Dr.WEB

Агент для Windows

Руководство пользователя

Агент Dr.Web для Windows
Версия 13.0
Руководство пользователя
15.04.2025

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 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 Агент Dr.Web для Windows, а также рекомендации по его использованию и решению типичных проблем, связанных с компьютерными угрозами. В основном рассматриваются стандартные режимы работы компонентов программы Агент Dr.Web для Windows (с настройками по умолчанию).

В Приложениях содержится общая справочная информация, а также дополнительные параметры для настройки программы Агент Dr.Web для Windows, 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 — Агент Dr.Web 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;
- URL — (от англ. Uniform Resource Locator) унифицированный локатор ресурса;
- ОС — операционная система;
- ПО — программное обеспечение.

2. О продукте

Агент Dr.Web 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.

Агент Dr.Web 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.

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

Агент Dr.Web для Windows осуществляет контроль целостности состава продукта каждый раз при загрузке обновлений, а также непрерывно защищает собственные файлы и процессы от случайных повреждений и несанкционированного вмешательства в процессе работы. Таким образом Агент Dr.Web для Windows обеспечивает защиту от вредоносных действий, направленных на работу антивирусных программ.

Информацию о версии продукта, составе компонентов, дате последнего обновления и идентификационный номер Агента Dr.Web вы можете найти на странице **Поддержка** в разделе О программе.

2.1. Компоненты защиты и модули управления

Агент Dr.Web 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

Компонент/модуль	Описание
	также обнаруживает проявления вредоносной активности.
SpIDer Gate	Компонент, который используется для антивирусной проверки HTTP-трафика. При настройках по умолчанию интернет-монитор SpIDer Gate автоматически проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих угрозы. Также по умолчанию включена URL-фильтрация нерекомендуемых сайтов и сайтов, известных как источники распространения угроз. Осуществляет проверку по протоколам HTTP, XMPP (Jabber) и TLS (SSL).
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. SpIDer Mail также может проверять письма на спам с помощью Антиспама Dr.Web.
Брандмауэр Dr.Web	Компонент, который позволяет ограничивать сетевые подключения согласно заданным параметрам.
Офисный контроль	Компонент, который ограничивает доступ к сайтам, файлам и папкам, а также позволяет ограничить время работы в интернете и за компьютером.
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 программ-шифровальщиков.
Сканер	Сканер с графическим интерфейсом, который запускается по запросу пользователя 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 и спама.
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 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 неизвестной угрозы 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.

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.

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.

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.

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

2.3. Системные требования

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

Параметр	Требования
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 22H2 или более ранняя; • Windows Server 2003 с пакетом обновлений SP1; • Windows Server 2008 с пакетом обновлений SP2 или более поздними. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7 с пакетом обновлений SP1 или более поздними; • Windows 8; • Windows 8.1; • Windows 10 22H2 или более ранняя; • Windows 11 22H2 или более ранняя; • Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows Server 2008 R2 с пакетом обновлений SP1 или более поздними; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022; • Windows Server 2025
Оперативная память	512 МБ и больше
Разрешение экрана	Рекомендуется не менее 1024 × 768
Поддержка виртуальных и облачных сред	Поддерживается функционирование программы в следующих средах: • VMware; • Hyper-V;

Параметр	Требования
	• Xen; • KVM
Прочее	Для обновления вирусных баз Dr.Web и компонентов Dr.Web требуется подключение к серверу централизованной защиты или интернету в Мобильном режиме. 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 Агент Dr.Web для Windows на Windows Vista, Windows 7, Windows Server 2008 или Windows Server 2008 R2 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».

Агент Dr.Web для Windows версии 13.0 совместим только с продуктами Dr.Web версии 12.0:

- Dr.Web Mail Security Suite (Microsoft Exchange Server);
- Dr.Web Mail Security Suite (IBM Lotus Domino Windows).

Стабильная и безошибочная работа Dr.Web не гарантируется на оборудовании с нестандартной конфигурацией, такой как разогнанные процессоры, измененные параметры памяти и напряжения питания.

3. Установка, изменение и удаление программы

Перед началом установки Агент Dr.Web 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 и ОС Windows Server); 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 межсетевые экраны;
- начиная с Windows Server 2016 отключить Защитник Windows вручную, используя групповые политики;
- закрыть активные приложения.

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

Dr.Web несовместим с другими антивирусными программами (в том числе с другими версиями антивирусных программ Dr.Web). Установка нескольких антивирусных продуктов на один компьютер может привести к системным ошибкам и потере важных данных. Если на компьютере уже установлен другой антивирус, то его необходимо удалить, используя установочный файл или стандартные средства операционной системы.

Установку, изменение и удаление Dr.Web можно осуществить двумя способами:

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

Установка Dr.Web возможна в одном из следующих режимов:

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

3.1. Установка при помощи полного инсталлятора

Полный инсталлятор `drweb-13.0.x-xxxxxxx-esuite-agent-full-windows.exe` осуществляет установку Агента Dr.Web и антивирусного пакета единовременно. Параметры подключения к серверу и параметры авторизации станции на сервере не включаются в инсталлятор.

Установка в режиме мастера установки

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 **Выход**.

Чтобы установить Dr.Web

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

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

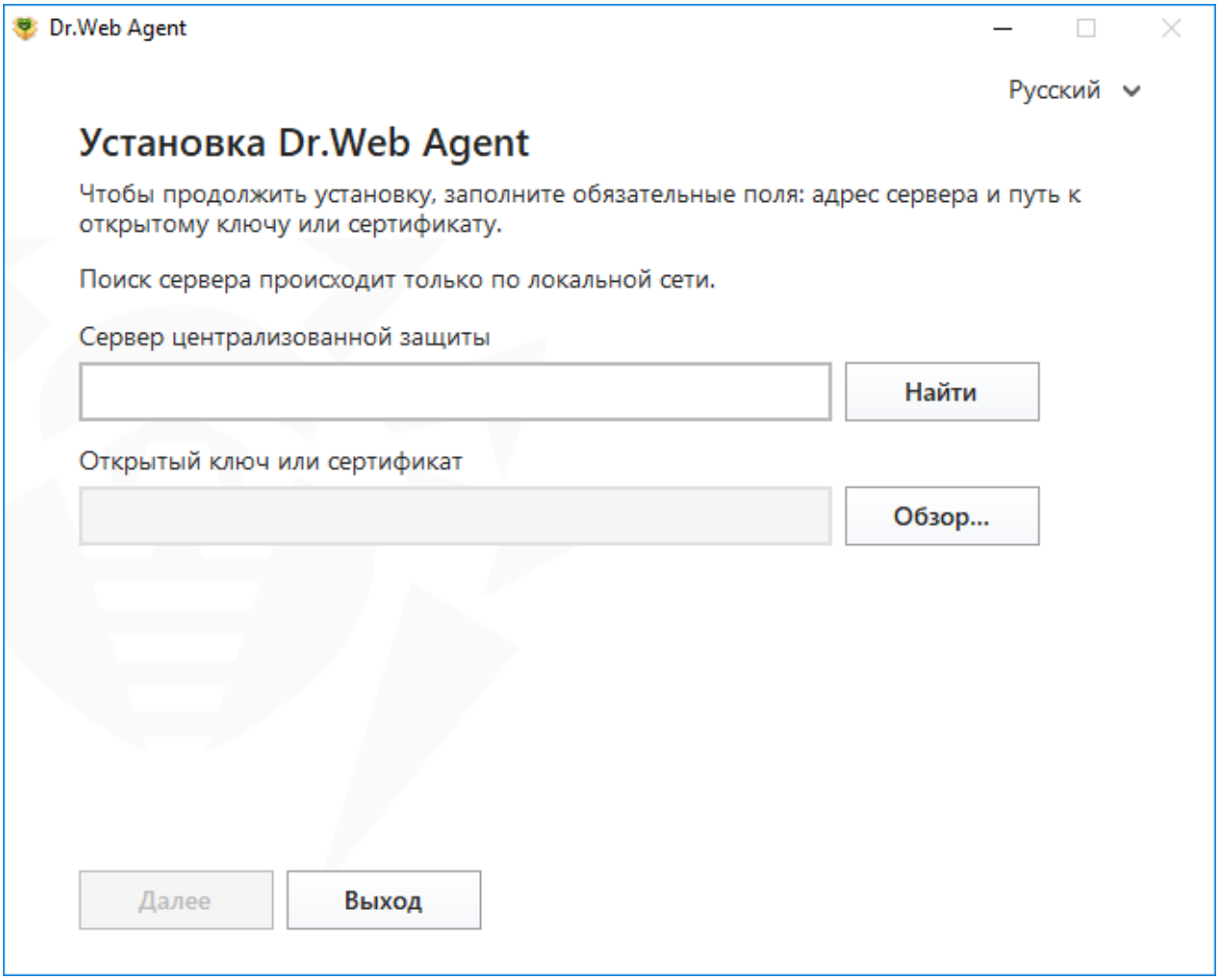

Рисунок 1. Мастер установки

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

   Для поиска активных серверов и указания параметров поиска нажмите кнопку **Найти**.

   Нажмите кнопку **Далее**.
3. Мастер установки проинформирует вас о готовности к установке.

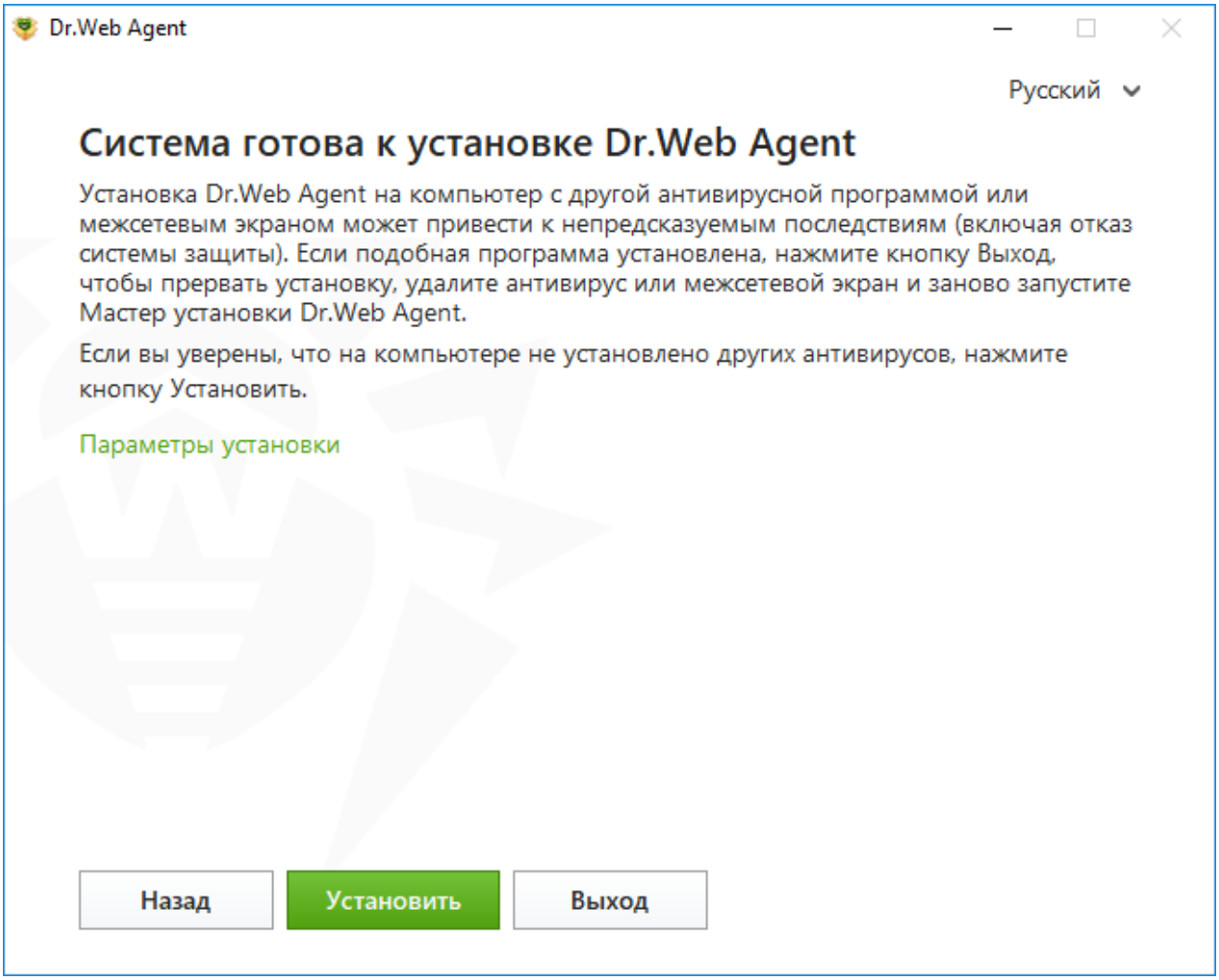

Рисунок 2. Готовность к установке

Вы можете запустить процесс установки с параметрами по умолчанию, нажав **Установить**.

Чтобы выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры установки, нажмите ссылку **Параметры установки**. Данная опция предназначена для опытных пользователей.

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

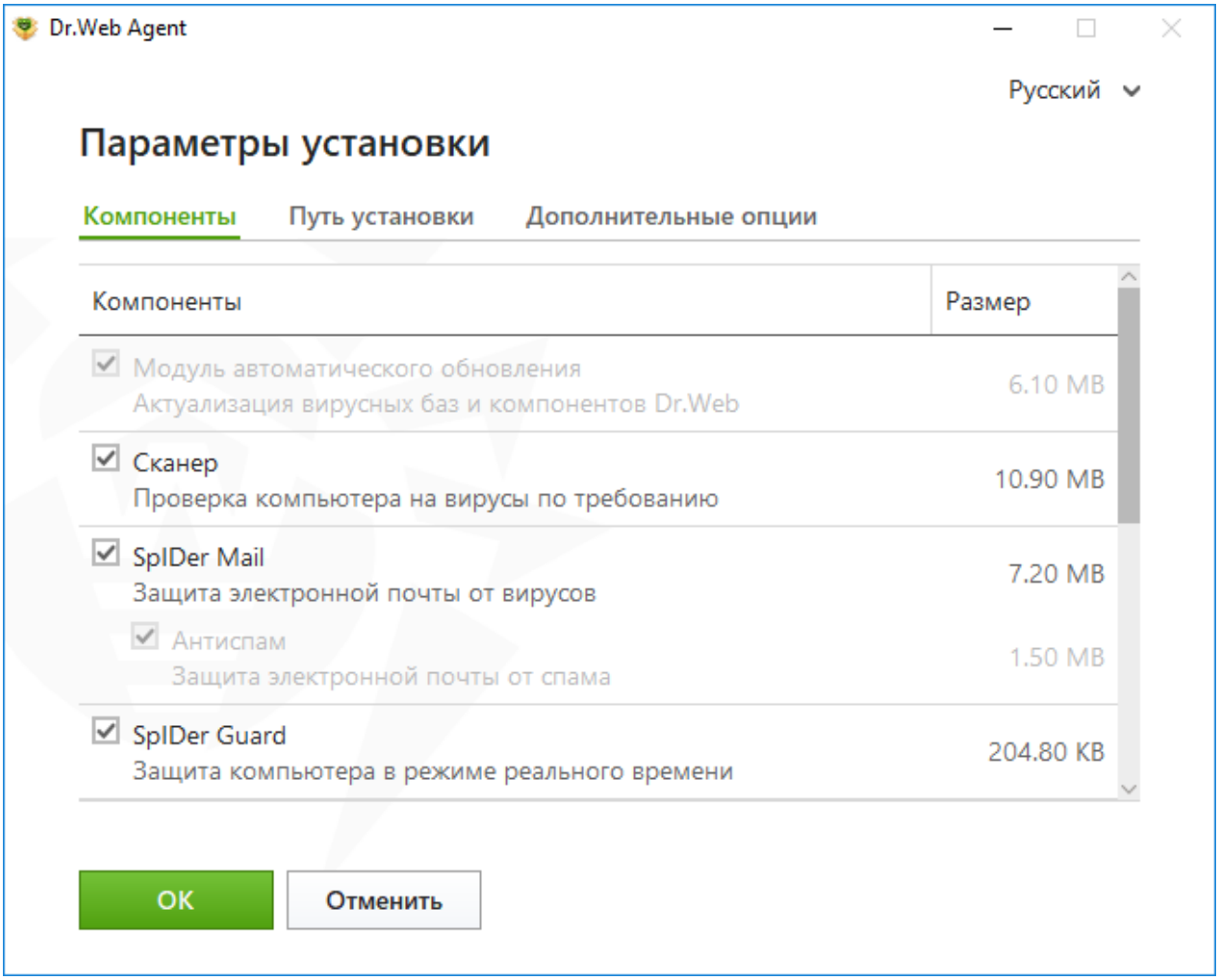

Рисунок 3. Параметры установки

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

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

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

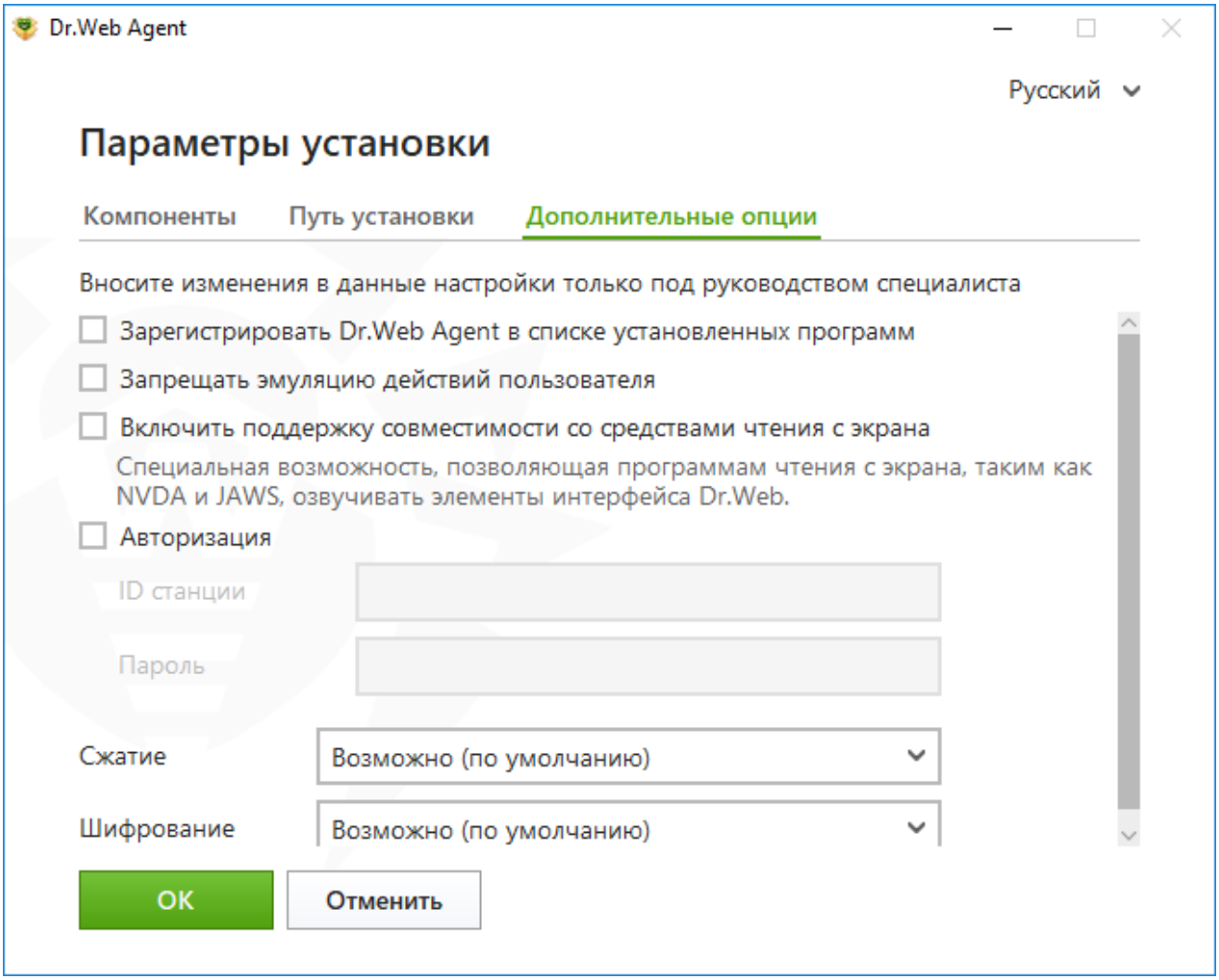

Рисунок 4. Дополнительные опции параметров установки

Доступны следующие опции:

- **Зарегистрировать Dr.Web Agent в списке установленных программ**. Данная опция позволяет, в том числе, осуществлять удаление и изменение компонентов программы Dr.Web с помощью Панели управления Windows.
- **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 и других действий, направленных на изменение работы Dr.Web).
- Для авторизации на сервере централизованной защиты вручную активируйте флажок **Авторизация**. Далее необходимо задать параметры авторизации станции:
  - **ID станции** — идентификатор станции на сервере;
  - **Пароль** — пароль для доступа к серверу.

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

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

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

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

Установка в режиме командной строки

Для запуска установки Dr.Web в режиме командной строки перейдите в папку, где расположен дистрибутив, после чего введите имя исполняемого файла установки (`drweb-13.0.x-xxxxxxx-esuite-agent-full-windows.exe`) с необходимыми параметрами.

Полный список параметров командной строки для инсталляционных пакетов приведен в Приложении А.

3.2. Установка при помощи персонального инсталляционного пакета

При установке программы при помощи персонального инсталляционного пакета производится установка продукта по сети.

Персональный инсталляционный пакет включает в себя инсталлятор Агента Dr.Web и набор параметров подключения к Серверу Dr.Web и авторизации станции на Сервере Dr.Web.

Установка в режиме мастера установки

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 **Выход**.

Чтобы установить Dr.Web

1. Запустите инсталляционный пакет `drweb_ess_windows_<имя станции>.exe`, полученный от администратора. Откроется Мастер установки Dr.Web.

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

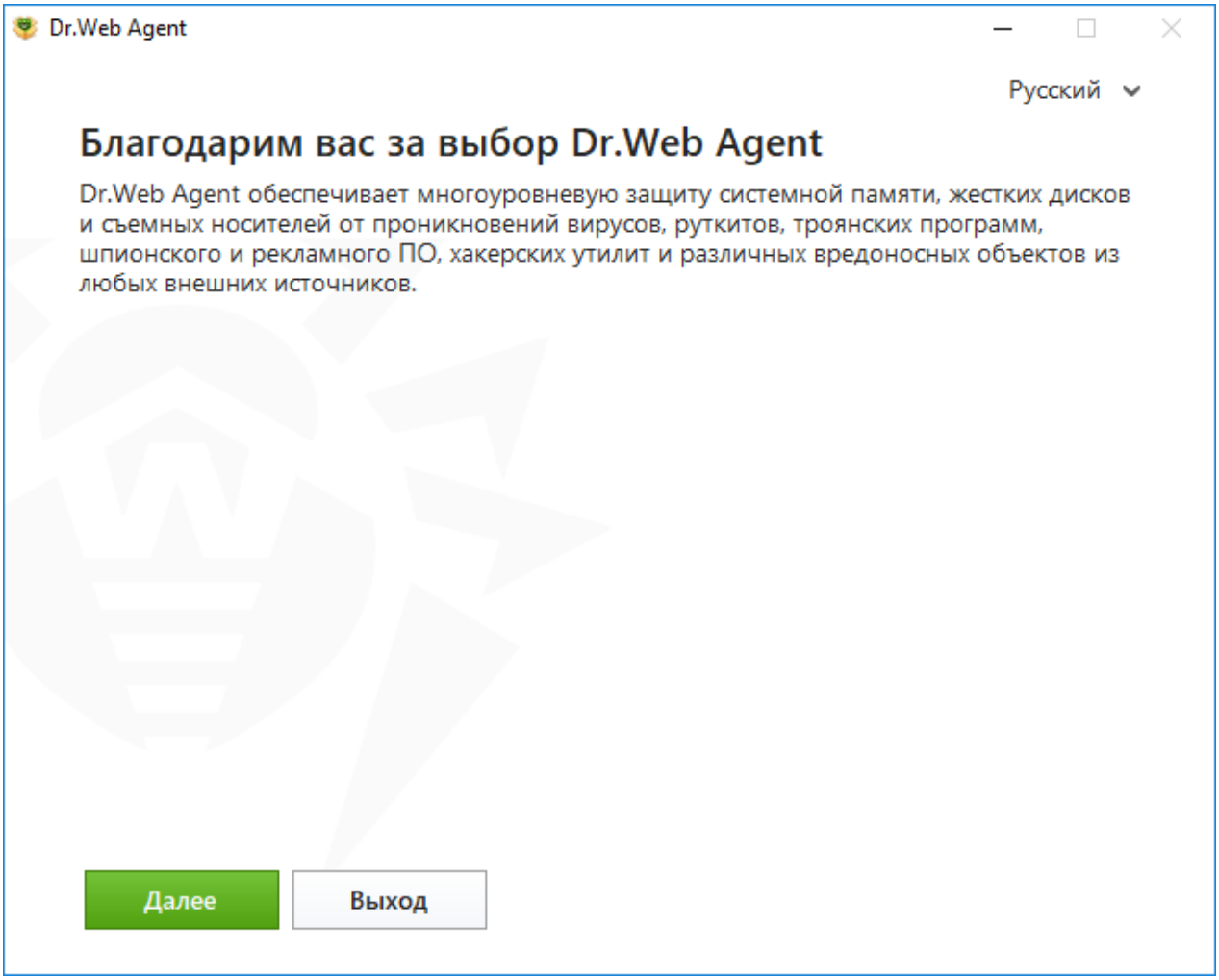

Рисунок 5. Мастер установки

2. Нажмите **Далее**.
3. На следующем шаге мастера укажите путь к открытому ключу шифрования (`drwcsd.pub`) или сертификату с расширением `.pem`, расположенному на вашем компьютере.

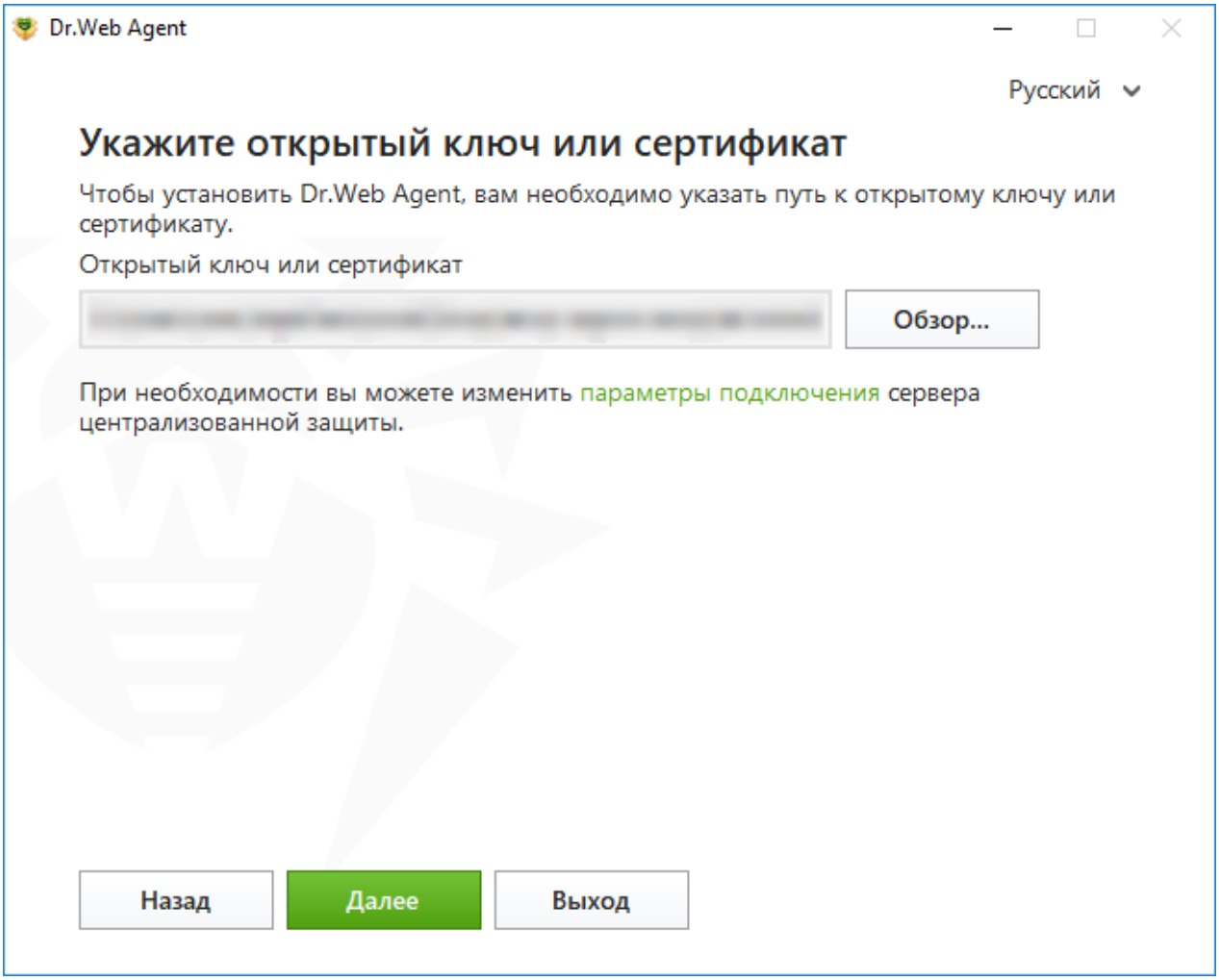

Рисунок 6. Указание открытого ключа или сертификата

4. При необходимости вы можете изменить параметры подключения к серверу централизованной защиты. Для этого перейдите по соответствующей ссылке. Откроется окно **Параметры соединения**. При установке при помощи персонального инсталляционного пакета все параметры соединения уже указаны.

