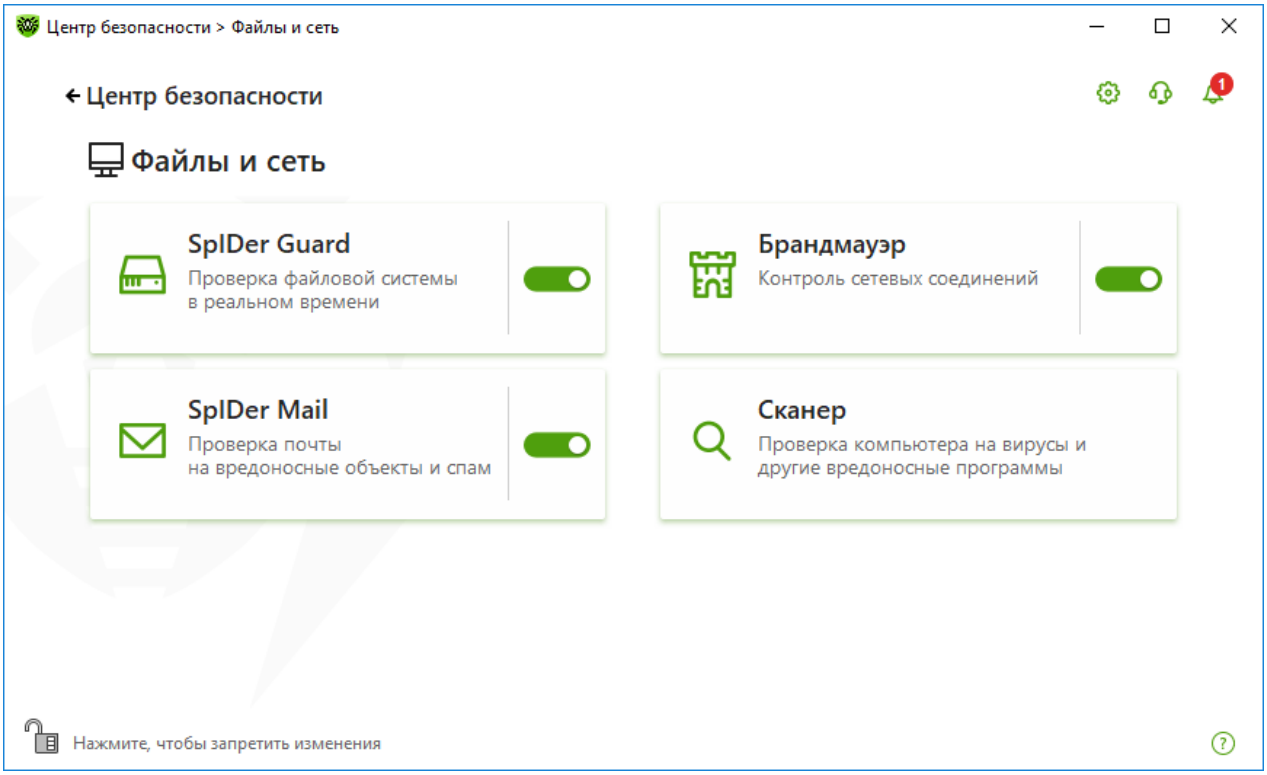

Рисунок 39. Включение/отключение SpIDer Guard

В этом разделе:

- Особенности работы SpIDer Guard
- Проверка съемных носителей
- Действия, применяемые к обнаруженным угрозам
- Выбор режима проверки монитором SpIDer Guard
- Дополнительные настройки

См. также:

- Исключение файлов и папок из проверки
- Исключение приложений из проверки

Особенности работы SpIDer Guard

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

Компонент SpIDer Guard не проверяет файлы внутри архивов, архивов электронной почты и файловых контейнеров. Если какой-либо файл в архиве или почтовом вложении инфицирован, то угроза будет обнаружена при извлечении файла до появления возможности заражения компьютера.

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

Параметры монитора файловой системы SpIDer Guard

При обнаружении зараженных объектов SpIDer Guard применяет к ним действия согласно установленным параметрам. Настройки программы по умолчанию являются оптимальными для большинства случаев, их не следует изменять без необходимости.

Чтобы перейти к параметрам компонента SpIDer Guard

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт» ). В противном случае нажмите на замок  .
2. Нажмите плитку **SpIDer Guard**. Откроется окно параметров компонента.

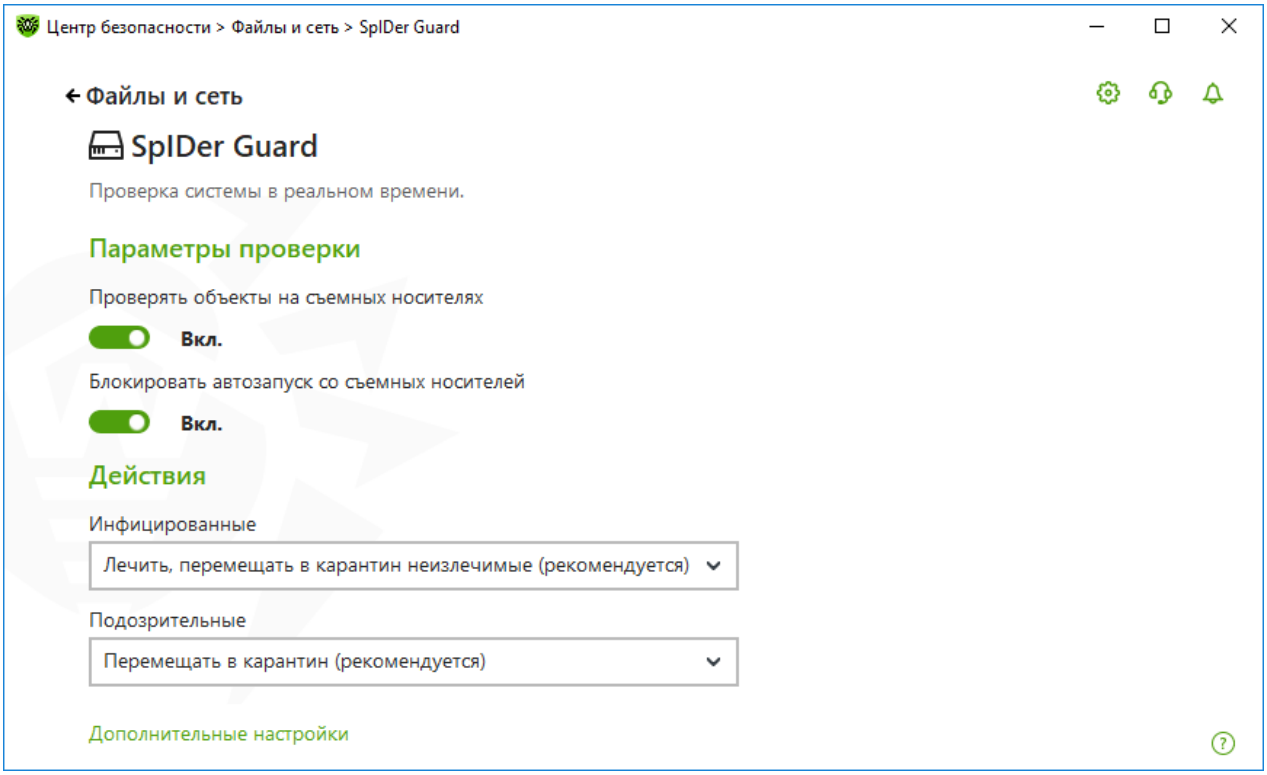

Рисунок 40. Параметры монитора файловой системы

Проверка съемных носителей

SpIDer Guard по умолчанию проверяет открываемые, изменяемые и запускаемые файлы на съемных носителях информации (CD/DVD-дисках, флеш-накопителях и т. д.), а также блокирует автоматический запуск их активного содержимого. Использование этих настроек помогает предотвратить заражение вашего компьютера через съемные носители.

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.

Вы можете включить или отключить опции **Проверять объекты на съемных носителях** и **Блокировать автозапуск со съемных носителей** при помощи переключателя в группе настроек **Параметры проверки**.

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

Действия, применяемые к обнаруженным угрозам

В этой группе настроек вы можете настроить действия, которые Dr.Web должен применять к угрозам в случае обнаружения их монитором файловой системы SpIDer Guard.

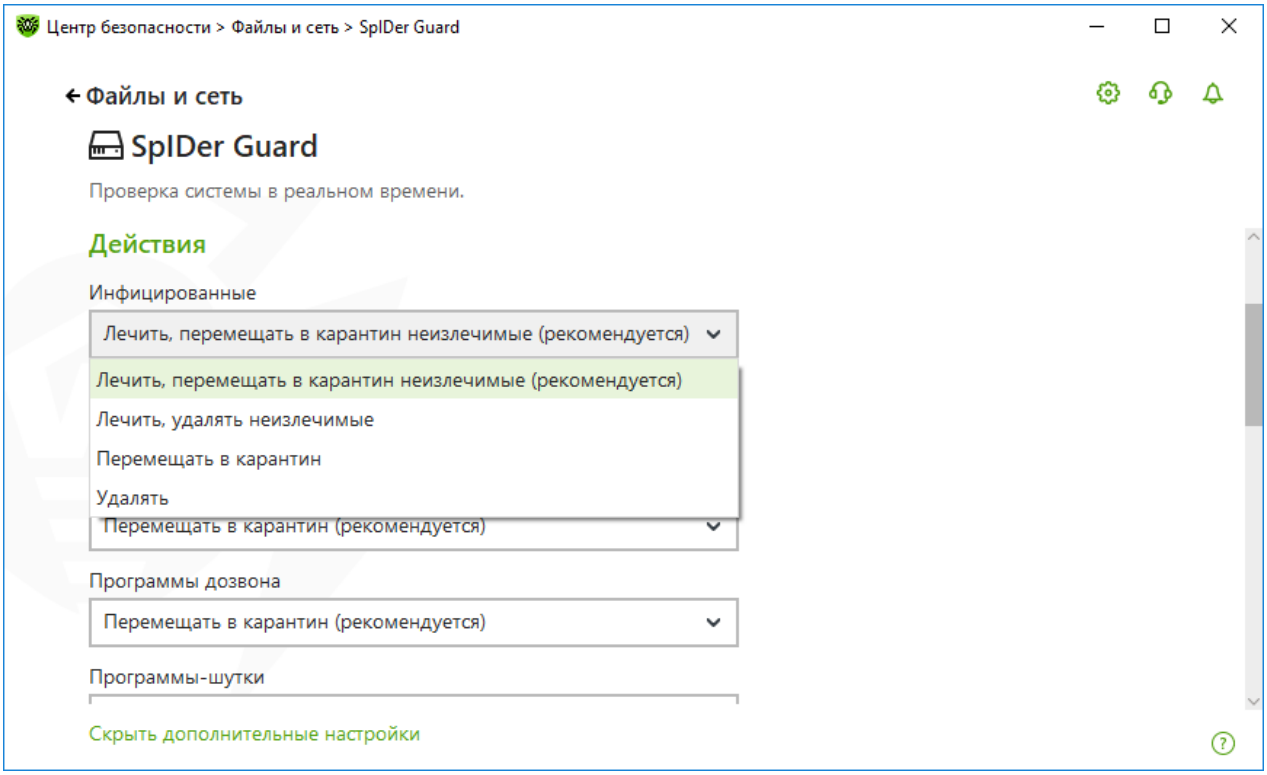

Рисунок 41. Настройка действий, применяемых к угрозам

Действия задаются отдельно для каждого типа вредоносных и подозрительных объектов. Состав доступных действий при этом зависит от типа объектов. По умолчанию установлены рекомендуемые действия для каждого типа объектов. Резервные копии обработанных объектов сохраняются в Карантине.

Возможные действия

К угрозам могут быть применены следующие действия:

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: рекламных программ, программ дозвона, программ-шуток, потенциально опасных программ и программ взлома.

Режим проверки компонентом SpIDer Guard

Для доступа к этому и следующему разделам нажмите ссылку **Дополнительные настройки**.

В этой группе настроек вы можете выбрать режим проверки файлов монитором SpIDer Guard.

Режим	Описание
Оптимальный, используется по умолчанию	В данном режиме проверка производится только в следующих случаях:

Режим	Описание
	• 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 (чтении, записи, запуске). Рекомендуется использовать после проверки всех жестких дисков при помощи Сканера Dr.Web. В этом случае будет исключена возможность проникновения на компьютер новых вирусов или других вредоносных программ через съемные носители, но при этом не будет проводиться повторной проверки уже проверенных, чистых, объектов.
Параноидальный	В данном режиме при любом обращении (создании, чтении, записи, запуске) производится проверка всех файлов и загрузочных секторов на жестких и сетевых дисках, а также на съемных носителях. Данный режим обеспечивает максимальный уровень защиты, но значительно увеличивает нагрузку на компьютер.

Дополнительные возможности

В этой группе настроек вы можете задать параметры проверки на лету, которые будут применяться вне зависимости от выбранного режима работы монитора файловой системы SpIDer Guard. Вы можете включить:

- использование эвристического анализатора;
- проверку загружаемых программ и модулей;
- проверку установочных файлов;
- проверку файлов на сетевых дисках (не рекомендуется);
- проверку компьютера на наличие руткитов (рекомендуется);
- проверку скриптов, выполняемых Windows Script Host и Power Shell (для Windows 10, Windows 11).

Эвристический анализ

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

Фоновая проверка на заражение

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

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

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

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

> При проведении фоновой проверки на наличие руткитов из проверки исключаются файлы и папки, заданные на соответствующей вкладке.

Фоновая проверка на руткиты включена по умолчанию.

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

10.2. Проверка электронной почты

Проверка электронный почты осуществляется компонентом SpIDer Mail. Почтовый антивирус SpIDer Mail устанавливается по умолчанию, постоянно находится в памяти и автоматически запускается при загрузке операционной системы.

SpIDer Mail поддерживает проверку зашифрованного почтового трафика по протоколам POP3S, SMTPS, IMAPS. Для этого необходимо включить опцию **Проверять зашифрованный трафик** в разделе Сеть.

Чтобы включить или отключить проверку электронной почты

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Файлы и сеть**.
3. Включите или отключите почтовый антивирус SpIDer Mail при помощи переключателя.

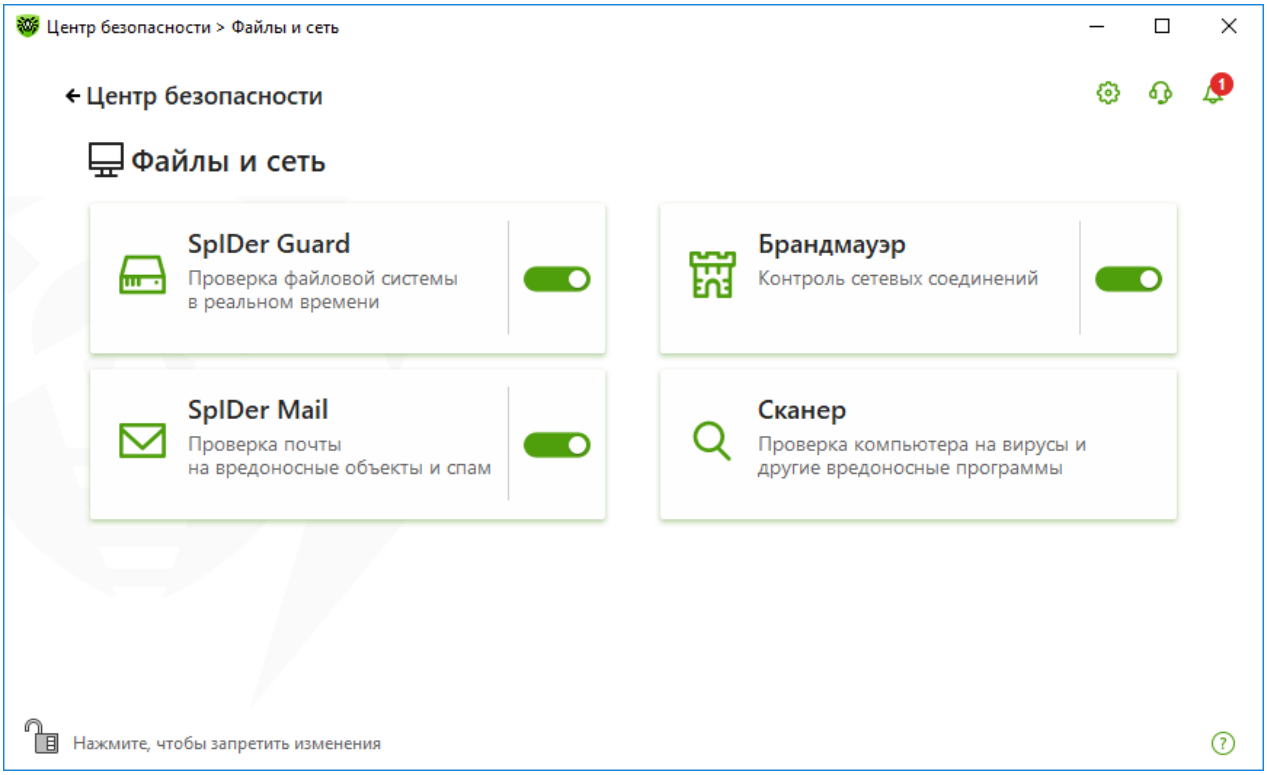

Рисунок 42. Включение/отключение SpIDer Mail

В этом разделе:

- Особенности обработки писем
- Проверка писем другими средствами

См. также:

- Параметры проверки писем

Особенности обработки писем

SpIDer Mail получает все входящие письма вместо почтового клиента и проверяет их. При отсутствии угроз письмо передается почтовому клиенту так, как если бы оно поступило непосредственно с сервера. Аналогично исходящие письма проверяются до отправки на сервер.

Реакция почтового антивируса SpIDer Mail на обнаружение инфицированных и подозрительных входящих писем, а также писем, не прошедших проверку (например, писем с чрезмерно сложной структурой), по умолчанию следующая:

Тип писем	Действие
Зараженные письма	Из таких писем удаляется вредоносное содержимое (это действие называется *лечением* письма), затем они доставляются обычным образом.

Тип писем	Действие
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 проверку	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).

Проверка писем другими средствами

Сканер также может обнаруживать вирусы в почтовых ящиках некоторых форматов, однако почтовый антивирус SpIDer Mail имеет перед ним ряд преимуществ:

- не все форматы почтовых ящиков популярных программ поддерживаются Сканером Dr.Web; при использовании SpIDer Mail зараженные письма даже не попадают в почтовые ящики;
- Сканер проверяет почтовые ящики, но только по запросу пользователя или по расписанию, а не в момент получения почты. Такая проверка является трудоемкой и может занять значительное время.

10.2.1. Параметры проверки писем

По умолчанию SpIDer Mail пытается вылечить письма, зараженные известным и потенциально излечимым вирусом. Неизлечимые и подозрительные письма, а также рекламные программы и программы дозвона перемещаются в Карантин. Остальные письма передаются почтовым монитором без изменений (*пропускаются*). Параметры проверки писем по умолчанию являются оптимальными в большинстве случаев, их не следует изменять без необходимости.

В этом разделе:

- Действия, применяемые к обнаруженным угрозам
- Настройка параметров проверки писем
- Проверка архивов
- Проверка писем, передаваемых по криптографическим протоколам

Параметры проверки писем

Настройки SpIDer 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).

Чтобы приступить к редактированию параметров проверки писем

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Файлы и сеть**.
3. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
4. Нажмите плитку **SpIDer Mail**. Откроется окно параметров компонента.

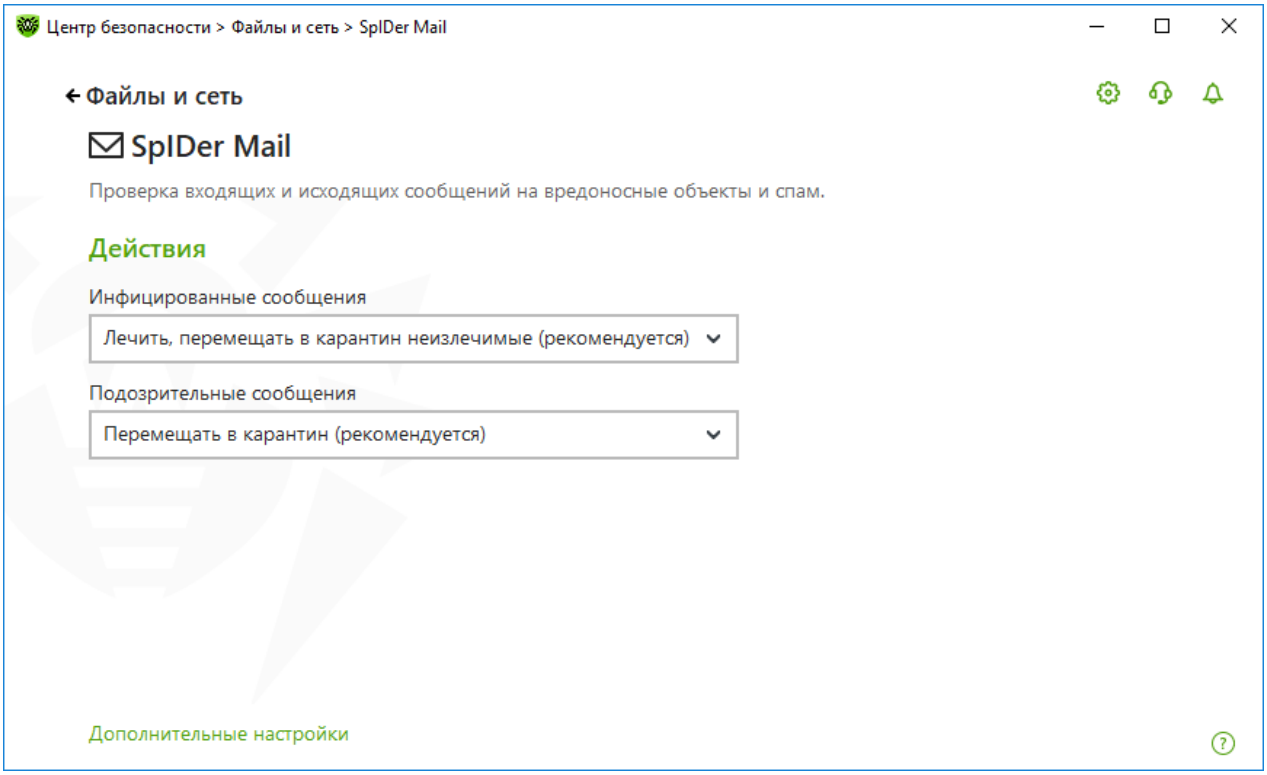

Рисунок 43. Параметры проверки писем

Действия, применяемые к обнаруженным угрозам

В этой группе настроек вы можете настроить действия, которые Dr.Web должен применять к письмам в случае обнаружения в них угрозы.

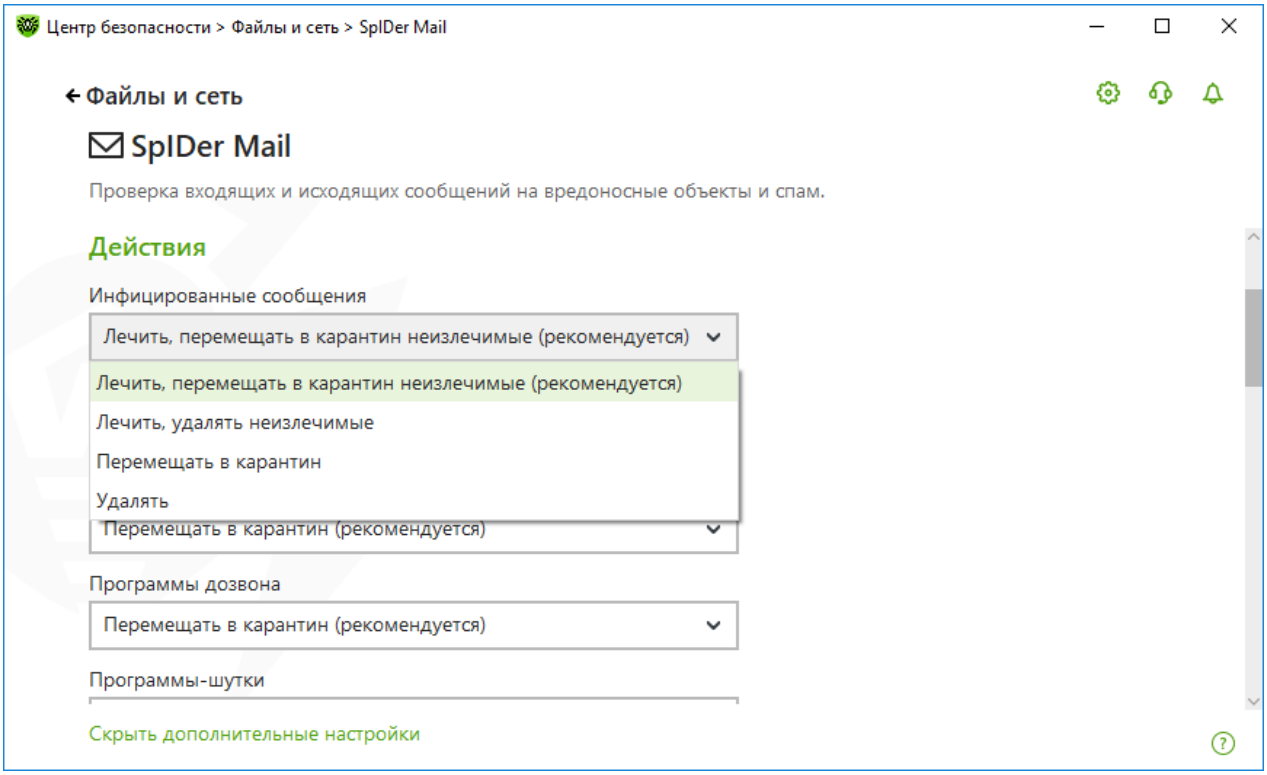

Рисунок 44. Настройка действий, применяемых к письмам

Возможные действия

К угрозам могут быть применены следующие действия:

Действие	Описание
Лечить, перемещать в карантин неизлечимые	Восстановить состояние письма до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для инфицированных писем, зараженных известным излечимым вирусом, за исключением троянских программ, которые при обнаружении удаляются. Лечение файлов в архивах невозможно вне зависимости от типа вируса. Приводит к отказу в передаче письма.
Лечить, удалять неизлечимые	Восстановить состояние письма до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален. Приводит к отказу в передаче письма.
Удалять	Удалить письмо. В этом случае электронное письмо не пересылается получателю, вместо этого почтовой программе передается сообщение о совершенной операции. Приводит к отказу в передаче письма.