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

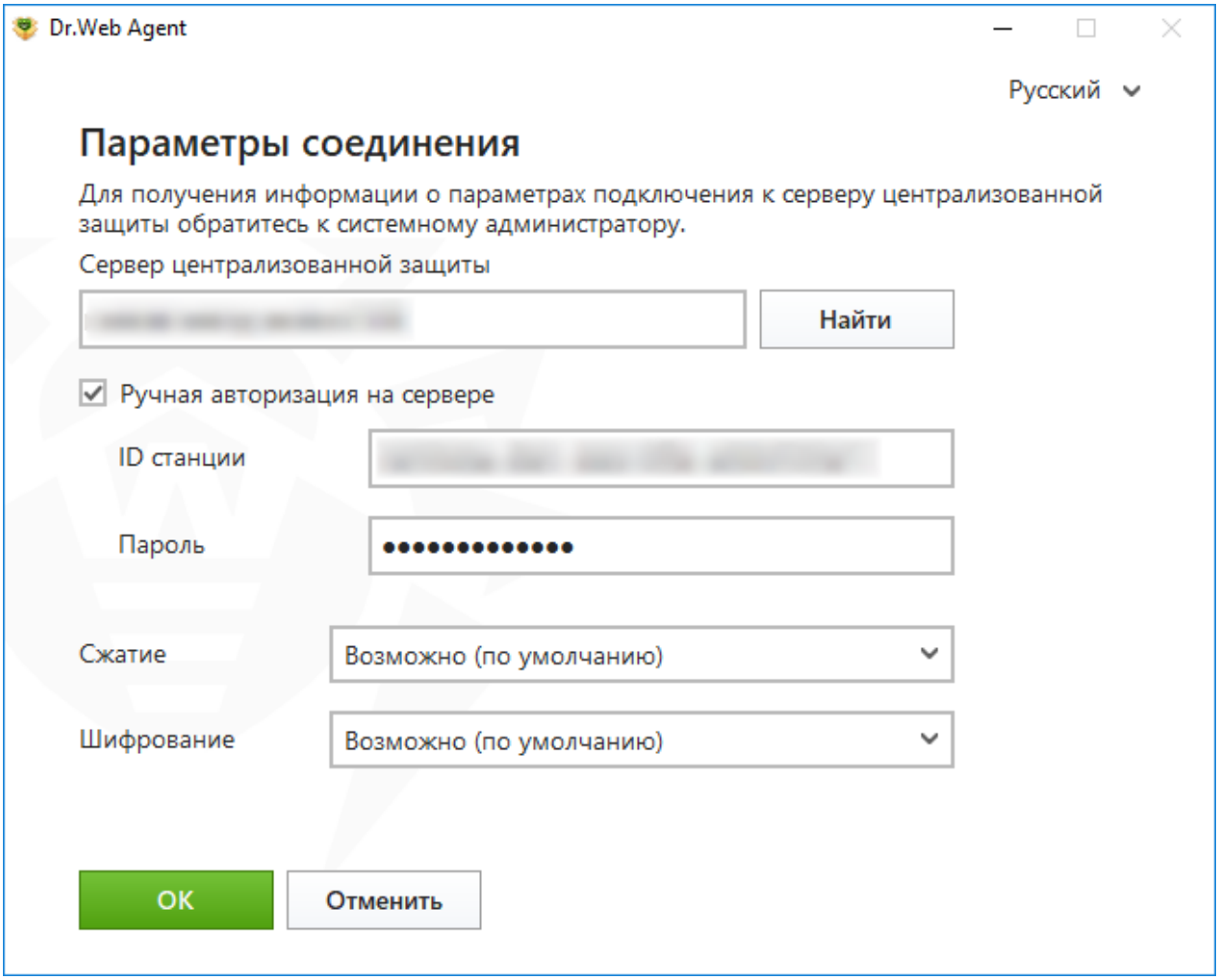

Рисунок 7. Установка параметров соединения с сервером централизованной защиты

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

В поле **Сервер централизованной защиты** вы можете задать сетевой адрес сервера, с которого будет производиться установка Dr.Web. По умолчанию в поле указаны данные сервера, на котором был создан установочный файл. Для поиска активных серверов и указания параметров поиска нажмите кнопку **Найти**.

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

- **ID станции** — идентификатор станции на сервере;
- **Пароль** — пароль для доступа к серверу.

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

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

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

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

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

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

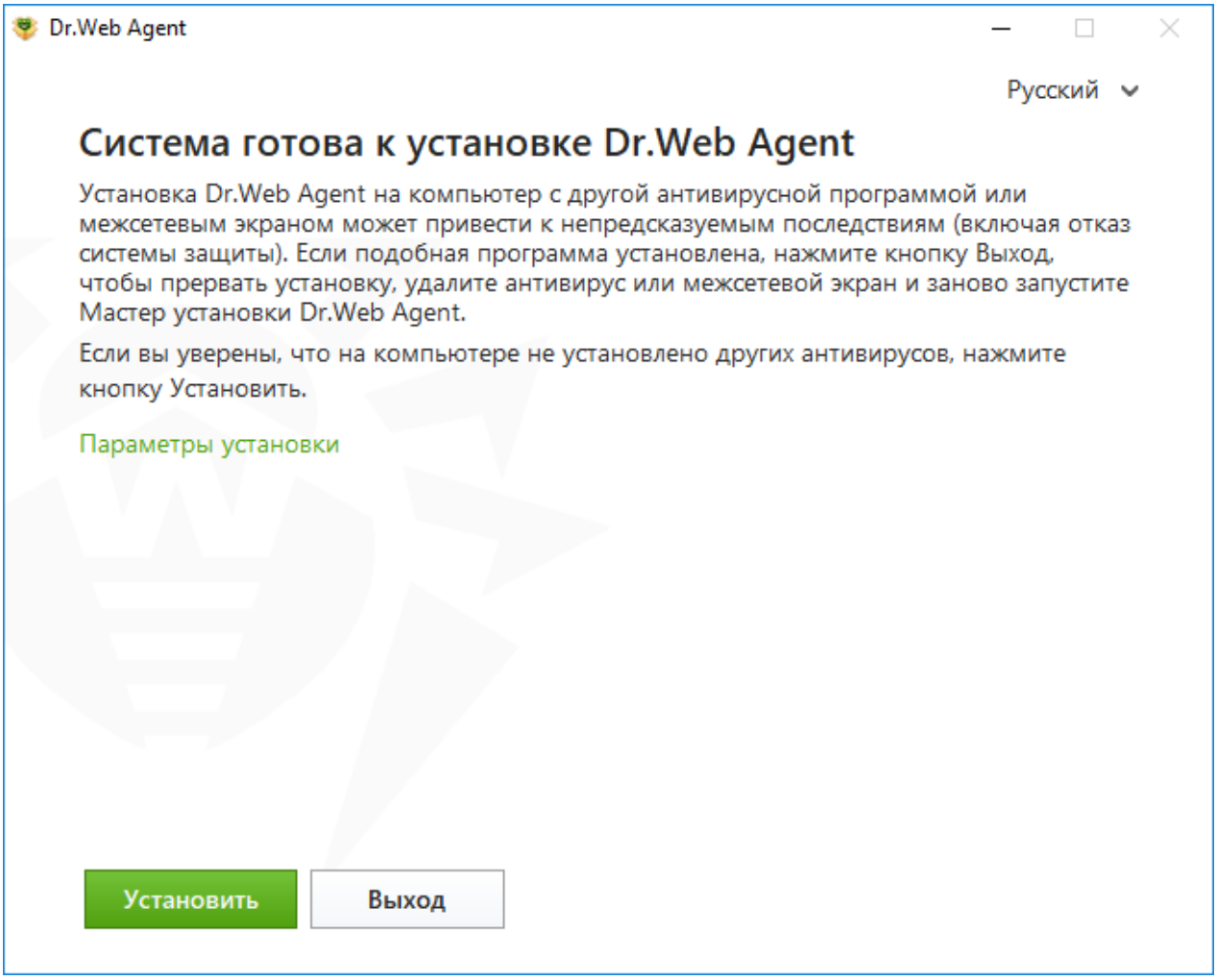

Рисунок 8. Готовность к установке

Чтобы выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры установки, нажмите ссылку **Параметры установки**. Данная опция предназначена для опытных пользователей.

6. Если на предыдущем шаге вы нажали кнопку **Установить**, то перейдите к шагу 9. В противном случае откроется окно **Параметры установки**.

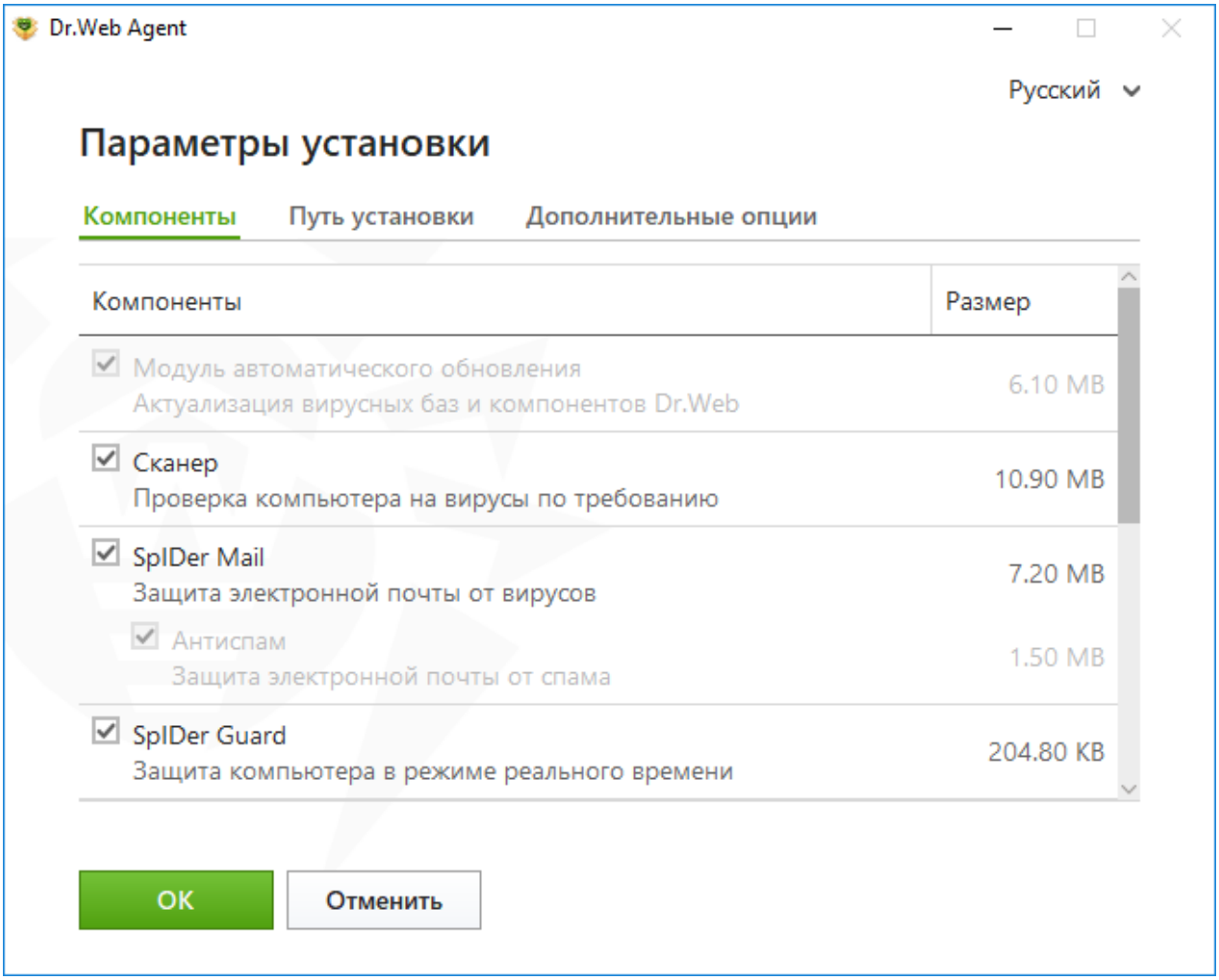

Рисунок 9. Параметры установки

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

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

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

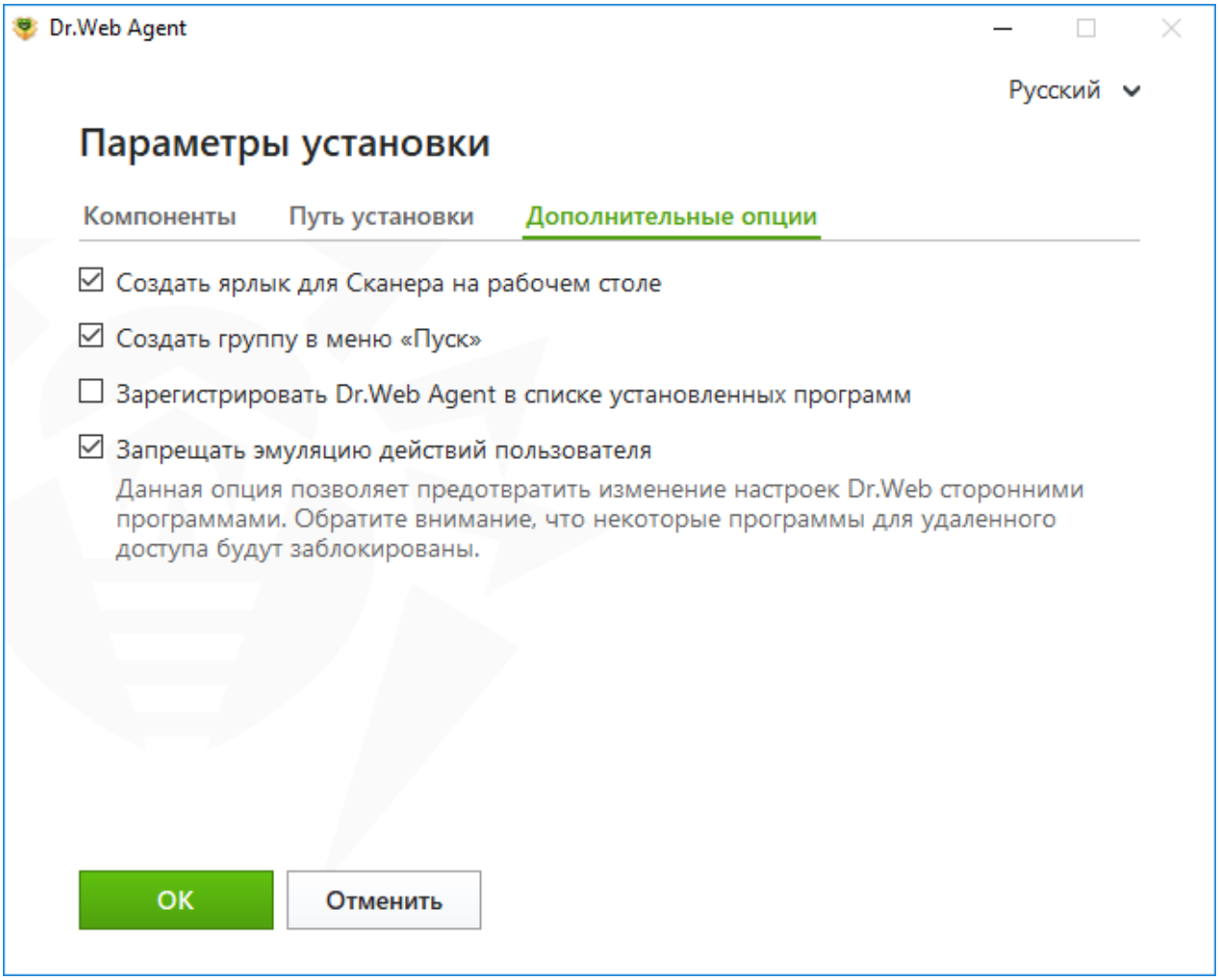

Рисунок 10. Дополнительные опции параметров установки

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

Опция **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 и других действий, направленных на изменение работы Dr.Web).

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

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

Установка в режиме командной строки

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

Полный список параметров командной строки для инсталляционных пакетов приведен в Приложении А.

Ошибка службы BFE при установке программы Dr.Web

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

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

1. Просканируйте систему станции при помощи лечащей утилиты CureNet! от компании «Доктор Веб». Вы можете запросить демонстрационную версию утилиты (диагностика без функции лечения) по адресу https://download.drweb.com/curenet/.

   Ознакомиться с условиями использования и стоимостью полной версии утилиты вы можете по адресу https://estore.drweb.com/utilities/.
2. Восстановите службу BFE. Для операционных систем Windows 7 и выше вы можете воспользоваться утилитой для устранения проблем в работе брандмауэра от компании Microsoft. На операционных системах Windows Server вручную запустите или перезапустите службу BFE. Если запустить службу BFE не удалось или служба отсутствует в списке, обратитесь в службу технической поддержки компании Microsoft.
3. Запустите Мастер установки Dr.Web и произведите установку согласно штатной процедуре, приведенной выше.

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

3.3. Изменение компонентов программы

Изменение компонентов программы возможно, если администратор антивирусной сети дал на это разрешение.

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. Перейдите в раздел Панели управления Windows, посвященный установке и удалению программ.
  2. В списке установленных программ выберите строку **Dr.Web Agent**.
  3. Нажмите кнопку **Изменить**.

Чтобы удалить или добавить компоненты

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

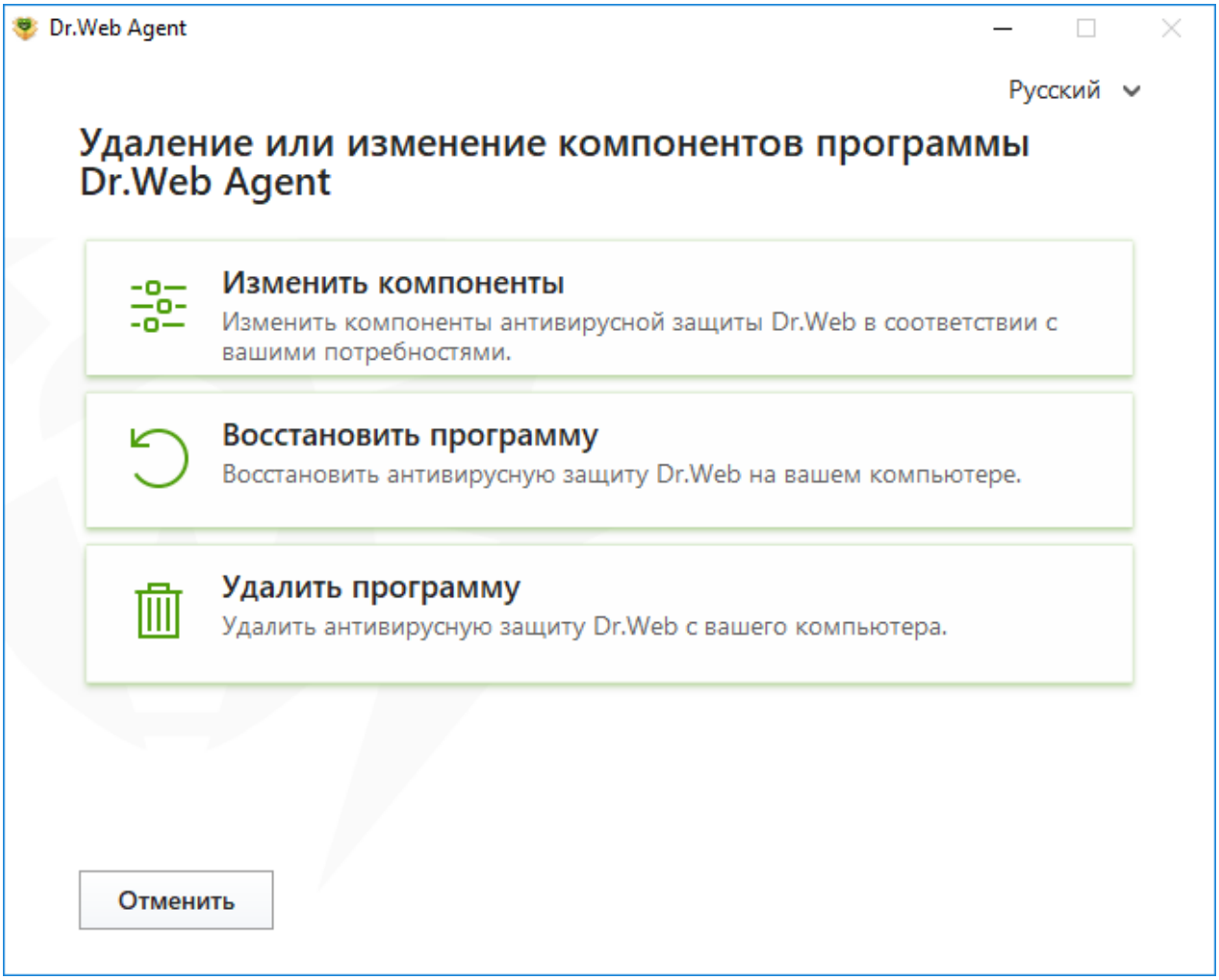

Рисунок 11. Мастер удаления/изменения компонентов

2. В открывшемся окне установите флажки напротив компонентов, которые хотите добавить, либо снимите флажки напротив удаляемых компонентов.
3. Нажмите **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.

3.4. Удаление и переустановка программы

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

После удаления Dr.Web ваш компьютер не будет защищен от угроз.

Удаление Dr.Web из Панели управления Windows

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

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

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

1. Для удаления Агент Dr.Web для Windows запустите компонент удаления программ операционной системы Windows.
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 Agent** и **Защищаемые копии файлов**. Нажмите кнопку **Далее**.
5. В следующем окне для подтверждения удаления Dr.Web нажмите кнопку **Удалить**.
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.

Удаление в режиме командной строки

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

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

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

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

Переустановка Dr.Web

1. Получите у администратора антивирусной сети актуальный инсталляционный пакет.
2. Удалите продукт, как описано выше.
3. Перезагрузите компьютер.
4. Заново установите программу, используя полученный инсталляционный пакет. На этапе установки укажите путь к ключевому файлу.
5. Перезагрузите компьютер.

4. Проверка работы программы

Проверка антивируса

Проверка с помощью файла EICAR

Вы можете проверить работоспособность антивирусных программ, обнаруживающих угрозы 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 угрозы. Программа test.com не является сама по себе вредоносной, но специально обрабатывается большинством антивирусных программ как угрозу. Dr.Web называет эту «угрозу» следующим образом: `EICAR Test File (Not a Virus!)`. Примерно так ее 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 описанной «угрозой».

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 целостности

После установки Dr.Web целостность программы поддерживается динамически в процессе ее работы и во время загрузки обновлений следующими способами:

- Самозащита беспрерывно защищает файлы и процессы Dr.Web от несанкционированных изменений.
- Dr.Web выполняет проверку целостности компонентов программы и вирусных баз по контрольным суммам загружаемых файлов во время каждого обновления.

Чтобы проверить целостность Dr.Web, не дожидаясь запуска обновления, вы можете воспользоваться опцией Восстановить программу в окне Мастера удаления/изменения компонентов.

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**.

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

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

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

Для доступа к параметрам компонентов необходимо ввести пароль, если в настройках вы включили опцию **Защищать настройки Dr.Web паролем**.

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

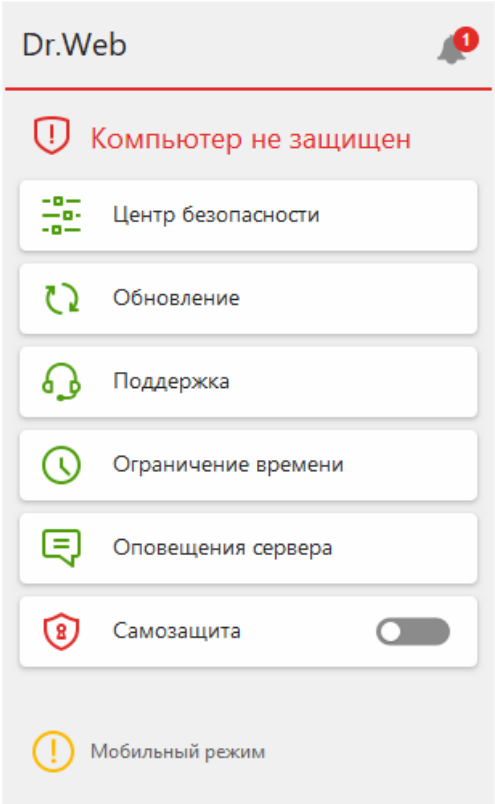

Рисунок 12. Меню программы

Пункты меню программы

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, в том числе компоненту Офисный контроль, и исключениям.

Обновление (появляется только при работе Dr.Web в мобильном режиме). Информация об актуальности вирусных баз и времени последнего обновления. Запускает обновление компонентов программы и вирусных баз.

Поддержка. Открывает окно поддержки.

Ограничение времени (появляется при включенной опции ограничения времени работы за компьютером и в интернете компонента Офисный контроль). Краткая информация об ограничениях работы за компьютером и в интернете, а также о длительности перерыва при интервальном ограничении.

Оповещения сервера (появляется при наличии оповещений, а также при включении соответствующей опции на сервере). Открывает окно просмотра оповещений сервера.

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

Статус подключения к серверу. Статус отображается, только если в данный момент станция не подключена к серверу. При успешном подключении статус в меню не отображается.

Всего отображается пять статусов:

Обозначение	Статус
	• Станция ожидает подтверждения на сервере • Мобильный режим • Подключение к серверу централизованной защиты
	• Нет соединения с сервером • Ошибка соединения

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, соединение с сервером централизованной защиты установлено.
	Самозащита или хотя бы один из компонентов отключены либо вирусные базы устарели, что ослабляет защиту антивируса и компьютера; либо ожидается соединение с сервером, но ещё не установлено. Возможно, сервер отклонил подключение рабочей станции или отказал в доступе к своим ресурсам. Включите Самозащиту или отключенный компонент, дождитесь соединения с сервером или обратитесь к администратору вашей антивирусной сети, если соединение не устанавливается.
	Ожидается запуск компонентов после старта операционной системы, дождитесь запуска компонентов программы; либо в процессе запуска одного из ключевых компонентов Dr.Web возникла ошибка, компьютер находится под угрозой заражения. Если иконка не изменится, обратитесь к администратору вашей антивирусной сети.

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**.

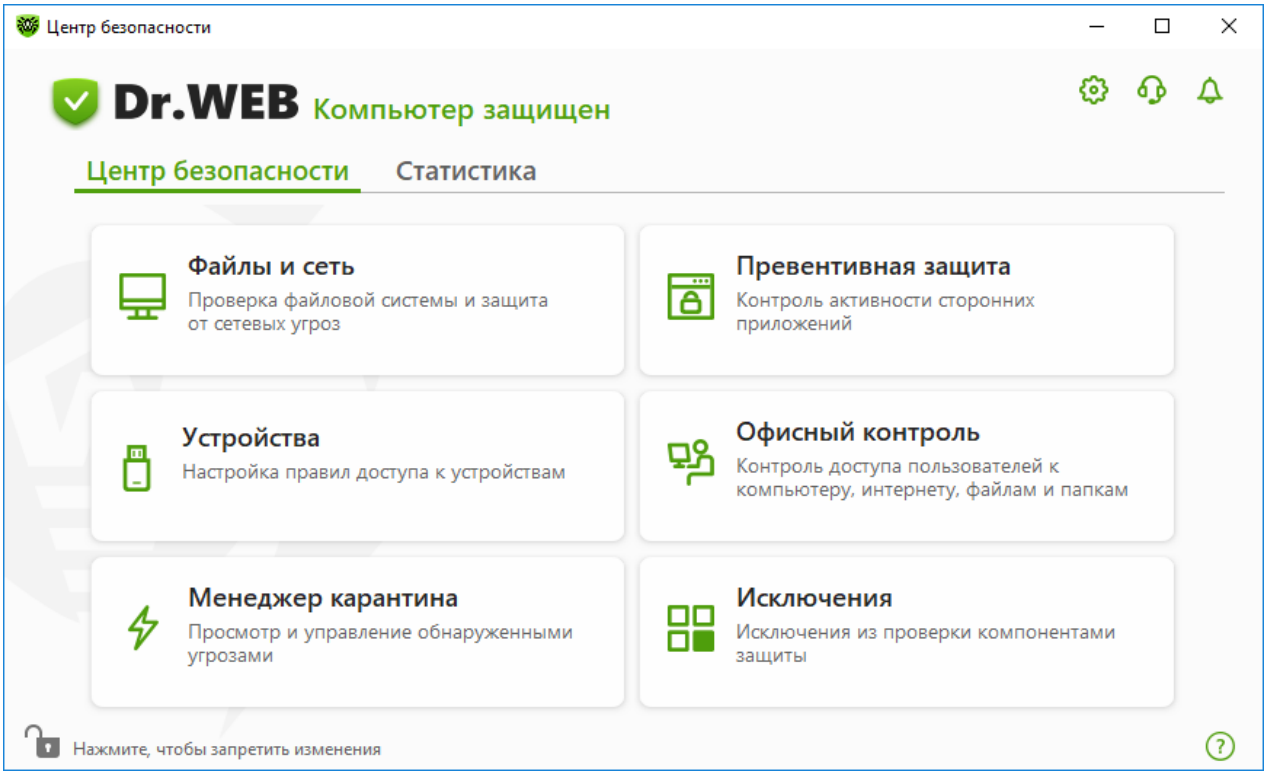

Рисунок 13. Окно Центр безопасности

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;

- Устройства;
- Офисный контроль;
- Менеджер карантина;
- 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 управления всеми группами 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 инструменту **Менеджер карантина**. Также, не переключая Dr.Web в режим администратора, вы можете включить любой из компонентов защиты и запустить Сканер. Выключение компонентов защиты, управление параметрами компонентов и изменение настроек программы возможны только в режиме администратора.

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

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.

7. 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.

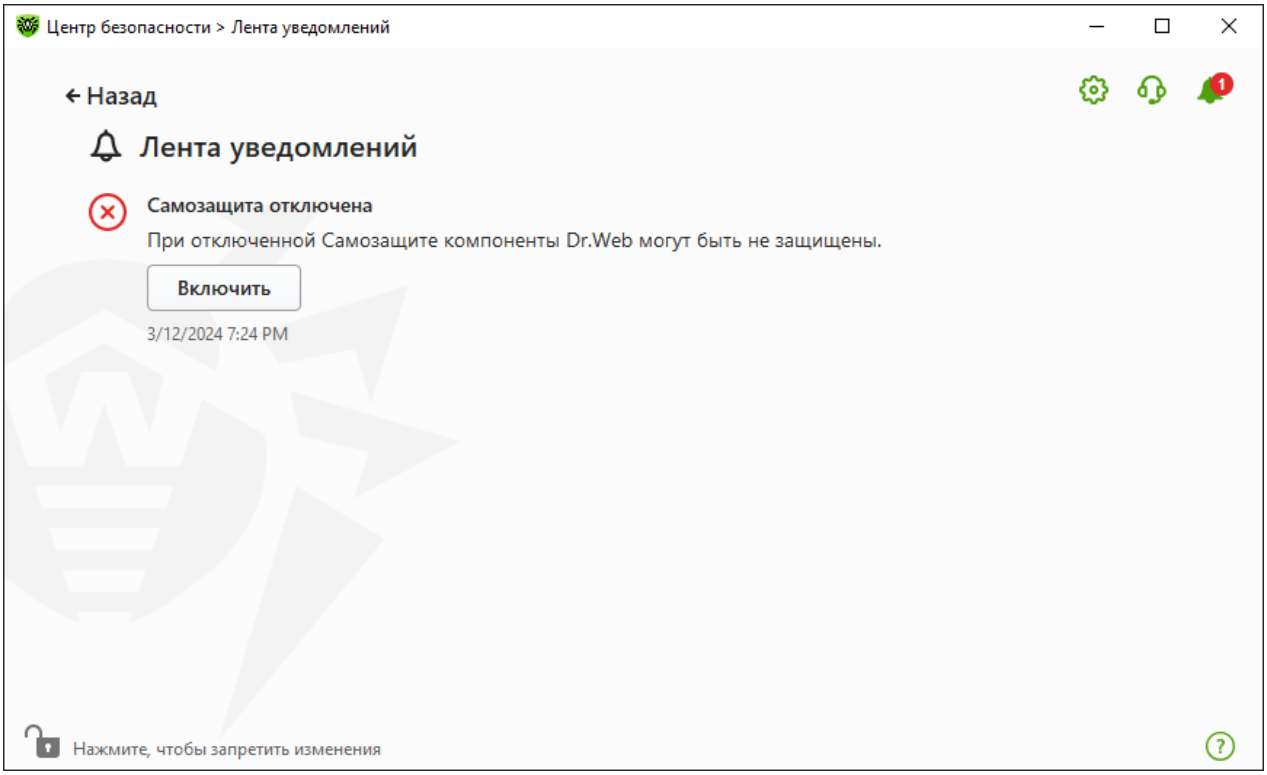

Рисунок 14. Окно ленты уведомлений

Срок хранения уведомлений

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

Типы уведомлений

Критические уведомления	
Угрозы	• Обнаружена угроза. • Требуется перезагрузка для обезвреживания угроз. • Вирусные базы устарели.
Соединение с сервером	• Соединение с сервером запрещено. • Ошибка подключения к серверу.
Запрет доступа к объектам и устройствам	• Устройство заблокировано в соответствии с настройками.
Важные уведомления	
Обновление	• Требуется перезагрузка, чтобы обновления вступили в силу.
Маловажные информационные уведомления	
Новая версия	• Доступна новая версия продукта.
Новое сообщение	• Администратором отправлено новое сообщение.

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).

8. 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.

> Изменение настроек возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.
>
> 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, выбор цвета темы интерфейса.
- Уведомления — настройка вывода уведомлений на экран.
- Самозащита — настройка дополнительных параметров безопасности.
- Параметры проверки файлов — настройка параметров работы Сканера.
- Сервер Dr.Web — настройка параметров подключения к серверу централизованной защиты.
- Оповещения сервера — настройка параметров отображения Оповещений сервера.

8.1. Общие настройки

К общим настройкам относятся следующие:

- защита настроек программы паролем;
- выбор цвета темы интерфейса;
- выбор языка программы;
- 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**.

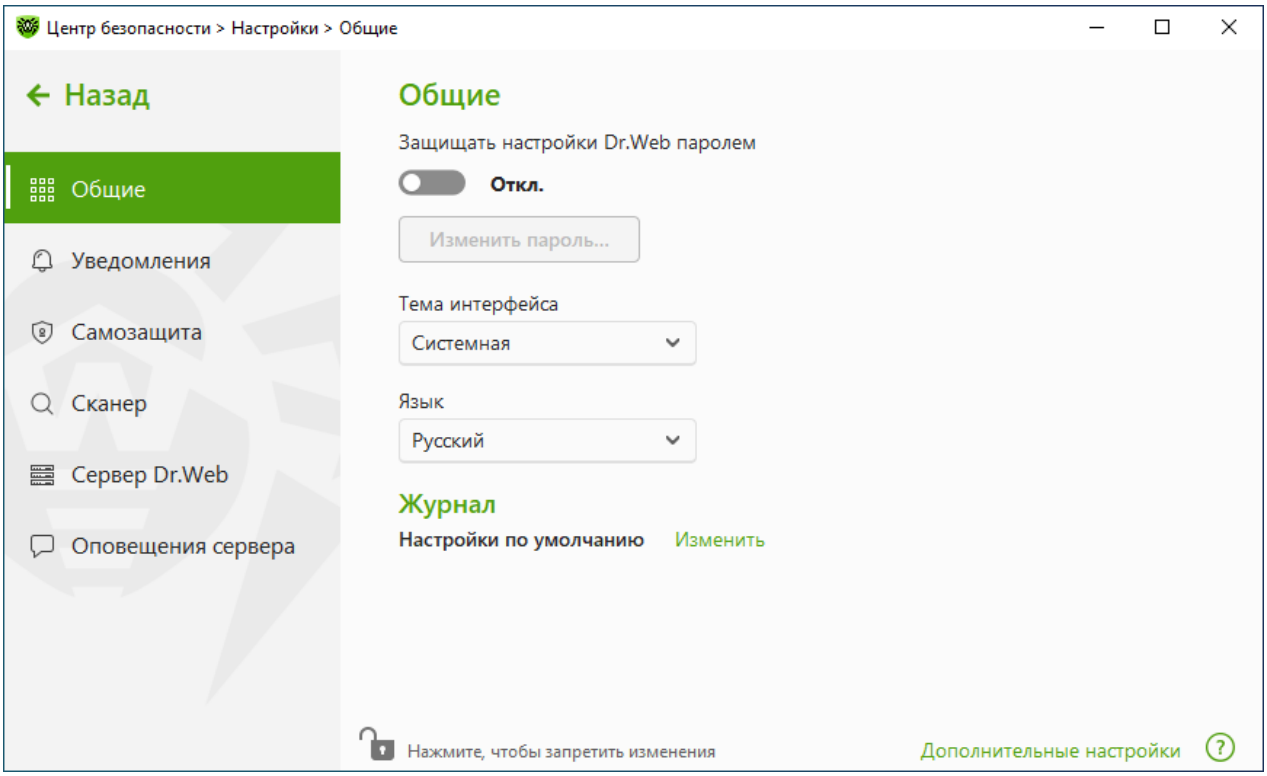

Рисунок 15. Общие настройки

8.1.1. 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 .

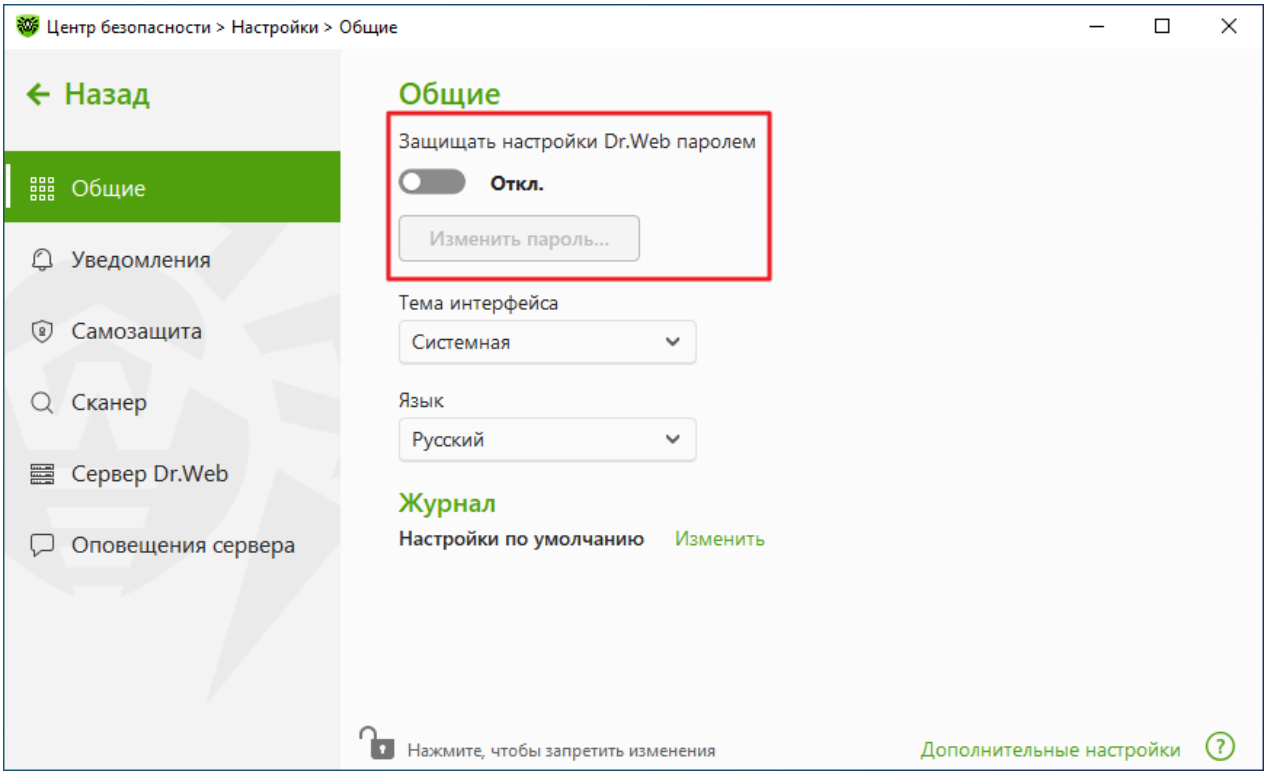

Рисунок 16. Защита настроек паролем

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

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

8.1.2. Выбор цвета темы интерфейса

При необходимости вы можете изменить цвет темы интерфейса программы. Для этого в выпадающем списке **Тема интерфейса** выберите одну из опций:

- **Светлая**, чтобы использовать светлое оформление программы.
- **Темная**, чтобы использовать темное оформление программы.
- **Системная**, чтобы использовать цвет интерфейса, соответствующий теме, выбранной в операционной системе. Эта опция выбрана по умолчанию.

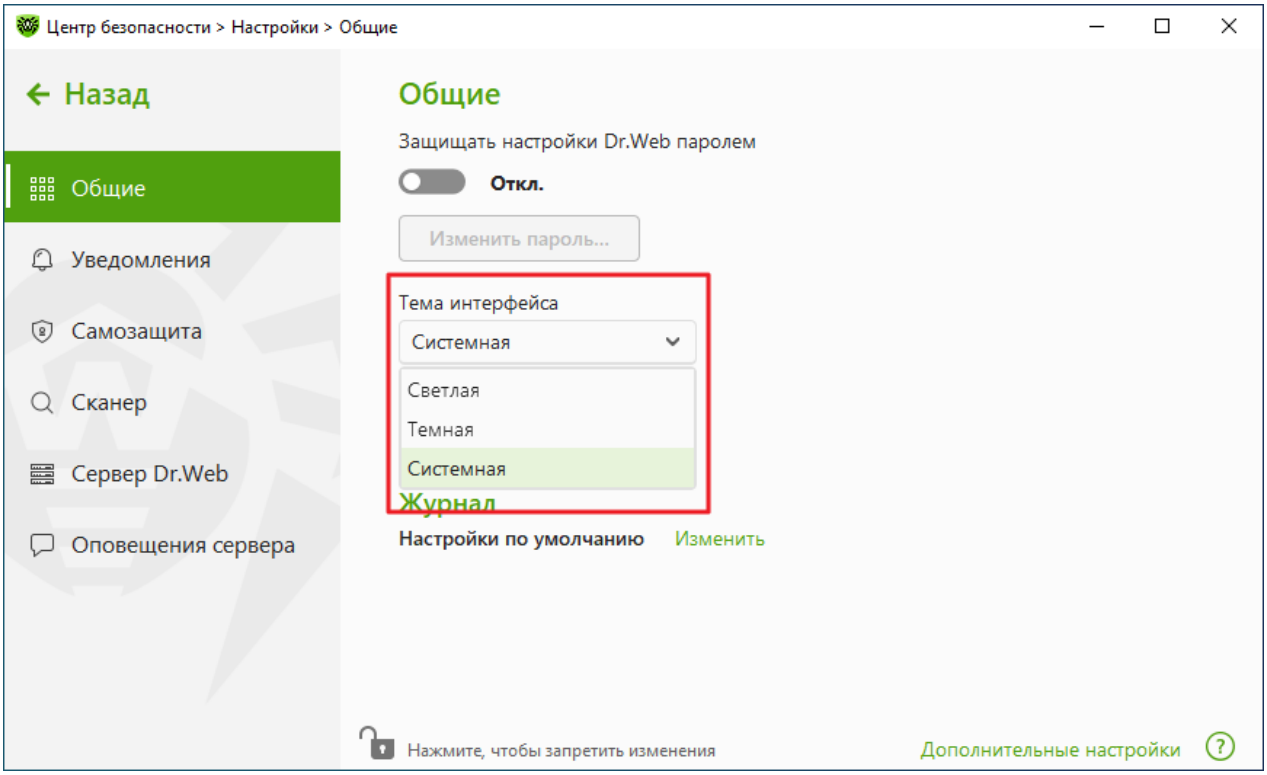

Рисунок 17. Выбор цвета темы интерфейса

Темная тема доступна только на компьютерах с операционной системой Windows 10 (начиная с версии 1909), Windows 11 и Windows Server 2019 (начиная с версии 1809) и более поздних. Настройки выбора цвета темы интерфейса скрыты для более ранних версий операционной системы.

Для корректного отображения темной темы интерфейса требуется установленное обновление KB5011503 или более позднее.

8.1.3. 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.

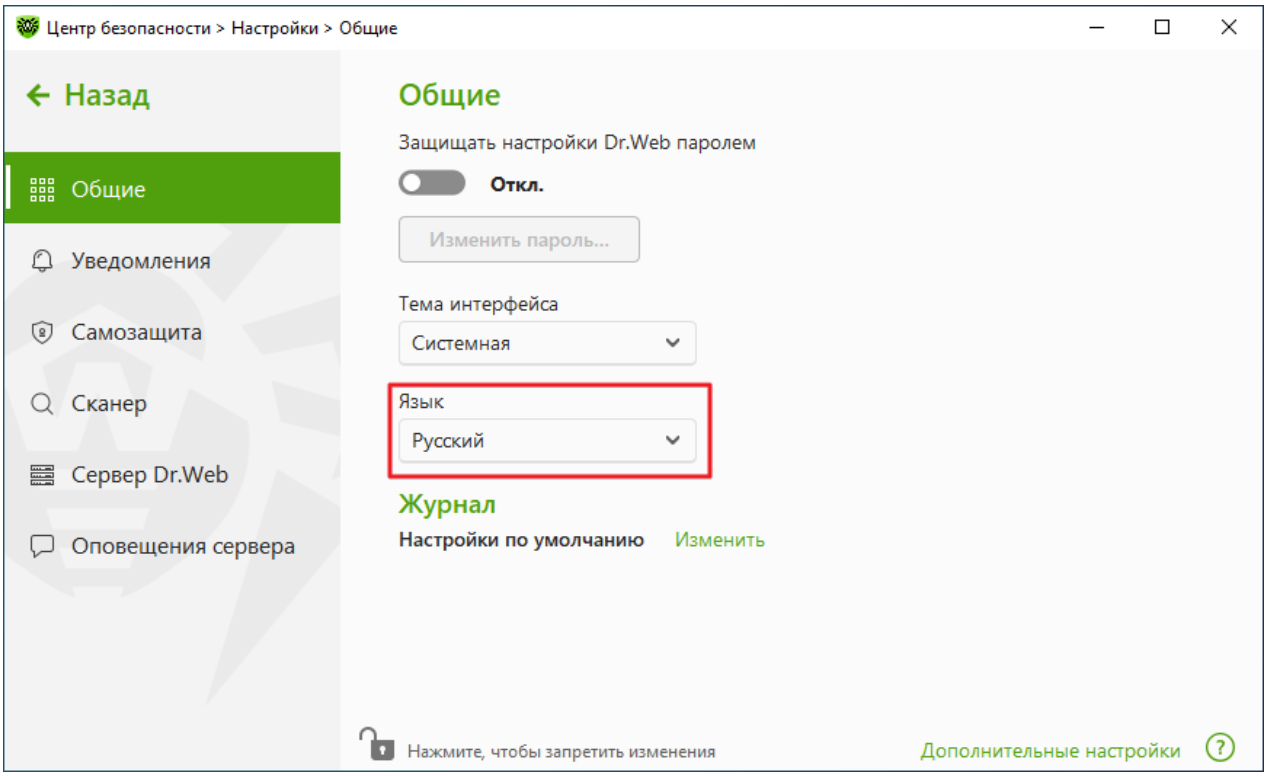

Рисунок 18. Выбор языка программы

8.1.4. Ведение журнала работы Dr.Web

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

Чтобы изменить настройки ведения журнала

1. В разделе настроек **Журнал** нажмите кнопку **Изменить**.

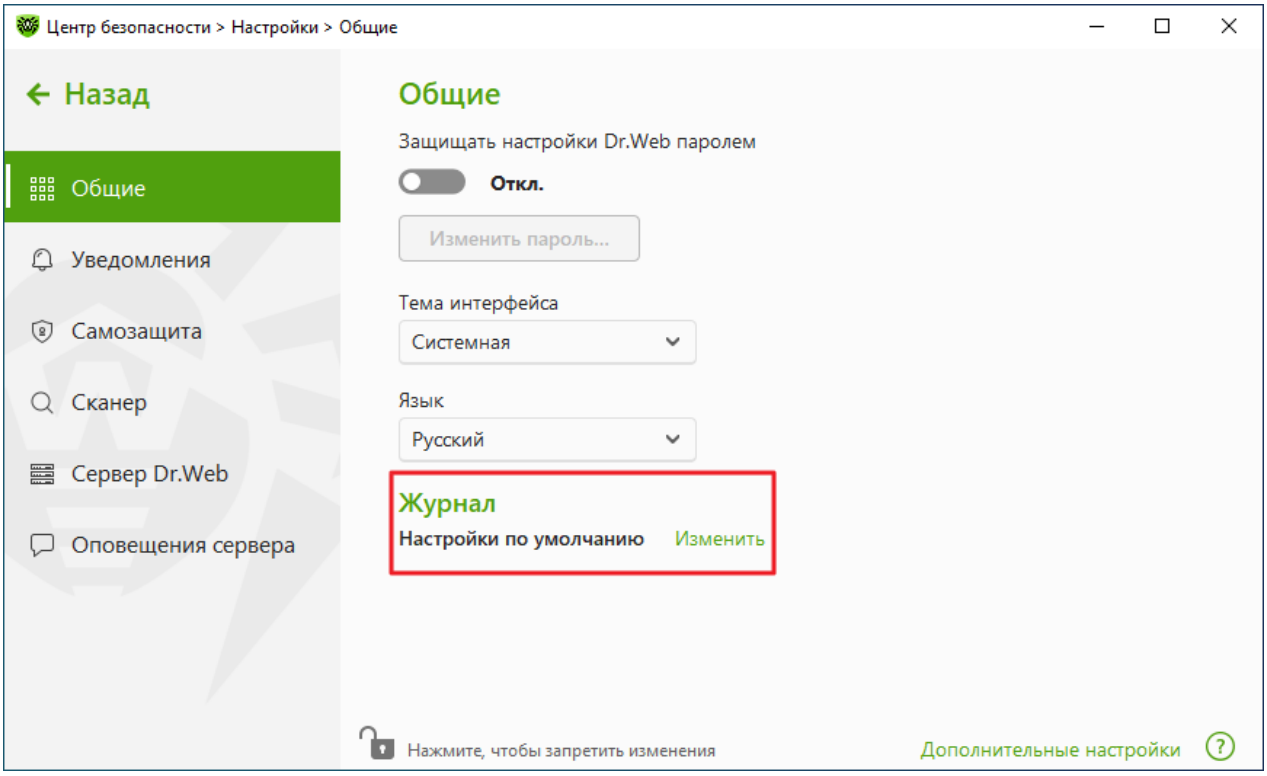

Рисунок 19. Общие настройки. Журнал

Откроется окно настроек ведения подробного журнала:

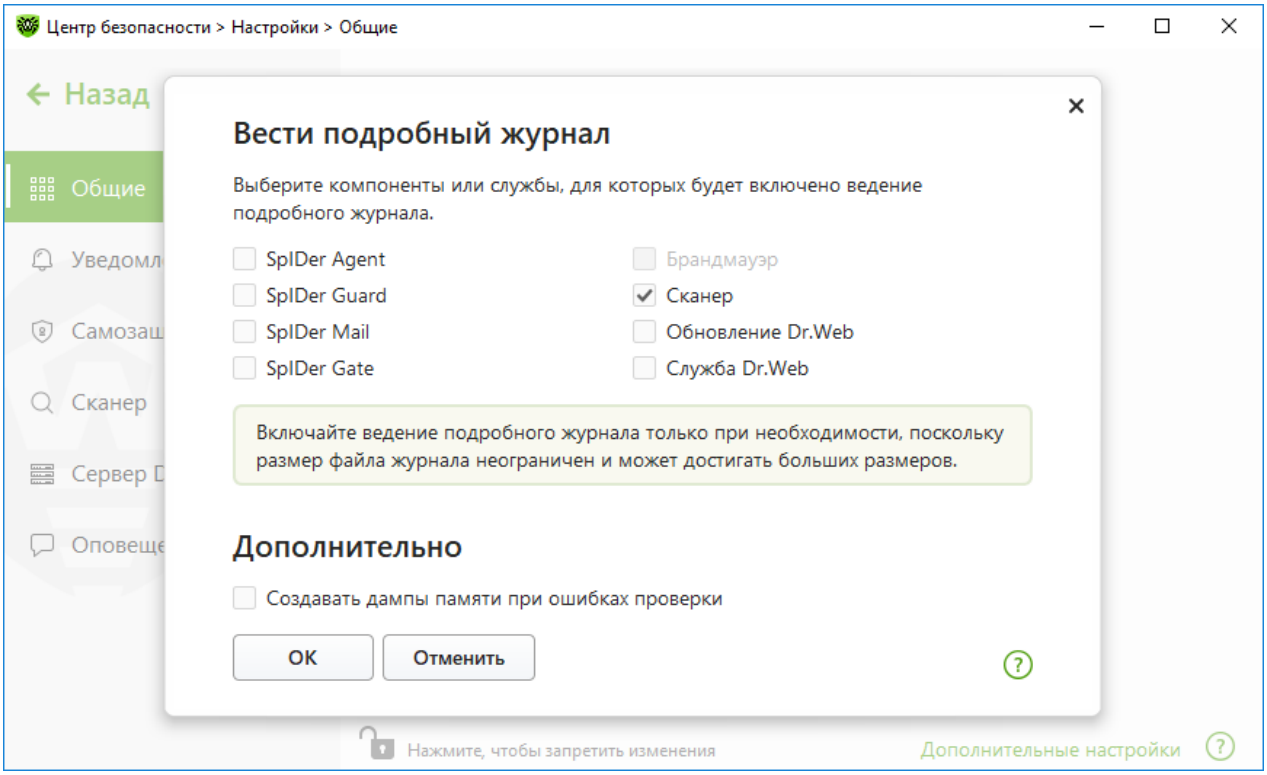

Рисунок 20. Настройки ведения журнала работы

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

Компонент	Информация
SpIDer Agent	Проведение обновлений, запуск и остановка SpIDer Agent, обнаруженные угрозы, соединение с сервером централизованной защиты, состояние работы компонентов Dr.Web, уведомления об ошибках, уведомления о перезагрузке системы. Рекомендуется использовать этот режим для получения детальной информации об источниках ошибок в работе программы.
SpIDer Guard	Проведение обновлений, запуск и остановка SpIDer Guard, обнаруженные угрозы, 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 SpIDer Guard проверяет наиболее часто. При необходимости добавьте такие объекты в список исключений, что может снизить нагрузку на компьютер.
SpIDer Mail	Проведение обновлений, запуск и остановка почтового антивируса SpIDer Mail, обнаруженные угрозы, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов. Рекомендуется использовать этот режим для проверки настроек перехвата соединений с почтовыми серверами.
SpIDer Gate	Проведение обновлений, запуск и остановка интернет-монитора SpIDer Gate, обнаруженные угрозы, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов. Рекомендуется использовать этот режим для получения более детальной информации о проверенных объектах и работе интернет-монитора.
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 службу 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 серверу централизованной защиты.

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 администратора вашей антивирусной сети.

1. Чтобы включить режим ведения подробного журнала для одного из компонентов Dr.Web, установите соответствующий флажок.
2. Сохраните изменения, нажав кнопку **OK**.

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

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ (для компонента 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.

8.1.5. 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 .

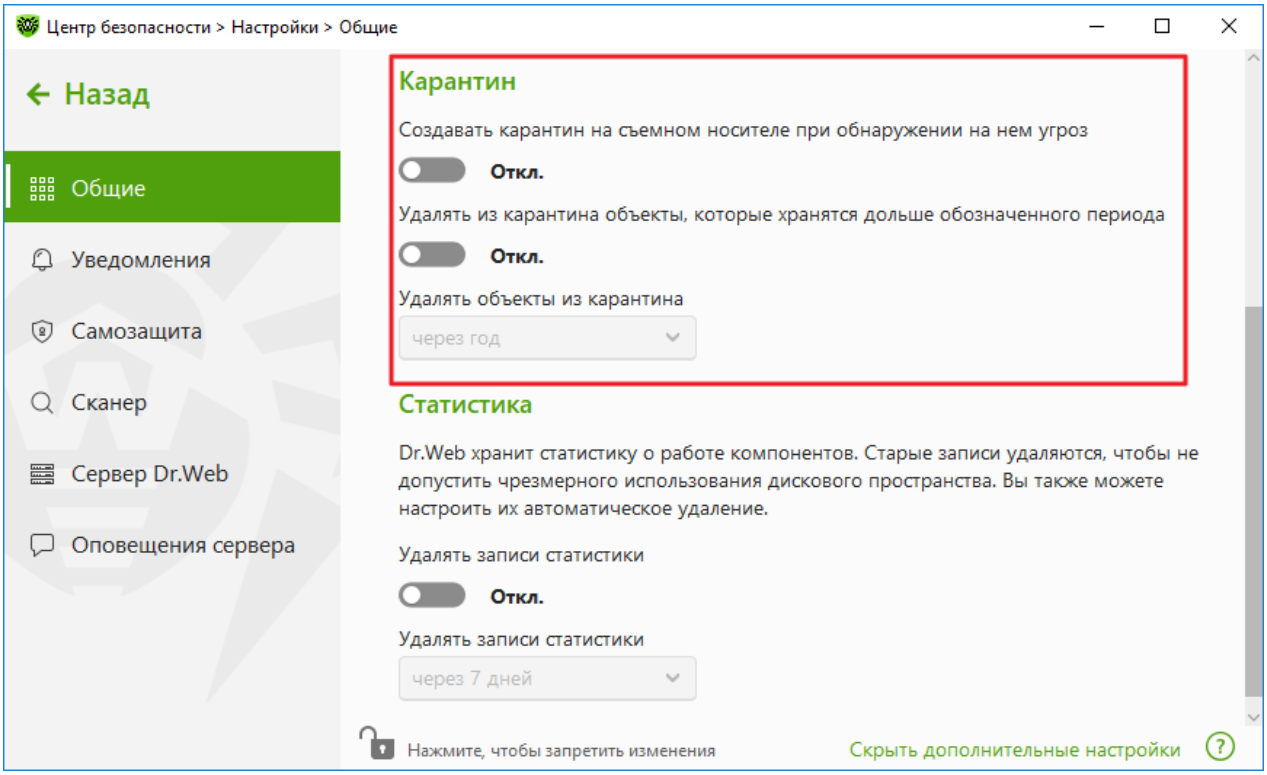

Рисунок 21. Настройки карантина

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.