Действие	Описание
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. Приводит к отказу в передаче письма.
Игнорировать	Передать письмо без выполнения каких-либо действий над ним.

Вы можете увеличить надежность антивирусной защиты по сравнению с уровнем, предусмотренным по умолчанию. Для этого нажмите ссылку **Дополнительные настройки** и выберите в списке **Непроверенные** пункт **Перемещать в карантин**. Файлы с перемещенными письмами в этом случае рекомендуется впоследствии проверить Сканером Dr.Web.

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

Настройка параметров проверки писем

Для доступа к параметрам проверки писем нажмите ссылку **Дополнительные настройки**.

Действия над письмами

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

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

Оптимизация проверки

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

Проверка архивов

Включите опцию **Проверять архивы**, чтобы SpIDer Mail проверял содержимое архивов, передаваемых по электронной почте. При необходимости включите следующие опции и настроить параметры проверки архивов:

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

> Ограничения для параметра отсутствуют, если задано значение 0.

Дополнительные возможности

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, воспользуйтесь переключателем **Использовать эвристический анализ (рекомендуется)**;
- проверка инсталляционных пакетов. Эта настройка по умолчанию выключена.

Настройка уведомлений

После выполнения предписанного действия SpIDer Mail по умолчанию может выводить соответствующее оповещение в область уведомлений Windows. Вы можете настроить вывод уведомлений на экран и отправку их на электронную почту.

Проверка почты по протоколам POP3S, SMTPS, IMAPS

Чтобы SpIDer Mail проверял данные, передаваемые по криптографическим протоколам, включите опцию **Проверять зашифрованный трафик** в окне Сеть.

10.3. 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 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.

Чтобы включить или отключить Брандмауэр

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Файлы и сеть**.
3. Включите или отключите Брандмауэр при помощи переключателя .

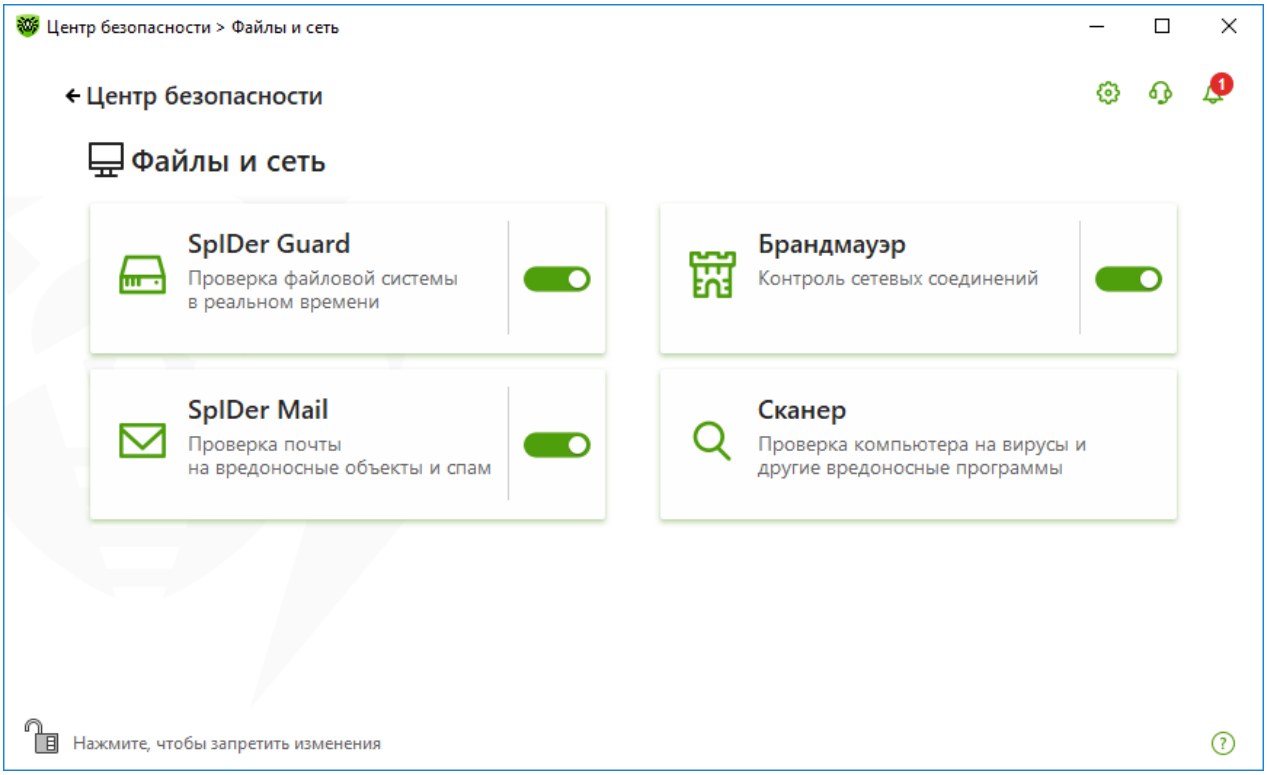

Рисунок 45. Включение/отключение Брандмауэра

В этом разделе:

- Настройка Брандмауэра
- Параметры для приложений
- Правила для приложений
- Настройка параметров правил для приложений
- Параметры для сетей
- Фильтр пакетов
- Набор правил фильтрации пакетов
- Создание правила фильтрации

10.3.1. Параметры работы 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 параметрам Брандмауэра запрашивается пароль, если в настройках вы включили опцию **Защищать настройки Dr.Web паролем**.

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.

Чтобы перейти к выбору режима работы и параметрам компонента Брандмауэр

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт» ). В противном случае нажмите на замок  .
2. Нажмите плитку **Брандмауэр**. Откроется окно параметров компонента.

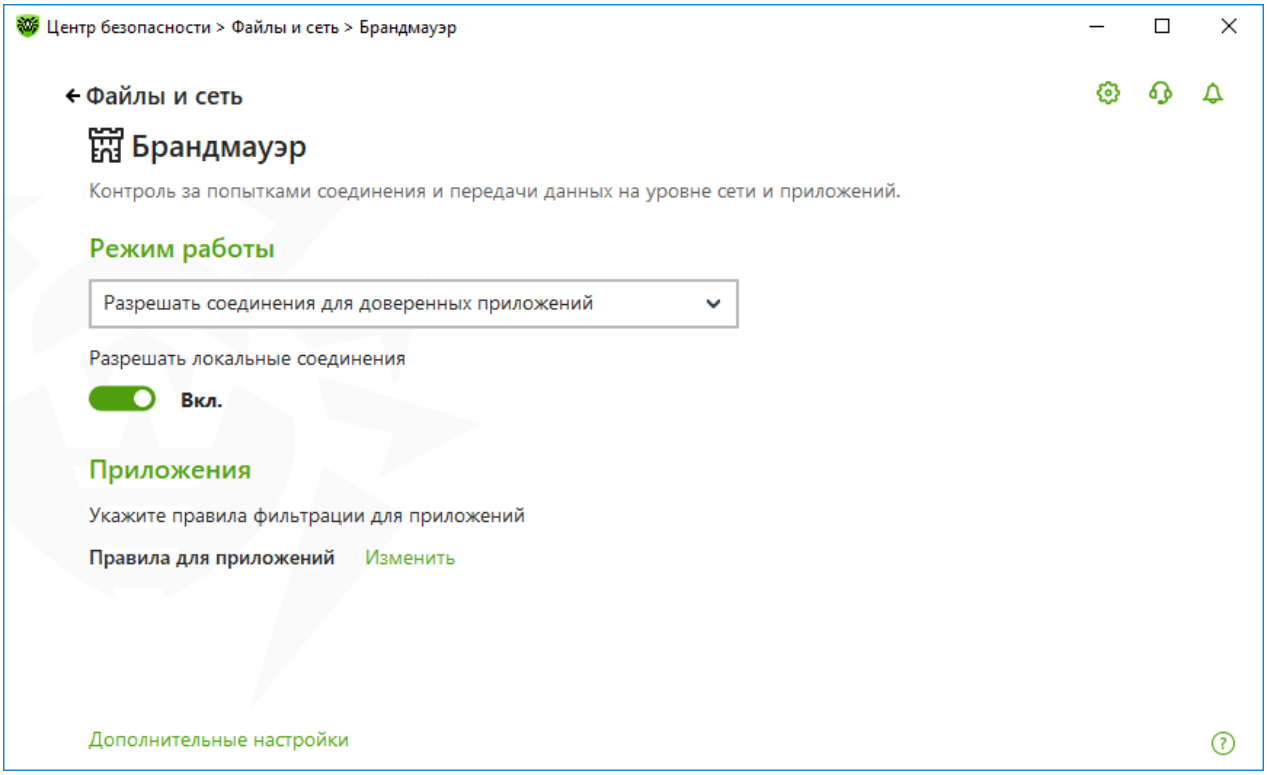

Рисунок 46. Параметры Брандмауэра

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:

Режим работы	Описание
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 с действительной цифровой подписью. Правила для таких приложений не отображаются в списке правил. Для других приложений Брандмауэр предоставляет вам возможность вручную запрещать или разрешать неизвестное соединение однократно, 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. 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

Режим работы	Описание
	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

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`.

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

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.

Правила для приложений

Чтобы перейти в окно Правила для приложений

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Файлы и сеть**.
3. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
4. Нажмите плитку **Брандмауэр**. Откроется окно параметров компонента.
5. В разделе настроек **Правила для приложений** нажмите **Изменить**. Откроется окно со списком приложений, для которых заданы правила.

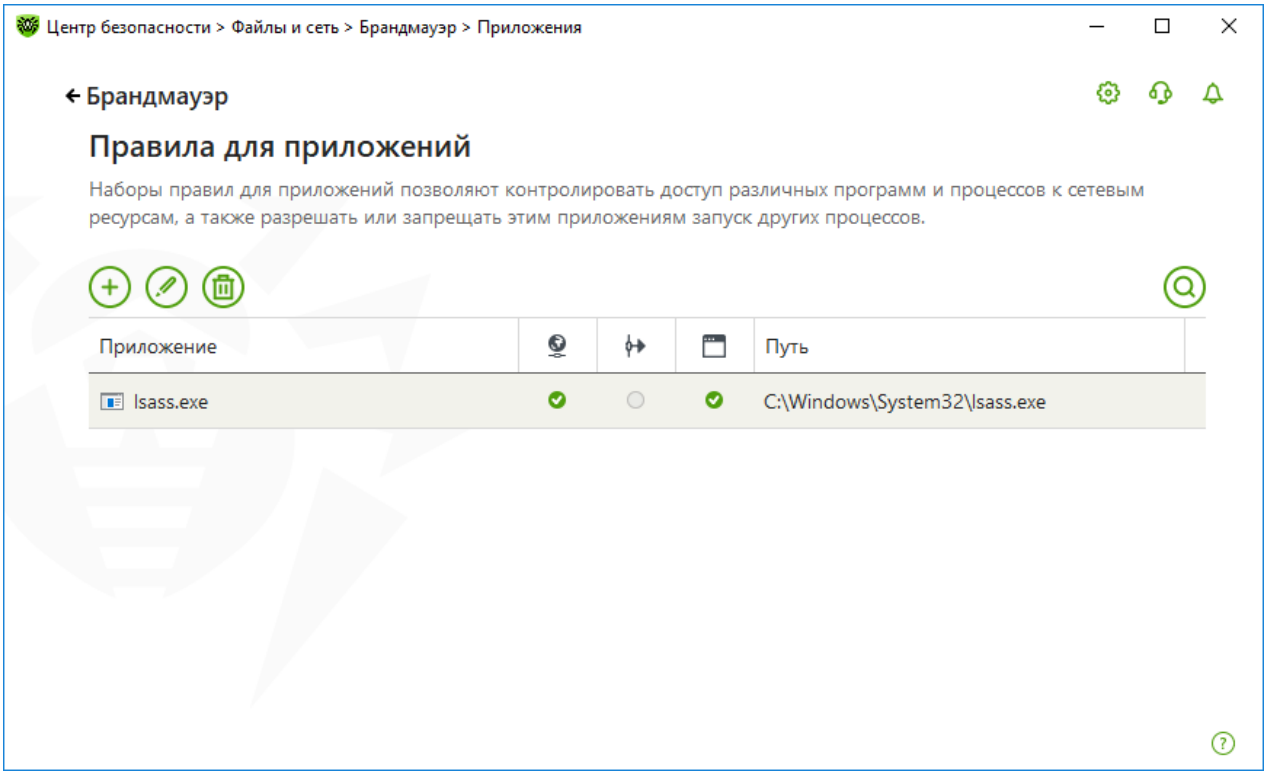

Рисунок 47. Правила для приложений

6. Для перехода к созданию нового набора правил или редактированию существующего нажмите кнопку ⊕ или выберите приложение из списка и нажмите кнопку ✎. Для поиска необходимого правила нажмите кнопку 🔍.

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.

Редактирование существующего или создание нового набора правил

Вы можете настроить доступ приложения к сетевым ресурсам, а также запретить или разрешить запуск других приложений в окне **Новый набор правил для приложения** (или **Редактировать набор правил для *<имя приложения>***).

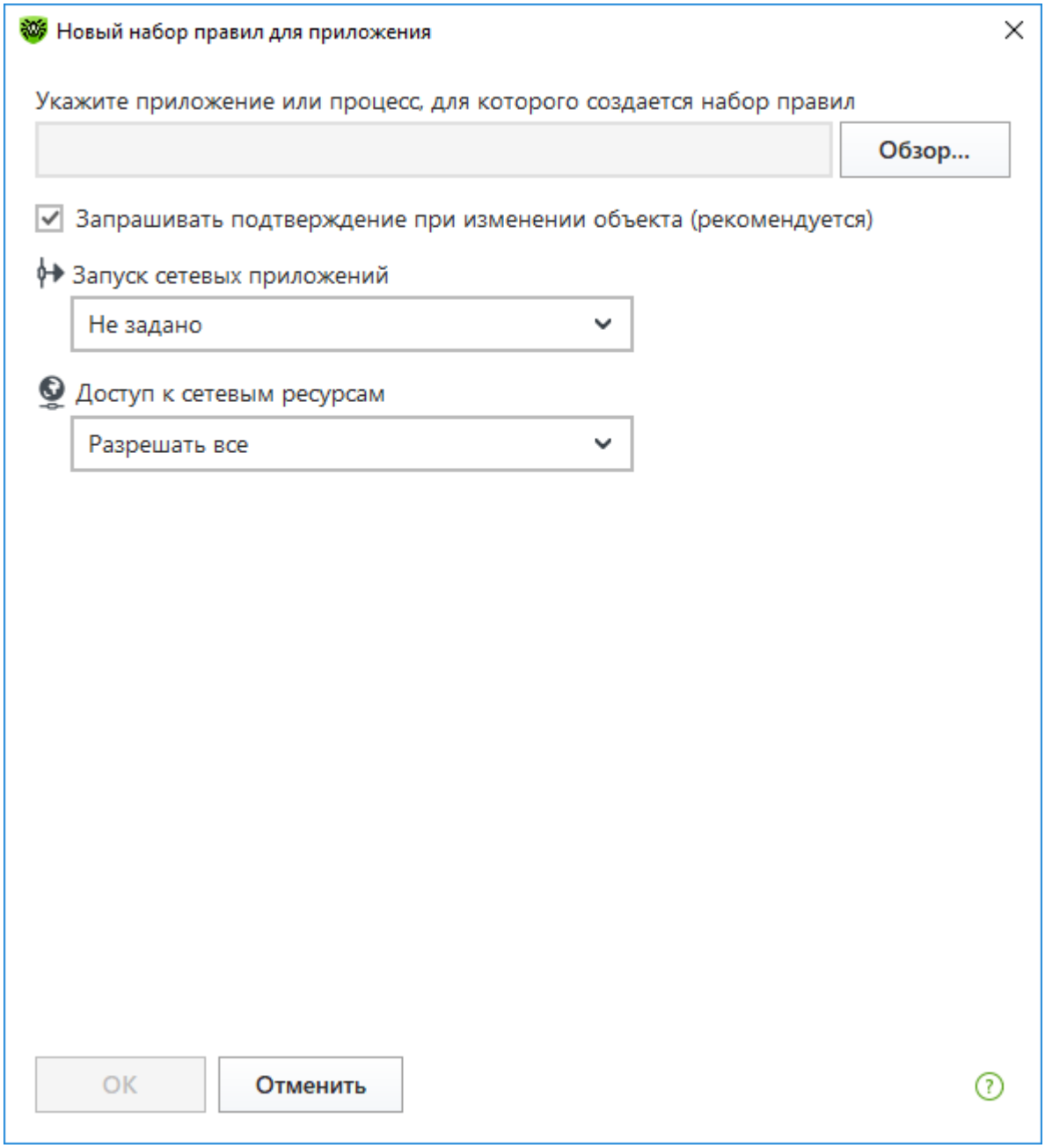

Рисунок 48. Создание нового набора правил

Запуск других приложений

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

- **Разрешать**, чтобы разрешить приложению запускать процессы;
- **Блокировать**, 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 интернету: • **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.

Создание правил для приложений из окна оповещения Брандмауэра

При работе Брандмауэра в интерактивном режиме либо в режиме Разрешать соединения для доверенных приложений, вы можете создать набор правил непосредственно из окна оповещения о попытке несанкционированного подключения.

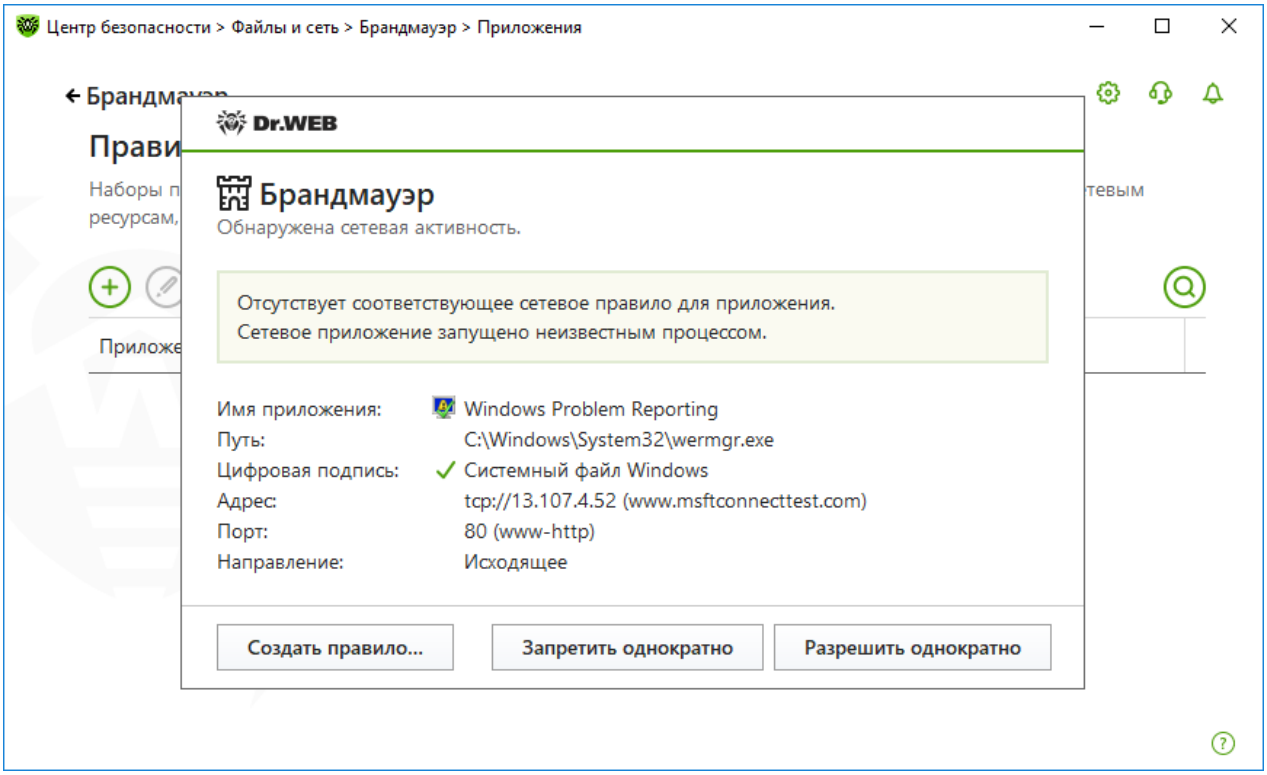

Рисунок 49. Пример предупреждения о попытке доступа к сети

При работе под учетной записью с ограниченными правами (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.

Чтобы задать правила для приложений

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

Поле	Описание
Имя приложения	Наименование программы. Удостоверьтесь, что путь к нему, указанный в поле **Путь**, соответствует правильному расположению программы.
Путь	Полный путь к исполняемому файлу приложения и его имя.

Поле	Описание
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 запретить обращение приложения по указанному порту, выберите действие **Запретить однократно**;
   - чтобы однократно разрешить приложению обращение по указанному порту, 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 по указанному порту, разрешите данное подключение.

Если 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.

Чтобы задать правила для родительских процессов

1. При обнаружении попытки подключения к сети со стороны приложения, запущенного неизвестной для Брандмауэра программой, ознакомьтесь с информацией об исполняемом файле родительской программы.
2. Когда вы примете решение о подходящей для данного случая операции, выполните одно из следующий действий:
   - чтобы однократно блокировать подключение приложения к сети, нажмите кнопку **Заблокировать**;
   - 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.

Настройка параметров правила

Правила фильтрации регулируют сетевое взаимодействие программы с конкретными хостами сети.

Чтобы создать или отредактировать правило

1. В пункте **Доступ к сетевым ресурсам** выберите режим **Пользовательский**.
2. В окне **Редактировать набор правил для** нажмите кнопку для добавления нового правила или выберите правило из списка и нажмите кнопку для редактирования правила.
3. 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 интернету: • **Блокировать пакеты** — блокировать попытку подключения; • **Разрешать пакеты** — разрешить подключение.
Состояние	Состояние правила: • **Включено** — правило применяется; • **Отключено** — правило временно не применяется.
Тип соединения	Направление соединения: • **Входящее** — правило применяется, если соединение инициируется из сети к программе на вашем компьютере;

Параметр	Описание
	• **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**.
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**.

4. Нажмите кнопку **OK**.

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.

Чтобы перейти в окно Сеть

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне выберите раздел **Файлы и сеть**.
3. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
4. Нажмите плитку **Брандмауэр**. Откроется окно параметров компонента.
5. Раскройте группу **Дополнительные настройки**.
6. В разделе настроек **Параметры работы для известных сетей** нажмите **Изменить**. Откроется окно со списком сетевых интерфейсов, для которых заданы правила.

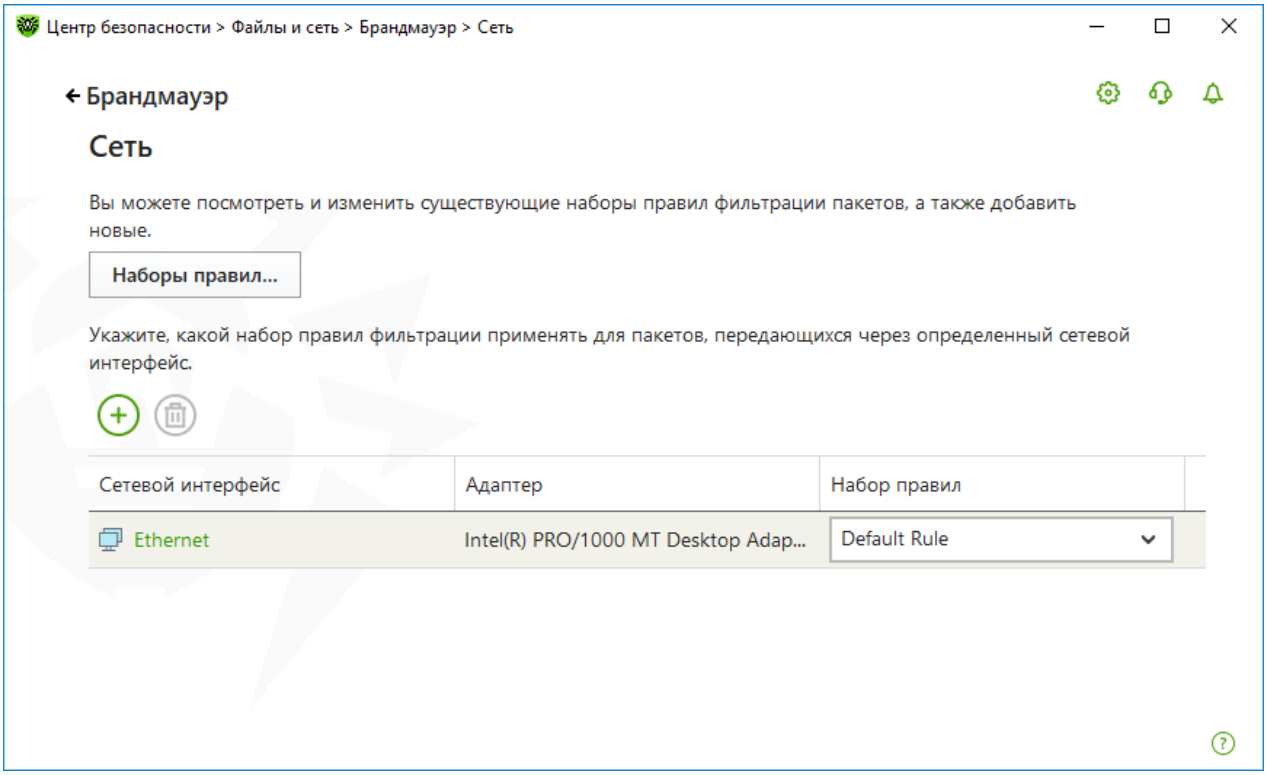

Рисунок 50. Наборы правил для сетевых интерфейсов

7. 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.

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 🗑.

Для просмотра параметров сетевого интерфейса нажмите на его название.

Настройки пакетного фильтра

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

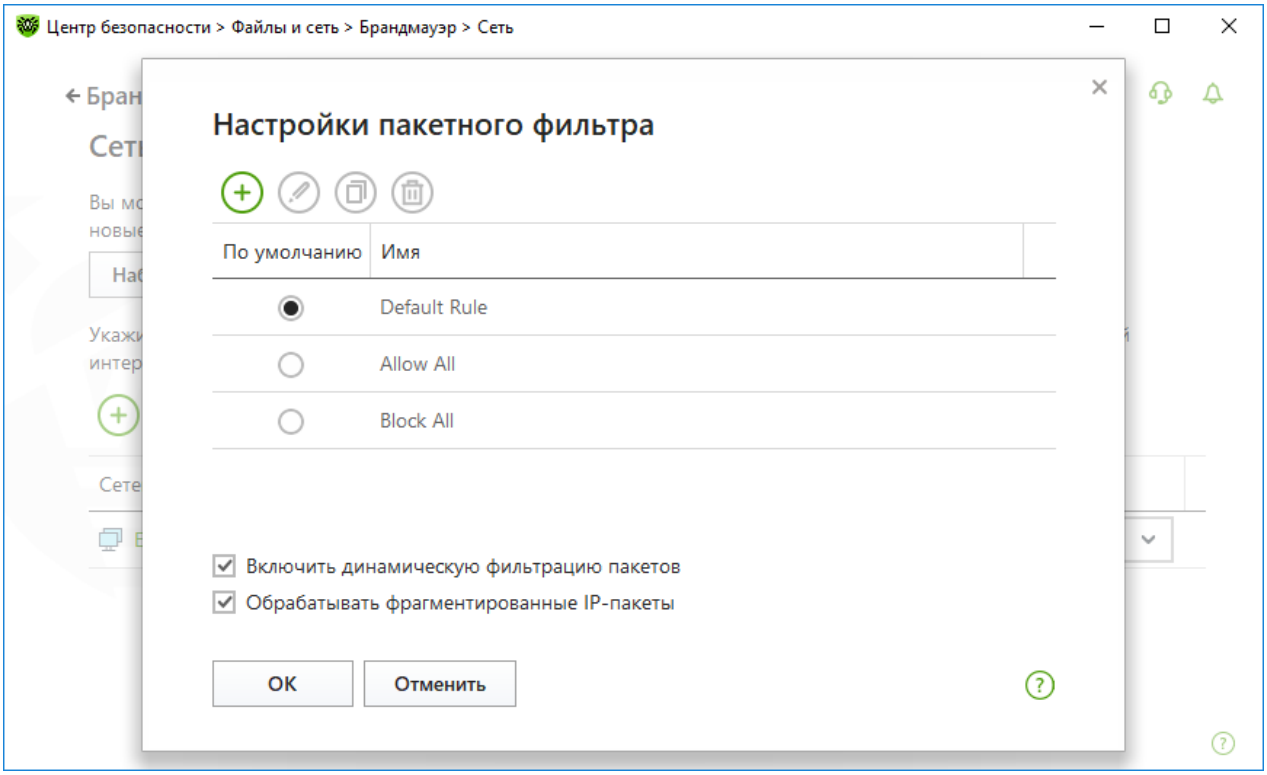

Рисунок 51. Окно Настройки пакетного фильтра

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

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

Набор правил фильтрации пакетов

В окне **Редактировать набор 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.

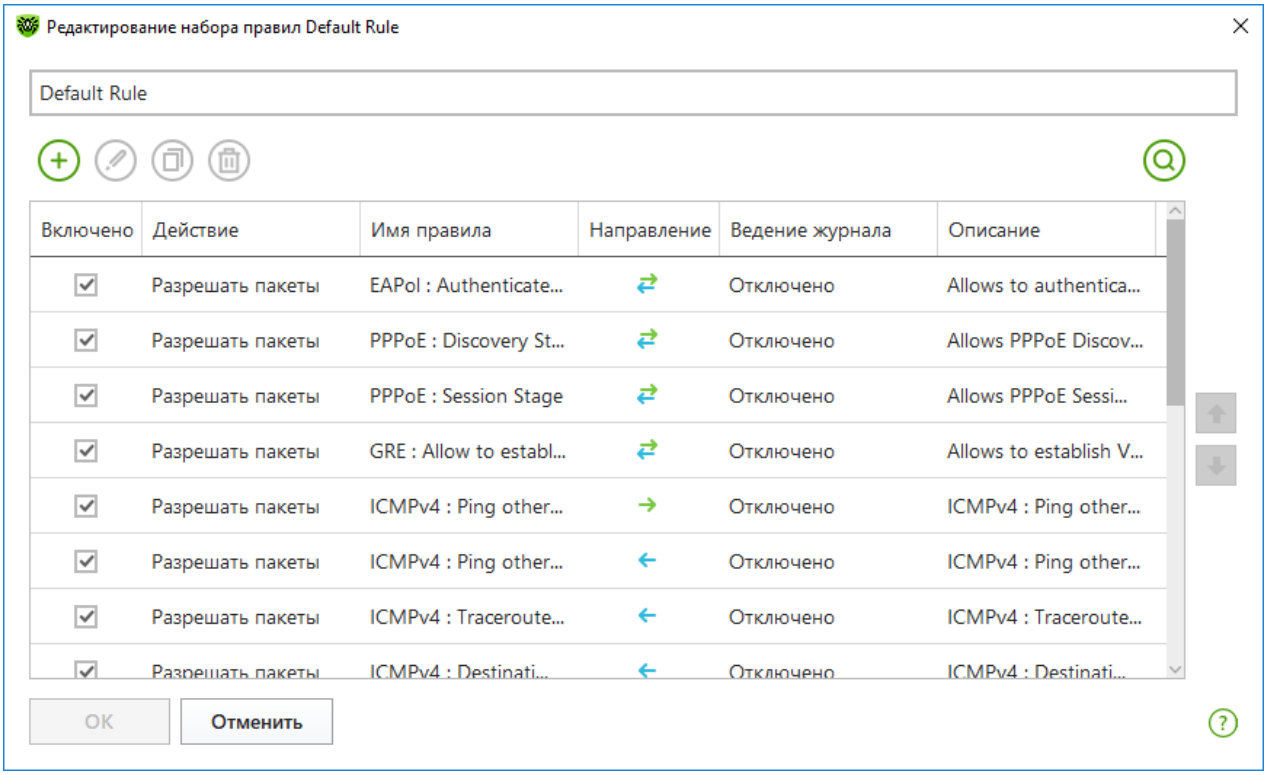

Рисунок 52. Набор правил фильтрации пакетов

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.

Чтобы отредактировать или создать набор 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  ;
   - чтобы найти необходимое правило в списке, 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 **OK** 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.

Настройка параметров правила фильтрации

Чтобы добавить или отредактировать правило фильтрации

1. В окне редактирования набора правил для пакетного фильтра нажмите кнопку  или кнопку  . Откроется окно создания или редактирования правила пакетной фильтрации.

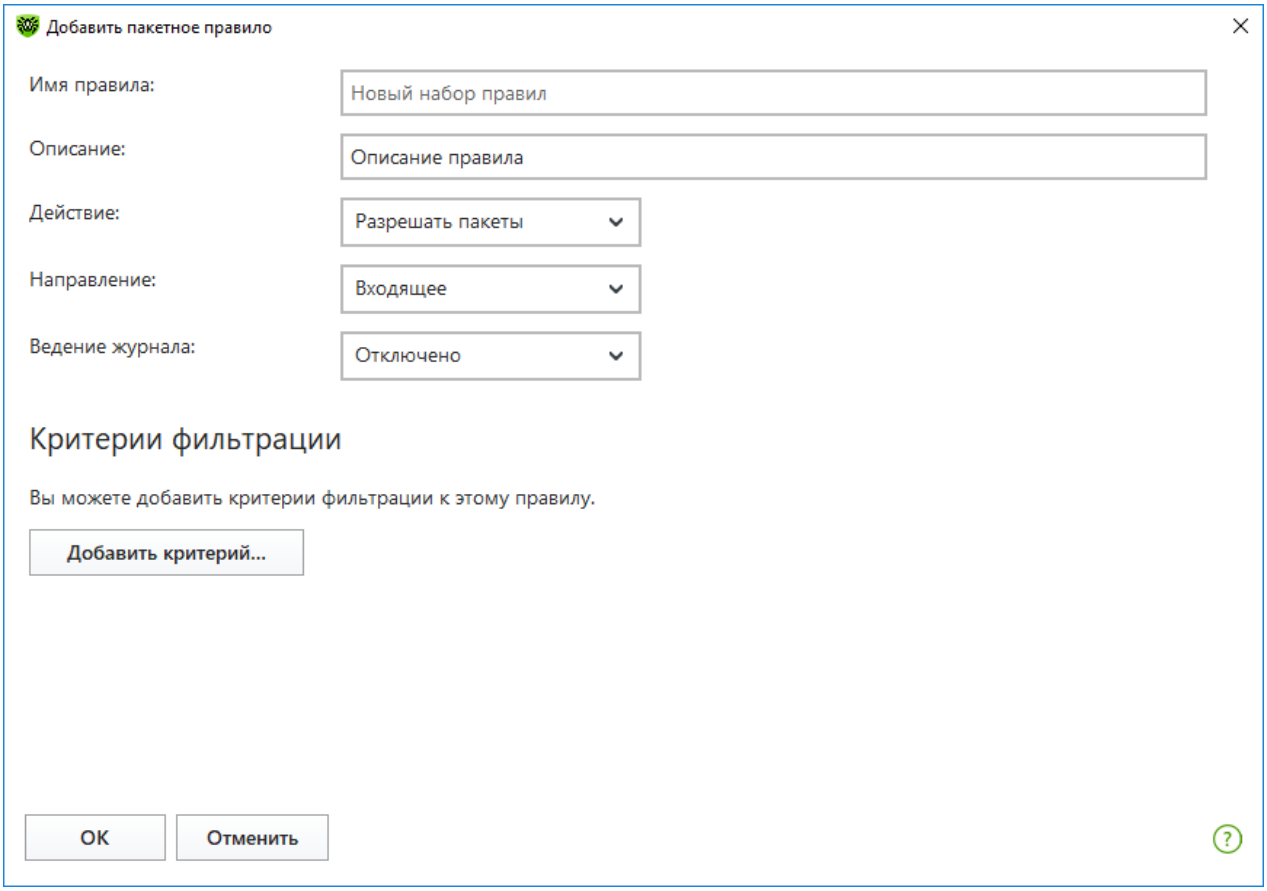

Рисунок 53. Добавление правила фильтрации

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;

Параметр	Описание
	• **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**:

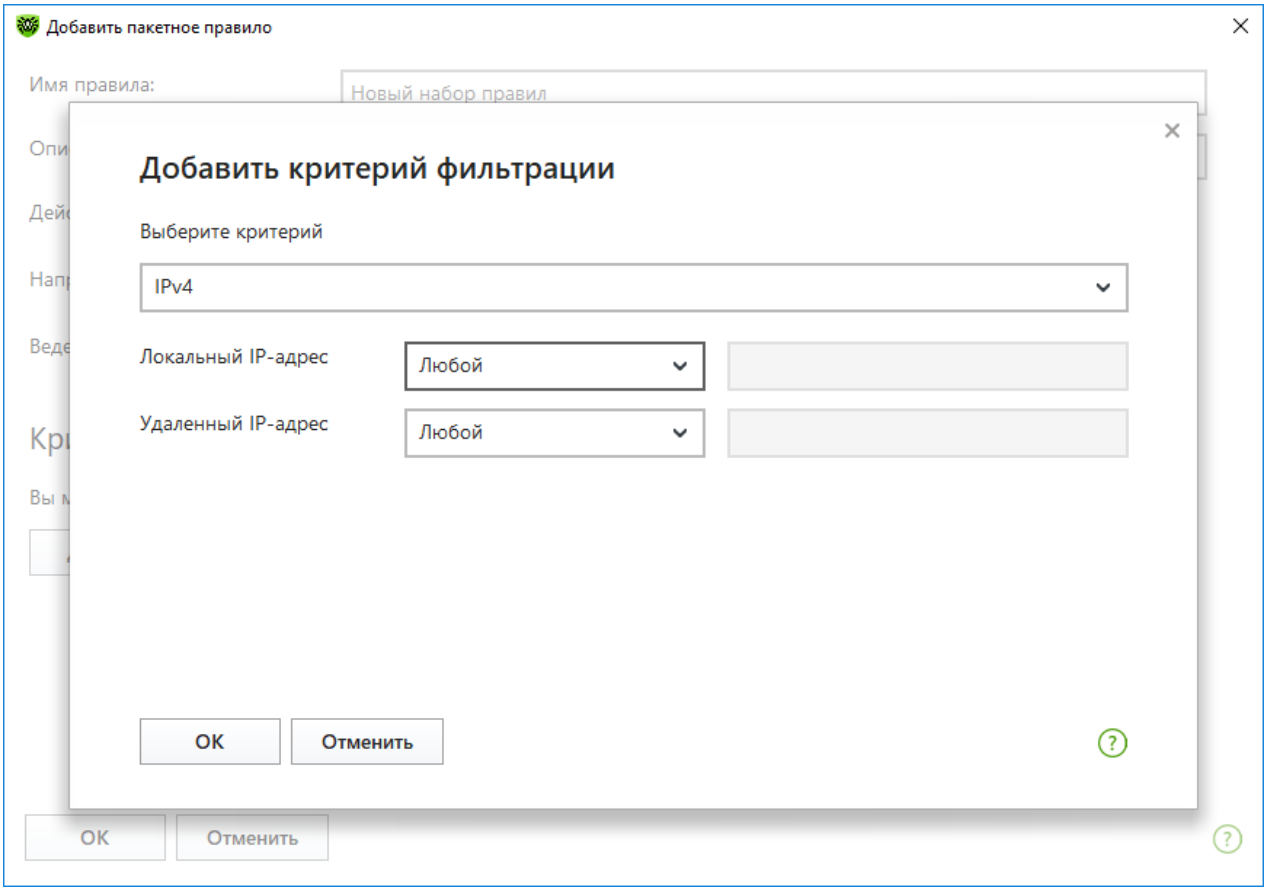

Рисунок 54. Добавление критерия фильтрации

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 **OK** 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.

10.4. Проверка компьютера

Антивирусная проверка компьютера осуществляется компонентом Сканер. Сканер проверяет загрузочные сектора, память, а также отдельные файлы и объекты в составе сложных структур (архивы, контейнеры, электронные письма с вложениями). Проверка производится с использованием всех методов обнаружения угроз.

При обнаружении вредоносного объекта Сканер 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 применить действия по умолчанию ко всем обнаруженным угрозам или выбрать необходимый метод обработки для отдельных объектов.

Действия по умолчанию являются оптимальными в большинстве случаев, но при необходимости вы можете изменить их в окне настройки параметров работы компонента Сканер. Если действие для отдельного объекта вы можете выбрать по окончании проверки, то общие настройки по обезвреживанию конкретных типов угроз необходимо задавать до начала проверки.

См. также:

- Параметры проверки файлов
- Запуск и режимы проверки
- Обезвреживание обнаруженных угроз

10.4.1. Запуск и режимы проверки

Чтобы запустить проверку файлов

> При работе под управлением операционных систем Windows Vista и более поздних Сканер 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.

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Файлы и сеть**, затем — плитку **Сканер**.

Также вы можете запустить проверку файлов, раскрыв в меню **Пуск** группу **Dr.Web** и выбрав пункт **Сканер Dr.Web**.

3. Выберите необходимый режим проверки:
   - пункт **Быстрая**, чтобы проверить только критические области Windows;
   - пункт **Полная**, чтобы проверить все файлы на логических дисках и съемных носителях;
   - пункт **Выборочная**, чтобы проверить только указанные вами объекты. Откроется окно выбора файлов для проверки Сканером.

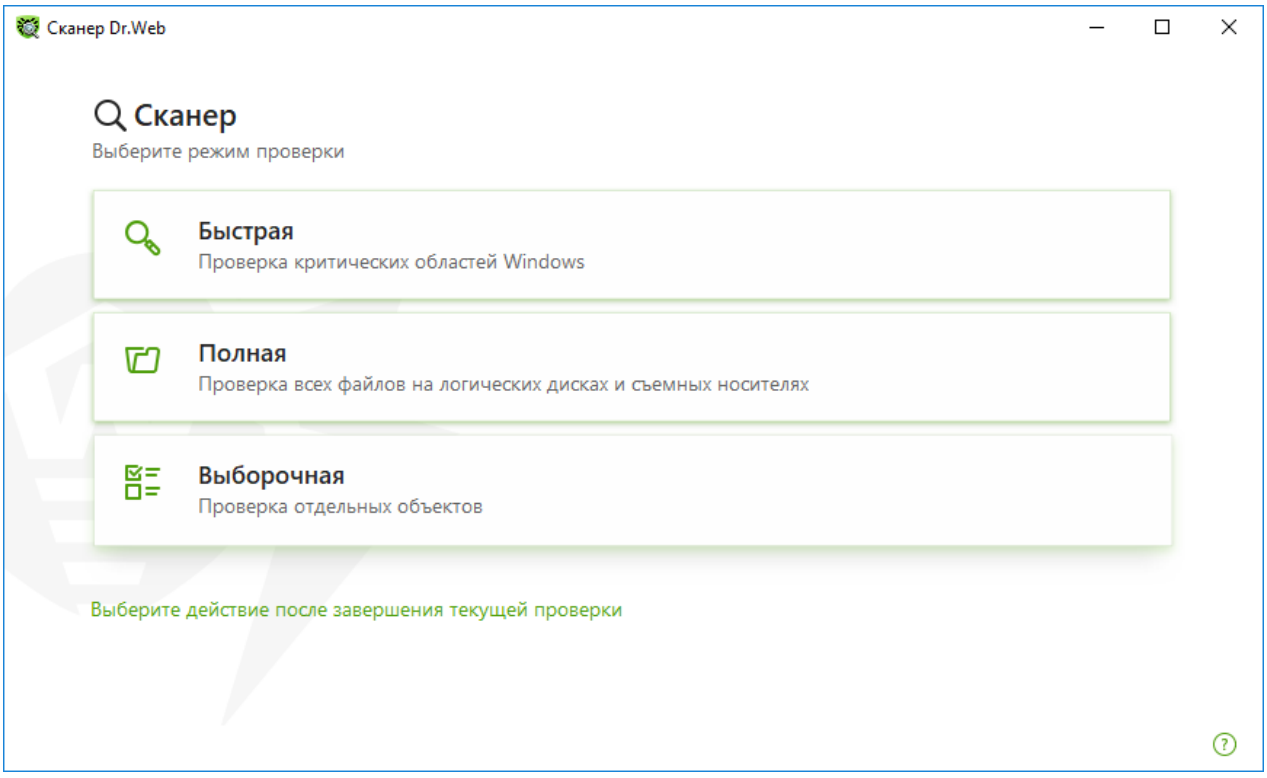

Рисунок 55. Выбор режима проверки

Также вы можете выбрать действие после текущего процесса сканирования, нажав соответствующую ссылку в нижней части окна. Это действие не зависит от выбранного в настройках Сканера и не влияет на общие настройки.

4. Начнется процесс проверки. Чтобы приостановить проверку, нажмите кнопку **Пауза**, чтобы полностью остановить проверку, нажмите кнопку **Стоп**.

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

По окончании проверки Сканер информирует вас об обнаруженных угрозах и предлагает их обезвредить.

Чтобы проверить конкретный файл или папку

1. Вызовите контекстное меню нажатием правой кнопки мыши по имени файла или папки (на рабочем столе или в проводнике операционной системы Windows).
2. Выберите пункт **Проверить с Dr.Web**. Проверка будет выполнена согласно настройкам по умолчанию.

Описание режимов проверки

Режим проверки	Описание
Быстрая	В данном режиме проверяются: • загрузочные секторы 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	В данном режиме производится полная проверка оперативной памяти и всех жестких дисков (включая загрузочные секторы), а также осуществляется проверка на наличие руткитов.
Выборочная	В данном режиме могут быть проверены любые файлы и папки, а также такие объекты, как оперативная память, загрузочные секторы и т. п. Чтобы добавить объекты в список проверки, нажмите кнопку ⊕.

10.4.2. Обезвреживание обнаруженных угроз

По окончании проверки Сканер информирует вас об обнаруженных угрозах и предлагает их обезвредить.

⚠ Если в настройках Сканера Dr.Web вы выбрали пункт **Обезвредить обнаруженные угрозы** или **Обезвредить обнаруженные угрозы и выключить компьютер** для настройки **После завершения проверки**, то обезвреживание угроз будет произведено автоматически.

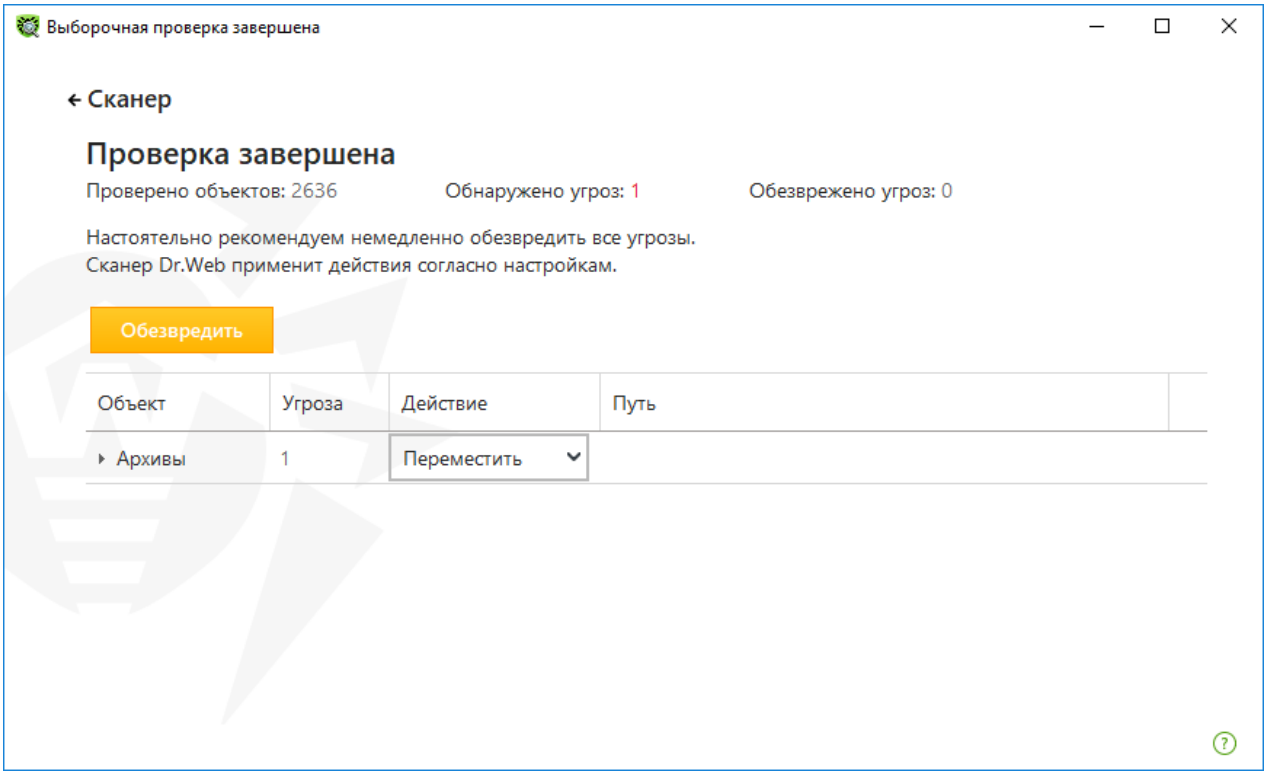

Рисунок 56. Выбор действия по окончании проверки

Таблица с результатами проверки содержит следующую информацию:

Столбец	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 компании «Доктор Веб». Для подозрительных объектов указывается, что объект «возможно, инфицирован» и указывается тип возможного вируса по классификации эвристического анализатора.
Действие	В этом столбце указано действие для найденной угрозы согласно настройкам Сканера. С помощью выпадающего списка вы можете задать действие для выбранной угрозы.
Путь	В этом столбце указан полный путь к соответствующему файлу.