8.1.6. 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 .

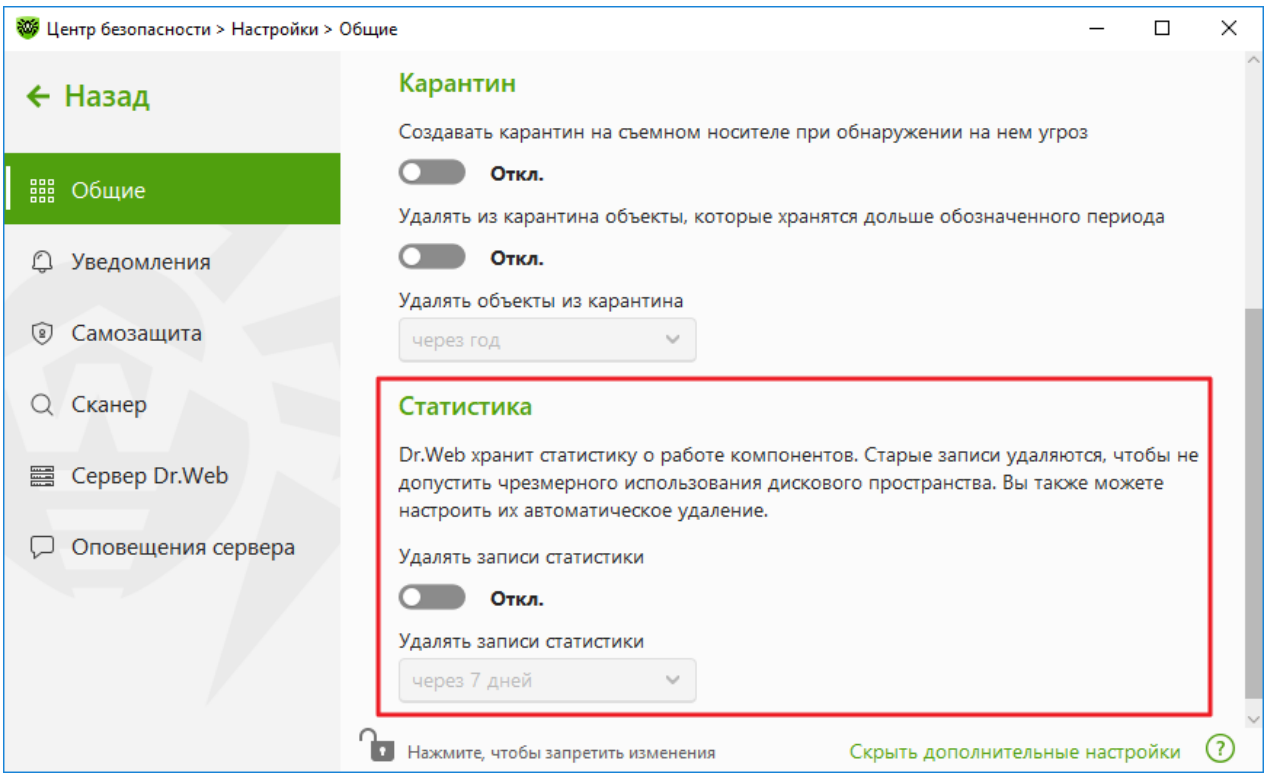

Рисунок 22. Настройки статистики

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

8.2. Настройки уведомлений

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

В этом разделе:

- Настройка параметров уведомлений

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**.

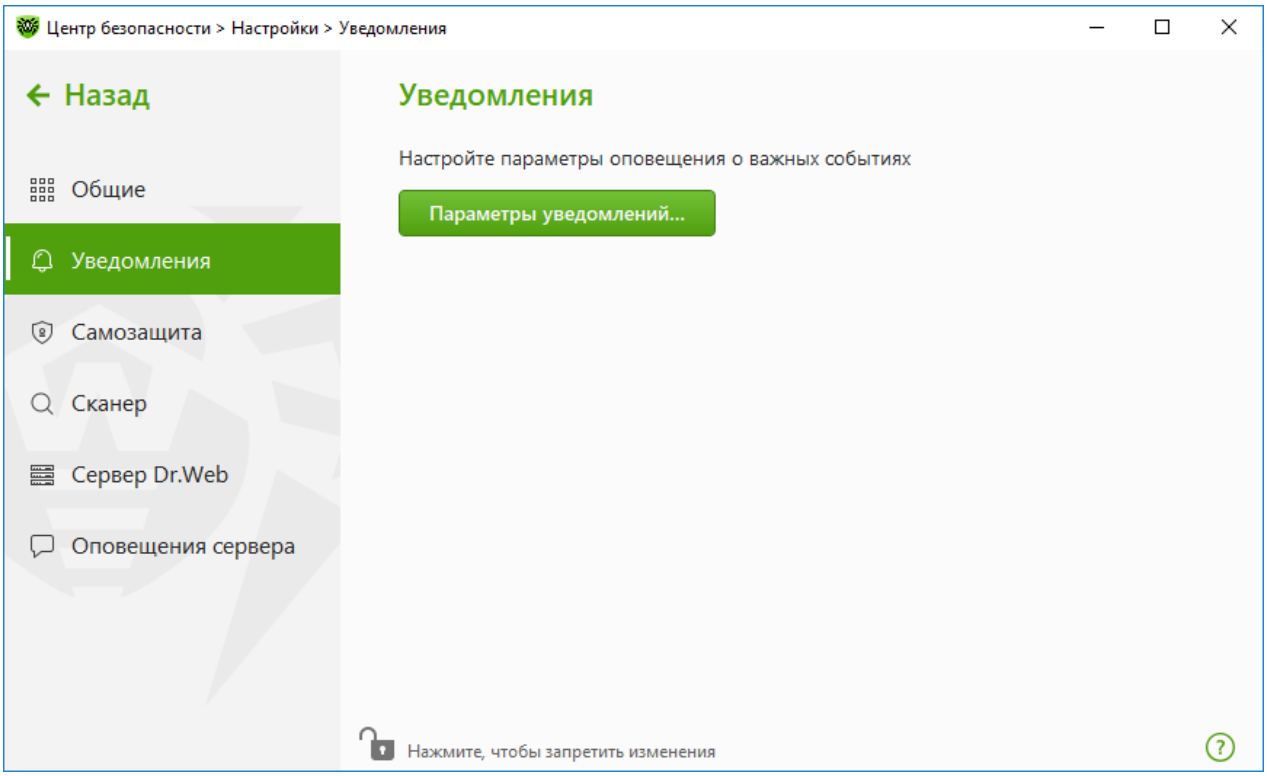

Рисунок 23. Настройки уведомлений

Чтобы настроить параметры уведомлений

1. Нажмите кнопку **Параметры уведомлений**.

2. Выберите уведомления, которые вы хотите получать. Чтобы отображать уведомления, установите флажки напротив нужных типов уведомлений.

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

Тип уведомления	Описание
Обнаружена угроза	Уведомления об угрозах, обнаруженных SpIDer Guard и SpIDer Gate. По умолчанию уведомления включены.
Критичные уведомления	Критичные уведомления о следующих событиях: • Обнаружены соединения, ожидающие ответа Брандмауэра. • Ваши имя пользователя и пароль уже используются для подключения к серверу централизованной защиты. По умолчанию уведомления включены.
Важные уведомления	Важные уведомления о следующих событиях: • Время работы за компьютером истекло. • Вирусные базы устарели (при работе в Мобильном режиме). • Устройство заблокировано. • 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. • Запуск процесса заблокирован администратором. • Установка пакета MSI заблокирована администратором. • Запуск скрипта заблокирован администратором. • Процессу запрещена загрузка объекта. • Процессу запрещено создание исполняемого файла. • Процессу запрещена модификация исполняемого файла. По умолчанию уведомления выключены.
Малозначительные уведомления	Малозначительные уведомления о следующих событиях: • URL был заблокирован модулем Офисный контроль. • URL был заблокирован SpIDer Gate. • Время работы в интернете истекло. • Доступ к защищаемому объекту заблокирован компонентом Офисный контроль. • Администратором антивирусной сети запущен процесс проверки вашего компьютера. • Процесс проверки вашего компьютера запущен по расписанию.

Тип уведомления	Описание
	• Проверка вашего компьютера завершена. • Успешное обновление. • Ошибка обновления. По умолчанию уведомления выключены.

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

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

- установка приоритетных обновлений, для которых требуется перезагрузка;
- перезагрузка для завершения обезвреживания угроз;
- автоматическая перезагрузка;
- запрос на разрешение процессу модификации объекта;
- сообщение, отправленное администратором сервера централизованной защиты;
- успешное подключение к серверу;
- подключена новая клавиатура.

8.3. 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**.

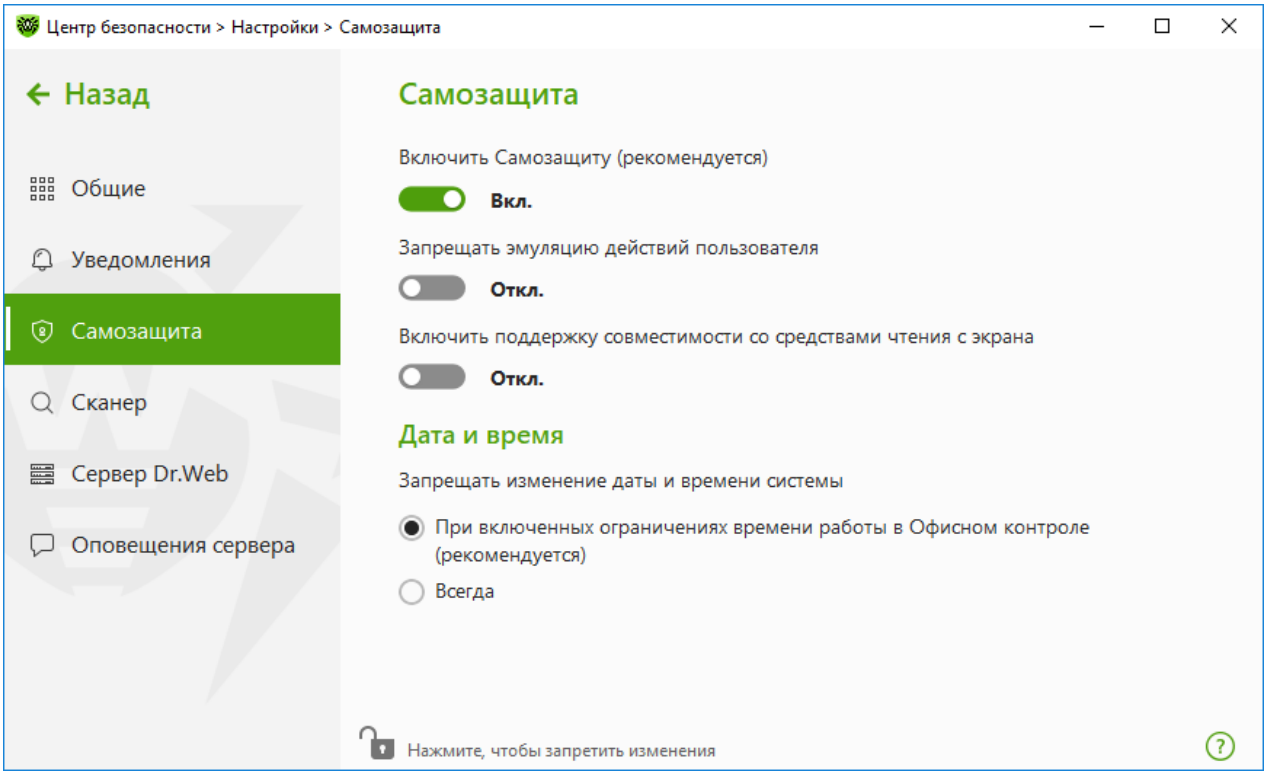

Рисунок 24. Параметры защиты Dr.Web

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 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. Данная настройка позволит точнее работать функции ограничения времени в модуле Офисный контроль. Если в модуле Офисный контроль заданы ограничения времени работы за компьютером или в интернете, эта настройка включается автоматически. Вы можете настроить получение уведомлений в том случае, если осуществлялась попытка изменить системное время.

8.4. 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**.

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

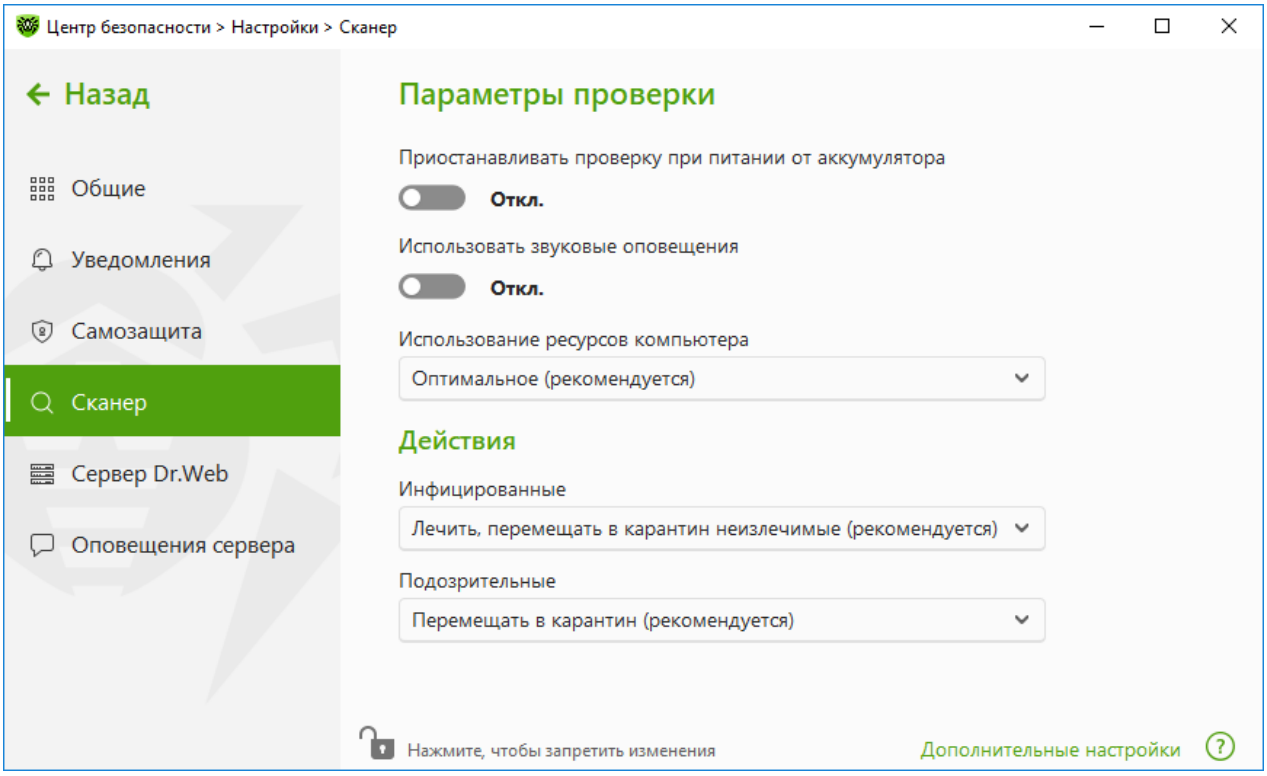

Рисунок 25. Настройка Сканера

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. Если питание от сети восстановится в течение 30 секунд, проверка возобновится автоматически. 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, в которых обнаружена известная и (предположительно) излечимая угроза;
- **Подозрительные** — объекты, предположительно содержащие угрозы;
- различные потенциально опасные объекты.

По умолчанию Сканер пытается вылечить файлы, в которых обнаружена известная и потенциально излечимая угроза, 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 угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, 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 угроза неизлечима или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).
Удалить	Удалить объект. Для загрузочных секторов никаких действий производиться не будет.
Перемещать в карантин	Переместить объект в специальную папку Карантина. Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропустить объект без выполнения каких-либо действий и не выводить оповещения. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

При обнаружении угроз 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 контейнеров, 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.

8.5. Сервер Dr.Web

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

В этом разделе:

- Параметры соединения
- Настройки подключения к серверу централизованной защиты
- Сертификаты
- Параметры подключения станции
- Дополнительные настройки
- Мобильный режим

Чтобы перейти к параметрам взаимодействия станции с сервером

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 **Сервер Dr.Web**.

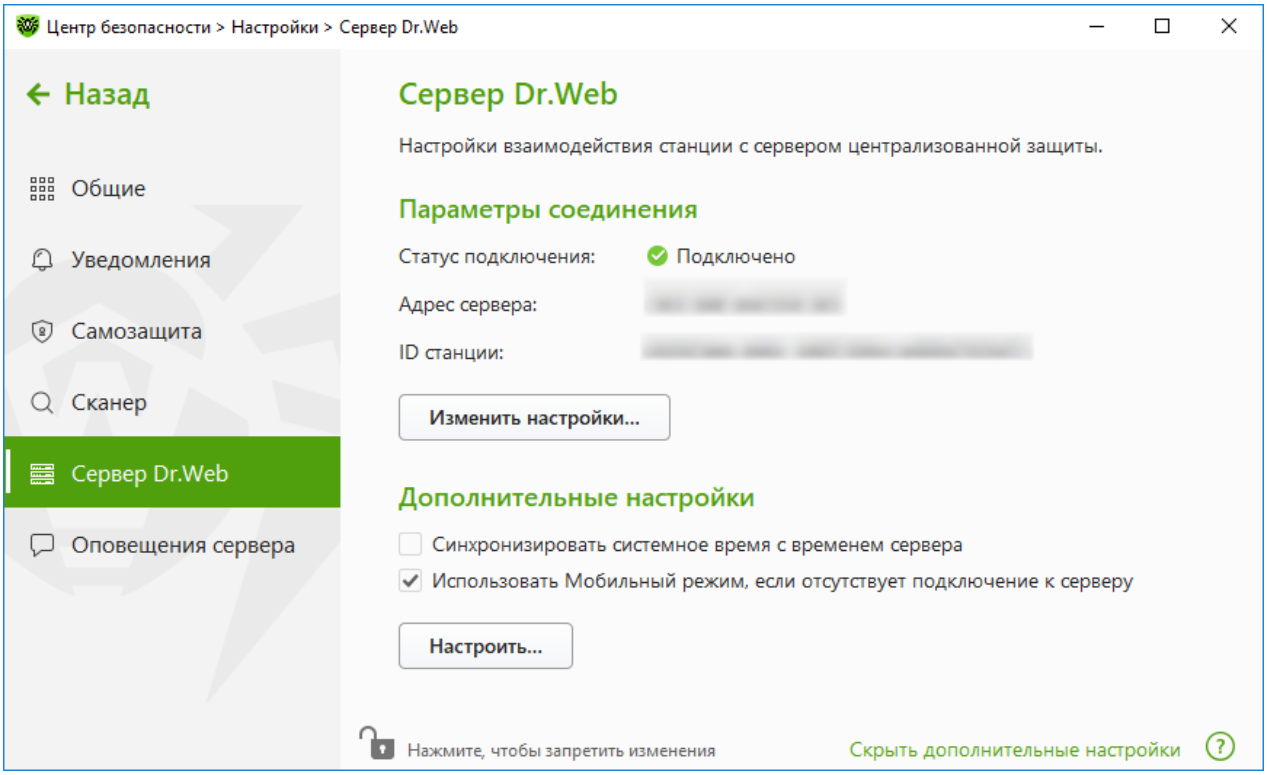

Рисунок 26. Настройки соединения станции

Параметры соединения

В группе **Параметры соединения** отображаются:

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

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

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

Настройки подключения

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

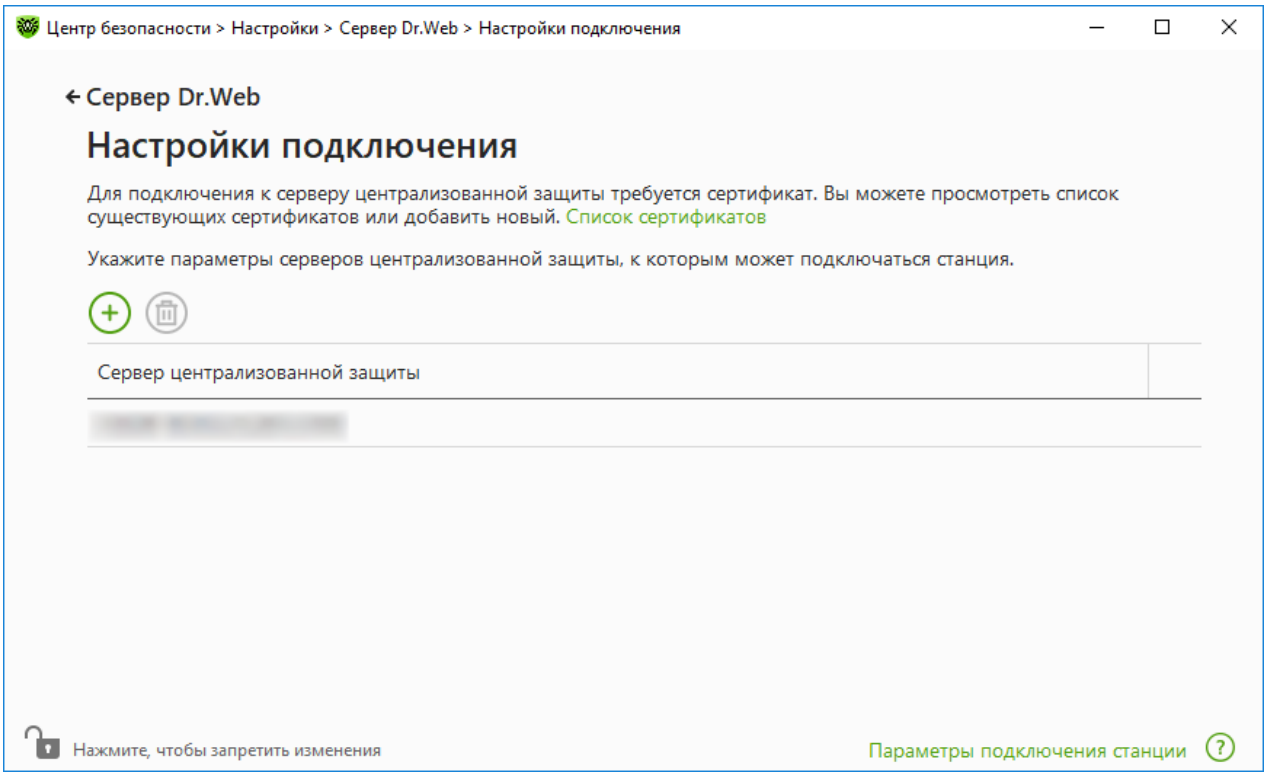

Рисунок 27. Настройки подключения к серверу

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

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — настройка соединения с другим сервером. В открывшемся окне необходимо указать адрес сервера централизованной защиты, предоставленный администратором.
- Кнопка 🗑 — удаление строки.

Сертификаты

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

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

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

Чтобы удалить неиспользуемый сертификат, нажмите кнопку  .

Параметры подключения станции

Чтобы изменить параметры подключения станции

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

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

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

Параметры соединения Виртуального агента

При определенных настройках на стороне сервера станция может подключаться к Сканирующему серверу. В этом случае станция считается *виртуальным агентом* и передает запросы на сканирование файлов и URL на сервер. Вирусные базы и встроенные фильтры не хранятся на станции.

При использовании Сканирующего сервера на станции отображается группа настроек **Параметры соединения Виртуального агента** со следующими данными:

- статусом подключения станции к Сканирующему серверу;
- ID Сканирующего сервера.

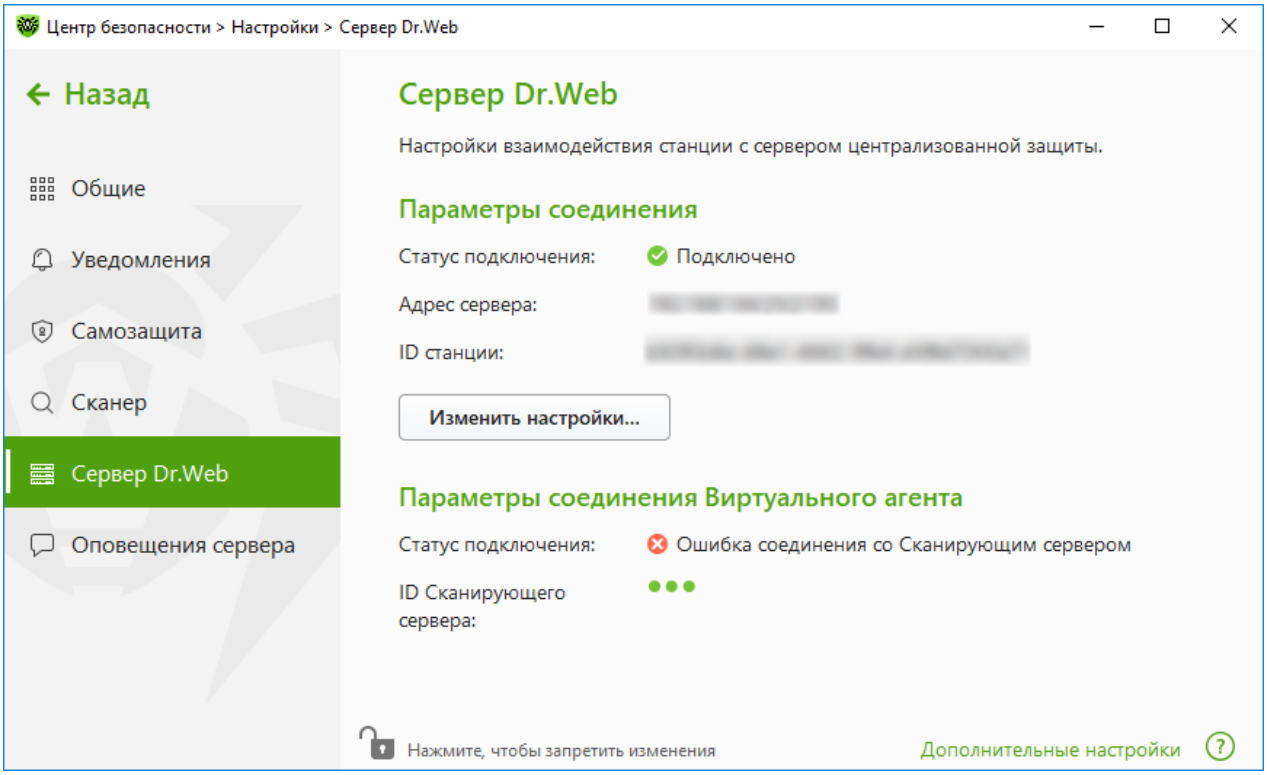

Рисунок 28. Подключение к Сканирующему серверу

При отсутствии подключения к Сканирующему серверу станция не защищена. Необходимо обратиться к администратору антивирусной сети.

Дополнительные настройки

Для перехода к дополнительным настройкам в окне **Сервер Dr.Web** (см. рисунок Настройки соединения станции) нажмите ссылку **Дополнительные настройки**. В группе **Дополнительные настройки** вы можете выбрать следующие опции:

- **Синхронизировать системное время с временем сервера** — для синхронизации системного времени на вашем компьютере со временем на сервере централизованной защиты. В данном режиме Dr.Web периодически устанавливает системное время на вашем компьютере в соответствии с временем на сервере.
- **Использовать Мобильный режим, если отсутствует подключение к серверу** — для своевременного получения обновлений вирусных баз.

Мобильный режим

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

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

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

Чтобы задать настройки Мобильного режима работы

1. Нажмите кнопку **Настроить**. Откроется окно **Мобильный режим**.
2. В выпадающем списке **Получать обновления** вы можете выбрать периодичность, с которой будет производиться проверка на наличие обновлений на серверах компании «Доктор Веб».

При выборе в списке **Получать обновления** опции **Вручную** автоматические обновления происходить не будут. Вы сможете запустить обновление в меню Dr.Web.

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

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

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

В Мобильном режиме производится обновление только вирусных баз.

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

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

8.6. Оповещения сервера

Для удобства работы с оповещениями на сервере централизованной защиты у администратора сети есть возможность включить отправку оповещений на станцию. В этом случае в окне **Общие** появится пункт **Оповещения сервера**.