Обезвреживание всех угроз в таблице

Для каждой угрозы указано действие согласно настройкам Сканера. Чтобы обезвредить все угрозы, применяя указанные в таблице действия, нажмите кнопку **Обезвредить**.

Чтобы изменить указанное в таблице действие для угрозы

1. Выберите объект или группу объектов.
2. В столбце **Действие** в выпадающем списке выберите необходимое действие.
3. Нажмите кнопку **Обезвредить**. При этом Сканер начнет обезвреживание всех угроз, указанных в таблице.

Обезвреживание выбранных угроз

Вы также можете обезвредить выбранные угрозы отдельно. Для этого:

1. Выберите объект, несколько объектов (удерживая нажатой клавишу CTRL) или группу объектов.
2. Откройте контекстное меню нажатием правой кнопки мыши и выберите необходимое действие. Сканер начнет обезвреживание только выбранной угрозы (угроз).

Ограничения при обезвреживании угроз

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, установочных пакетов или в составе писем невозможны — действие в таких случаях применяется только ко всему объекту целиком.

Отчет о работе Сканера

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

10.4.3. Дополнительные возможности

В этом разделе содержится информация о дополнительных возможностях работы Сканера:

- Запуск Сканера с параметрами командной строки
- Консольный сканер
- Запуск проверки по расписанию

Запуск Сканера с параметрами командной строки

Вы можете запускать Сканер в режиме командной строки. Такой способ позволяет задать дополнительные настройки текущего сеанса проверки и перечень проверяемых объектов в качестве параметров запуска. Именно в таком режиме возможен автоматический запуск Сканера по расписанию.

Синтаксис команды запуска следующий:

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

Ключи — параметры 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.

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.

Чаще употребляются 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.

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.

Консольный сканер помещает подозрительные объекты 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

Запуск проверки в Планировщике заданий Windows

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.

10.5. Dr.Web для Microsoft Outlook

Основные функции компонента

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

- антивирусную проверку вложенных файлов входящих почтовых сообщений;
- проверку почты, поступающей по зашифрованному соединению SSL;
- обнаружение и нейтрализацию вредоносного программного обеспечения;
- эвристический анализ для дополнительной защиты от неизвестных вирусов.

Настройка модуля Dr.Web для Microsoft Outlook

Настройка параметров и просмотр статистики работы программы осуществляются 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 Microsoft 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;
- Статистика — показывает данные об объектах, проверенных и обработанных программой.

10.5.1. Проверка на вирусы

Dr.Web для Microsoft 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 Microsoft 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 Microsoft 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 Microsoft 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;
- **Удалить** — означает, что объект будет удален;
- **Переместить в карантин** — означает, что объект будет изолирован в папке Карантина;
- **Игнорировать** — означает, что объект будет пропущен без изменений.

10.5.2. Регистрация событий

Dr.Web для Microsoft 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 ключевого файла: действительность или недействительность лицензии, срок действия лицензии (информация заносится при запуске программы, в процессе ее работы и при замене ключевого файла);
- параметры модулей программы: сканера, ядра, вирусных баз (информация заносится при запуске программы и при обновлении модулей);
- сообщение о недействительности лицензии: отсутствие ключевого файла, отсутствие в ключевом файле разрешения на использование модулей программы, лицензия заблокирована, нарушение целостности ключевого файла (информация заносится при запуске программы и в процессе ее работы);
- сообщения об обнаружении вирусов;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 день до окончания срока).

Чтобы просмотреть журнал регистрации событий операционной системы

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

Текстовый журнал отладки

В текстовый журнал отладки заносится следующая информация:

- сообщения о действительности или недействительности лицензии;
- сообщения об обнаружении вирусов;
- сообщения об ошибках записи или чтения файлов, ошибках анализа архивов или файлов, защищенных паролем;
- параметры модулей программы: сканера, ядра, вирусных баз;
- сообщения об экстренных остановках ядра программы;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 день до окончания срока).

Чтобы настроить регистрацию 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 Microsoft 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.

Чтобы просмотреть журнал событий программы

1. На вкладке **Антивирус Dr.Web** нажмите кнопку **Журнал**. Откроется окно настроек журнала.
2. Нажмите кнопку **Показать в папке**. Откроется папка, в которой хранится журнал.

10.5.3. Статистика проверки

В почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web** (для Microsoft Outlook 2010 в разделе **Файл** → **Параметры** → **Надстройки** необходимо выбрать **Dr.Web для Microsoft 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 объектов и писем;
- **Инфицированных** — общее количество зараженных объектов во вложениях писем;
- **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 объектов и 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;
- **Проигнорировано** — количество объектов, пропущенных без изменений;
- **Спам-писем** — количество писем, распознанных как спам.

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

Статистическая информация накапливается в рамках одной сессии. После перезагрузки компьютера или при рестарте Антивирус для Windows статистика обнуляется.

11. Превентивная защита

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

Чтобы перейти в группу настроек Превентивная защита

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.

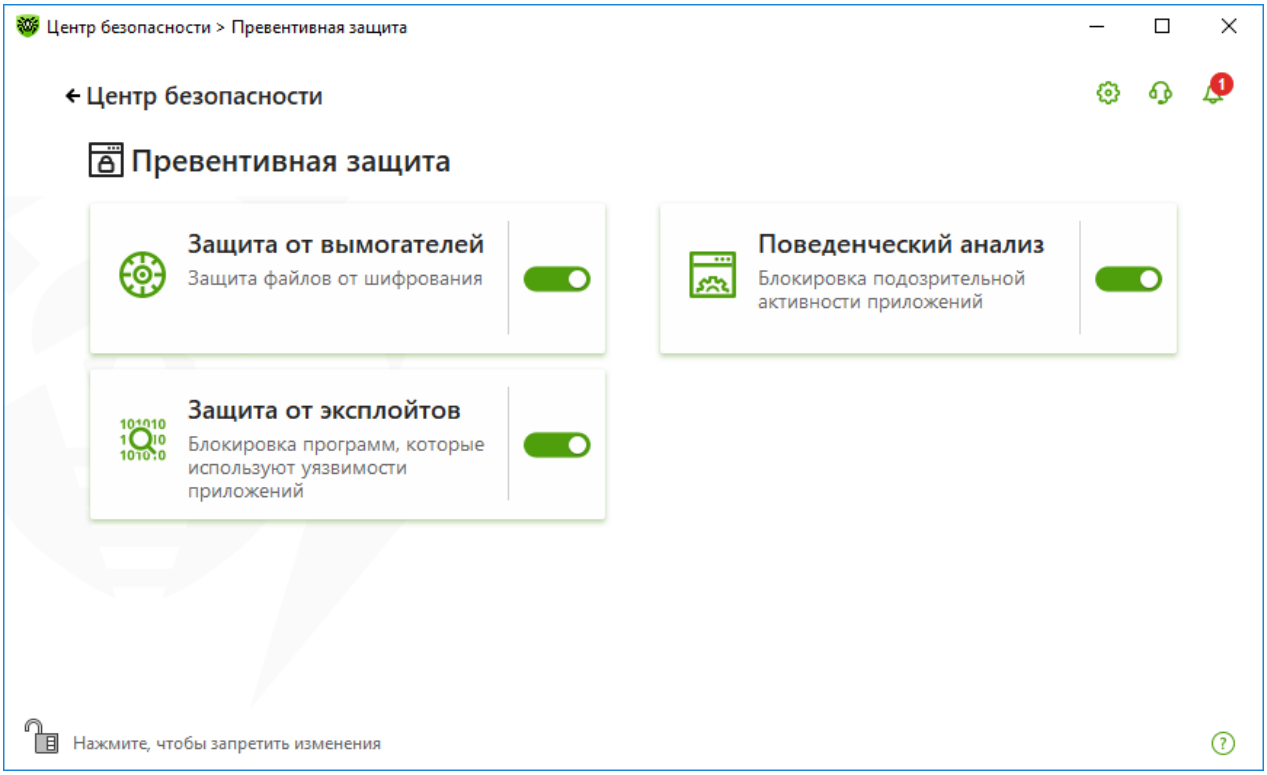

Рисунок 57. Окно Превентивная защита

Включение и отключение компонентов защиты

Включите или отключите необходимый компонент при помощи переключателя .

Чтобы перейти к параметрам компонентов

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку необходимого компонента.

В этом разделе:

- Поведенческий анализ — параметры запрета доступа приложений к системным объектам.
- Защита от вымогателей — параметры запрета шифрования файлов пользователей.
- Защита от эксплойтов — параметры запрета использования уязвимостей в приложениях.

> Чтобы *отключить* какой-либо из компонентов, Dr.Web должен работать в режиме администратора. Для этого нажмите на замок в нижней части окна программы.

11.1. Защита от вымогателей

Компонент Защита от вымогателей позволяет отслеживать процессы, которые пытаются зашифровать пользовательские файлы по известному алгоритму, свидетельствующему о том, что такие процессы являются угрозой безопасности компьютера. К таким процессам относятся *троянцы-шифровальщики*. Данные вредоносные программы, попадая на компьютер пользователя, блокируют доступ к данным, после чего вымогают деньги за расшифровку. Они являются одними из самых распространенных вредоносных программ и ежегодно приносят большие убытки как компаниям, так и обычным пользователям. Основной путь заражения — почтовые рассылки, содержащие вредоносный файл или ссылку на вирус.

По статистике компании «Доктор Веб» расшифровка поврежденных троянцем файлов возможна только в 10 % случаев, поэтому наиболее эффективный метод борьбы — предотвратить заражение. В последнее время число пользователей, пострадавших от данного типа вирусов, снижается. Тем не менее, количество запросов в службу технической поддержки компании «Доктор Веб» на расшифровку данных достигает 1000 в месяц.

Чтобы включить или отключить компонент Защита от вымогателей

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.
3. Включите или отключите компонент Защита от вымогателей при помощи переключателя.

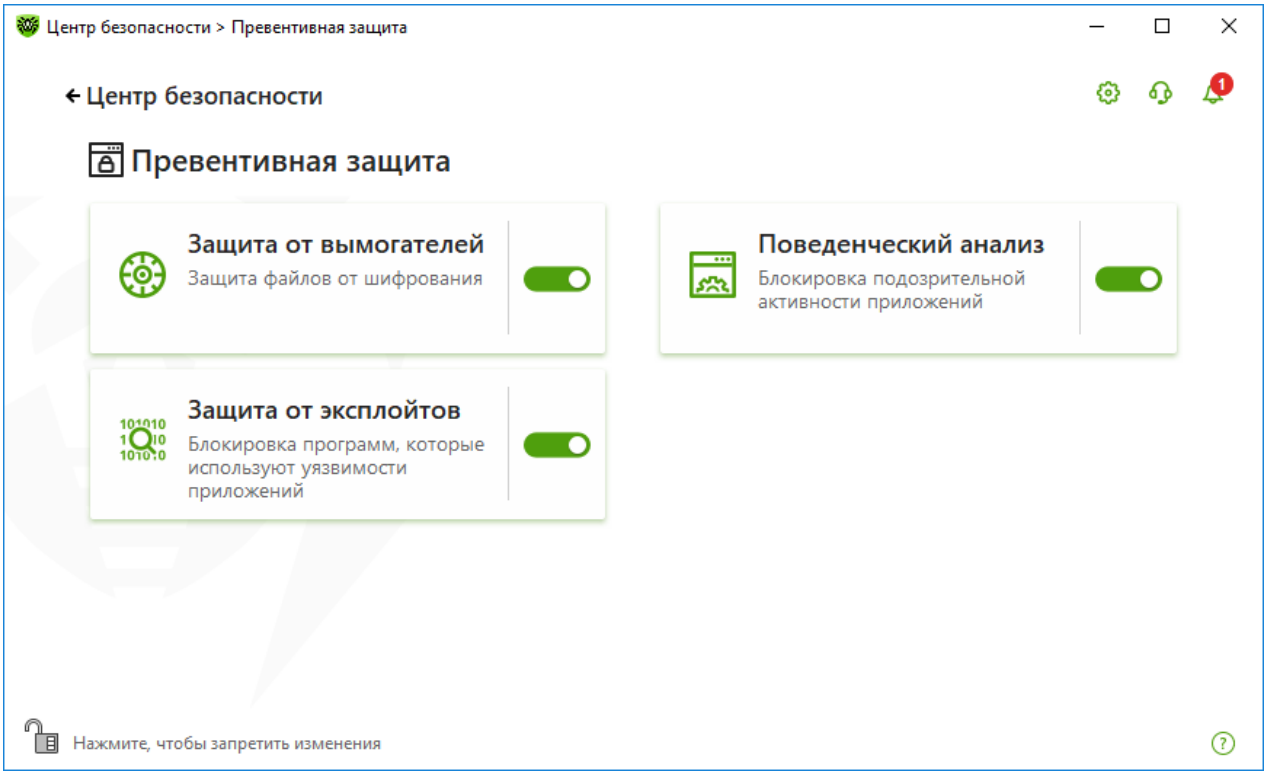

Рисунок 58. Включение/отключение компонента Защита от вымогателей

В этом разделе:

- Настройка реакции на попытки приложений зашифровать файлы
- Исключения из проверки

Реакция Dr.Web на попытки приложений зашифровать файл

Чтобы настроить параметры компонента Защита от вымогателей

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку **Защита от вымогателей**. Откроется окно параметров компонента.
3. В выпадающем меню выберите действие, которое будет применяться для всех приложений.

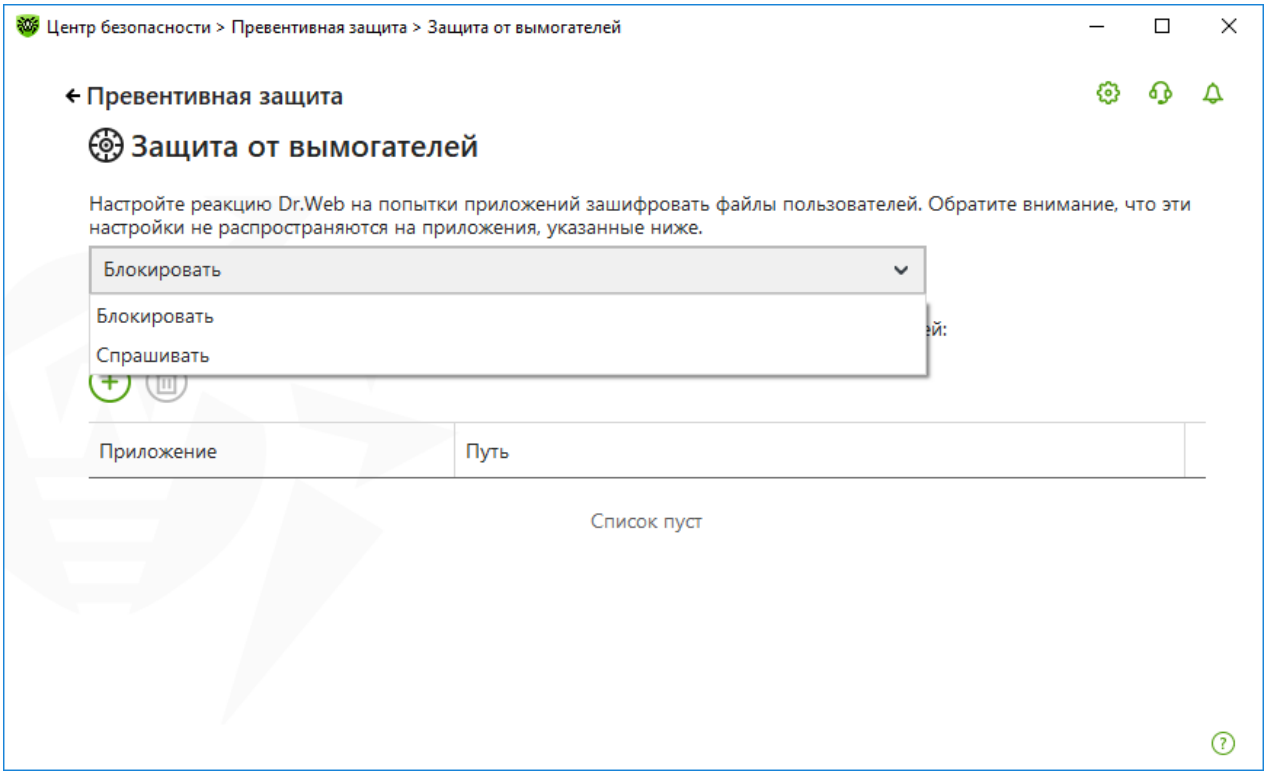

Рисунок 59. Выбор реакции Dr.Web

- **Блокировать** — всем приложениям будет запрещено шифровать файлы пользователя. Этот режим установлен по умолчанию. При попытке приложения зашифровать файлы пользователя будет показано уведомление:

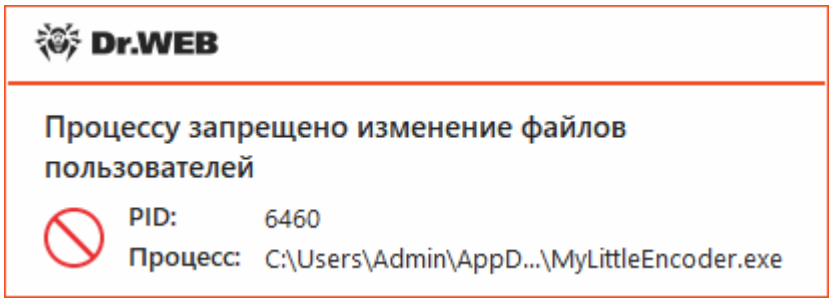

Рисунок 60. Пример уведомления о запрете изменения файлов пользователя

- **Спрашивать** — при попытке приложения зашифровать файл пользователя будет показываться уведомление, где вы сможете запретить приложению это действие или проигнорировать его:

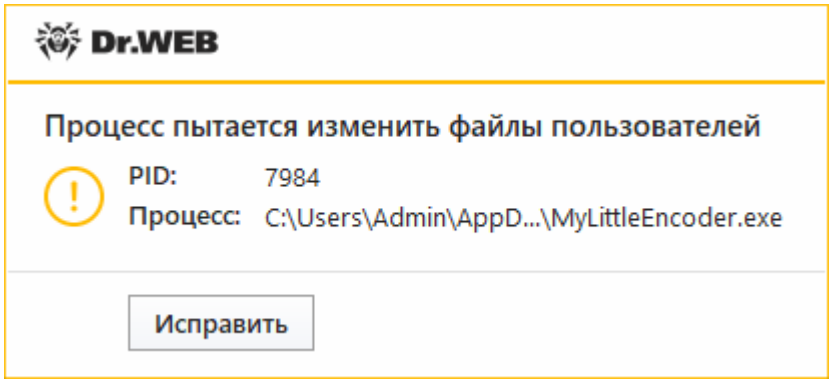

Рисунок 61. Пример уведомления о попытке изменения файлов пользователя

- Если вы нажмете кнопку **Исправить**, процесс будет заблокирован и занесен в карантин. Даже при восстановлении приложения из карантина оно не сможет быть запущено до перезагрузки компьютера.
- Если вы закроете окно уведомления, приложение не будет обезврежено.

Получение уведомлений

Вы можете настроить вывод уведомлений о действиях компонента Защита от вымогателей на экран и отправку этих уведомлений на электронную почту.

См. также:

- Уведомления

Список приложений, исключенных из проверки

Вы можете сформировать список приложений, которые будут исключены из проверок компонентом Защита от вымогателей. Для работы с объектами в списке доступны следующие элементы управления:

- Кнопка ⊕ — добавление приложения в исключение из проверки.
- Кнопка 🗑 — удаление приложения из списка исключений.

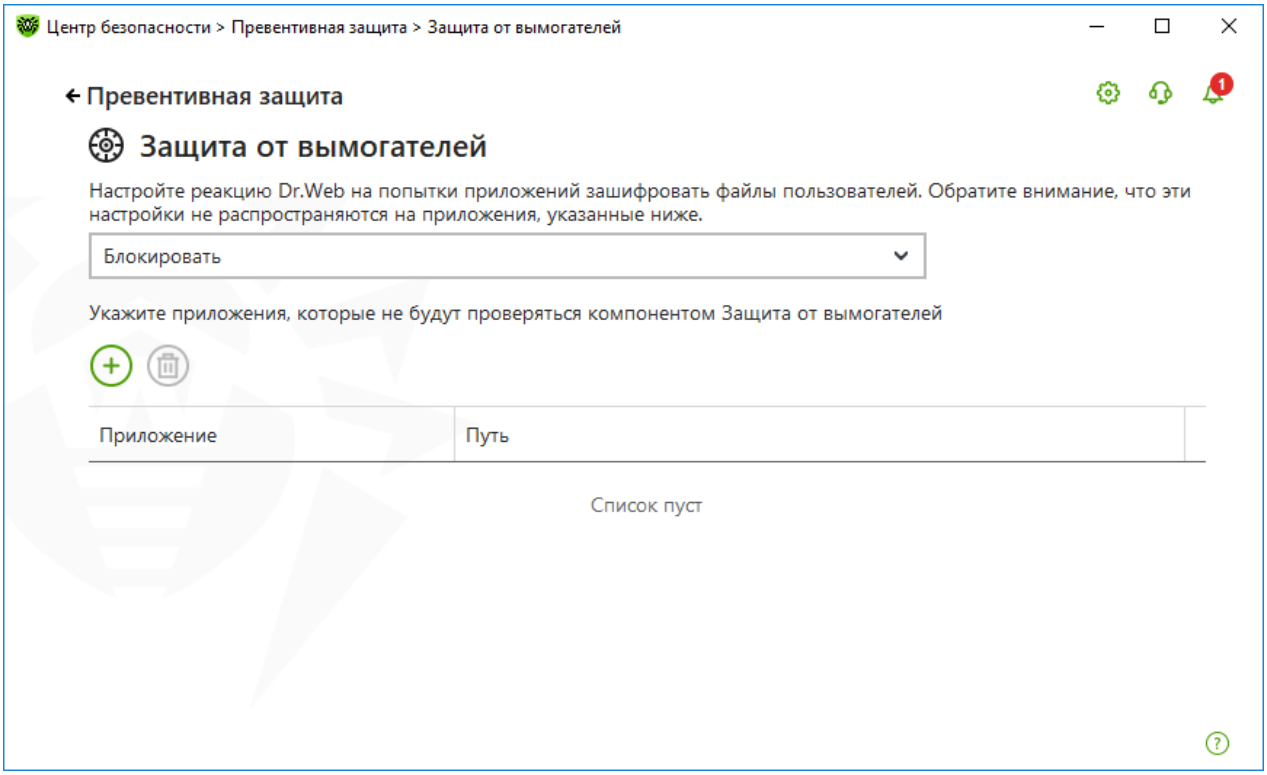

Рисунок 62. Исключения из проверки Защитой от вымогателей

Чтобы добавить приложение в список

1. Нажмите кнопку ⊕ и в открывшемся окне выберите необходимое приложение.
2. Нажмите **ОК**.

11.2. Поведенческий анализ

Компонент Поведенческий анализ позволяет настроить реакцию Dr.Web на действия сторонних приложений, которые могут привести к заражению вашего компьютера, например на попытки модифицировать файл HOSTS или изменить критически важные системные ветки реестра. При включении компонента Поведенческий анализ программа запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствует о попытке вредоносного воздействия на операционную систему. Поведенческий анализ защищает систему от ранее неизвестных вредоносных программ, которые способны избежать обнаружения традиционными сигнатурными и эвристическими механизмами. Для определения вредоносности приложений используются наиболее актуальные данные облачного сервиса Dr.Web.

Чтобы включить или отключить компонент Поведенческий анализ

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.

3. Включите или отключите компонент Поведенческий анализ при помощи переключателя .

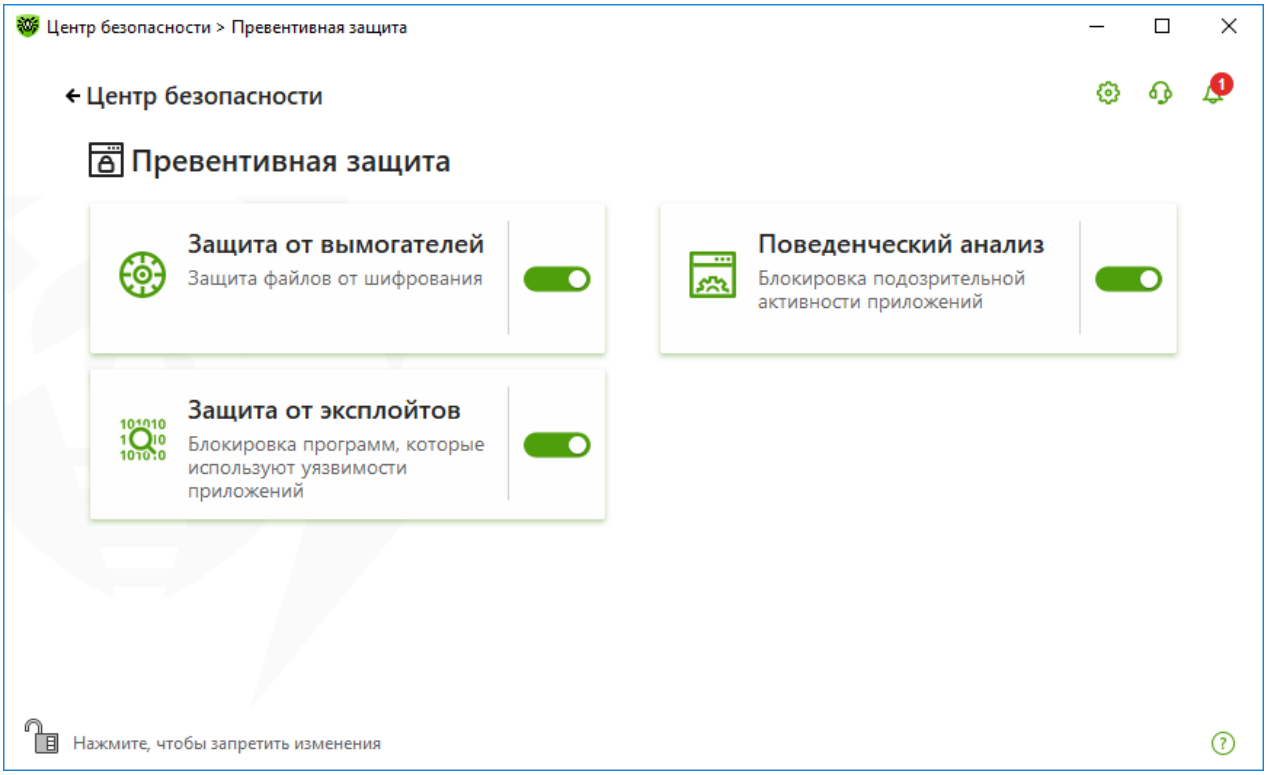

Рисунок 63. Включение/отключение компонента Поведенческий анализ

В этом разделе:

- Режимы работы компонента
- Создание и изменение отдельных правил для приложений
- Описание защищаемых объектов

Параметры Поведенческого анализа

Настройки программы по умолчанию являются оптимальными в большинстве случаев, их не следует изменять без необходимости.

Чтобы перейти к параметрам компонента Поведенческий анализ

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку **Поведенческий анализ**. Откроется окно параметров компонента.

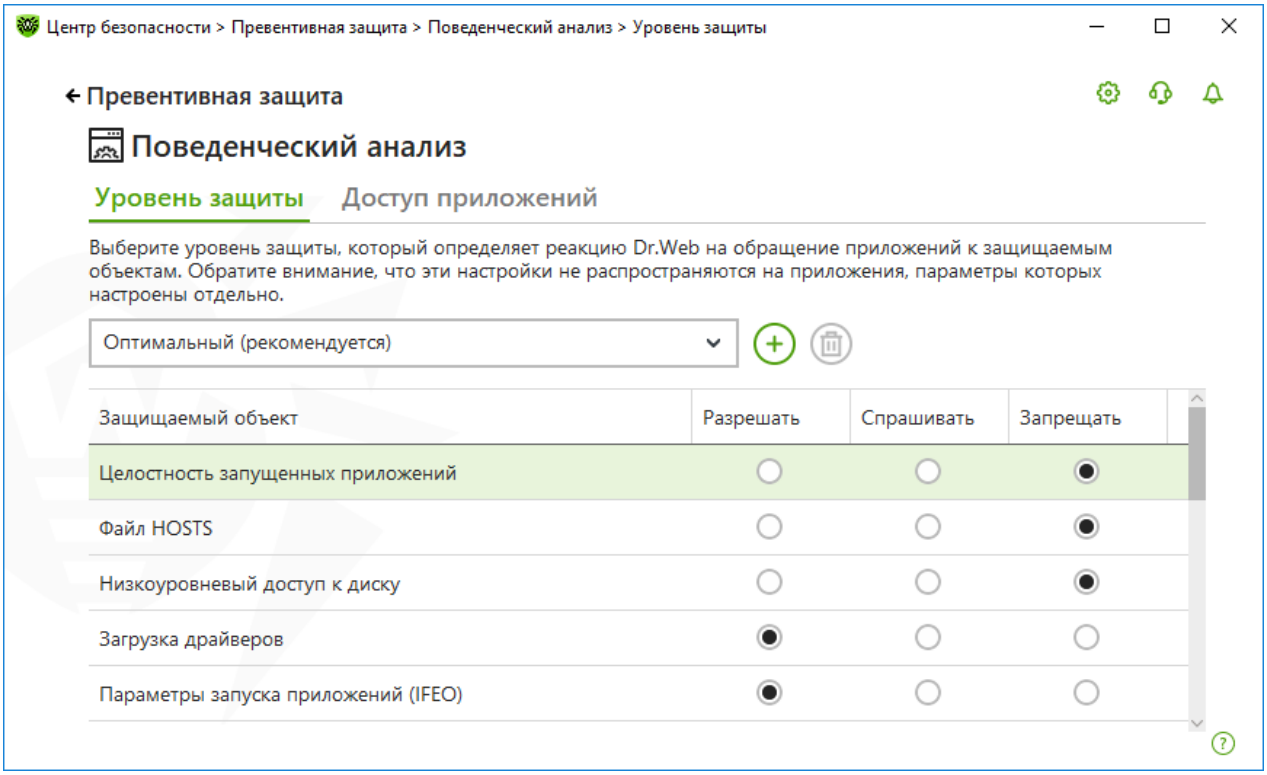

Рисунок 64. Параметры Поведенческого анализа

Вы можете задать отдельный уровень защиты для конкретных объектов и процессов и общий уровень, настройки которого будут применяться ко всем остальным процессам. Для задания общего уровня защиты на вкладке **Уровень защиты** выберите необходимый уровень из выпадающего списка.

Уровни защиты

Уровень защиты	Описание
Оптимальный (рекомендуется)	Используется по умолчанию. Dr.Web запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему. Также запрещаются низкоуровневый доступ к диску и модификация файла HOSTS приложениям, действия которых однозначно определяются как попытка вредоносного воздействия на операционную систему. ⚠ Блокируются только действия приложений, которые не являются доверенными.
Средний	Этот 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	Этот уровень защиты необходим для полного контроля за доступом к критическим объектам Windows. В данном режиме вам также будет доступен интерактивный контроль за загрузкой драйверов и автоматическим запуском программ.
Пользовательский	В этом режиме вы можете выбрать уровни защиты для каждого объекта по своему усмотрению.

Пользовательский режим

Все изменения в настройках сохраняются в Пользовательском режиме работы. В этом окне вы также можете создать новый уровень защиты для сохранения нужных настроек. При любых настройках компонента защищаемые объекты будут доступны для чтения.

Вы можете выбрать одну из реакций Dr.Web на попытки приложений модифицировать защищаемые объекты:

- **Разрешать** — доступ к защищаемому объекту будет разрешен для всех приложений.
- **Спрашивать** — при попытке приложения модифицировать защищаемый объект будет показано уведомление:

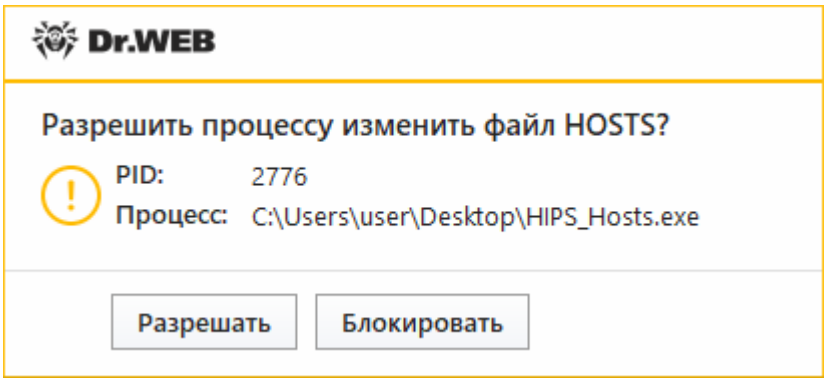

Рисунок 65. Пример уведомления с запросом доступа к защищаемому объекту

- **Блокировать** — при попытке приложения модифицировать защищаемый объект приложению будет отказано в доступе. При этом будет показано уведомление:

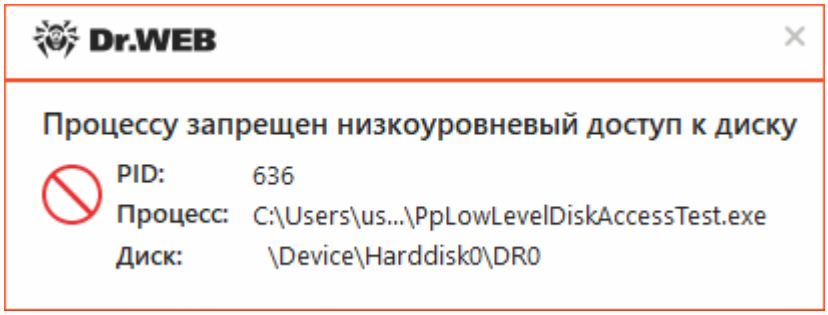

Рисунок 66. Пример уведомления о запрете доступа к защищаемому объекту

Чтобы создать новый уровень защиты

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

Чтобы удалить уровень защиты

1. Из выпадающего списка выберите созданный уровень защиты, который вы хотите удалить.
2. Нажмите кнопку 🗑. Предустановленные профили удалить нельзя.
3. Нажмите **OK**, чтобы подтвердить удаление.

Получение уведомлений

Вы можете настроить вывод уведомлений о действиях компонента Поведенческий анализ на экран и отправку этих уведомлений на электронную почту.

См. также:

- Уведомления

Доступ приложений

Чтобы задать отдельные параметры доступа для конкретных приложений перейдите на вкладку **Доступ приложений**. Здесь вы можете добавить новое правило для приложения, отредактировать уже созданное правило или удалить ненужное.

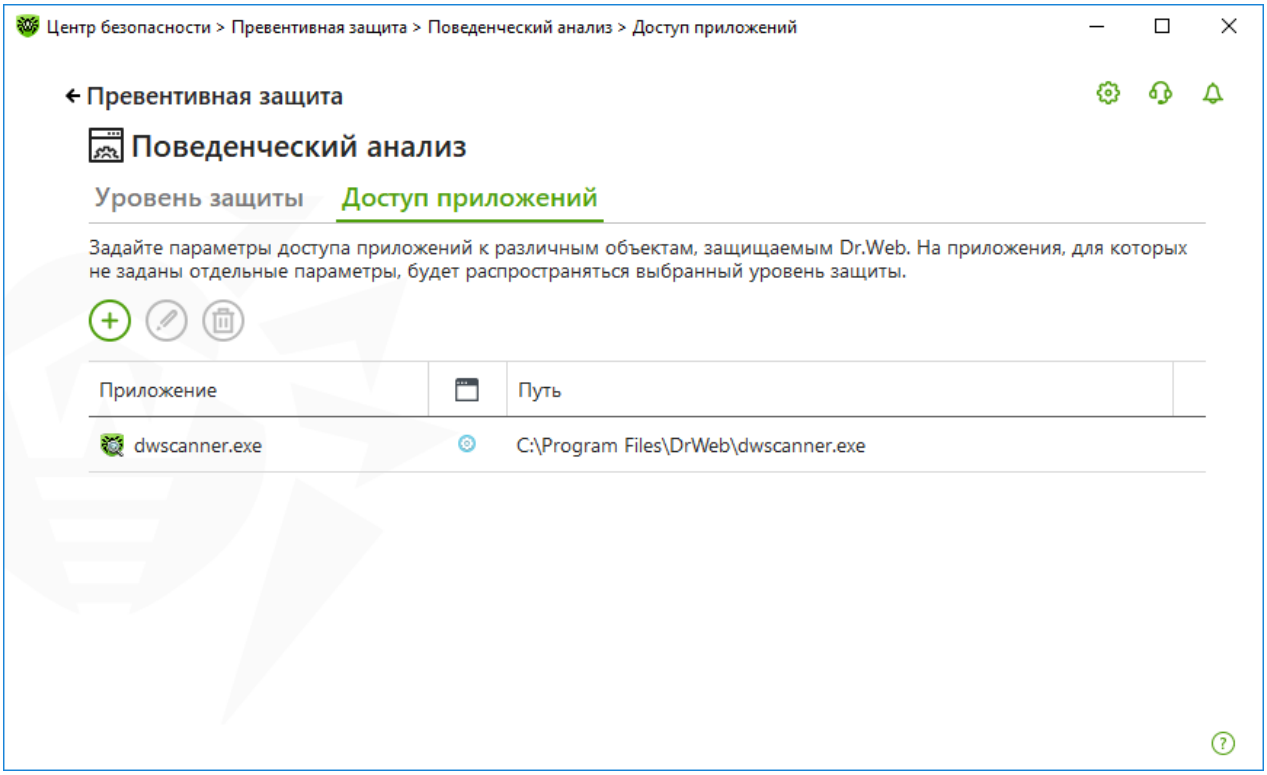

Рисунок 67. Параметры доступа для приложений

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление набора правил для приложения.
- Кнопка ✎ — редактирование существующих наборов правил.
- Кнопка 🗑 — удаление набора правил.

В столбце (**Тип правила**) может отображаться три типа правил:

- ✔ — задано правило **Разрешать все** для всех защищаемых объектов.
- ⚙ — заданы разные правила для защищаемых объектов.
- ⛔ — задано правило **Блокировать все** для всех защищаемых объектов.

Чтобы добавить правило для приложения

1. Нажмите кнопку ⊕.
2. В открывшемся окне нажмите кнопку **Обзор** и укажите путь к исполняемому файлу приложения.

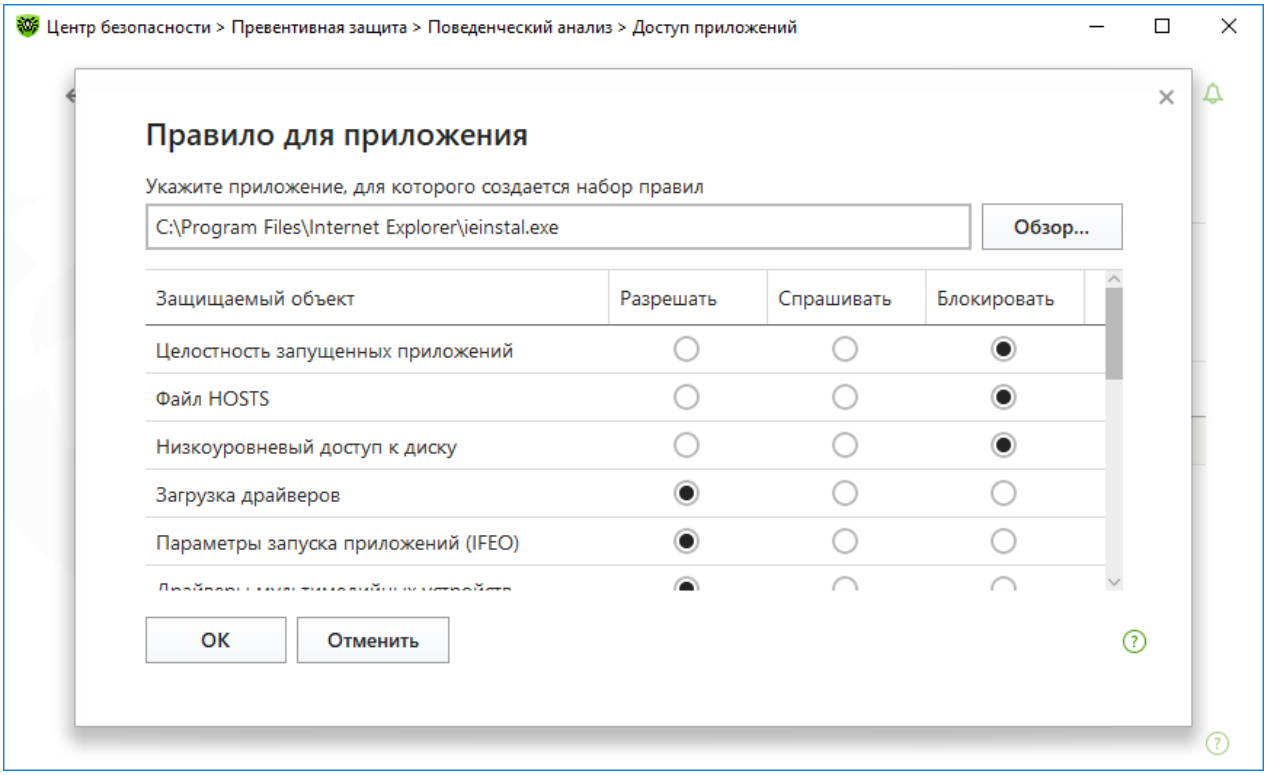

Рисунок 68. Добавление набора правил для приложения

3. Просмотрите настройки защиты, заданные по умолчанию и, при необходимости, отредактируйте их.
4. Нажмите **OK**.

Защищаемые объекты

Защищаемый объект	**Описание**
Целостность запущенных приложений	Данная настройка позволяет отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера.
Файл HOSTS	Файл HOSTS используется операционной системой для упрощения доступа к интернету. 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 параметрам запуска приложений (IFEO):

Защищаемый объект	Описание
	• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Драйверы мультимедийных устройств: • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Параметры оболочки Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Нотификаторы Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Автозапуск оболочки Windows: • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Ассоциации исполняемых файлов: • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (ключи) Политики ограничения запуска программ (SRP): • Software\Policies\Microsoft\Windows\Safer Плагины Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Автозапуск программ: • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Автозапуск политик: • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Конфигурация безопасного режима: • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network Параметры Менеджера сессий:

Защищаемый объект	Описание
	• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows Системные службы: • System\CurrentControlXXX\Services

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

11.3. Защита от эксплойтов

Компонент Защита от эксплойтов позволяет блокировать вредоносные объекты, которые используют уязвимости в популярных приложениях. При определении вредоносности объекта используются в том числе данные из облачного сервиса Dr.Web.

Чтобы включить или отключить компонент Защита от эксплойтов

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.
3. Включите или отключите компонент Защита от эксплойтов при помощи переключателя.

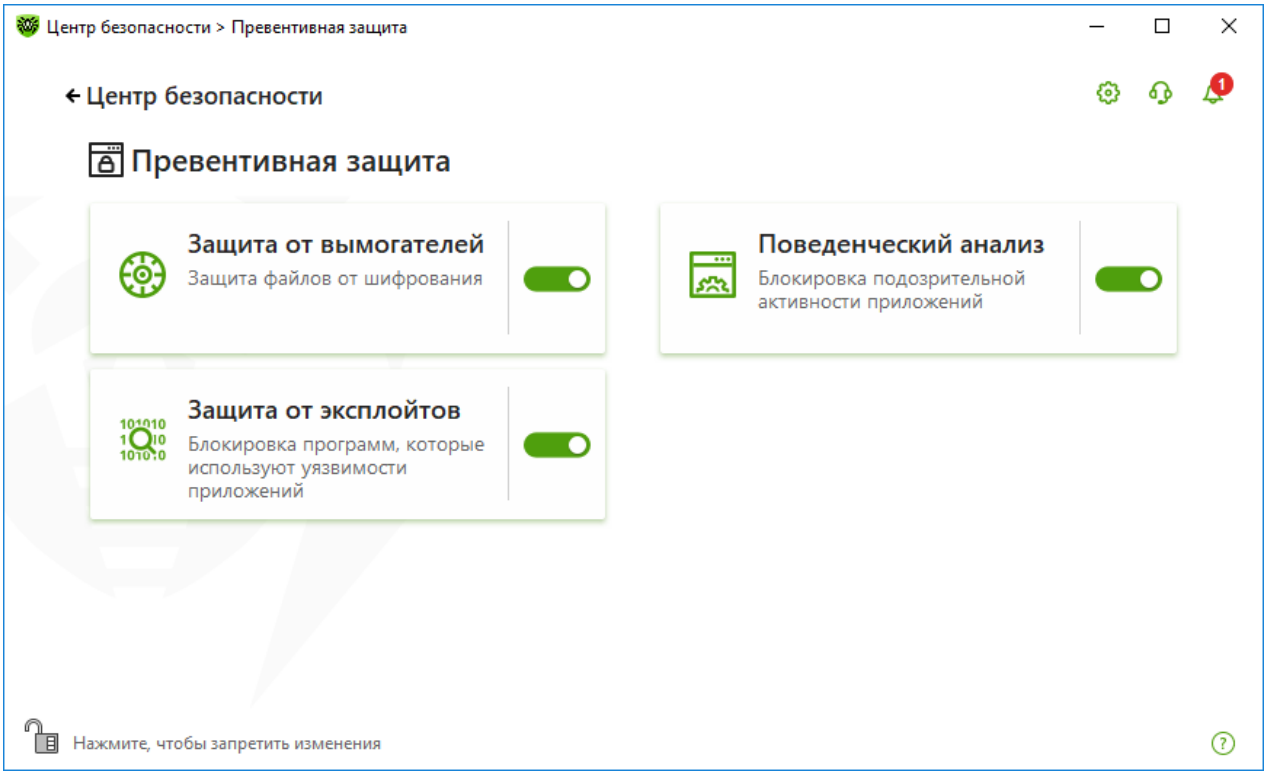

Рисунок 69. Включение/отключение компонента Защита от эксплойтов

Чтобы перейти к параметрам компонента Защита от эксплойтов

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку **Защита от эксплойтов**. Откроется окно параметров компонента.

В соответствующем выпадающем списке в окне параметров компонента выберите подходящий уровень защиты от эксплойтов.

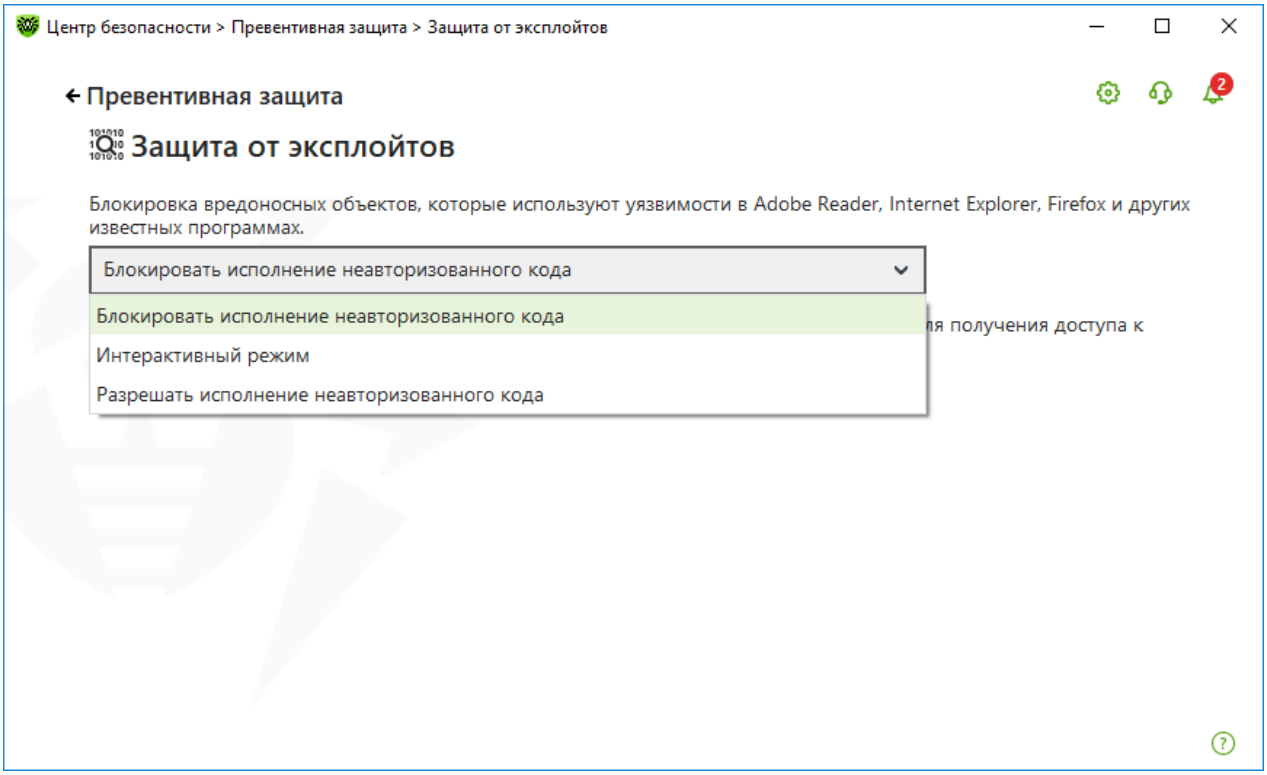

Рисунок 70. Выбор уровня защиты

Уровни защиты

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.

Получение уведомлений

Вы можете настроить вывод уведомлений о действиях компонента Защита от эксплойтов на экран и отправку этих уведомлений на электронную почту.