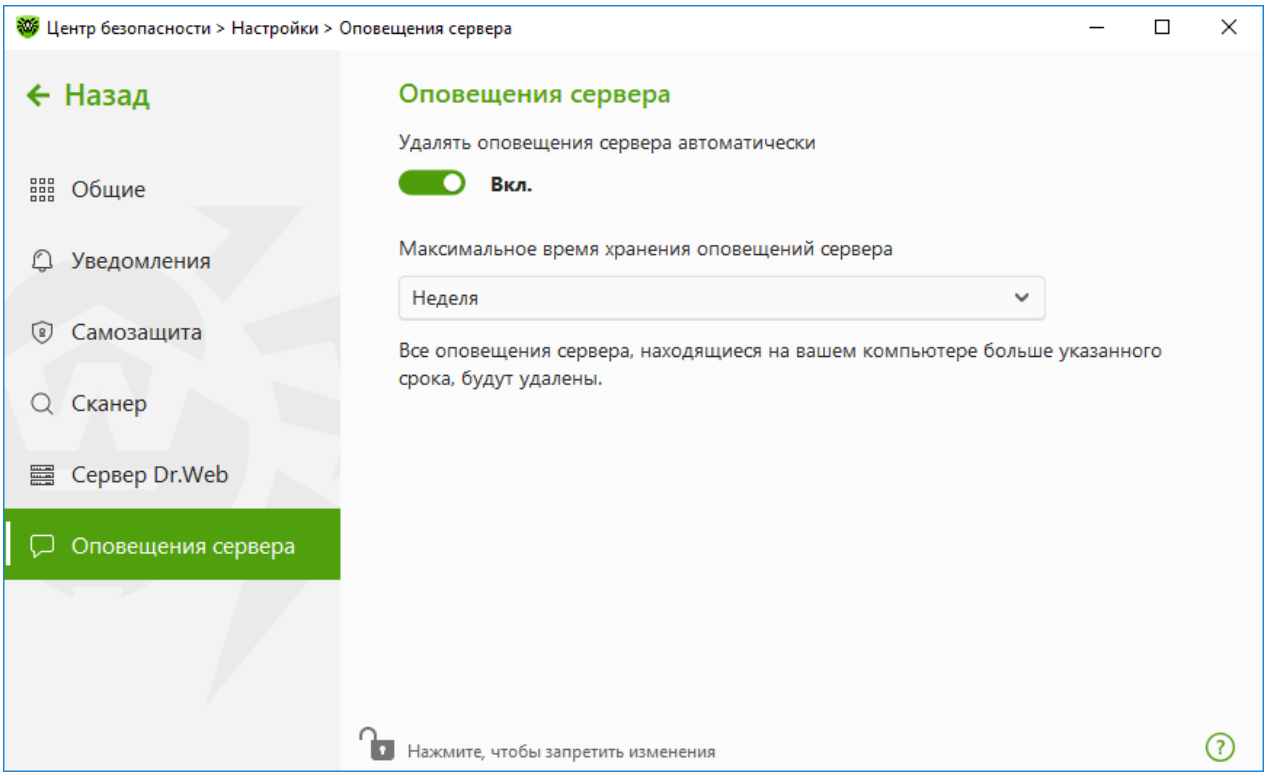

Рисунок 29. Настройки автоматического удаления оповещений сервера

Чтобы включить или отключить автоматическое удаление оповещений сервера

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 **Оповещения сервера**.
5. Включите или отключите опцию **Удалять оповещения сервера автоматически** при помощи переключателя .
6. При включении автоматического удаления оповещений в пункте **Максимальное время хранения оповещений сервера** в выпадающем списке выберите необходимый период времени. Оповещения будут удаляться по истечении этого срока.

9. 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**.

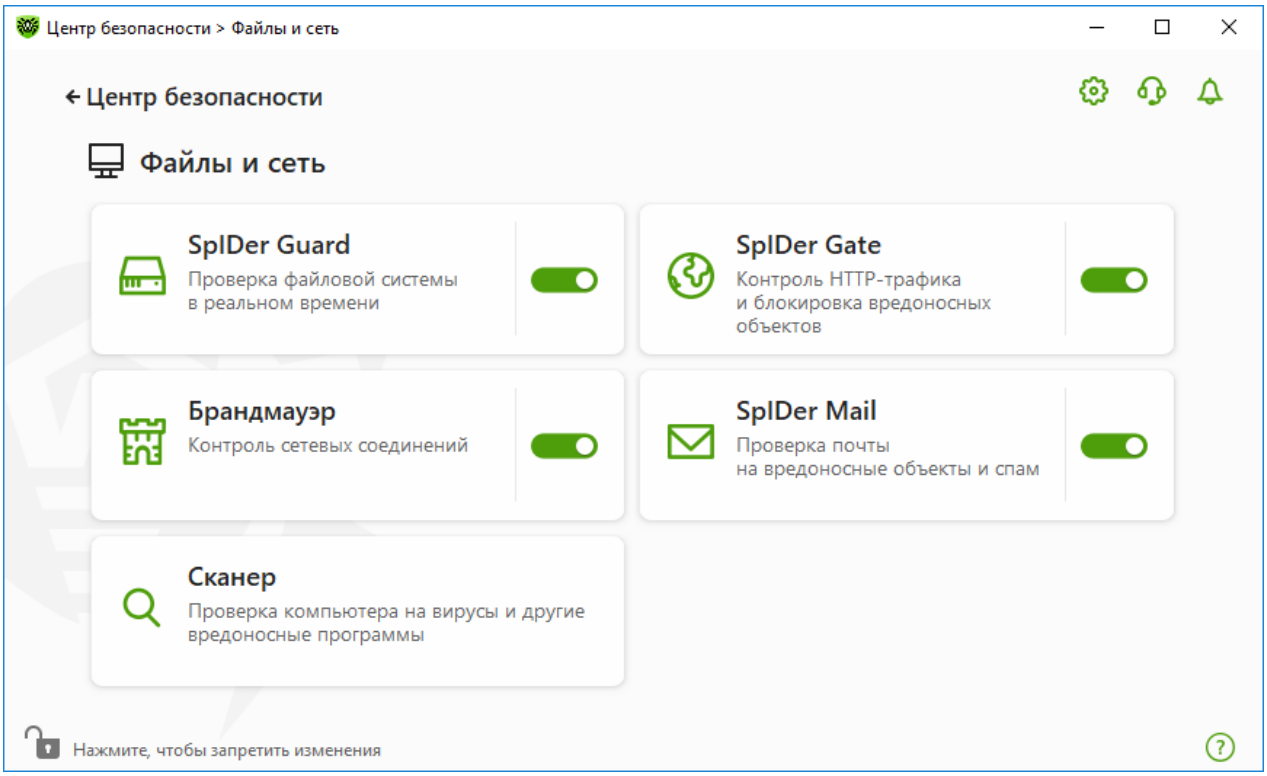

Рисунок 30. Окно Файлы и сеть

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 SplDer Guard — компонент, проверяющий файлы во время их открытия, запуска или изменения, а также запускаемые процессы в режиме реального времени.
- Интернет-монитор SplDer Gate — компонент, проверяющий HTTP-трафик.
- Почтовый антивирус SplDer 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.

9.1. Постоянная защита файловой системы

Монитор файловой системы SplDer Guard защищает компьютер в режиме реального времени и предотвращает его заражение. SplDer 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 SplDer Guard при помощи переключателя.

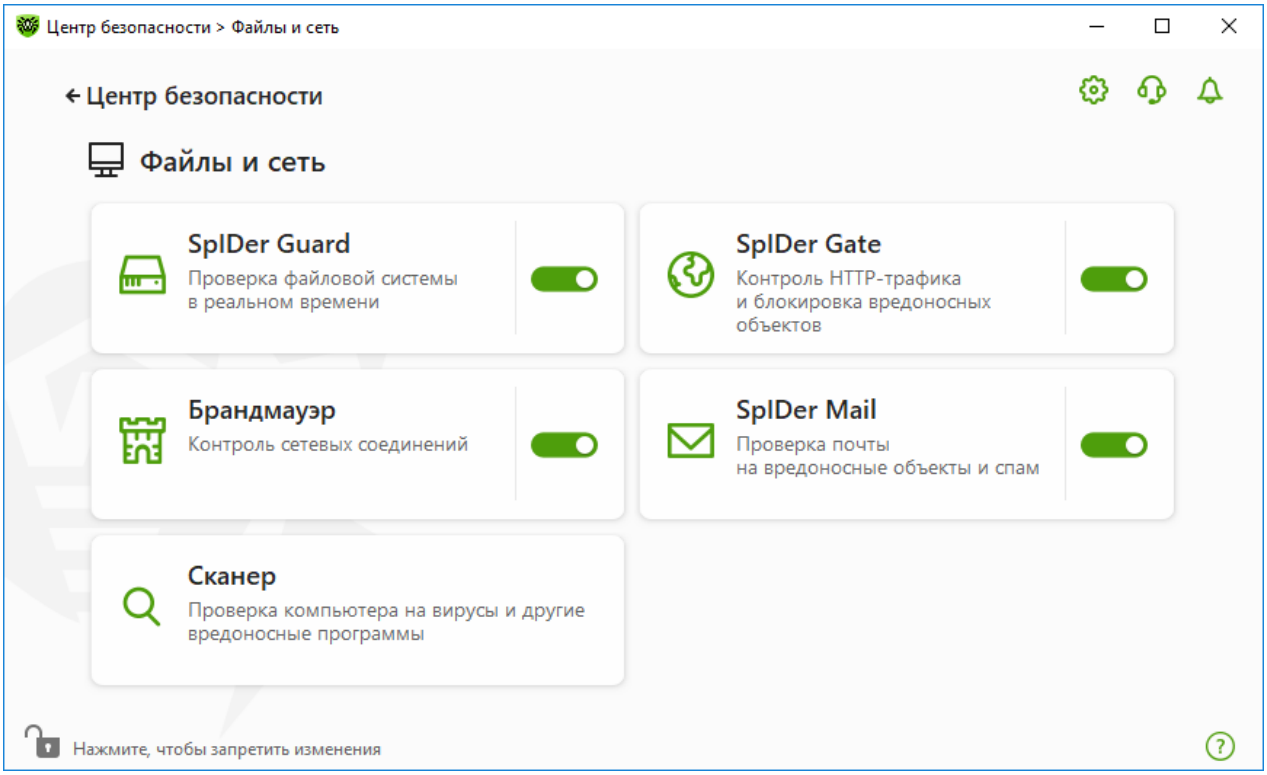

Рисунок 31. Включение/отключение SpIDer Guard

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 всех запущенных процессов и блокирует процессы с поведением, характерным для вредоносных программ.

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.

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

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.

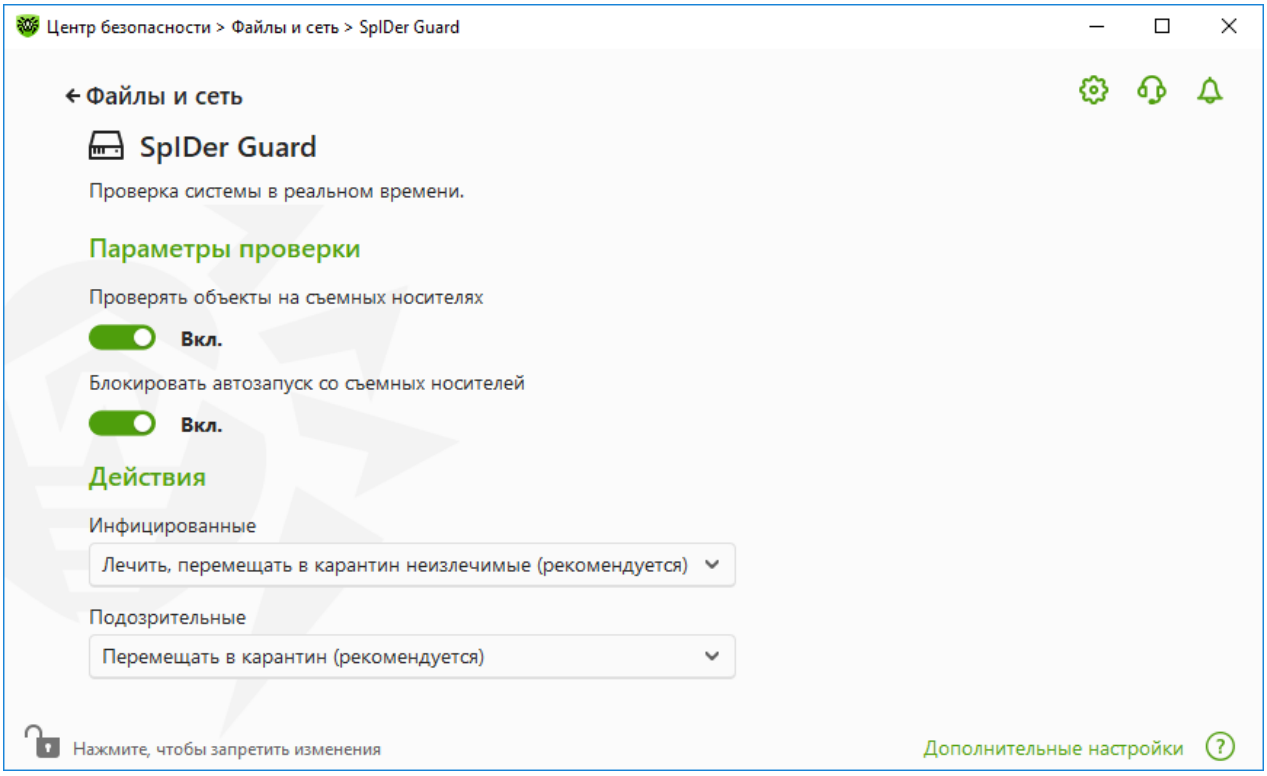

Рисунок 32. Параметры монитора файловой системы

Проверка съемных носителей

SpIDer Guard по умолчанию проверяет файлы на съемных носителях информации (CD/DVD-дисках, флеш-накопителях и т. д.) при создании, чтении, изменении и запуске этих файлов, а также блокирует автоматический запуск их активного содержимого. Этот метод помогает предотвратить заражение вашего компьютера через съемные носители, так как SpIDer Guard в режиме реального времени отслеживает обращения к файловой системе и блокирует исполнение вредоносного кода.

Некоторые съемные носители (в частности, мобильные жесткие диски с интерфейсом USB) могут представляться в системе как жесткие диски. В этом случае в области уведомлений Windows не отображается значок «Безопасное извлечение устройств и дисков». При чтении файла с такого диска SpIDer Guard не осуществляет проверку, если не выбран параноидальный режим, поэтому такие диски рекомендуется проверять на угрозы 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.

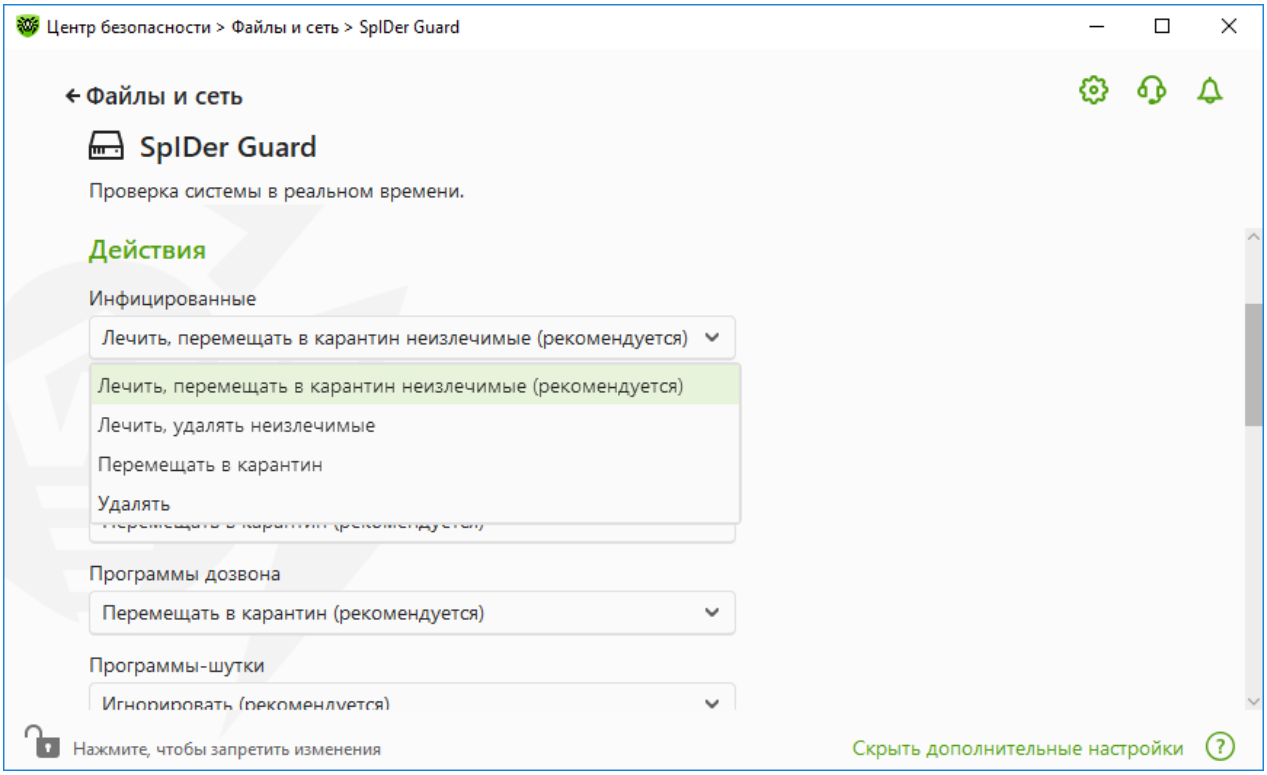

Рисунок 33. Настройка действий, применяемых к угрозам

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 угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, 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 угроза неизлечима или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

Действие	Описание
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.
Сообщать	Выводить оповещение и пропустить объект без выполнения каких-либо действий. Данное действие возможно только для подозрительных объектов и вредоносных программ.

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: • 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 угроз 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

Режим	Описание
	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 контейнеров;
- 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 угроз.

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.

9.2. Проверка веб-трафика

Компонент SpIDer Gate проверяет HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы. Через протокол HTTP работают браузеры, менеджеры загрузки и другие приложения, работающие с интернетом.

Зашифрованный трафик не проверяется, чтобы избежать сбоев в работе с сетевыми ресурсами. Это связано с тем, что для установки защищенных соединений в корпоративной сети вместо сертификатов установленного ПО используется сертификат Dr.Web, что может привести к ошибкам программ, использующих защищенный протокол для соединения и следящих за целостностью трафика.

При настройках по умолчанию SpIDer Gate также осуществляет фильтрацию нерекомендуемых сайтов и сайтов, известных как источники распространения угроз.

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

Чтобы включить или отключить проверку веб-трафика и фильтрации нерекомендуемых сайтов

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

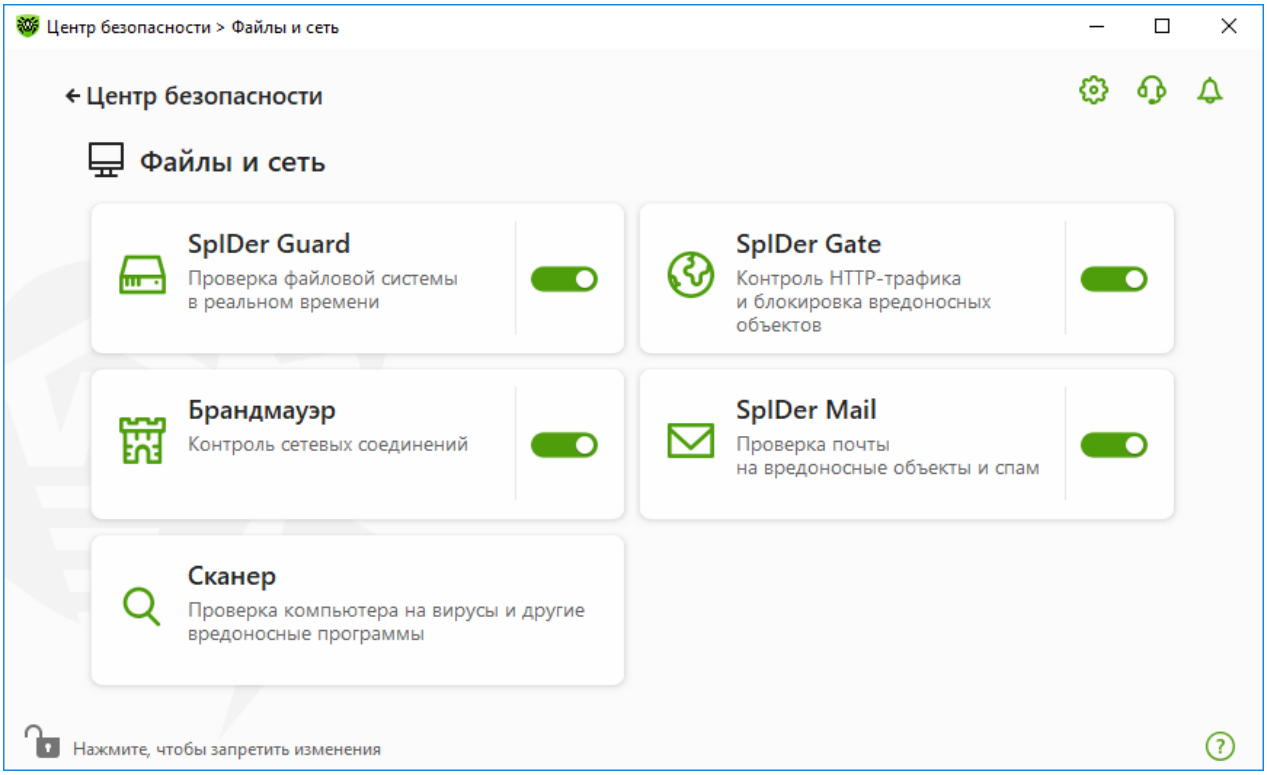

Рисунок 34. Включение/отключение SpIDer Gate

В этом разделе:

- Проверка трафика и URL в IM-клиентах
- Параметры блокировки сайтов
- Блокировка программ
- Блокировка непроверенных или поврежденных объектов
- Проверка архивов и контейнеров
- Использование системных ресурсов при проверке
- Направление проверяемого трафика

См. также:

- Исключение сайтов из проверки
- Исключение приложений из проверки

Параметры проверки веб-трафика

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

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

Чтобы перейти к параметрам компонента SplDer Gate

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

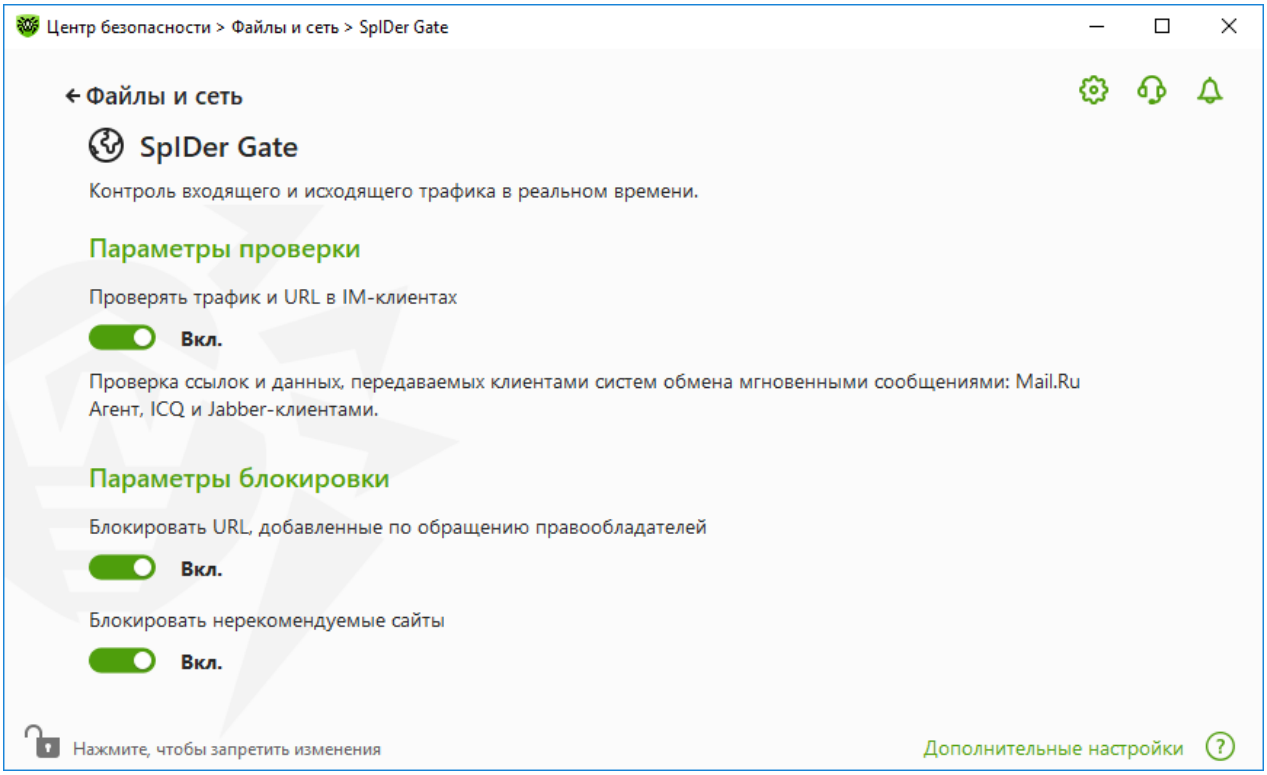

Рисунок 35. Параметры проверки HTTP-трафика

Проверка трафика и URL в IM-клиентах

В группе настроек **Параметры проверки** вы можете включить проверку ссылок и файлов, передаваемых клиентами систем обмена мгновенными сообщениями (IM-клиентов), например Mail.ru Агент, ICQ, а также клиентов, работающих по протоколу Jabber. Проверяется только входящий трафик. По умолчанию опция включена.

К найденным угрозам применяются следующие действия:

Объект	Действие
Проверка ссылок	
Сайты, известные как источники распространения угроз	Блокируются автоматически.
Нерекомендуемые сайты и URL, добавленные по обращению правообладателя	Блокируются согласно параметрам в группе настроек **Параметры блокировки**.
Проверка файлов	
Вирусы	Блокируются автоматически.
Вредоносные программы: • подозрительные; • потенциально опасные; • программы дозвона; • программы взлома; • рекламные программы; • программы-шутки.	Блокируются согласно параметрам в группе настроек **Блокировать программы**.

При проверке ссылок в передаваемых сообщениях также учитываются сайты и приложения, исключаемые из проверки.

Параметры блокировки сайтов

В группе настроек **Параметры блокировки** вы можете установить автоматическую блокировку доступа к URL, добавленным по обращению правообладателя, а также к нерекомендуемым сайтам, известным как неблагонадежные. Для этого включите соответствующую опцию.

Чтобы разрешить доступ к необходимым сайтам, укажите исключения в группе настроек программы **Исключения**.

SpIDer Gate по умолчанию блокирует доступ к сайтам, известным как источники угроз. При этом учитывается список сайтов, исключаемых из проверки.

Блокировка программ

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

Компонент SpIDer Gate может блокировать следующие вредоносные программы:

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

Чтобы включить блокировку вредоносных программ, нажмите ссылку **Дополнительные настройки** и используйте соответствующие переключатели в группе настроек **Блокировать программы**. Блокировка подозрительных и рекламных программ, а также программ дозвона включена по умолчанию.

Блокировка объектов

SpIDer Gate может блокировать непроверенные или поврежденные объекты. По умолчанию эти опции выключены. Для доступа к настройкам блокировки объектов нажмите ссылку **Дополнительные настройки**.

Дополнительные возможности

Настройки **Проверять архивы** и **Проверять контейнеры**. По умолчанию эти опции отключены.

Настройка **Уровень потребления системных ресурсов**. В некоторых случаях Dr.Web не может определить конечный размер файла, например, при его загрузке. В таком случае файл отправляется на проверку частями. Это требует использование ресурсов компьютера. Вы можете настроить уровень использования системных ресурсов и тем самым определить, как часто файлы неизвестного размера будут отправляться на проверку. При максимальном использовании ресурсов компьютера файлы будут отправляться чаще и проверка файлов будет производиться быстрее, но нагрузка на процессор увеличится.

Настройка **Режим проверки трафика**. По умолчанию проверяется только входящий трафик. При необходимости выберите тип проверяемого HTTP-трафика.

Во время проверки трафика учитываются заданные параметры компонента SpIDer Gate, белый список сайтов и приложения, исключаемые из проверки.

9.3. 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. SplDer Mail также может проверять письма на спам с помощью Антиспама Dr.Web.

> Зашифрованный трафик не проверяется, чтобы избежать сбоев в работе с сетевыми ресурсами. Это связано с тем, что для установки защищенных соединений в корпоративной сети вместо сертификатов установленного ПО используется сертификат Dr.Web, что может привести к ошибкам программ, использующих защищенный протокол для соединения и следящих за целостностью трафика.
>
> Чтобы проверять зашифрованный почтовый трафик, воспользуйтесь подключаемым модулем Dr.Web для Microsoft Outlook или серверными продуктами Dr.Web Mail Security Suite.

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 SplDer Mail при помощи переключателя.

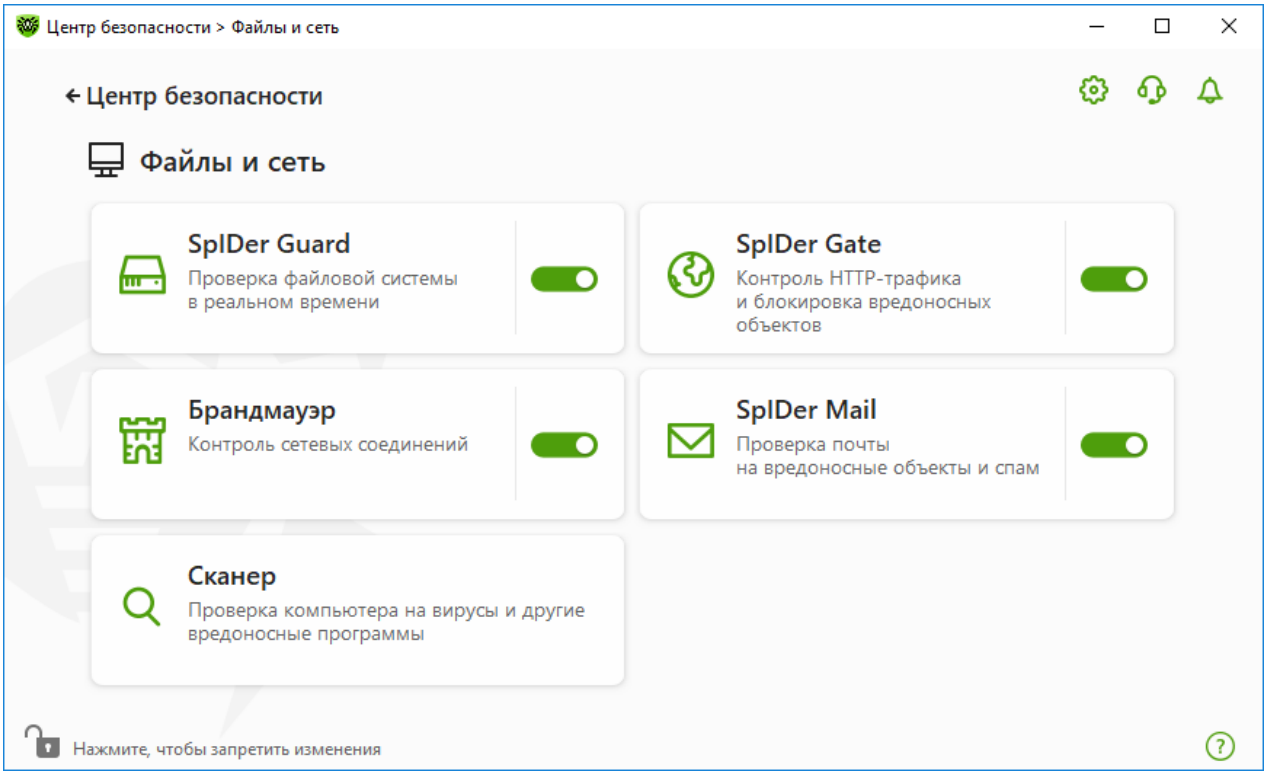

Рисунок 36. Включение/отключение SplDer Mail

В этом разделе:

- Особенности обработки писем
- Проверка писем другими средствами

См. также:

- Параметры проверки писем
- Параметры Антиспама

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.
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 угрозы 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, а не в момент получения почты. Такая проверка является трудоемкой и может занять значительное время.