См. также:

- Уведомления

12. Инструменты

В этом окне предоставляется доступ к дополнительным инструментам управления продуктом Dr.Web.

Чтобы перейти в группу настроек Инструменты

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Инструменты**.

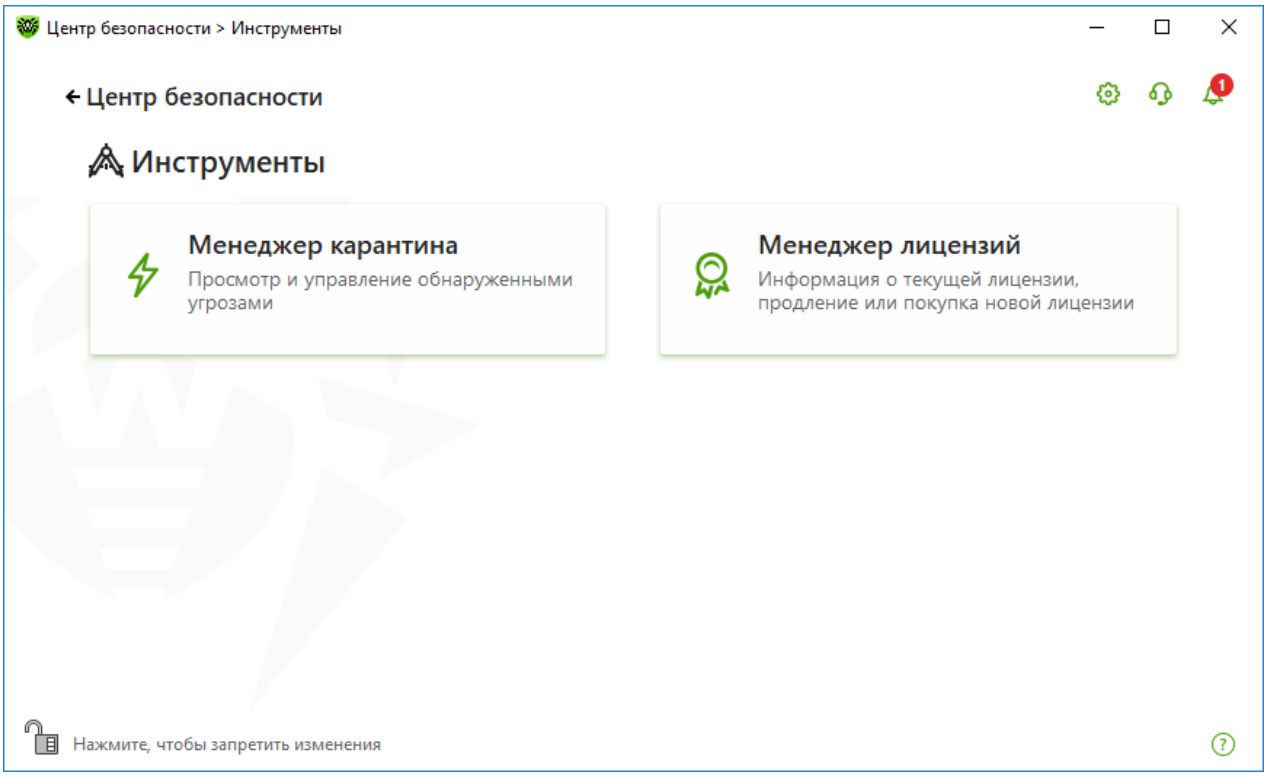

Рисунок 71. Окно Инструменты

Для перехода к необходимому инструменту нажмите соответствующую плитку.

В этом разделе:

- Менеджер карантина — список изолированных файлов и возможность их восстановления.
- Менеджер лицензий — информация о лицензии, получение новой лицензии.

12.1. Менеджер карантина

Менеджер карантина — инструмент, позволяющий управлять изолированными файлами. В карантине содержатся файлы, в которых были обнаружены вредоносные объекты. Также в карантин помещаются резервные копии файлов, обработанных

Dr.Web. Менеджер карантина предоставляет возможность удаления, перепроверки и восстановления изолированных файлов.

Чтобы перейти в окно Менеджер карантина

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Инструменты**.
3. Нажмите плитку **Менеджер карантина**.

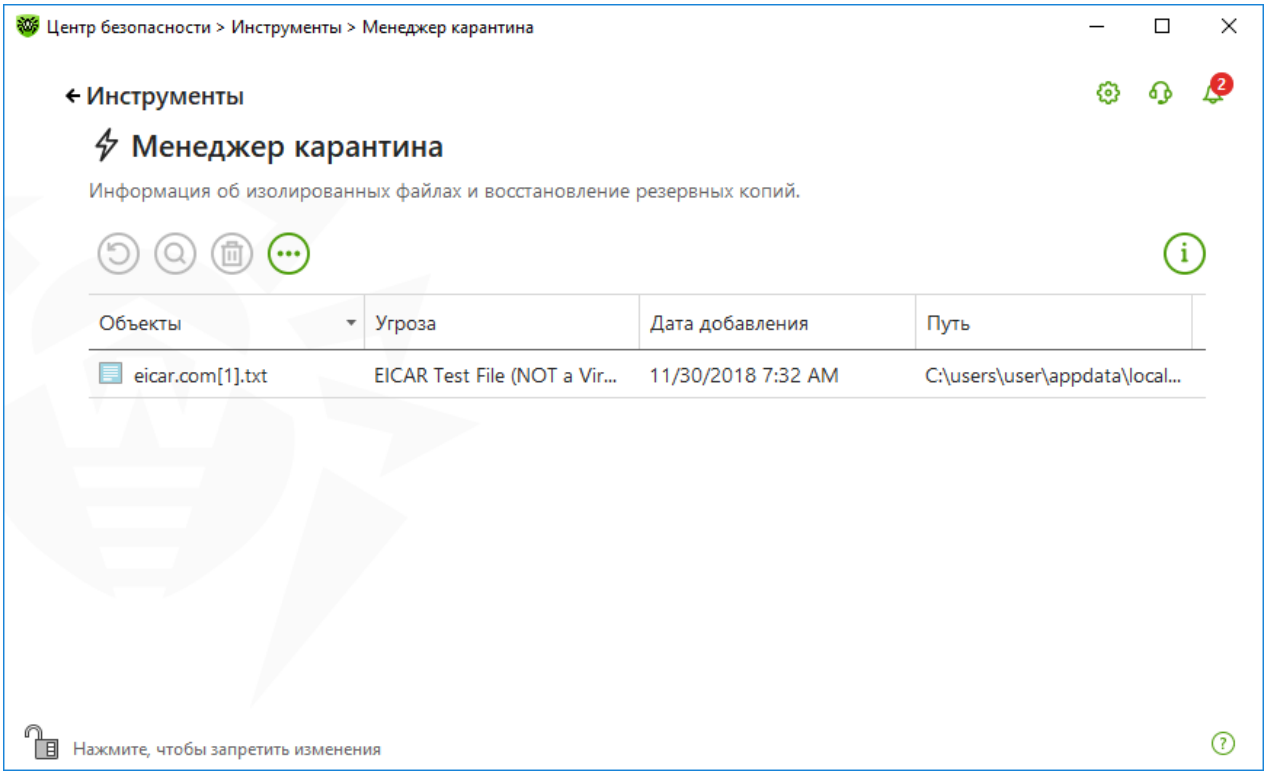

Рисунок 72. Объекты в карантине

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:

- Кнопка (**Восстановить**) — переместить один или несколько выбранных объектов в нужную папку;

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

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

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

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

Дополнительно

Для настройки опций хранения и автоматического удаления записей в карантине перейдите в настройки Менеджера карантина.

12.2. Менеджер лицензий

Этот инструмент позволяет просмотреть информацию обо всех лицензиях Dr.Web, хранящихся на вашем компьютере, а также изменить текущую лицензию, продлить ее или купить новую и активировать для использования.

Чтобы перейти в окно Менеджер лицензий из Центра безопасности

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Инструменты**.
3. Нажмите плитку **Менеджер лицензий**.

Чтобы перейти в окно Менеджер лицензий из Меню программы

1. Откройте меню Dr.Web.
2. Выберите пункт **Менеджер лицензий**.

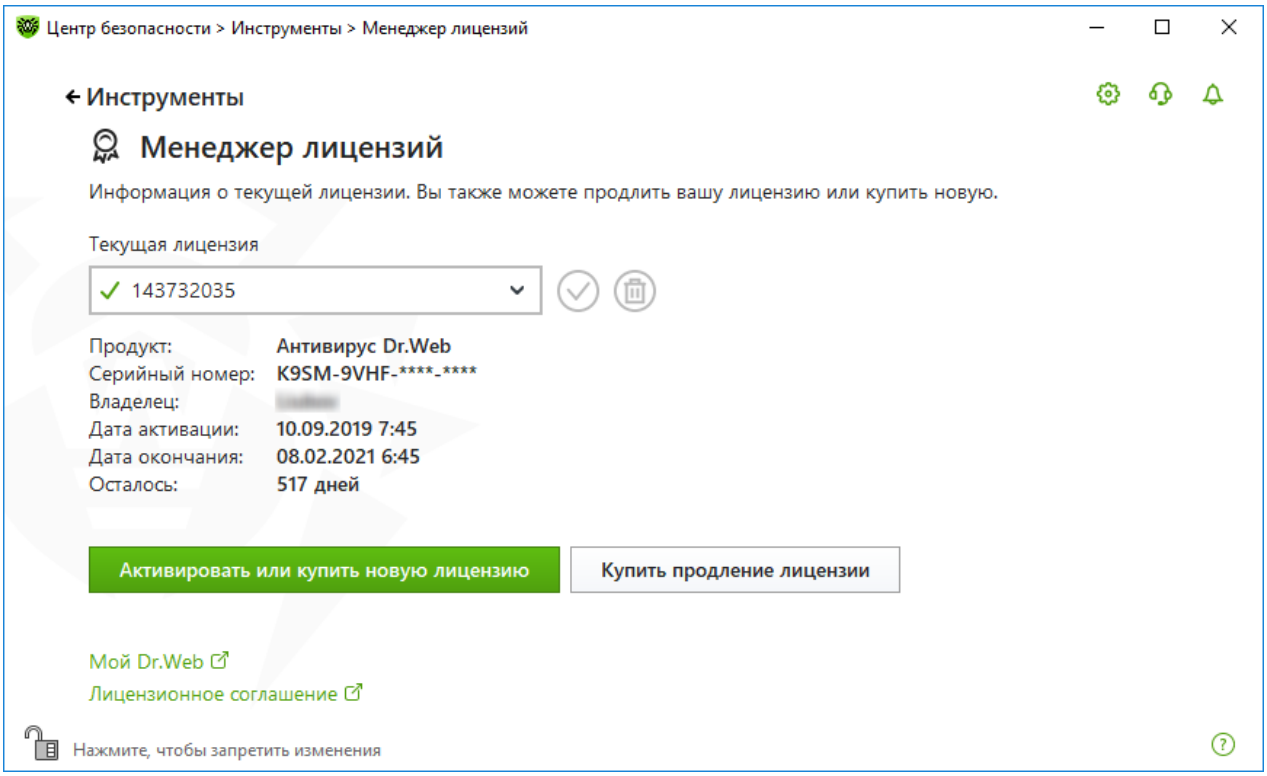

Рисунок 73. Данные о текущей лицензии

Чтобы просмотреть информацию о лицензии, которая на данный момент не является текущей, выберите ее в выпадающем списке.

Если действие лицензии распространяется на несколько продуктов, список продуктов доступен в раскрывающемся списке по ссылке **Еще**.

Если активировано несколько действующих лицензий одновременно, срок действия каждой лицензии будет истекать. Чтобы этого не произошло, при активации новой лицензии укажите серийные номера предыдущих активированных лицензий. Тогда сроки действия лицензий суммируются.

Чтобы удалить лицензию

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок.
2. Выберите из выпадающего списка лицензию, которую вы хотите удалить, и нажмите кнопку. Обратите внимание, что последнюю действующую лицензию удалить нельзя.

Чтобы назначить текущую лицензию

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт» ). В противном случае нажмите на замок  .
2. Выберите из выпадающего списка лицензию, которую вы хотите назначить текущей, и нажмите кнопку  .

При нажатии кнопки **Активировать или купить новую лицензию** программа откроет окно, в котором вы можете купить или активировать новую лицензию.

При нажатии кнопки **Купить продление лицензии** программа откроет страницу продления лицензии на сайте компании «Доктор Веб», на которую будут переданы параметры используемой лицензии.

Дополнительно

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

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

13. Исключения

В данной группе настроек вы можете настроить исключения из проверок компонентами SpIDer Guard, SpIDer Mail и Сканер.

Чтобы перейти в группу настроек Исключения

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Исключения**.

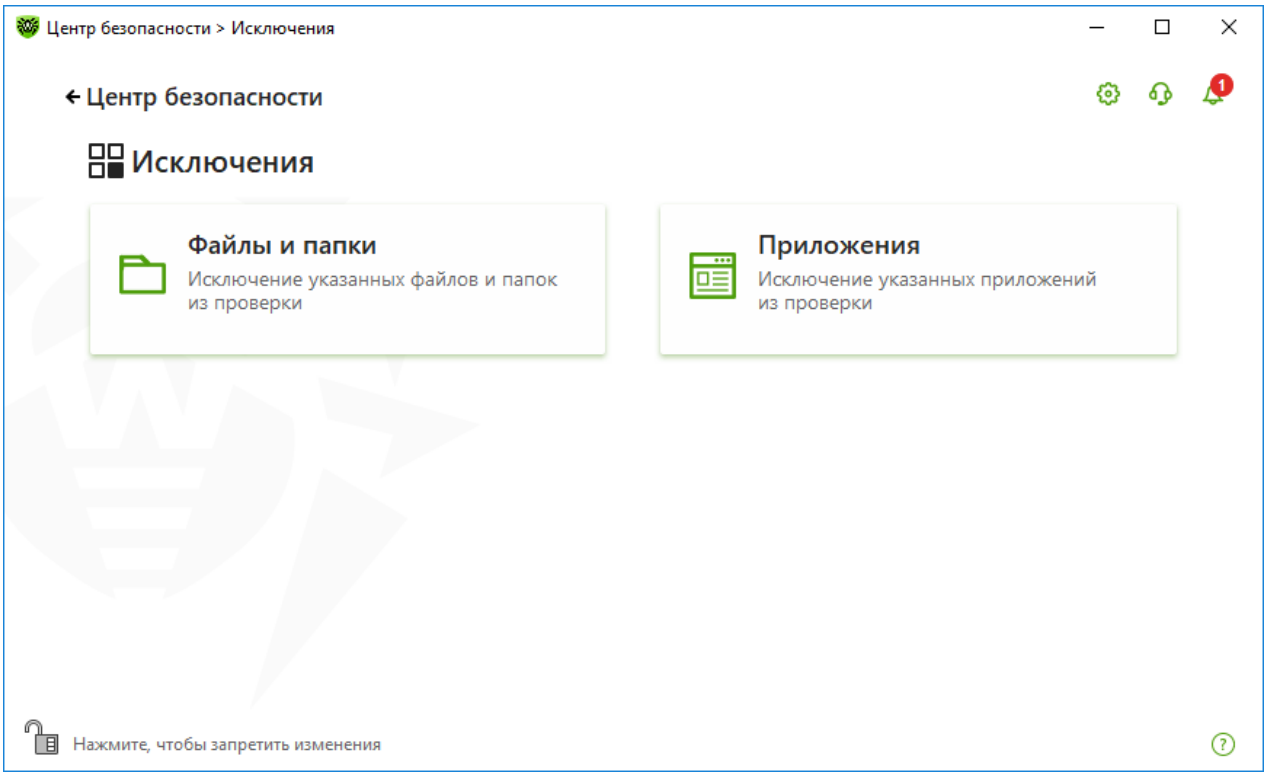

Рисунок 74. Окно Исключения

Чтобы перейти к параметрам исключений

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку соответствующего раздела.

В этом разделе:

- Файлы и папки — исключение определенных файлов и папок из проверки компонентами SpIDer Guard и Сканер.
- Приложения — исключение определенных процессов из проверки компонентами SpIDer Guard и SpIDer Mail.

13.1. Файлы и папки

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

Чтобы настроить список исключаемых файлов и папок

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Исключения**.
3. Нажмите плитку **Файлы и папки**.

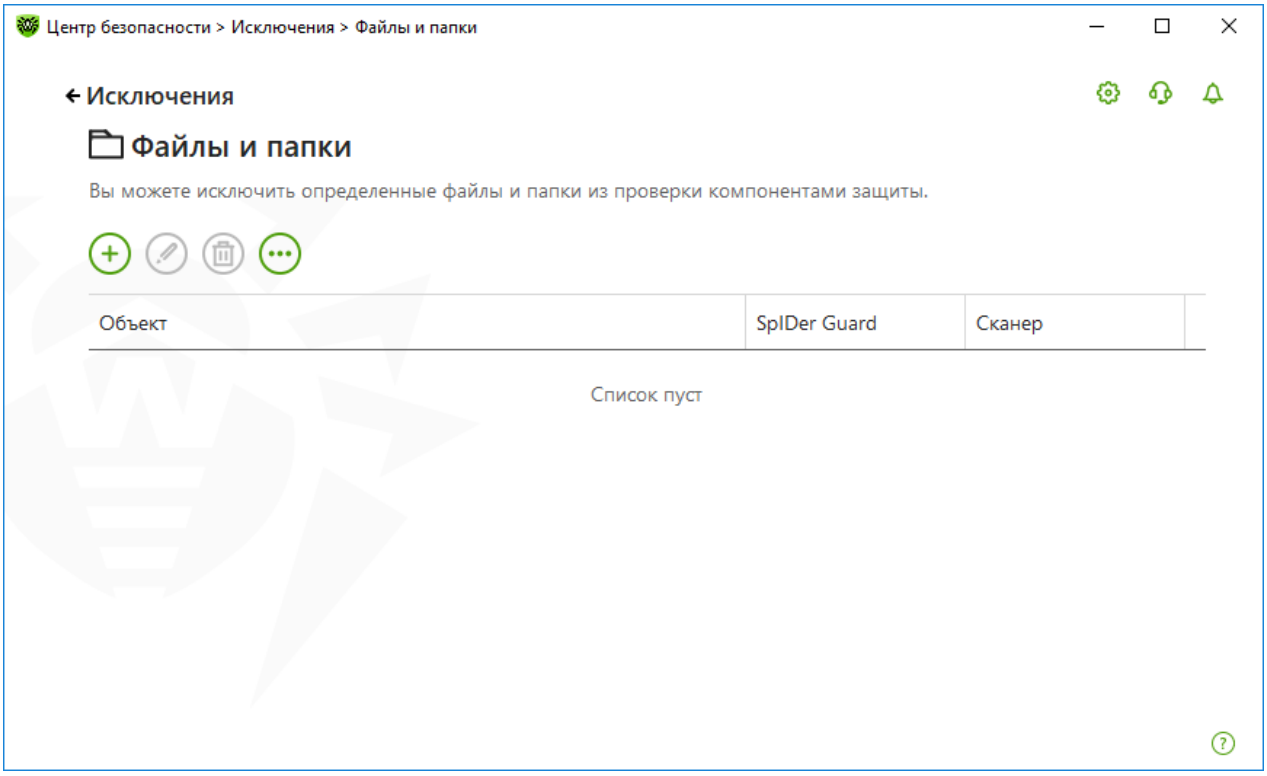

Рисунок 75. Список исключаемых файлов и папок

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.

Чтобы добавить файлы и папки в список 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**, чтобы выбрать папку или файл. 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`, `photomama09.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 добавления файла или папки укажите, какие компоненты не должны проводить проверку выбранного объекта.
3. Нажмите кнопку **OK**. Выбранный файл или папка появится в списке.
4. При необходимости повторите шаги 1–3 для добавления других файлов или папок.

Работа с объектами в списке

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление объекта в список исключений.
- Кнопка ✎ — редактирование выбранного объекта в списке исключений.
- Кнопка 🗑 — удаление выбранного объекта из списка исключений.

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

13.2. Приложения

Вы можете задать список программ и процессов, активность которых исключается из проверки файловым монитором SpIDer Guard и почтовым антивирусом SpIDer Mail. Исключаются из проверки объекты, изменяемые в результате работы данных приложений.

Чтобы настроить список исключаемых приложений

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Исключения**.
3. Нажмите плитку **Приложения**.

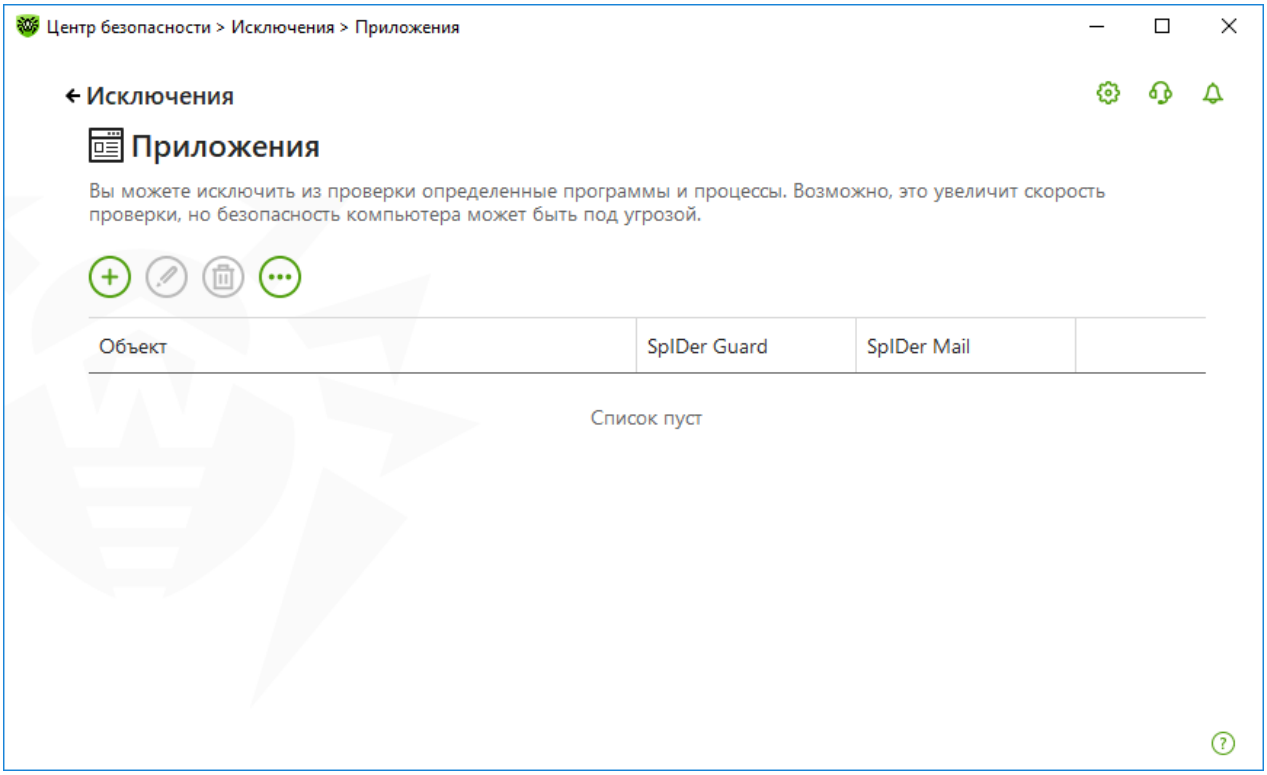

Рисунок 76. Список исключаемых приложений

По умолчанию список пуст.

Чтобы добавить приложения в исключения

1. Чтобы добавить программу или процесс к списку исключений, нажмите ⊕. Выполните одно из следующих действий:
   - в открывшемся окне нажмите кнопку **Обзор**, чтобы выбрать приложение. 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.

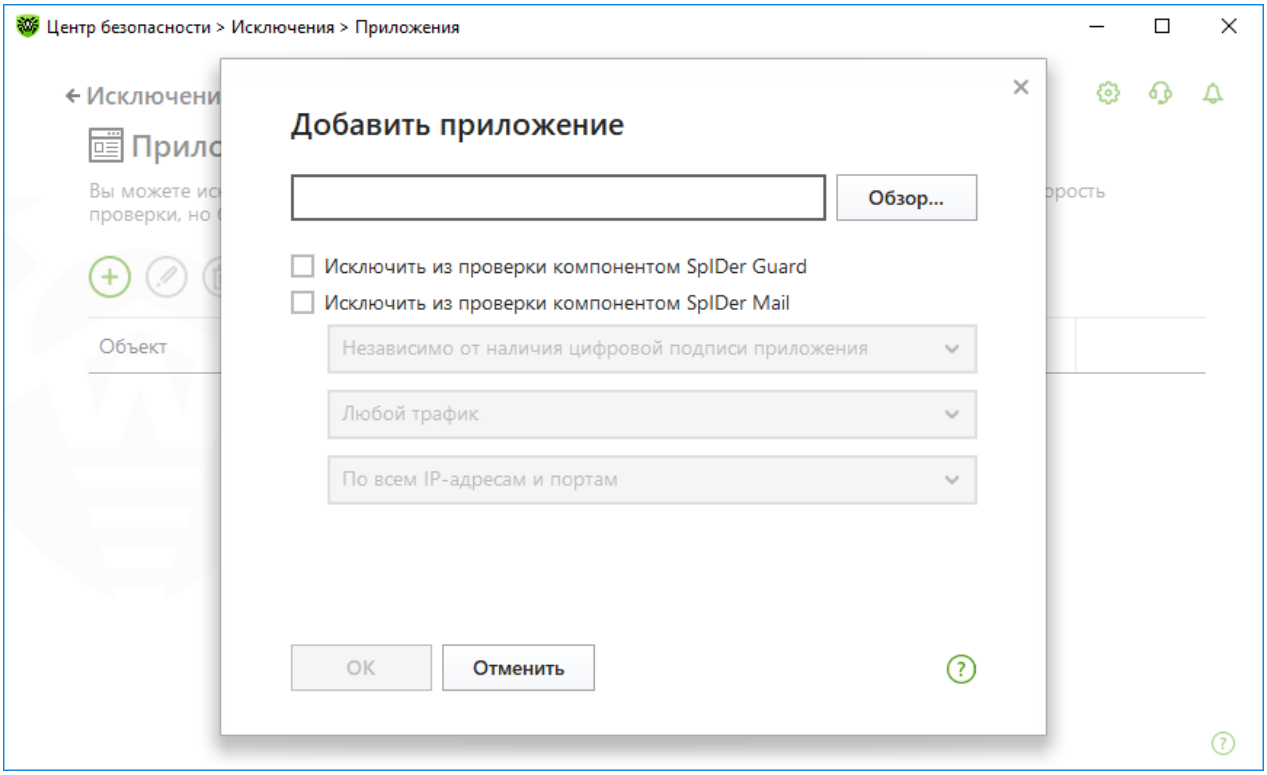

Рисунок 77. Добавление приложений в исключения

3. Для объектов, исключаемых из проверки компонентом SpIDer 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.

Параметр	Описание
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, `site.com:80`; • для исключения из проверки трафика по нестандартному порту (например, 1111) необходимо указать: `*:1111`; • для исключения из проверки трафика от домена по любому порту укажите: `site:*`

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

Работа с объектами в списке

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление объекта в список исключений.
- Кнопка ✎ — редактирование выбранного объекта в списке исключений.
- Кнопка 🗑 — удаление выбранного объекта из списка исключений.

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

14. Статистика работы компонентов

У вас есть возможность просматривать статистику работы основных компонентов Dr.Web.

Чтобы перейти к просмотру статистики по важным событиям в работе компонентов защиты

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне выберите вкладку **Статистика**.
3. Откроется окно просмотра статистики, из которого доступны отчеты для следующих групп:
   - Подробный отчет
   - Угрозы
   - Брандмауэр

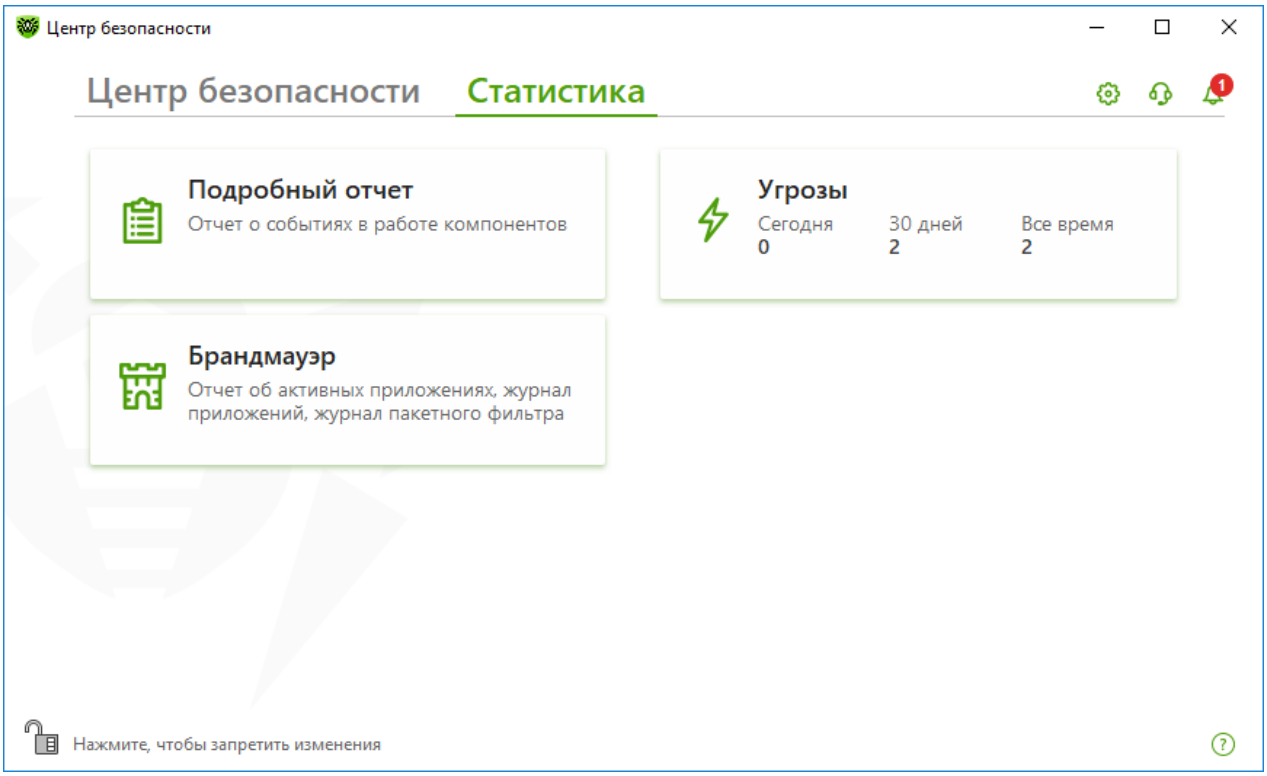

Рисунок 78. Статистика работы компонентов

4. Выберите группу для просмотра отчетов.

Подробный отчет

В этом окне собирается подробная информация обо всех событиях за все время работы.

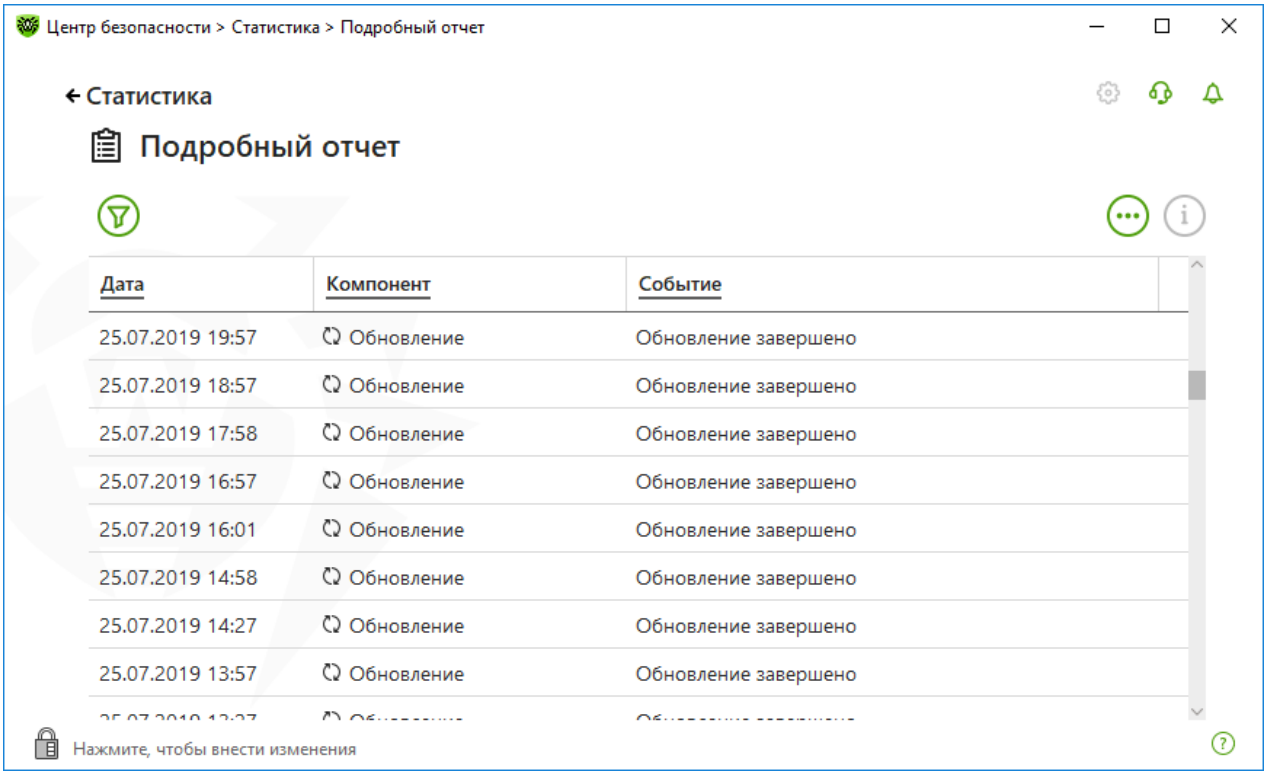

Рисунок 79. Окно подробного отчета

В отчете фиксируются следующие сведения:

- **Дата** — дата и время события;
- **Компонент** — компонент или модуль, к которому относится событие;
- **Событие** — краткое описание события.

По умолчанию отображаются все события за все время.

Для работы с объектами в таблице используются элементы управления , , .

Для отбора событий можно воспользоваться дополнительными фильтрами.

Угрозы

В основном окне просмотра статистики на плитке **Угрозы** собрана информация о количестве угроз за определенный промежуток времени.

При выборе этой опции откроется окно **Подробный отчет** с предустановленными фильтрами по всем угрозам.

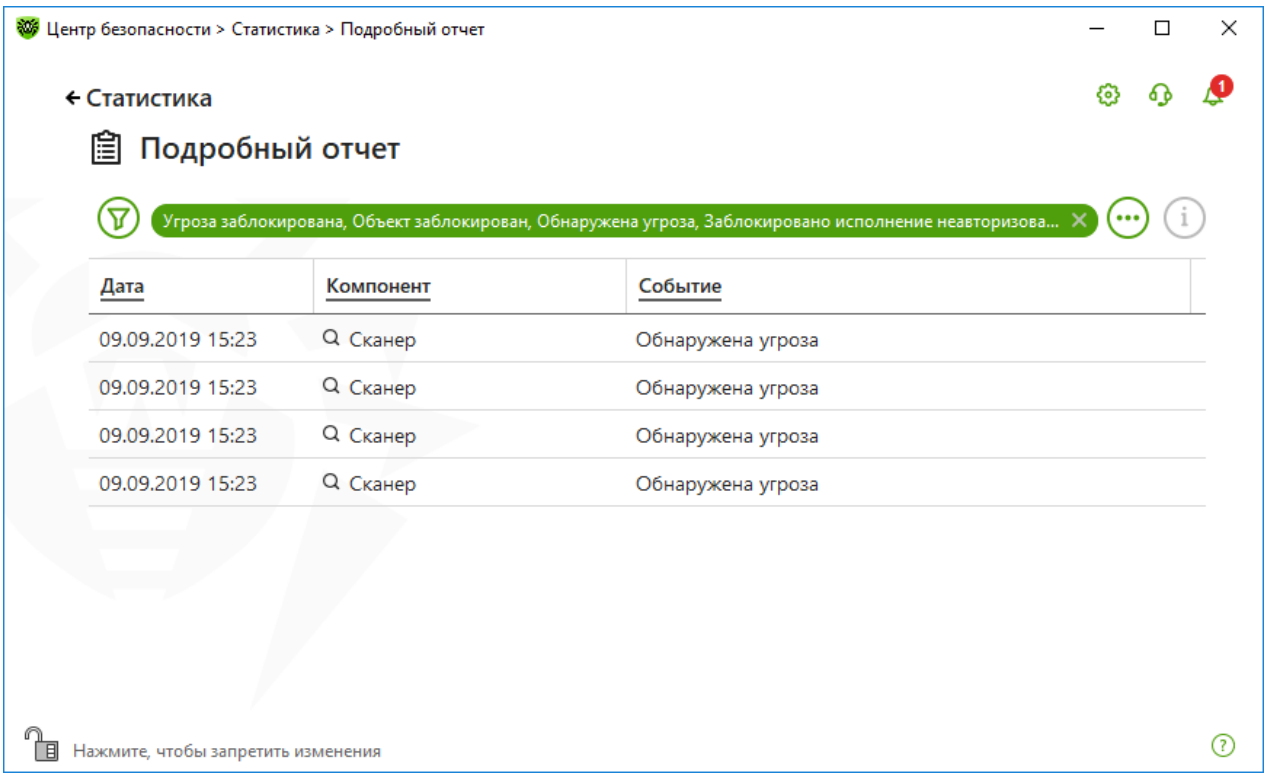

Рисунок 80. Окно статистики по угрозам

В отчете фиксируются следующие сведения:

- **Дата** — дата и время обнаружения угрозы;
- **Компонент** — компонент, обнаруживший угрозу;
- **Событие** — краткое описание события.

По умолчанию отображаются все события за все время.

Для работы с объектами в таблице используются элементы управления , , .

Для отбора событий можно воспользоваться дополнительными фильтрами.

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.

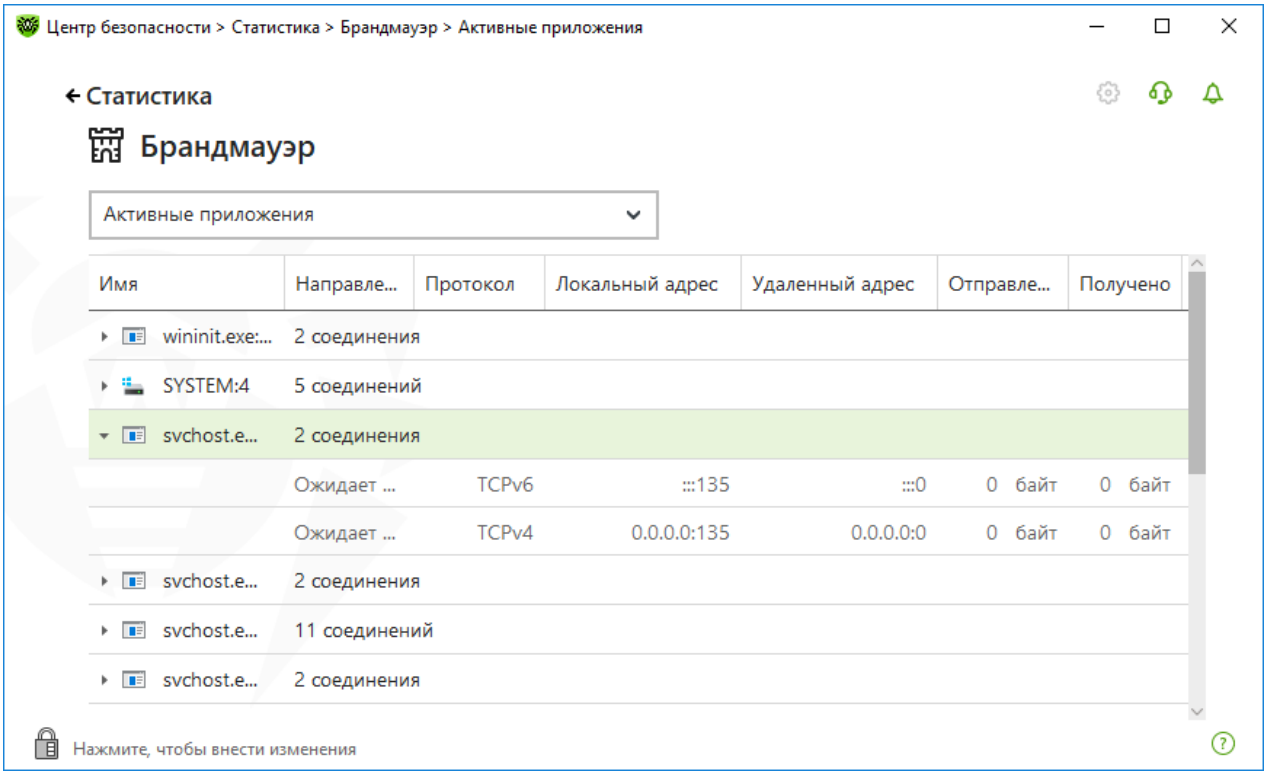

Рисунок 81. Окно статистики сетевой активности

Для каждого активного приложения отображаются следующие данные:

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

Вы можете заблокировать одно из текущих соединений или разрешить ранее заблокированное соединение. Для этого выберите необходимое соединение и нажмите правой кнопкой мыши. Доступна только одна опция, зависящая от статуса соединения.

В журнале приложений отображаются следующие данные:

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

Включить запись журнала приложений можно в окне добавления или редактирования правила для приложения в разделе **Брандмауэр**. Подробнее см. в разделе Настройка параметров правила для приложений.

В журнале пакетного фильтра отображаются следующие данные:

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

Включить запись журнала пакетного фильтра можно в окне добавления или редактирования пакетного правила в разделе **Брандмауэр**. Подробнее см. в разделе Набор правил фильтрации пакетов.

При клике на какой-либо из столбцов события сортируются в столбце по убыванию или возрастанию.

Фильтры

Чтобы посмотреть в списке только те события, которые соответствуют определенным параметрам, воспользуйтесь фильтрами. Для всех отчетов имеются предустановленные фильтры, которые доступны по нажатию. Также вы можете создавать собственные фильтры событий.

Кнопки управления элементами в таблице:

- При нажатии кнопки доступны следующие действия:
  - Выбор предустановленного фильтра за установленный период времени или фильтра по событию обновления.
  - Сохранение текущего пользовательского фильтра. Также возможно удаление уже созданного пользовательского фильтра.
  - Удаление всех установленных на данный момент фильтров.
- При нажатии кнопки доступны следующие действия:
  - **Копировать выделенное** — позволяет скопировать выделенную строку (строки) в буфер обмена.
  - **Экспортировать выделенное** — позволяет экспортировать выделенную строку (строки) в заданную папку в формате .csv.
  - **Экспортировать все** — позволяет экспортировать все строки таблицы в заданную папку в формате .csv.
  - **Удалить выделенное** — позволяет удалить выделенное событие (события).

- **Удалить все** — позволяет удалить все события из таблицы статистики.

- При нажатии кнопки ⓘ отображается подробная информация о событии. Доступна при выборе какой-либо строки. Повторное нажатие этой кнопки скроет подробные данные о событии.

Чтобы задать пользовательский фильтр

1. Для сортировки по определенному параметру нажмите на заголовок необходимого столбца:
   - Сортировка по дате. Вы можете выбрать один из предустановленных периодов, указанных в левой части окна, или задать свой. Чтобы задать необходимый период, выберите в календаре дату начала и дату окончания периода, либо укажите даты в строке **Период**. Также доступна сортировка по дате по возрастанию или убыванию.

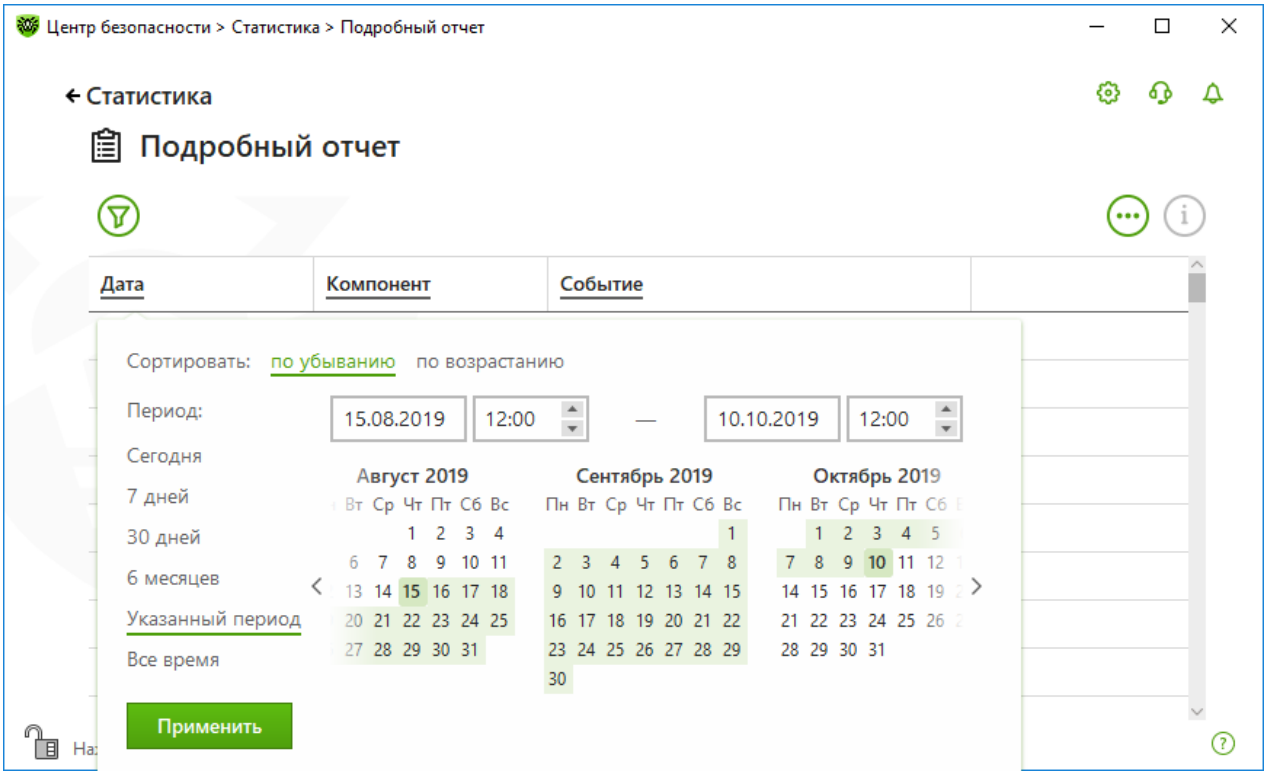

Рисунок 82. Сортировка по дате

   - Сортировка по компоненту. Вы можете отметить те компоненты, информация от которых будет отображаться в отчете, либо отсортировать записи по возрастанию или убыванию.
   - Сортировка по событию. Вы можете отметить события для отображения в отчете либо отсортировать записи по возрастанию или убыванию.
2. После выбора параметров фильтрации нажмите **Применить**. Выбранные элементы будут отображаться над таблицей.
3. Чтобы сохранить фильтр, нажмите ⧩ и выберите **Сохранить фильтр**.
4. В открывшемся окне укажите название нового фильтра. Нажмите **Сохранить**.

15. 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/.

15.1. Помощь в решении проблем

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

Чтобы создать отчет при помощи Мастера отчетов

1. Откройте меню Dr.Web и выберите пункт **Поддержка**.
2. В открывшемся окне нажмите кнопку **Перейти к Мастеру отчетов**.

Также вы можете открыть это окно, нажав на кнопку в правой верхней части окна **Центр безопасности**.

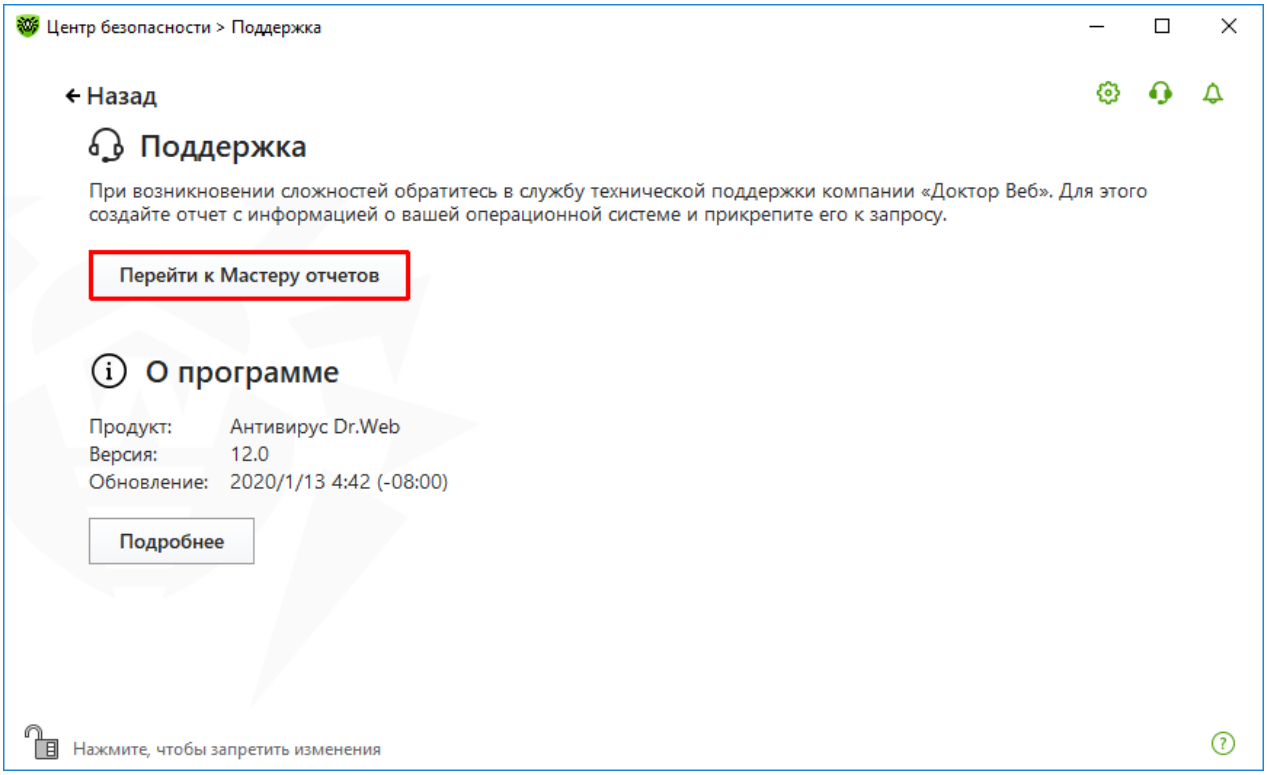

Рисунок 83. Поддержка

3. В открывшемся окне нажмите кнопку **Создать отчет**.