9.3.1. Параметры проверки писем

По умолчанию SpIDer Mail пытается вылечить письма, в которых обнаружена известная и потенциально излечимая угроза. 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

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).

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

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.

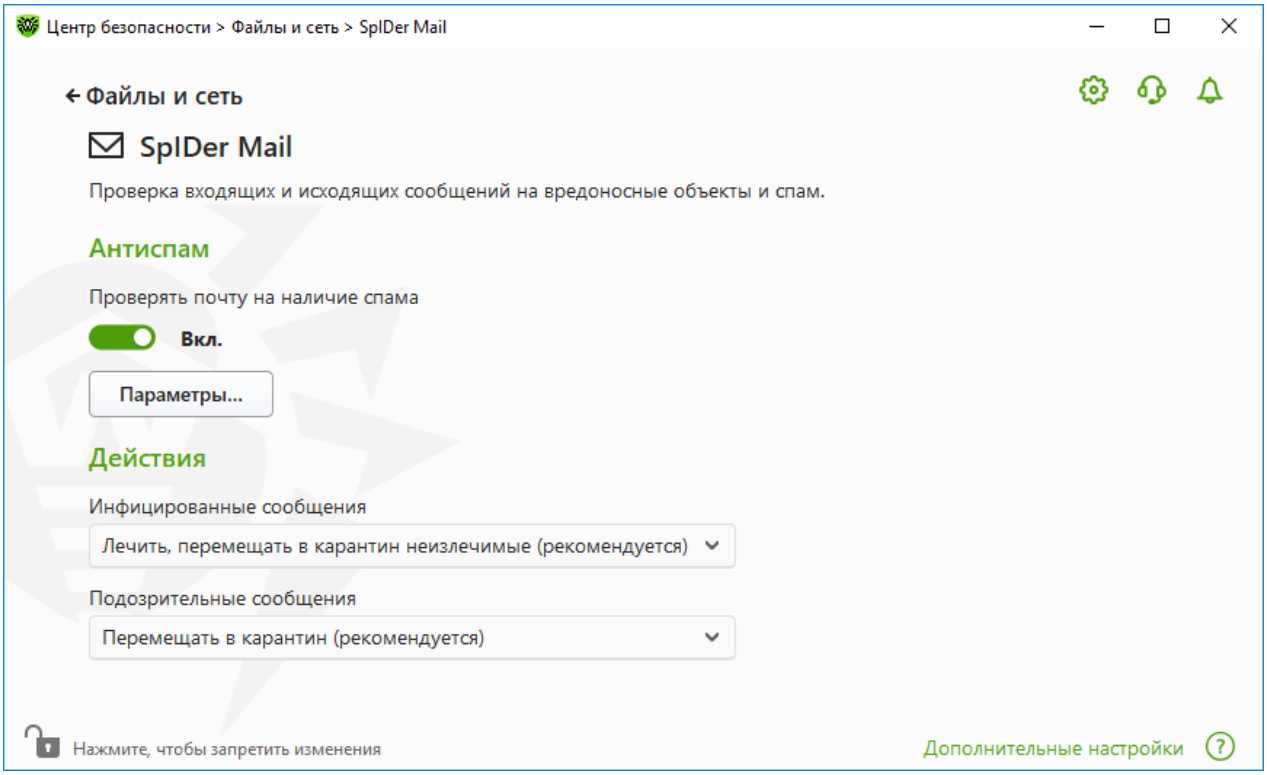

Рисунок 37. Параметры проверки писем

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.

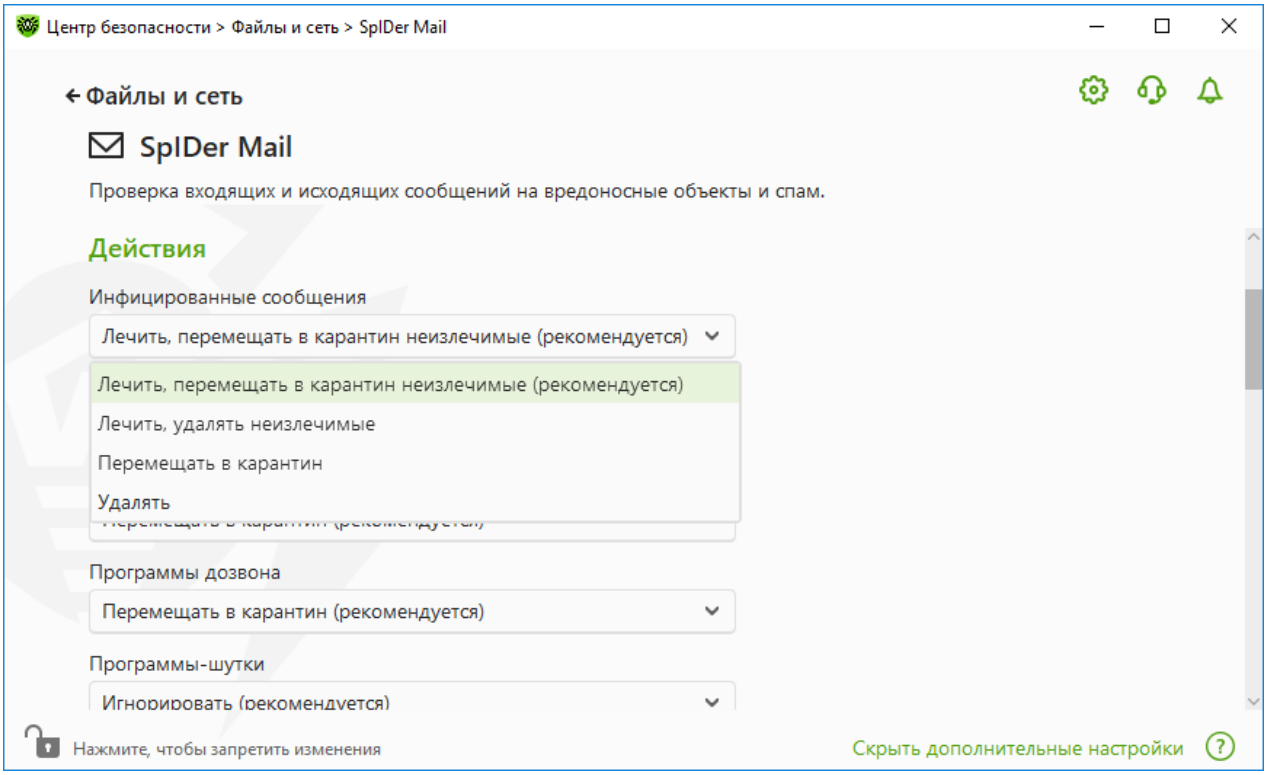

Рисунок 38. Настройка действий, применяемых к письмам

Возможные действия

К угрозам могут быть применены следующие действия:

Действие	Описание
Лечить, перемещать в карантин неизлечимые	Восстановить состояние письма до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для инфицированных писем, в которых обнаружена известная излечимая угроза, за исключением троянских программ, которые при обнаружении удаляются. Лечение файлов в архивах невозможно вне зависимости от типа угрозы. Приводит к отказу в передаче письма.
Лечить, удалять неизлечимые	Восстановить состояние письма до заражения. Если угроза неизлечима 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 угрозами. Чтобы отключить эвристический анализ, воспользуйтесь переключателем **Использовать эвристический анализ (рекомендуется)**;
- проверка контейнеров. 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.

9.3.2. Параметры Антиспама

Настройки по умолчанию SpIDer Mail, в том числе и Антиспама, являются оптимальными в большинстве случаев, их не следует изменять без необходимости.

Чтобы включить или отключить проверку почты на наличие спама

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.

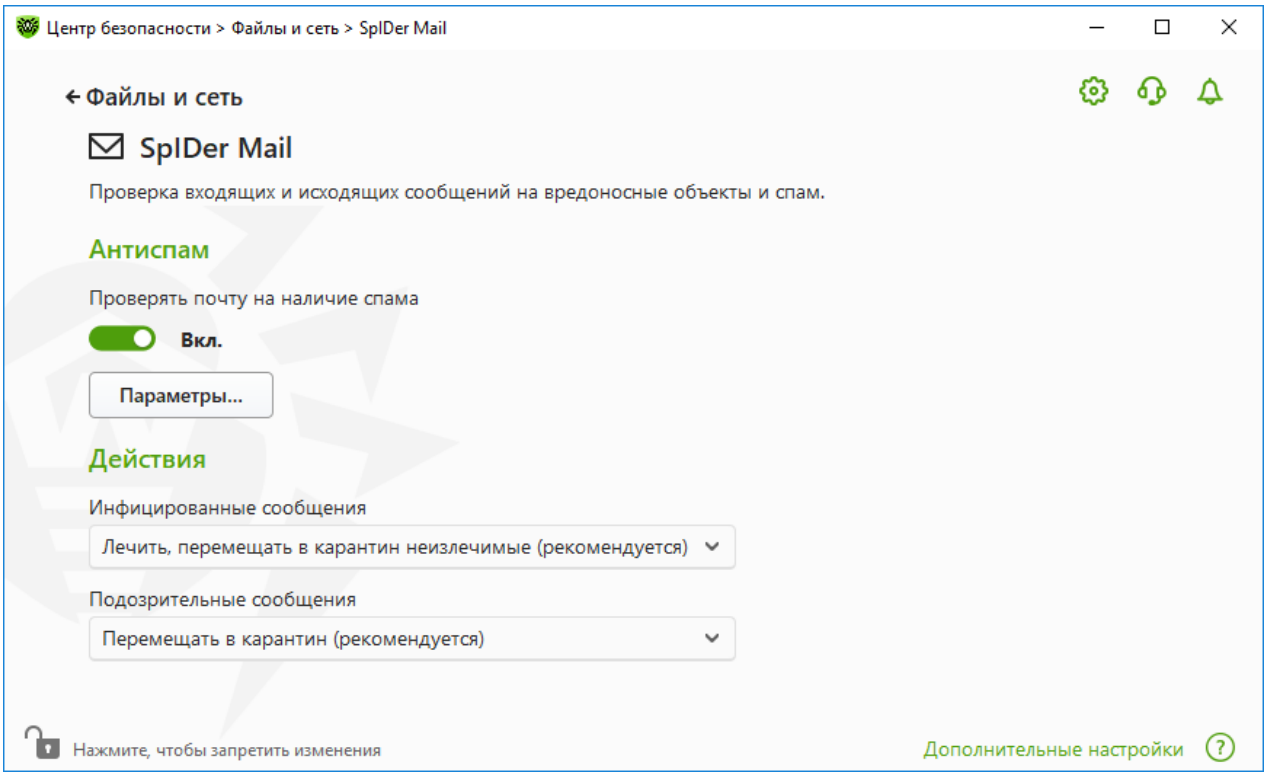

Рисунок 39. Параметры проверки почты

5. В разделе настроек **Антиспам** включите или отключите проверку почты на спам при помощи соответствующего переключателя .

> Почтовые сообщения не проверяются на спам на Windows XP.

Настройка параметров работы Антиспама

1. В группе настроек **Антиспам** нажмите кнопку **Параметры**.

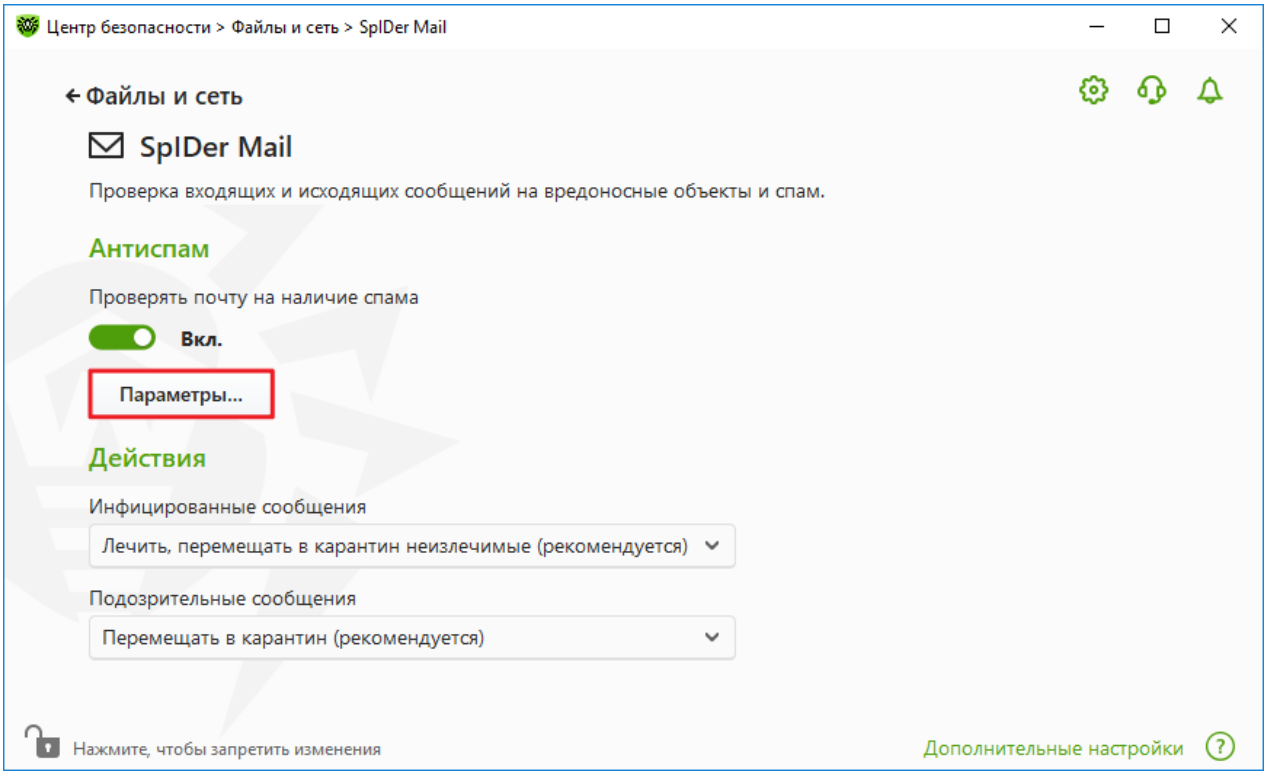

Рисунок 40. Изменение параметров Антиспама

2. В открывшемся окне **Параметры Антиспама** включите или отключите необходимые опции.

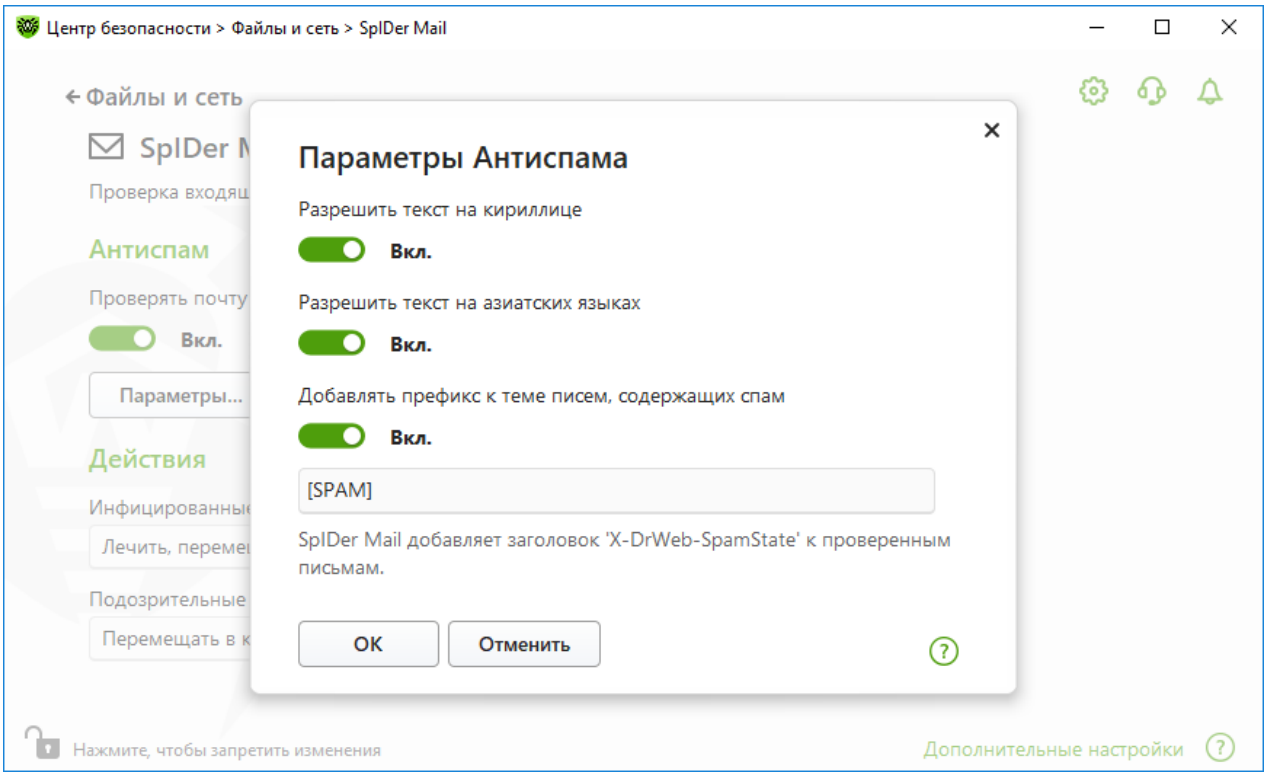

Рисунок 41. Параметры Антиспама

Доступные настройки проверки (включены по умолчанию)

Настройка	Описание
Разрешить текст на кириллице	Данная настройка указывает компоненту SplDer Mail без предварительного анализа не причислять к спаму письма, написанные в соответствии с установленной кириллической кодировкой. Если этот флажок снят, то такие письма с большой вероятностью будут отмечены фильтром как спам.
Разрешить текст на азиатских языках	Данная настройка указывает компоненту SplDer Mail без предварительного анализа не причислять к спаму письма, написанные в соответствии с наиболее распространенными кодировками азиатских языков. Если этот флажок снят, то такие письма с большой вероятностью будут отмечены фильтром как спам.
Добавлять префикс к теме писем, содержащих спам	В начало темы спам-писем по умолчанию добавляется подстрока «[SPAM]». Вы можете изменить это значение. Данная настройка указывает компоненту SplDer Mail добавлять указанный префикс к темам писем, распознаваемых как спам. Добавление префикса поможет вам создать правила для фильтрации почтовых сообщений, помеченных как спам, в тех почтовых клиентах (например, MS Outlook Express), в которых невозможно настроить фильтры по заголовкам писем.

3. Нажмите **OK**, чтобы сохранить настройки.

Дополнительная информация

Технологии антиспам-фильтра

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

- **Эвристический анализ** — технология эмпирического разбора всех частей письма: поля заголовка, тела, содержания вложения.
- **Фильтрация противодействия** — технология, которая состоит в распознавании уловок, используемых спамерами для обхода антиспам-фильтров.
- **Анализ на основе HTML-сигнатур** — технология, при которой сообщения, в состав которых входит HTML-код, сравниваются с образцами библиотеки HTML-сигнатур антиспама. Такое сравнение, в сочетании с данными о размерах изображений, обычно используемых отправителями спама, защищает пользователей от спам-сообщений, содержащих ссылки на веб-страницы.
- **Семантический анализ** — технология, при которой сравнение слов и выражений сообщения со словами и идиомами, типичными для спама, производится по

специальному словарю. Анализу подвергаются как видимые, так и визуально скрытые специальными техническими уловками слова, выражения и символы.

- **Анти-скамминг технология** — технология фильтрации скамминг- и фарминг-сообщений, к которым относятся так называемые «нигерийские письма», сообщения о выигрышах в лотерею, казино, поддельные письма банков.
- **Фильтрация технического спама** — технология определения так называемых bounce-сообщений, которые возникают как реакция на угрозы или как проявление вредоносной активности. Специальный модуль антиспама определяет такие сообщения как нежелательные.

Обработка писем спам-фильтром

Компонент SpIDer Mail добавляет ко всем проверенным письмам следующие заголовки:

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

Используйте эти заголовки и префикс в теме письма (если выбрана соответствующая опция) для настройки фильтрации спама вашей почтовой программой.

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

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

Для повышения качества работы спам-фильтра вы можете сообщать компании «Доктор Веб» об ошибках распознавания спама.

Исправление ошибок распознавания

При обнаружении ошибки в работе спам-фильтра:

1. Создайте новое письмо и приложите к нему неправильно распознанное сообщение. Сообщения, отправленные в тексте письма, анализироваться не будут.
2. Отправьте письмо с вложением на один из следующих адресов:
   - письмо, ошибочно оцененное как спам, — на адрес nonspam@drweb.com;
   - спам, нераспознанный системой фильтрации, — на адрес spam@drweb.com.

9.4. Брандмауэр

Брандмауэр Dr.Web предназначен для контроля подключения и фильтрации соединений 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.

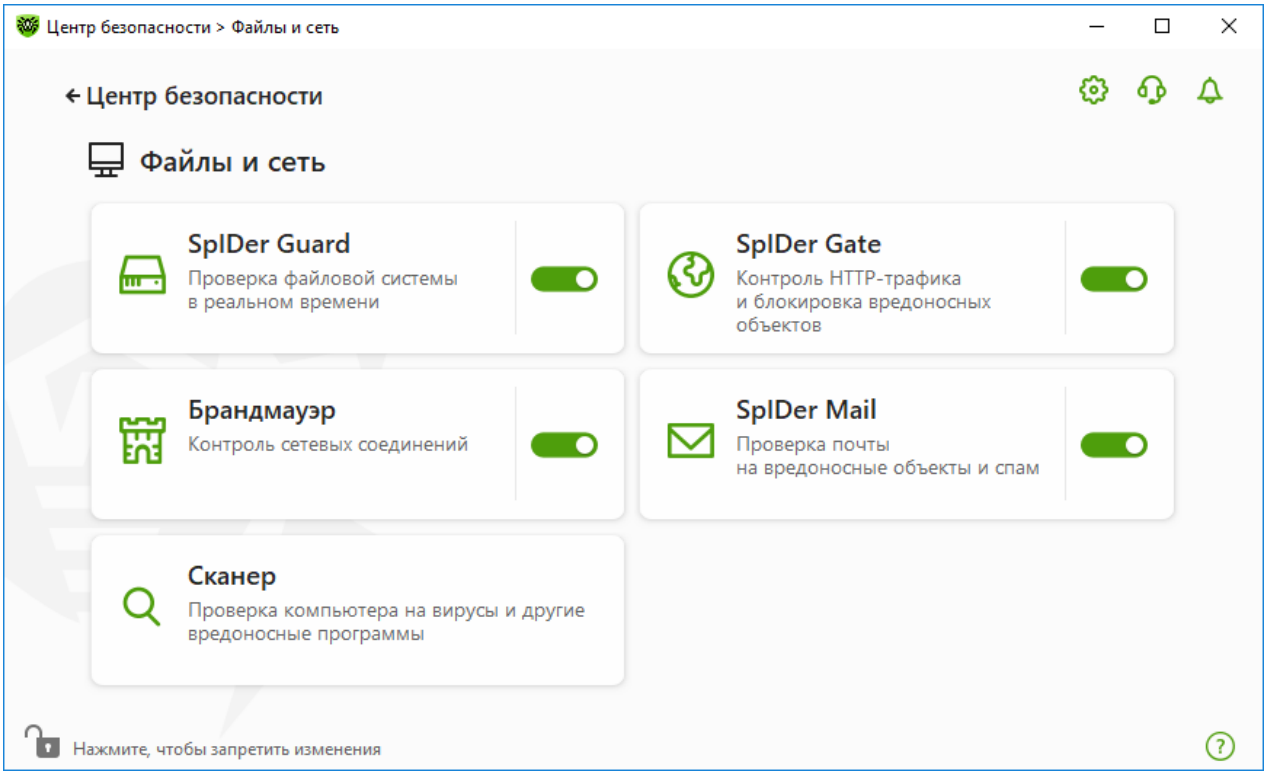

Рисунок 42. Включение/отключение Брандмауэра

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

9.4.1. 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.

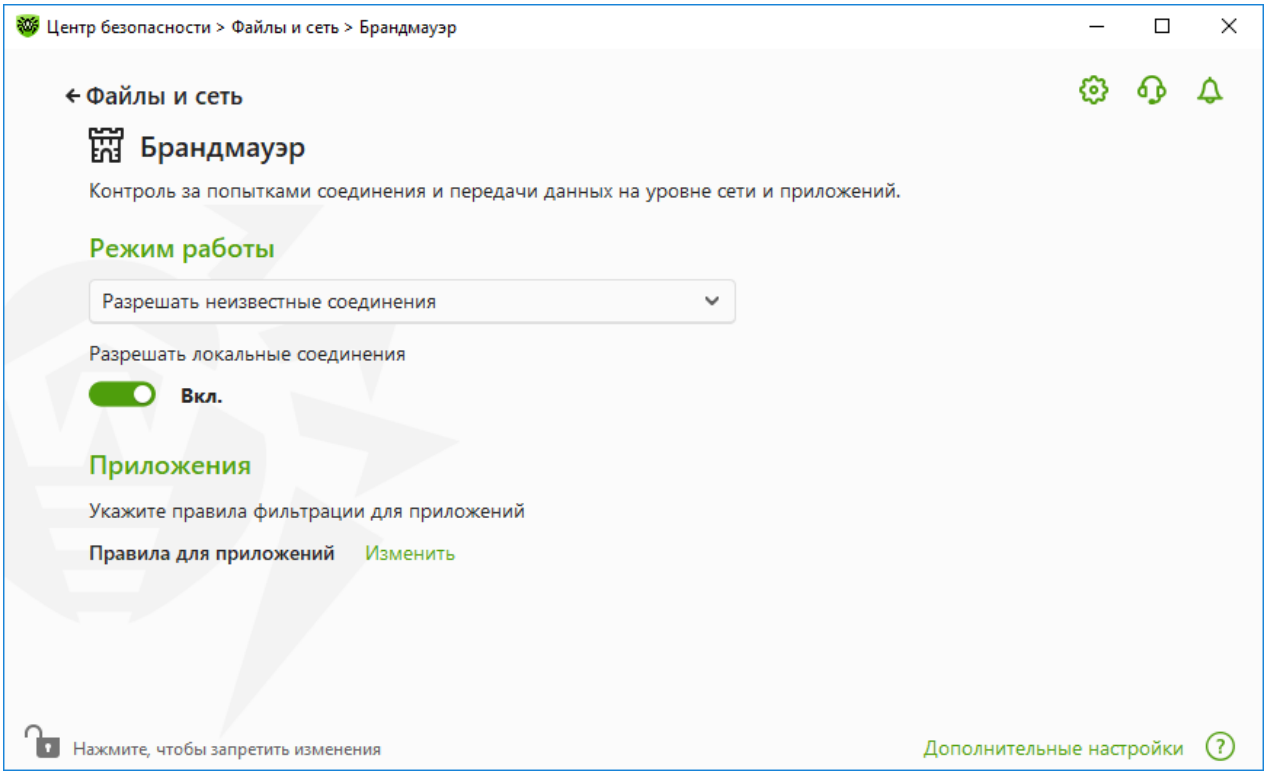

Рисунок 43. Параметры Брандмауэра

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.

Режим работы	Описание
	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 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.

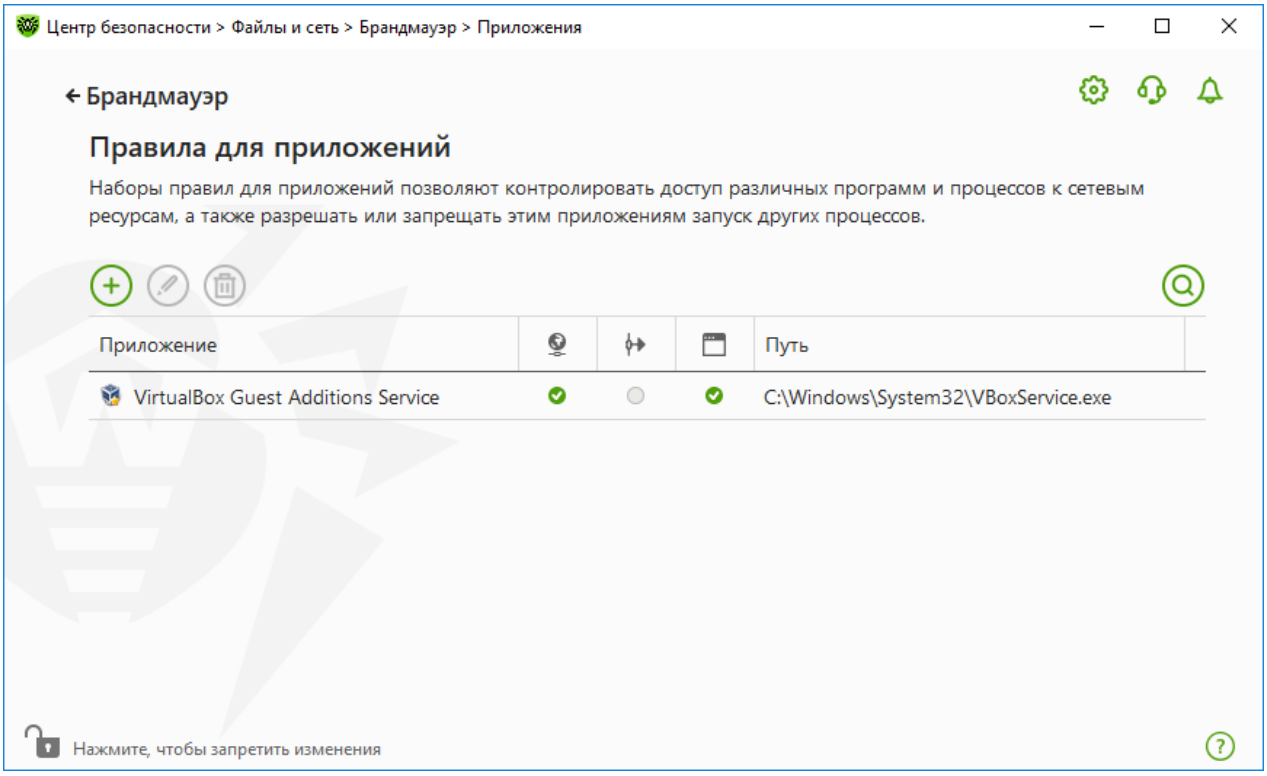

Рисунок 44. Правила для приложений

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>***).

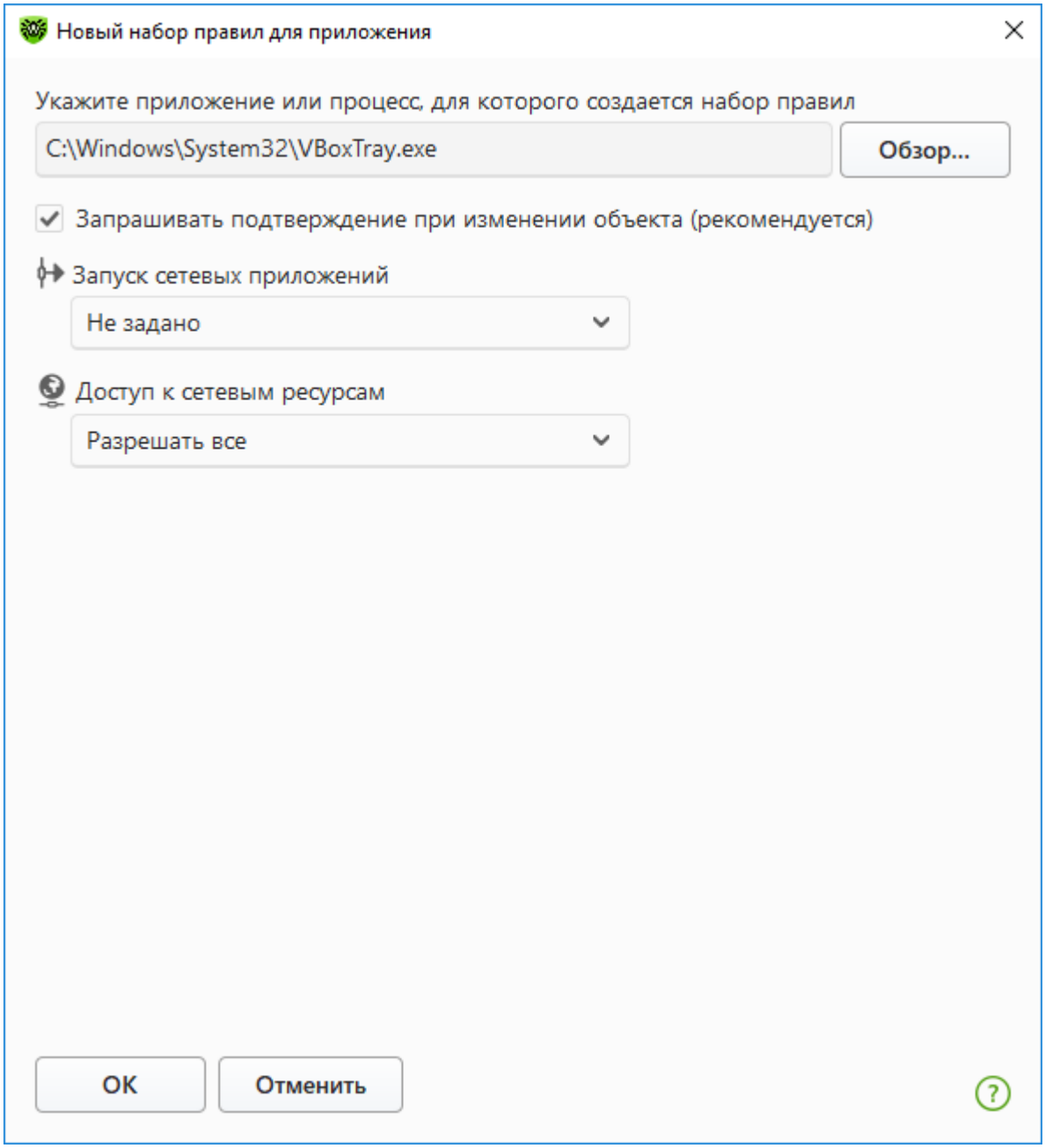

Рисунок 45. Создание нового набора правил

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.

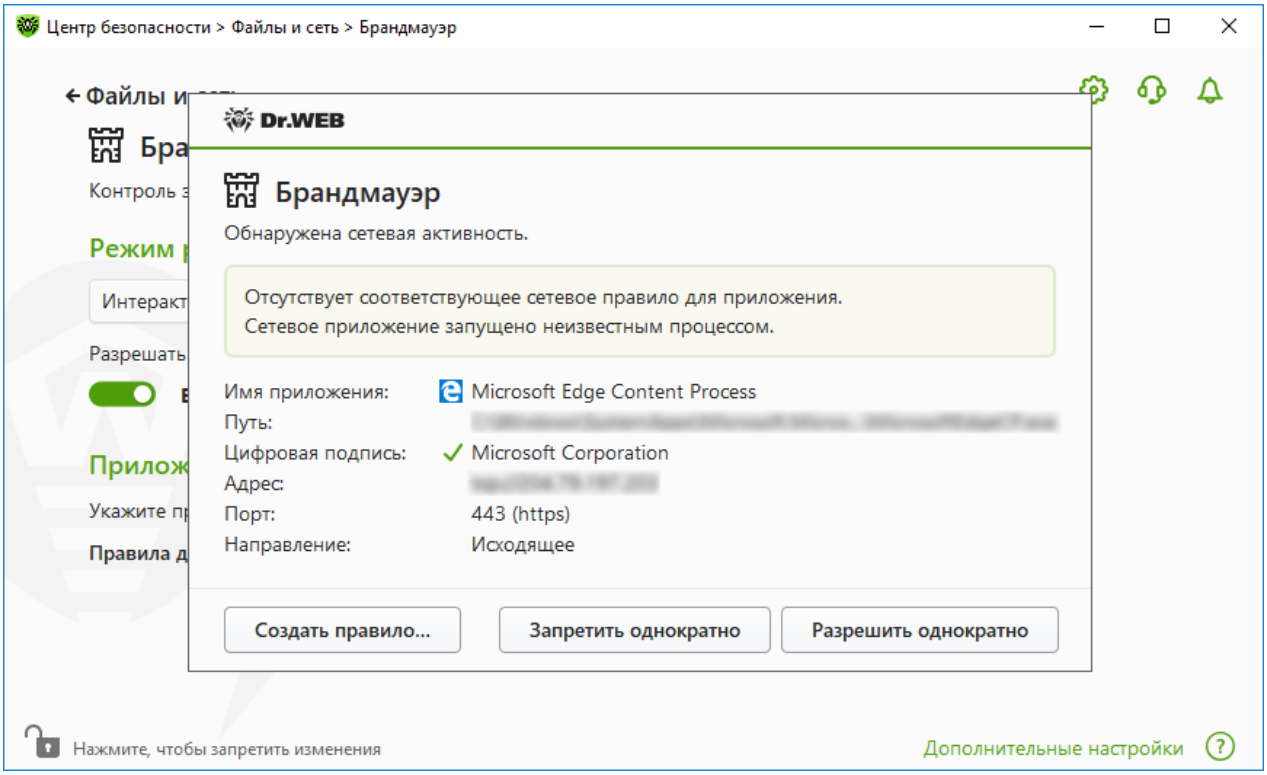

Рисунок 46. Пример предупреждения о попытке доступа к сети

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 **ОК**.

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.

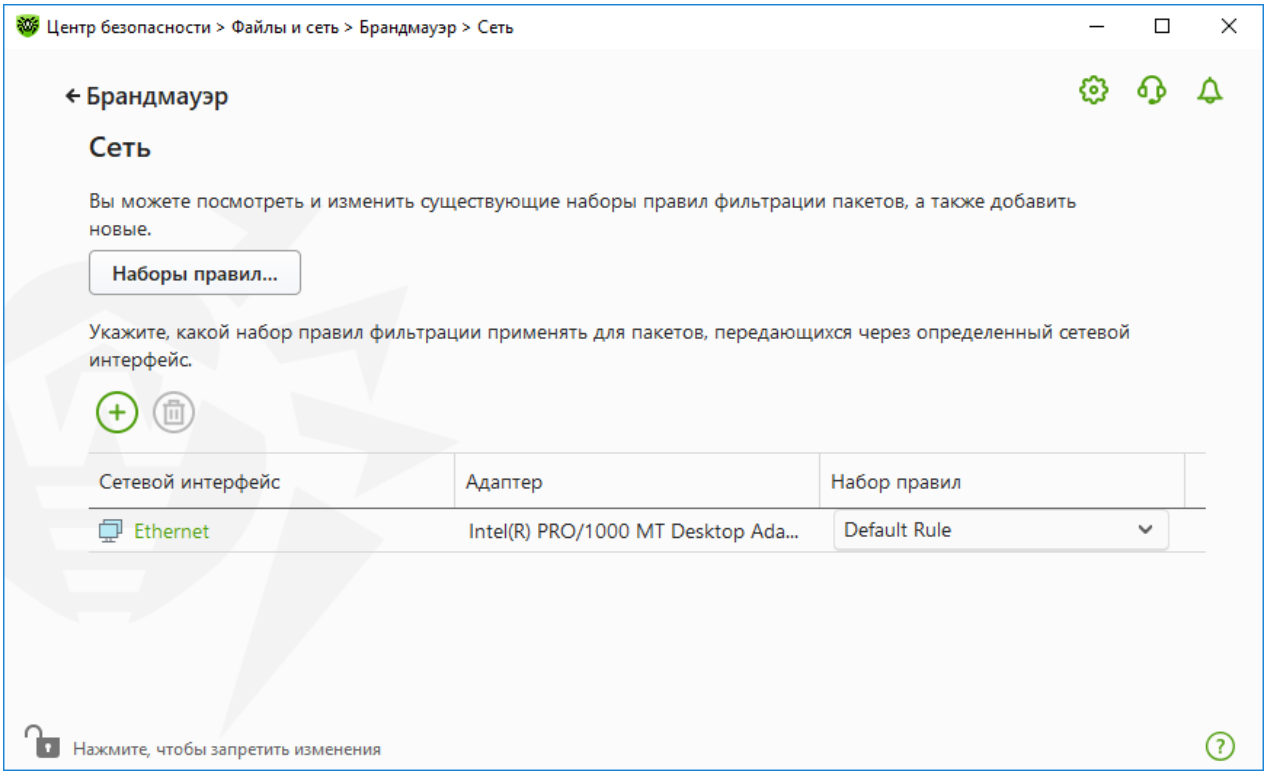

Рисунок 47. Наборы правил для сетевых интерфейсов

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**.

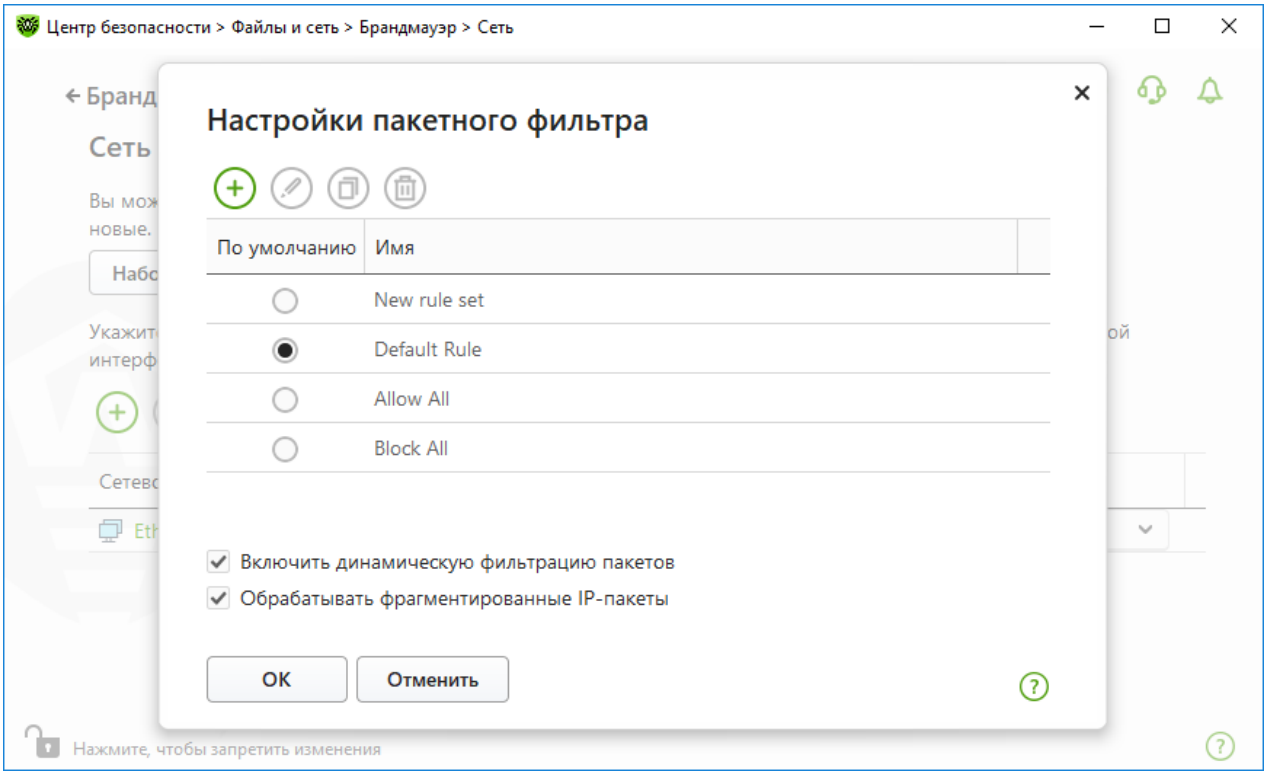

Рисунок 48. Окно Настройки пакетного фильтра

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.

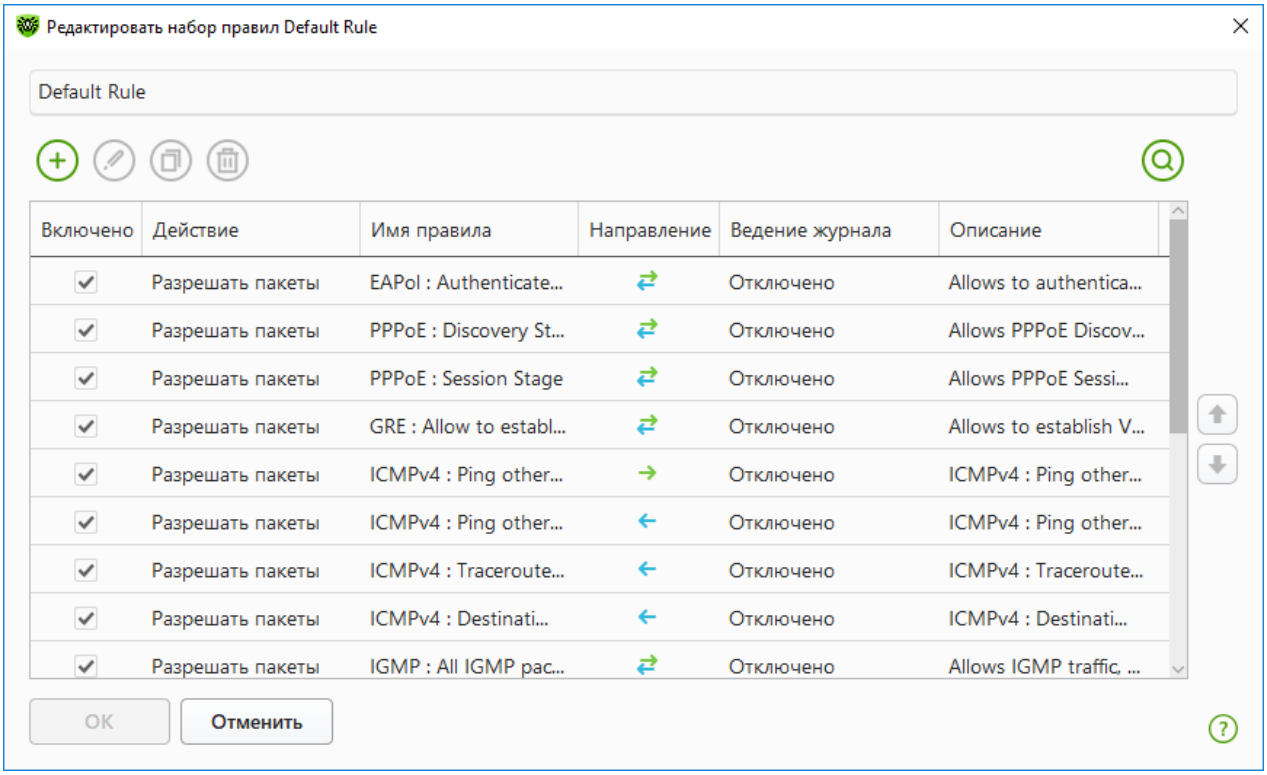

Рисунок 49. Набор правил фильтрации пакетов

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.

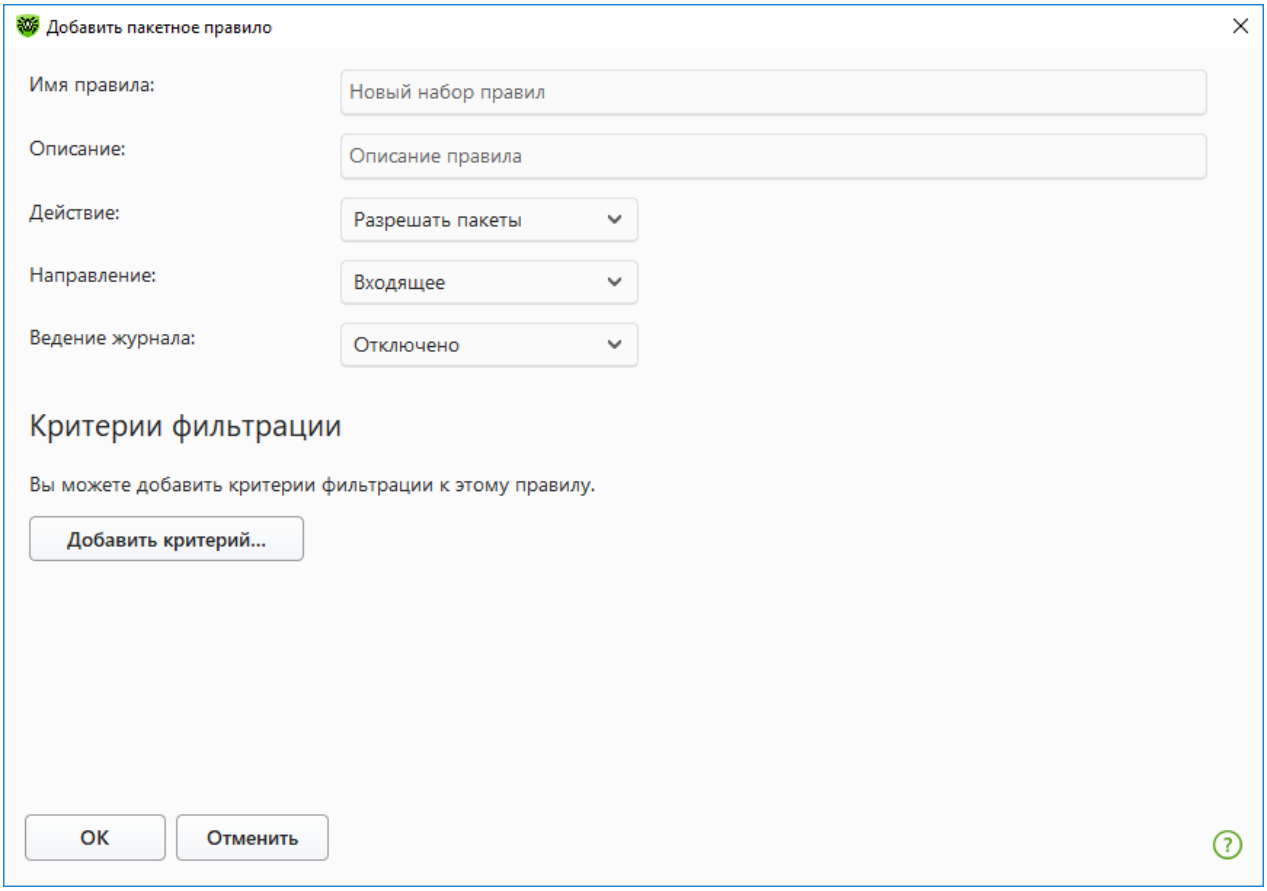

Рисунок 50. Добавление правила фильтрации

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**:

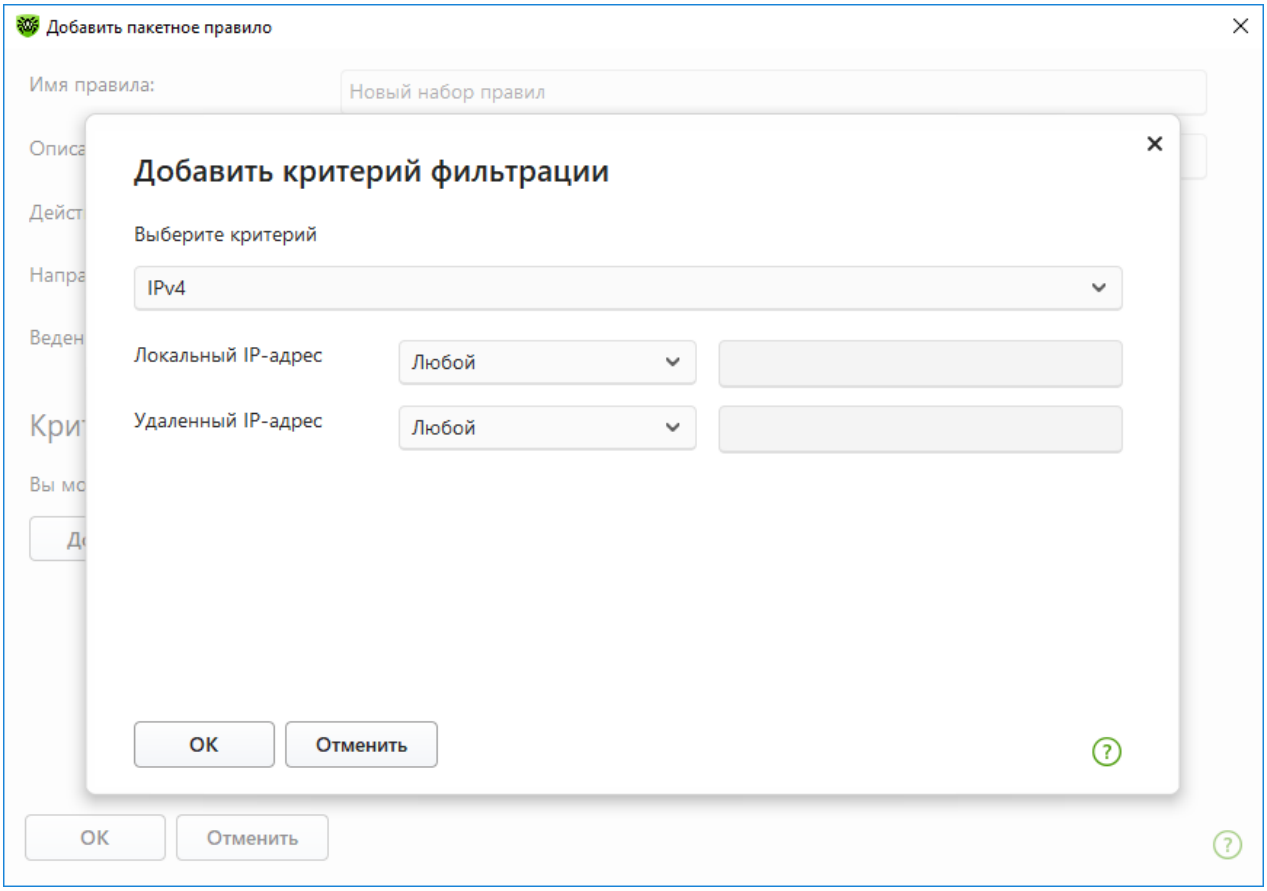

Рисунок 51. Добавление критерия фильтрации

Выберите нужный критерий в выпадающем списке. В этом же окне вы можете настроить параметры для выбранного критерия. Вы можете добавить любое необходимое количество критериев.

Для срабатывания критерия достаточно соответствие хотя бы одному из его параметров.

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

Чтобы действие из правила было применено к пакету, пакет должен соответствовать всем критериям правила.

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

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

Если в данном правиле внутри заголовка IPv4 для параметров **Локальный IP-адрес** и **Удаленный IP-адрес** указать значение **Любой**, правило сработает для любого пакета, содержащего заголовок IPv4. *Локальный IP-адрес* — это IP-адрес сетевого адаптера на компьютере, на котором настраивается Брандмауэр, а *Удаленный IP-адрес* — это адрес узла, с которого принимаются входящие пакеты или на который направляются исходящие пакеты.

9.5. 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

9.5.1. Запуск и режимы проверки

Чтобы запустить проверку файлов

> При работе под управлением операционных систем Windows Vista, Windows Server 2003 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.

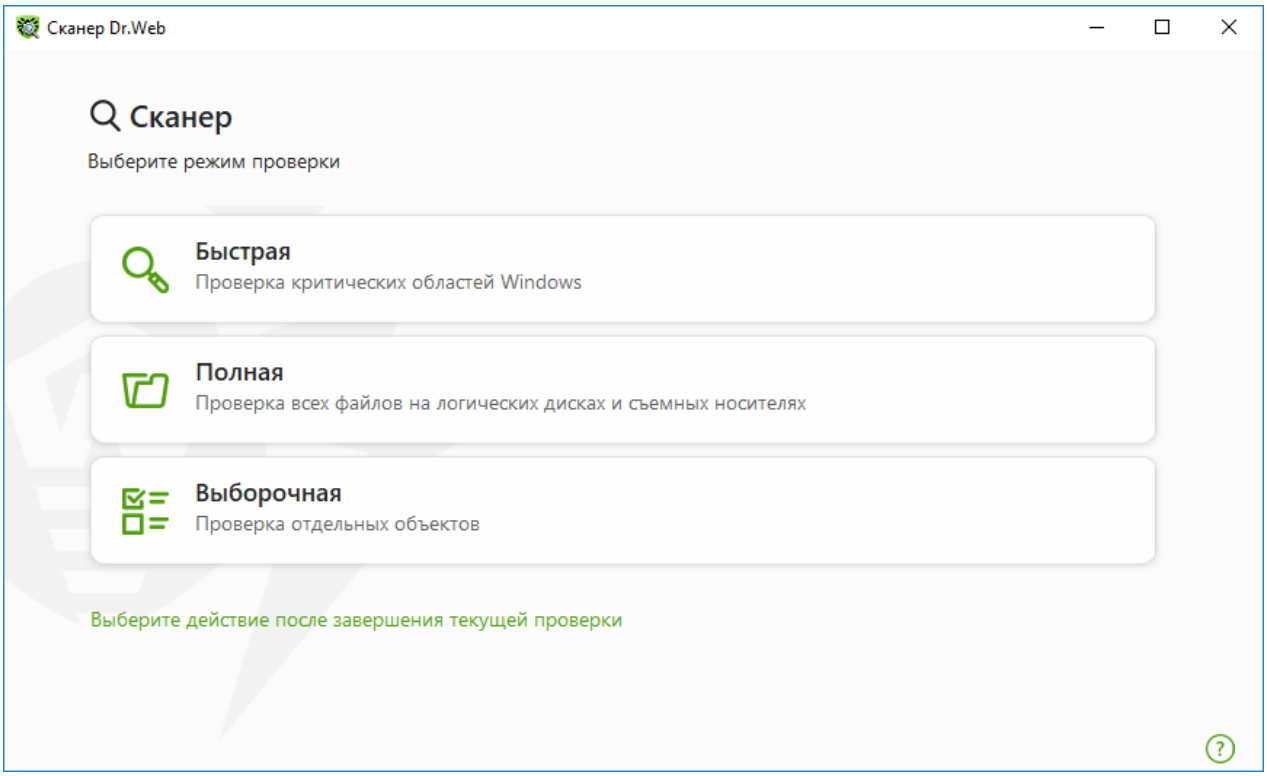

Рисунок 52. Выбор режима проверки

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

Режим проверки	Описание
	добавить объекты в список проверки, нажмите кнопку ⊕.