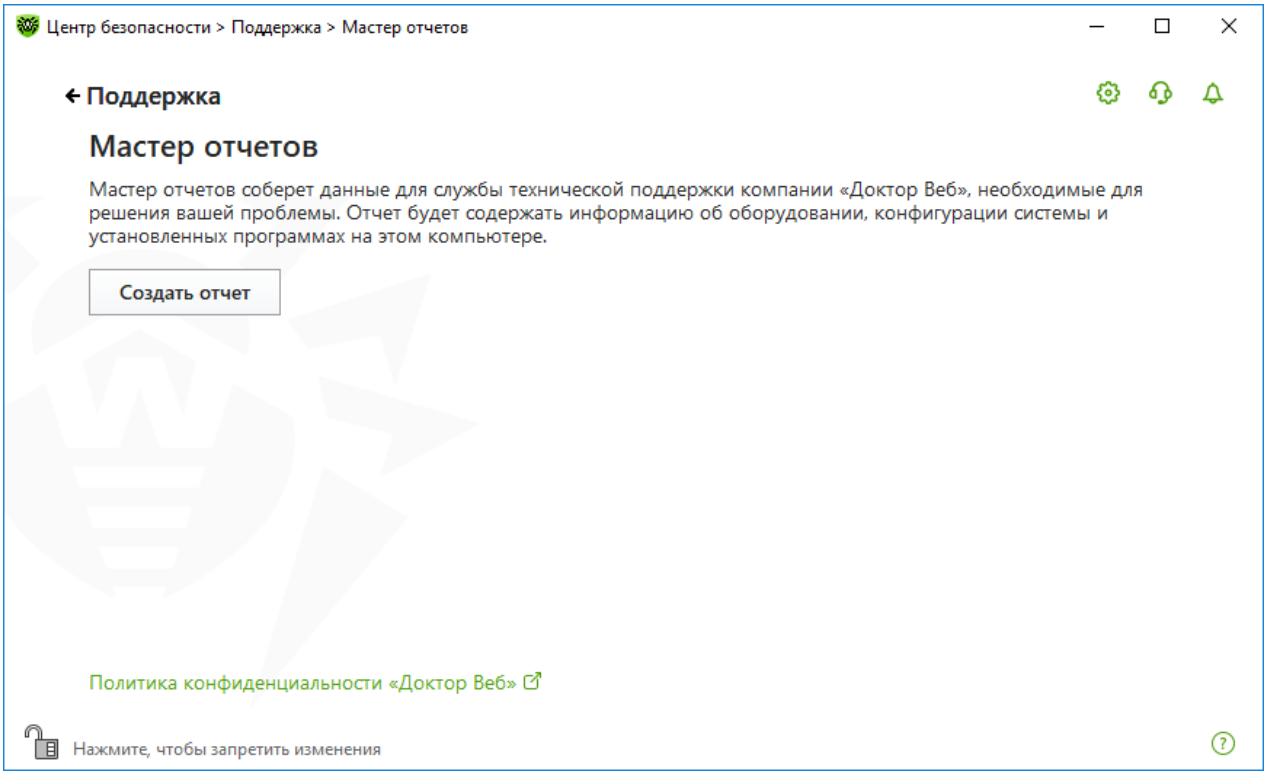

Рисунок 84. Создание отчета для технической поддержки

4. Начнется создание отчета.

Создание отчета при помощи командной строки

Чтобы сформировать отчет, воспользуйтесь следующей командой:

`/auto`, например: `dwsysinfo.exe /auto`

Также вы можете использовать команду:

`/auto /report:[<полный_путь_к файлу_отчета>]`, например: `dwsysinfo.exe /auto /report:C:\report.zip`

Отчет будет сохранен в виде архива в папке Doctor Web, расположенной в папке профиля пользователя %USERPROFILE%. Вы можете получить доступ к архиву, нажав кнопку **Открыть папку** после завершения создания архива.

Информация, которая включается в отчет

В отчет включается следующая информация:

1. Техническая информация об операционной системе:
   - общие сведения о компьютере,
   - информация о запущенных процессах,
   - информация о запланированных заданиях,
   - информация о службах, драйверах,
   - информация о браузере по умолчанию,
   - информация об установленных приложениях,
   - информация о политиках ограничений,
   - информация о файле HOSTS,
   - информация 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 установленном продукте Dr.Web:
   - тип и версия установленного продукта Dr.Web;
   - информация о составе установленных компонентов; сведения о модулях Dr.Web;
   - настройки и параметры конфигурации продукта Dr.Web;

- информация о лицензии;
- журналы работы Dr.Web.

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

15.2. О программе

Блок **О программе** содержит информацию о:

- версии продукта;
- дате и времени последнего обновления.

Информацию о версии установленных компонентов и дате обновления вирусных баз вы можете найти в окне **О программе Dr.Web**.

Чтобы перейти к этому окну

1. Откройте основное меню и выберите пункт **Поддержка**.
2. В открывшемся окне нажмите кнопку **Подробнее**.

Также вы можете открыть это окно, нажав на кнопку в правой верхней части окна **Центр безопасности**.

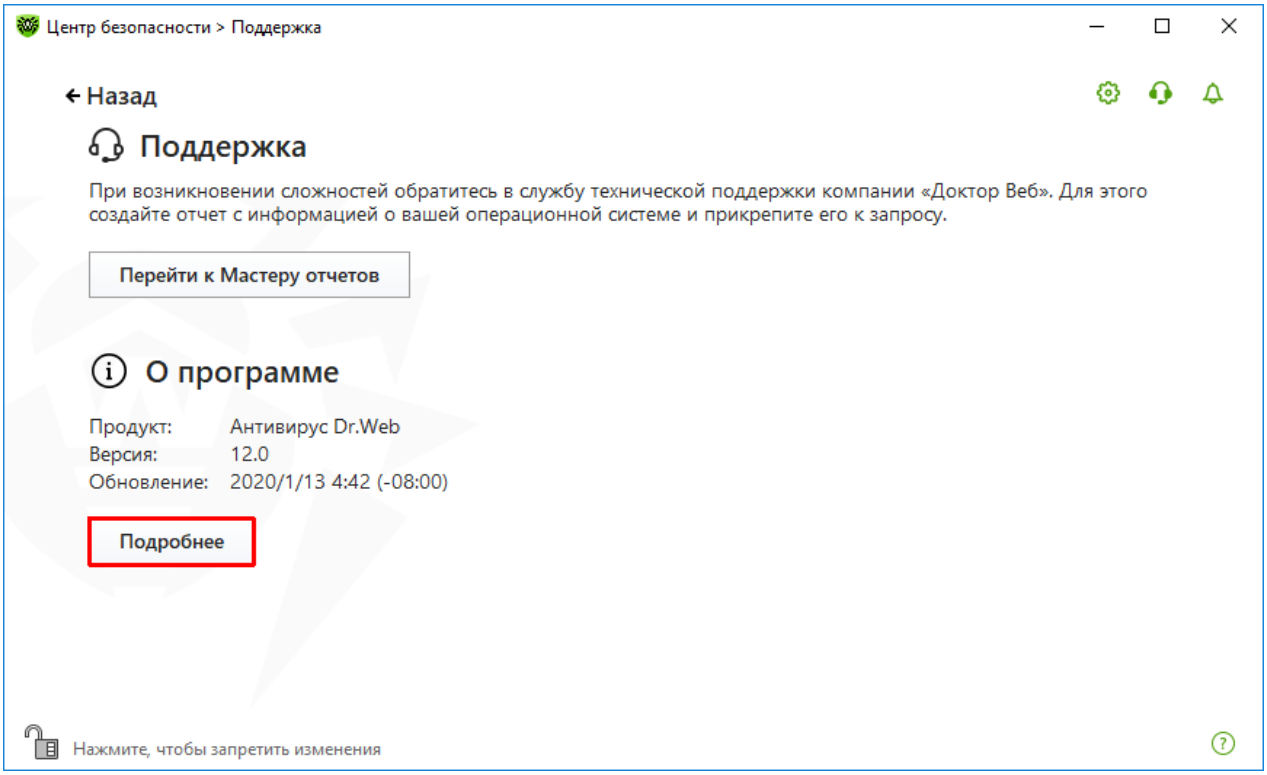

Рисунок 85. Доступ к окну О программе Dr.Web

16. 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, Консольному сканеру и к Модулю автоматического обновления. При этом ключи могут задавать параметры, отсутствующие в конфигурационном файле, а для тех параметров, которые в нем заданы, имеют более высокий приоритет.

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

16.1. 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.
/BI	Вывести информацию о вирусных базах. По умолчанию опция включена.

Ключ	Описание
/CUSTOM	Запустить Сканер на странице выборочной проверки. Если при этом заданы дополнительные параметры (например, объекты для проверки или параметры /TM, /TB), то будет запущена выборочная проверка указанных объектов. (Только для Сканера).
/CL	Использовать облачный сервис Dr.Web. По умолчанию опция включена. (Только для Консольного Сканера).
/DCT	Не отображать расчетное время проверки. (Только для Консольного Сканера).
/DR	Рекурсивно проверять папки (проверять подпапки). По умолчанию опция включена.
/E:<*количество_потоков*>	Провести проверку в указанное количество потоков.
/FAST	Произвести быструю проверку системы. Если при этом заданы дополнительные параметры (например, объекты для проверки или параметры /TM, /TB), то указанные объекты также будут проверены. (Только для Сканера).
/FL:<*имя_файла*>	Проверять пути, указанные в файле.
/FM:<*маска*>	Проверять файлы по маске. По умолчанию проверке подвергаются все файлы.
/FR:<*регулярное_выражение*>	Проверять файлы по регулярному выражению. По умолчанию проверке подвергаются все файлы.
/FULL	Произвести полную проверку всех жестких дисков и съемных носителей (включая загрузочные секторы). Если при этом заданы дополнительные параметры (например, объекты для проверки или параметры /TM, /TB), то будет произведена быстрая проверка и проверка указанных объектов. (Только для Сканера).
/FX:<*маска*>	Не проверять файлы, соответствующие маске. (Только для Консольного Сканера).
/GO	Режим работы Сканера, при котором вопросы, подразумевающие ожидание ответа от пользователя, пропускаются; решения, требующие выбора, принимаются автоматически. Этот режим полезно использовать для автоматической проверки файлов, например, при ежедневной или еженедельной проверке жесткого диска. В командной строке необходимо указать объект для проверки. Вместе с параметром /GO также можно использовать параметры /LITE, /FAST, /FULL. В этом режиме при переходе на работу от батареи проверка прекращается.

Ключ	Описание
/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.
/OK	Выводить полный список проверяемых объектов, сопровождая незараженные пометкой Ok. По умолчанию опция отключена.
/P:<*приоритет*>	Приоритет запущенной задачи проверки в общей очереди задач на проверку: 0 — низший. L — низкий. N — обычный. Приоритет по умолчанию. H — высокий.

Ключ	Описание
	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 (при запуске Сканера из командной строки).
/REP	Проверять по символьным ссылкам. По умолчанию опция отключена.
/RK	Проверка на наличие руткитов. По умолчанию опция отключена.
/RP:<*имя файла*>	Записать отчет о работе программы в указанный файл. По умолчанию запись в файл журнала не производится (при запуске Сканера из командной строки).
/RPC:<*сек*>	Тайм-аут соединения со сканирующим ядром 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).

Ключ	Описание
/RPCH:<*имя_хоста*>	Использовать указанное имя хоста для вызовов RPC. (Только для Консольного Сканера).
/RPCP:<*протокол*>	Использовать указанный протокол RPC. Возможно использование протоколов: lpc, np, tcp. (Только для Консольного Сканера).
/SCC	Выводить содержимое составных объектов. По умолчанию опция отключена.
/SCN	Выводить название инсталляционного пакета. По умолчанию опция отключена.
/SLS	Выводить логи на экран. По умолчанию опция включена. (Только для Консольного Сканера).
/SPN	Выводить название упаковщика. По умолчанию опция отключена.
/SPS	Отображать процесс проведения проверки. По умолчанию опция включена. (Только для Консольного Сканера).
/SST	Выводить время проверки объекта. По умолчанию опция отключена.
/ST	Запуск Сканера в фоновом режиме. Если не задан параметр /GO, то графический режим отображается только при обнаружении угроз. В этом режиме при переходе на работу от батареи проверка прекращается.
/TB	Выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.
/TM	Выполнять поиск угроз в оперативной памяти (включая системную область Windows).
/TR	Проверять системные точки восстановления.
/W:<*сек*>	Максимальное время проверки, в секундах. По умолчанию — без ограничений.
/WCL	Вывод, совместимый с drwebwcl. (Только для Консольного Сканера).
/X:S[:R]	По окончании проверки перевести машину в указанный режим: выключение/перезагрузка/ждущий режим/спящий режим.

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

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)
/AHT: <*действие*>	действия с программами взлома (возможные действия: DQIR)
/AIC: <*действие*>	действия с неизлечимыми файлами (возможные действия: DQR)
/AIN: <*действие*>	действия с инфицированными файлами (возможные действия: CDQR)
/AJK: <*действие*>	действия с программами-шутками (возможные действия: DQIR)
/AML: <*действие*>	действия с инфицированными почтовыми файлами (возможные действия: QIR)
/ARW: <*действие*>	действия с потенциально опасными файлами (возможные действия: DQIR)
/ASU: <*действие*>	действия с подозрительными файлами (возможные действия: DQIR)

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

/AC-	режим явно отключается
/AC, /AC+	режим явно включается

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

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

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

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

Пример использования ключей при запуске Консольного сканера:

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

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

16.2. Параметры для Модуля обновления

Общие параметры:

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

Параметры команды обновления (update):

Параметр	Описание
-p [--product] arg	Название продукта. Если название указано, то будет произведено обновление только этого продукта. Если продукт не указан и не указаны конкретные компоненты, будет произведено обновление всех продуктов. Если указаны компоненты, будет произведено обновление указанных компонентов.
-n [--component] arg	Перечень компонентов, которые необходимо обновить до определенной модификации. Формат: <*name*> , <*target revision*>.
-x [--selfrestart] arg (=yes)	Перезапуск после обновления Модуля обновления. По умолчанию значение `yes`. Если указано значение `no`, то выводится предупреждение о необходимости перезапуска.
--geo-update	Получить список IP-адресов `update.drweb.com` перед обновлением.

Параметр	Описание
--type arg (=normal)	Может быть одним из следующих: • `reset-all` — принудительное обновление всех компонентов; • `reset-failed` — сбросить все изменения для поврежденных компонентов; • `normal-failed` — попытаться обновить компоненты, включая поврежденные, до последней либо до указанной версии; • `update-revision` — обновить компоненты в пределах текущей ревизии; • `normal` — обновить все компоненты.
-g [--proxy] arg	Прокси-сервер для обновления в формате *<адрес>: <порт>*.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
--param arg	Передать дополнительные параметры в скрипт. Формат: *<имя>: <значение>*.
-l [--progress-to-console]	Вывести на консоль информацию о загрузке и выполнении скрипта.

Параметры команды получения компонентов (getcomponents):

Параметр	Описание
-s [--version] arg	Номер версии.
-p [--product] arg	Укажите имя продукта, чтобы увидеть, какие компоненты он включает. Если продукт не указан, будут выведены все компоненты этой версии.

Параметры команды получения изменений (getrevisions):

Параметр	Описание
-s [--version] arg	Номер версии.
-n [--component] arg	Имя компонента.

Параметры команды удаления (uninstall):

Параметр	Описание
-n [--component] arg	Имя компонента, который необходимо удалить.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.
--param arg	Передать дополнительные параметры в скрипт. Формат: <*имя*>: <*значение*>.
-e [--add-to-exclude]	Компоненты, которые будут удалены и их обновление производиться не будет.

Параметры команды автоматического обновления ключа (keyupdate):

Параметр	Описание
-m [--md5] arg	Контрольная сумма md5 старого ключевого файла.
-o [--output] arg	Имя файла.
-b [--backup]	Резервное копирование старого ключевого файла, если он существует.
-g [--proxy] arg	Прокси-сервер для обновления в формате <*адрес*>: <*порт*>.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-l [--progress-to-console]	Вывести на консоль информацию о загрузке ключевого файла.

Параметры команды скачивания (download):

Параметр	Описание
--zones arg	Файл, содержащий список зон.
--key-dir arg	Папка, в которой находится ключевой файл.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.
-g [--proxy] arg	Прокси-сервер для обновления в формате <*адрес*>: <*порт*>.
-u [--user] arg	Имя пользователя прокси-сервера.

Параметр	Описание
-k [--password] arg	Пароль пользователя прокси-сервера.
-s [--version] arg	Имя версии.
-p [--product] arg	Название продукта, который необходимо скачать.

16.3. 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.
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.

17. 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 компании «Доктор Веб».

17.1. Виды компьютерных 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 также могут нанести вред пользователю.

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 инфицированному файлу.
- *Макро-вирусы* инфицируют документы, которые используют программы из пакета Microsoft Office (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). *Макросы* – это встроенные программы, 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 инфицируют 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* инфицируют 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 инфицировании, 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.
- *Стелс-вирусы* (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т. д.) и по инфицируемым ими 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, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через интернет) 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.).
- *Чат-черви* распространяются, используя популярные программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т. д.).

Троянские программы

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

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполнять другие типы угроз, принято приписывать только троянским программам. 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.
- *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*).
- *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 (DDoS-атак).
- *Прокси-трояны* предоставляют злоумышленнику анонимный выход в интернет через компьютер жертвы.

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).

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

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-серверы 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».

17.2. Действия для обезвреживания угроз

Существует множество различных методов борьбы с компьютерными угрозами. Для надежной защиты компьютеров и сетей продукты компании «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).
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** — это также действие, позволяющее обезвредить вредоносные программы, при котором, однако, в файловой системе остаются их полноценные копии. Блокируются любые попытки обращения от и к вредоносному объекту.

18. 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 компании «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 95/98/Me;
- `WinNT` — 32-разрядные и 64-разрядные программы ОС Windows NT/2000/XP/Vista/7/8/8.1/10;
- `Win32` — 32-разрядные программы различных сред ОС Windows 95/98/Me и ОС Windows NT/2000/XP/Vista/7/8/8.1/10;
- `Win64` — 64-разрядные программы ОС Windows XP/Vista/7/8/8.1/10/11;
- `Win32.NET` — программы в ОС Microsoft .NET Framework;
- `OS2` — программы ОС OS/2;
- `Unix` — программы различных UNIX-систем;
- `Linux` — программы ОС Linux;
- `FreeBSD` — программы ОС FreeBSD;
- `SunOS` — программы ОС SunOS (Solaris);

- Symbian — программы ОС Symbian OS (мобильная ОС).

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

Вирусы, поражающие файлы MS Office

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

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

Префиксы языка разработки

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

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

К группе префиксов языка разработки можно также отнести:

- Java — вирусы для среды виртуальной машины Java.

Троянские программы

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

- PWS — троянец, ворующий пароли;
- Backdoor — троянец с RAT-функцией (Remote Administration Tool — утилита удаленного администрирования);

- IRC — троянец, использующий для своего функционирования среду Internet Relayed Chat channels;
- DownLoader — троянец, скрытно от пользователя загружающий различные вредоносные файлы из интернета;
- MulDrop — троянец, скрытно от пользователя загружающий различные вирусы, содержащиеся непосредственно в его теле;
- Proxy — троянец, позволяющий злоумышленнику работать в интернете анонимно через пораженный компьютер;
- StartPage (синоним: Seeker) — троянец, несанкционированно подменяющий адрес страницы, указанной браузеру в качестве домашней (стартовой);
- Click — троянец, организующий перенаправление пользовательских запросов браузеру на определенный сайт (или сайты);
- KeyLogger — троянец-шпион; отслеживает и записывает нажатия клавиш на клавиатуре; может периодически пересылать собранные данные злоумышленнику;
- AVKill — останавливает работу программ антивирусной защиты, сетевые экраны и т. п.; также может удалять эти программы с диска;
- KillFiles, KillDisk, DiskEraser — удаляют некоторое множество файлов (файлы в определенных каталогах, файлы по маске, все файлы на диске и т. п.);
- DelWin — удаляет необходимые для работы операционной системы (Windows) файлы;
- FormatC — форматирует диск C: (синоним: FormatAll — форматирует несколько или все диски);
- KillMBR — портит или стирает содержимое главного загрузочного сектора (MBR);
- KillCMOS — портит или стирает содержимое CMOS.

Средство использования уязвимостей

- Exploit — средство, использующее известные уязвимости некоторой операционной системы или приложения для внедрения в систему вредоносного кода, вируса или выполнения каких-либо несанкционированных действий.

Средства для сетевых атак

- Nuke — средства для сетевых атак на некоторые известные уязвимости операционных систем с целью вызвать аварийное завершение работы атакуемой системы;
- DDoS — программа-агент для проведения распределенных сетевых атак типа «отказ в обслуживании» (Distributed Denial Of Service);
- FDOS (синоним: Flooder) — Flooder Denial Of Service — программы для разного рода вредоносных действий в Сети, так или иначе использующие идею атаки типа «отказ в обслуживании»; в отличие от DDoS, где против одной цели одновременно используется множество агентов, работающих на разных компьютерах, FDOS-программа работает как отдельная, «самодостаточная» программа.

Скрипт-вирусы

Префиксы вирусов, написанных на различных языках сценариев:

- `VBS` — Visual Basic Script;
- `JS` — Java Script;
- `Wscript` — Visual Basic Script и/или Java Script;
- `Perl` — Perl;
- `PHP` — PHP;
- `BAT` — язык командного интерпретатора ОС MS-DOS.

Вредоносные программы

Префиксы объектов, являющихся не вирусами, а иными вредоносными программами:

- `Adware` — рекламная программа;
- `Dialer` — программа дозвона (перенаправляющая звонок модема на заранее запрограммированный платный номер или платный ресурс);
- `Joke` — программа-шутка;
- `Program` — потенциально опасная программа (riskware);
- `Tool` — программа-инструмент взлома (hacktool).

Разное

Префикс `generic` используется после другого префикса, обозначающего среду или метод разработки, для обозначения типичного представителя этого типа вирусов. Такой вирус не обладает никакими характерными признаками (как текстовые строки, специальные эффекты и т. д.), которые позволили бы присвоить ему какое-то особенное название.

Ранее для именования простейших безликих вирусов использовался префикс `Silly` с различными модификаторами.

Суффиксы

Суффиксы используются для именования некоторых специфических вирусных объектов:

- `generator` — объект является не вирусом, а вирусным генератором;
- `based` — вирус разработан с помощью указанного вирусного генератора или путем видоизменения указанного вируса. В обоих случаях имена этого типа являются родовыми и могут обозначать сотни и иногда даже тысячи вирусов;
- `dropper` — указывает, что объект является не вирусом, а инсталлятором указанного вируса.

19. Приложение Г. Основные термины и понятия

А

Антивирусная сеть — совокупность компьютеров, на которых установлены продукты Dr.Web (Антивирус Dr.Web для Windows, Антивирус Dr.Web для серверов Windows и Dr.Web Security Space) и которые подключены к одной локальной сети.

Д

Доверенные приложения — приложения, подписи которых добавлены в список доверенных в drwbase.db. К доверенным приложениям относится популярное ПО, такое как Google Chrome, Firefox, приложения Microsoft.

З

Зеркало обновлений — папка, в которую копируются обновления. Зеркало обновлений может быть использовано как источник обновлений Dr.Web для компьютеров в локальной сети, которые не подключены к интернету.

К

Классы устройств — устройства, выполняющие одинаковые функции (например, устройства для печати).

М

Модификация вируса — код, полученный таким изменением известного вируса, что при этом он опознается сканером, но алгоритмы лечения исходного вируса к нему неприменимы.

Р

Режим администратора — режим Dr.Web, в котором предоставляется доступ ко всем параметрам компонентов защиты и настройкам программы. Для перехода в режим администратора необходимо нажать на замок .

С

Сигнатура (вирусная запись) — непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы.

Х

Хеш-сумма — уникальный идентификатор файла, представляющий собой последовательность цифр и букв заданной длины. Используется для проверки целостности данных.

Ш

Шины устройств — подсистемы передачи данных между функциональными блоками компьютера (например, шина USB).

Э

Эвристика — предположение, статистическая значимость которого подтверждена опытным путем.

Эксплойт — программа, фрагмент кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на систему.

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки. полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Эмуляция — имитация работы одной системы средствами другой без потери функциональных возможностей и искажений результатов посредством использования специальных программных средств.