9.5.2. 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.

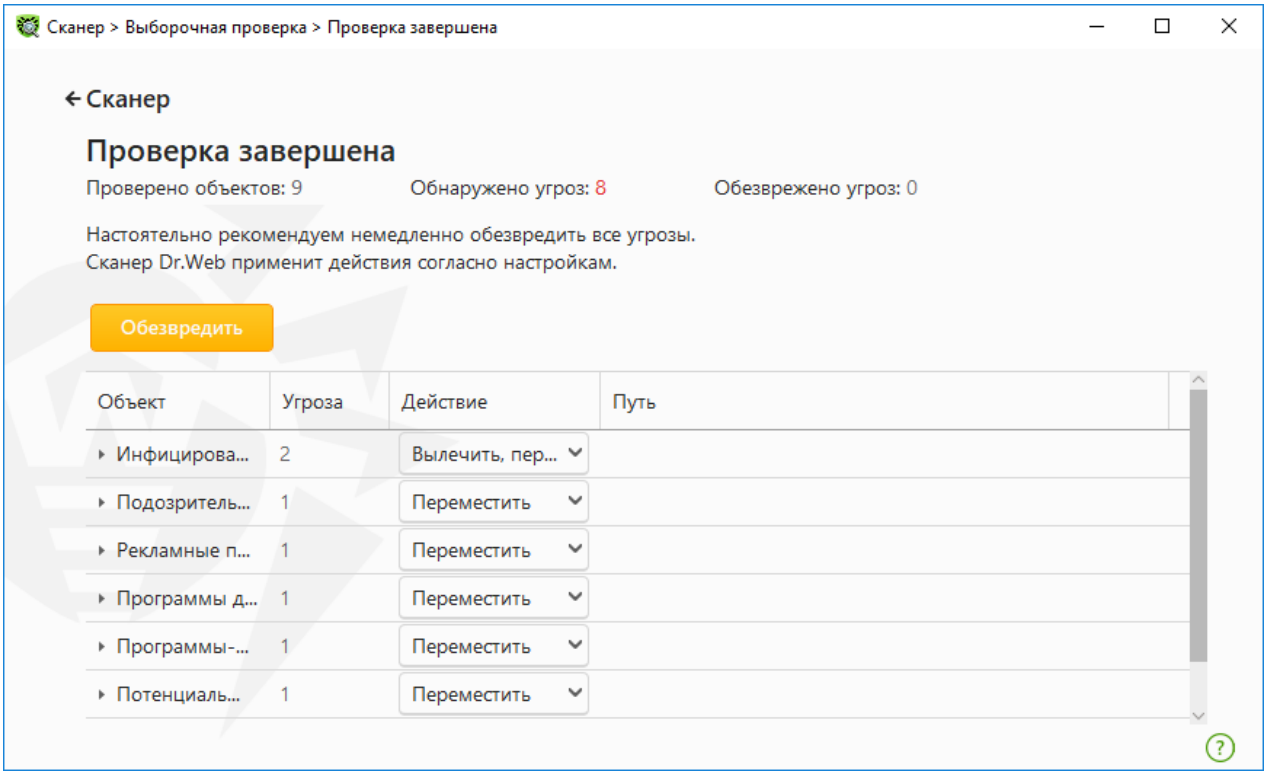

Рисунок 53. Выбор действия по окончании проверки

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).

Столбец	Описание
Угроза	В этом столбце указано наименование угрозы или ее модификации по внутренней классификации компании «Доктор Веб». Для подозрительных объектов указывается, что объект «возможно, инфицирован» и указывается тип возможной угрозы 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, контейнеров 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`.

9.5.3. Дополнительные возможности

В этом разделе содержится информация о дополнительных возможностях работы Сканера:

- Запуск Сканера с параметрами командной строки
- Консольный сканер

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.

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

12 — не запущен Scanning Engine

255 — проверка прервана пользователем

9.6. 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 почтовых сообщений на спам;
- обнаружение и нейтрализацию вредоносного программного обеспечения;
- эвристический анализ для дополнительной защиты от неизвестных угроз.

При проверке электронной почты с помощью Dr.Web для Microsoft Outlook рекомендуется использовать режим кеширования Exchange.

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;
- Антиспам-фильтр — позволяет определить действия программы для спам-сообщений, а также создать белый и черный списки электронных адресов;
- Статистика — показывает данные об объектах, проверенных и обработанных программой.

9.6.1. Проверка на угрозы

Dr.Web для Microsoft Outlook использует различные методы обнаружения угроз. 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, в которых обнаружены известные и (предположительно) излечимые угрозы;
- выпадающий список **Невылеченные** задает реакцию на обнаружение объектов, в которых обнаружены известные неизлечимые угрозы, а также когда предпринятая попытка излечения не принесла успеха;
- выпадающий список **Подозрительные** задает реакцию на обнаружение объектов, в которых предположительно обнаружена угроза (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 обнаруженной угрозы.

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.

9.6.2. Проверка на спам

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

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

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

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

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

Настройка антиспам-фильтра

Чтобы настроить параметры антиспам-фильтра

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

Если некоторые письма были неправильно распознаны, следует отправить их на специальные почтовые адреса для анализа и повышения качества работы фильтра:

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

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

Белый и черный списки

Белый и черный списки электронных адресов служат для фильтрации сообщений.

Для просмотра и редактирования белого или черного списка в настройках антиспам-фильтра нажмите кнопку **Белый список** или **Черный список** соответственно.

Чтобы добавить адрес в белый или черный список

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

Чтобы изменить адрес в списке

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

Чтобы удалить адрес из списка

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

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

Белый список

Если адрес отправителя добавлен в белый список, письмо не подвергается анализу на содержание спама. Методы ввода:

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

  Например, допускаются следующие варианты:
  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

  

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

  Символ «@» обязателен.

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

Черный список

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

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

  Например, допускаются следующие варианты:
  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

  

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

  Символ «@» обязателен.

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

9.6.3. 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 модулей программы: сканера, ядра, вирусных баз (информация заносится при запуске программы и при обновлении модулей);
- сообщения об обнаружении угроз.

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 об обнаружении угроз;
- 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.

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.

9.6.4. 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, в которых предположительно обнаружены угрозы (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 Агент Dr.Web для Windows статистика обнуляется.

10. 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**.

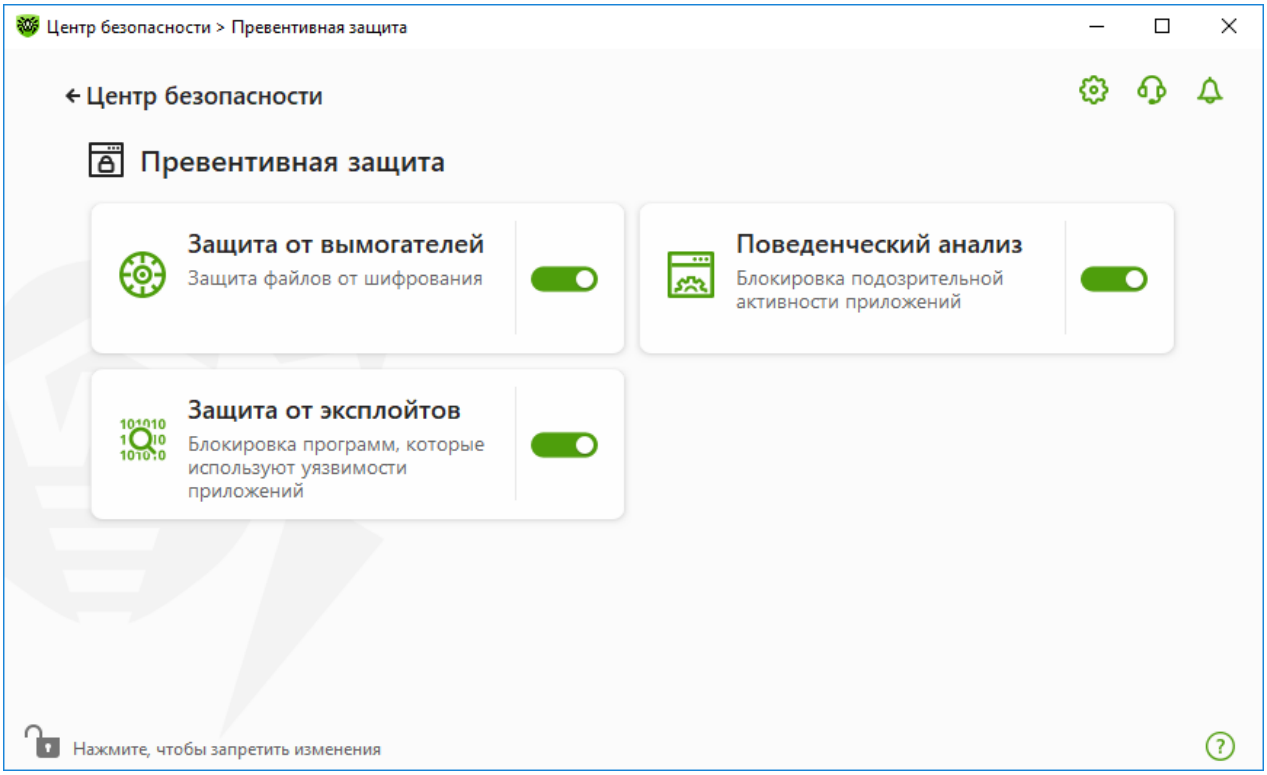

Рисунок 54. Окно Превентивная защита

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.

Включение и выключение Превентивной защиты и изменение параметров компонентов возможно, если администратор сервера централизованной защиты, к которому подключается Dr.Web, дал на это разрешение.

В этом разделе:

- Защита от вымогателей — параметры запрета шифрования файлов пользователей.
- Поведенческий анализ — параметры запрета доступа приложений к системным объектам.
- 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.

10.1. 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 вредоносную программу.

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 угроз, 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.

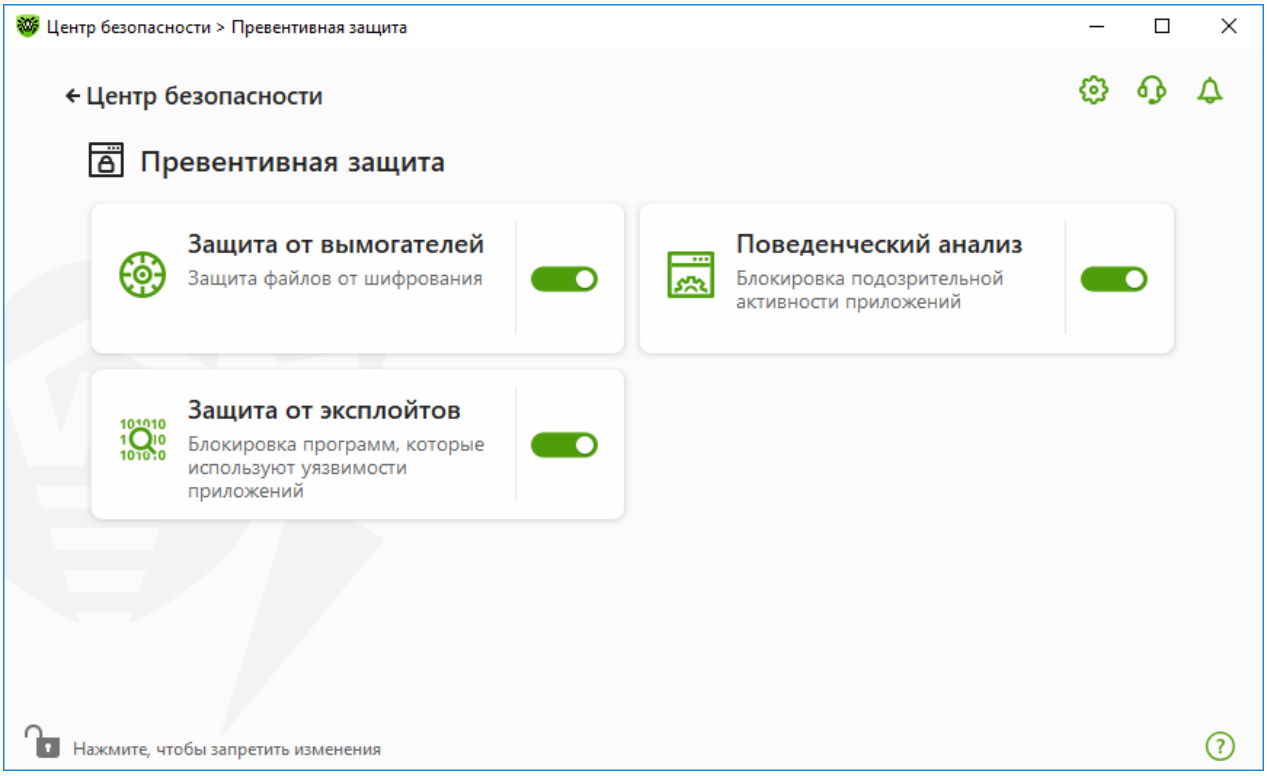

Рисунок 55. Включение/отключение компонента Защита от вымогателей

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

В этом разделе:

- Настройка реакции на попытки приложений зашифровать файлы
- Отдельные правила для приложений

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.

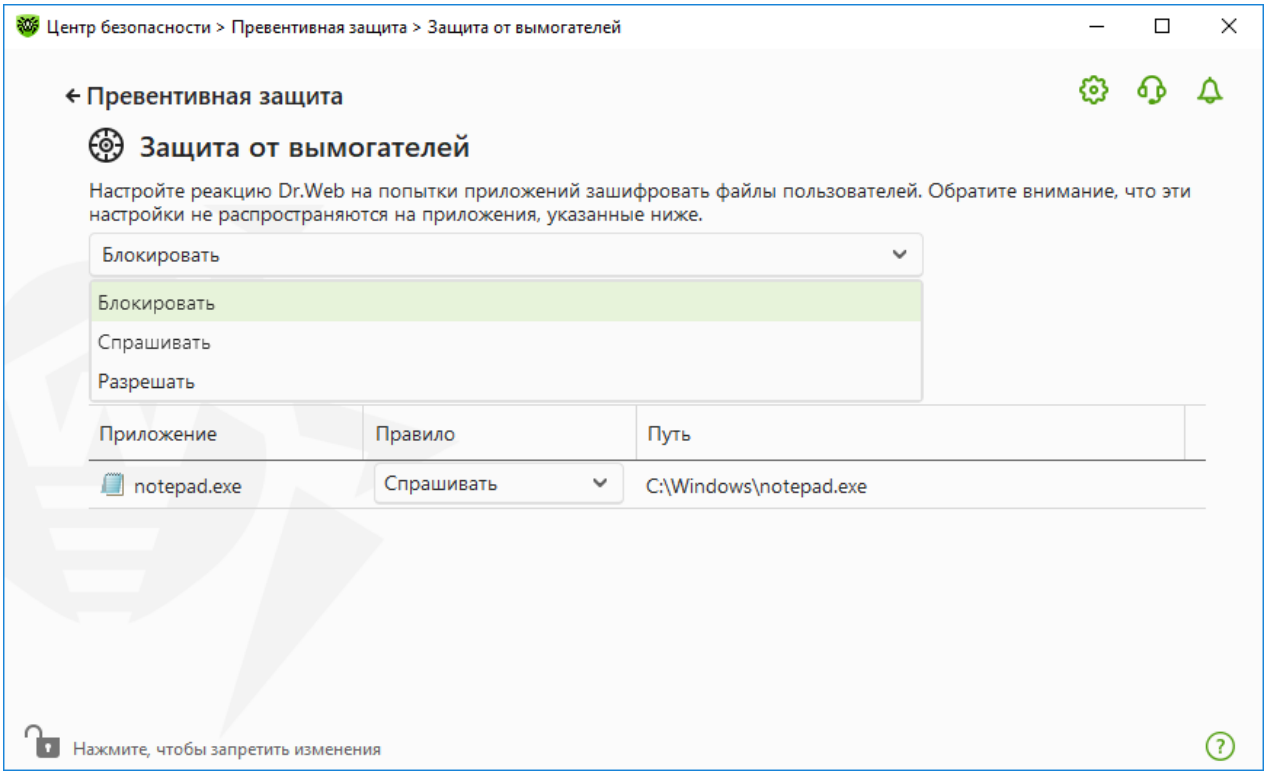

Рисунок 56. Выбор реакции Dr.Web

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

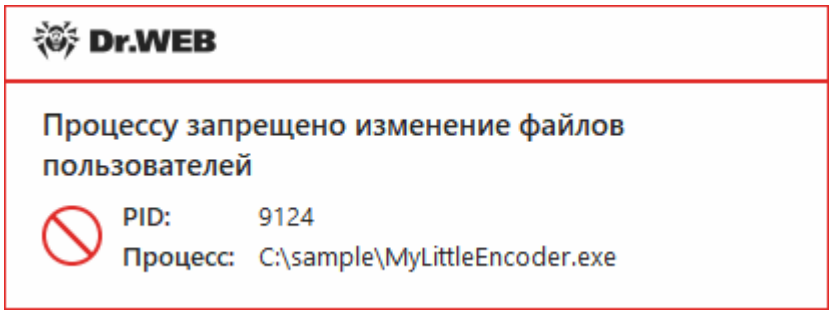

Рисунок 57. Пример уведомления о запрете изменения файлов пользователя

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

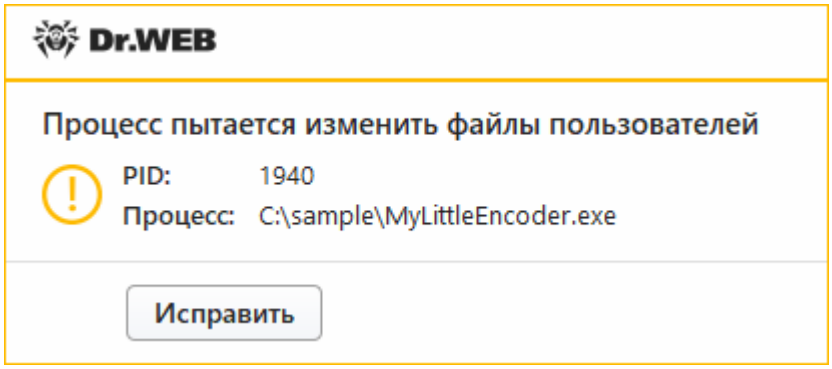

Рисунок 58. Пример уведомления о попытке изменения файлов пользователя

- 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.

См. также:

- Уведомления

Отдельные правила для приложений

Вы можете настроить реакцию компонента Защита от вымогателей на действия отдельных приложений. Для этого необходимо добавить приложение в список и выбрать необходимую реакцию компонента. Для работы с объектами в списке доступны следующие элементы управления:

- Кнопка ⊕ — добавление приложения в список приложений с отдельными правилами.
- Кнопка 🗑 — удаление приложения из списка приложений с отдельными правилами.

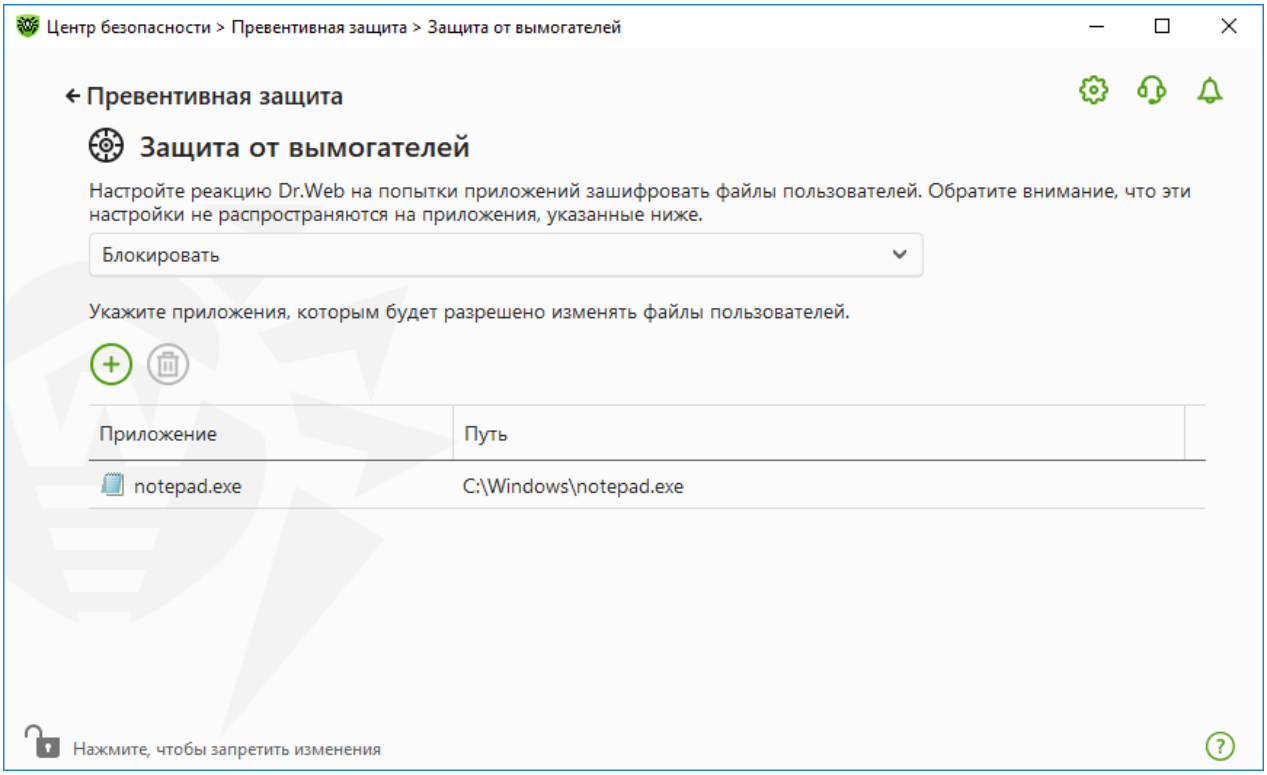

Рисунок 59. Приложения, на которые не распространяется общее правило

Чтобы добавить приложение в список

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

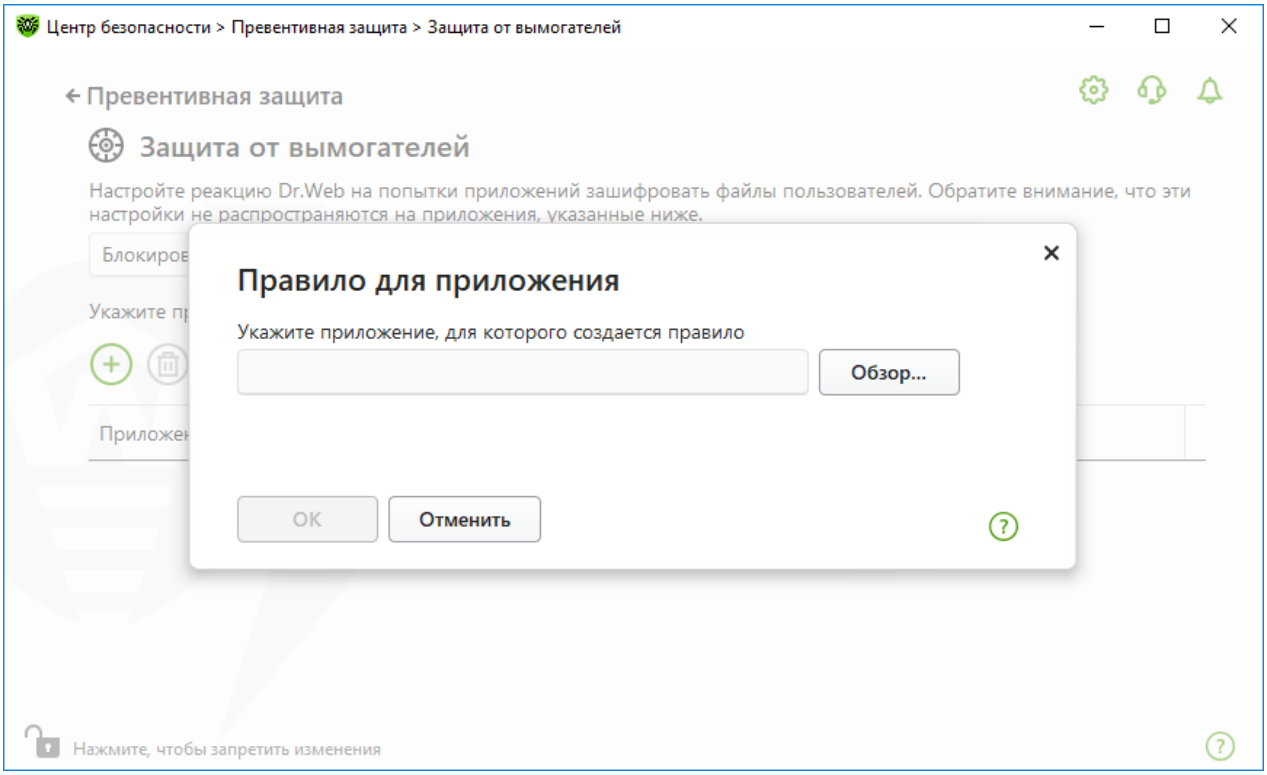

Рисунок 60. Выбор правила для приложения

3. Выберите необходимую реакцию из выпадающего списка.
4. Нажмите **OK**.

Также вы можете изменить уже заданное правило.

Чтобы изменить реакцию Dr.Web для приложений с заданными правилами

1. На основном окне параметров компонента Защита от вымогателей выберите необходимое приложение.
2. В соответствующей строке в столбце **Правило** из выпадающего списка выберите необходимую реакцию на попытки приложения зашифровать файлы пользователя.

10.2. Поведенческий анализ

Компонент Поведенческий анализ позволяет настроить реакцию Dr.Web на действия сторонних приложений, не являющихся доверенными, 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.

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.

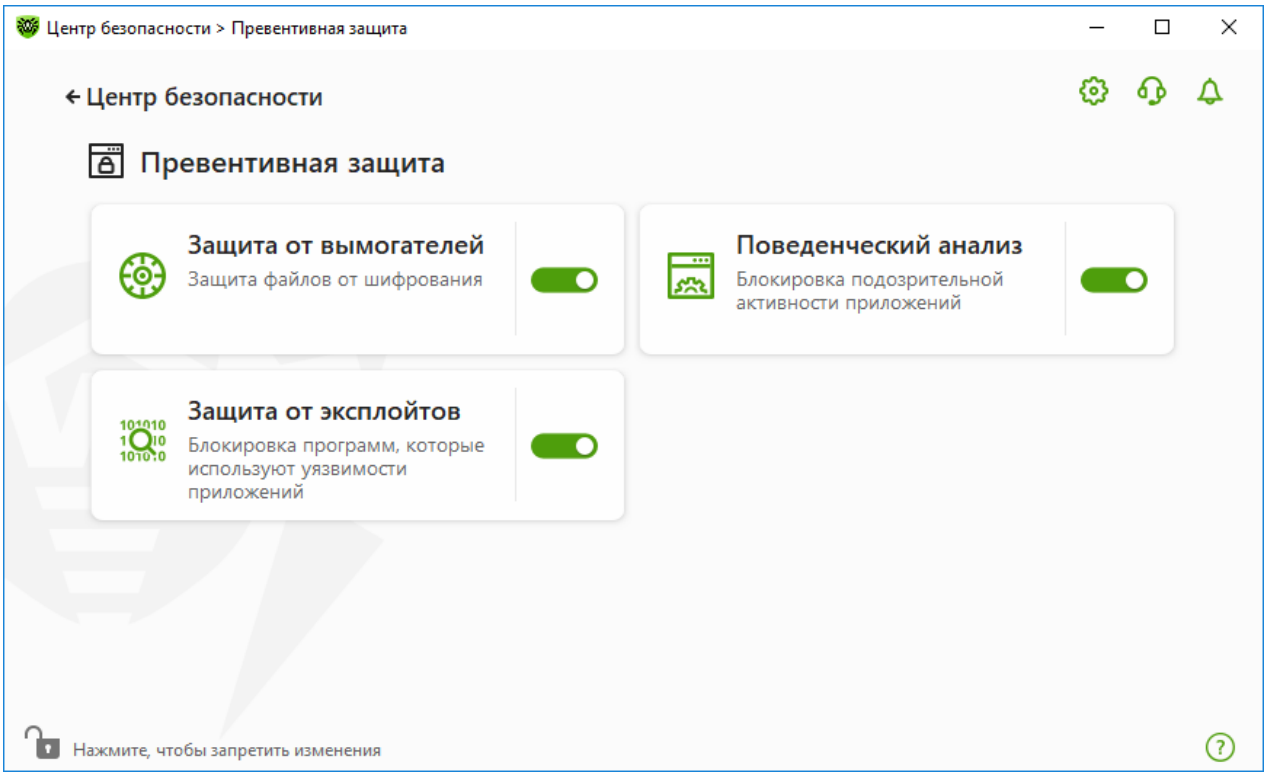

Рисунок 61. Включение/отключение компонента Поведенческий анализ

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

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.

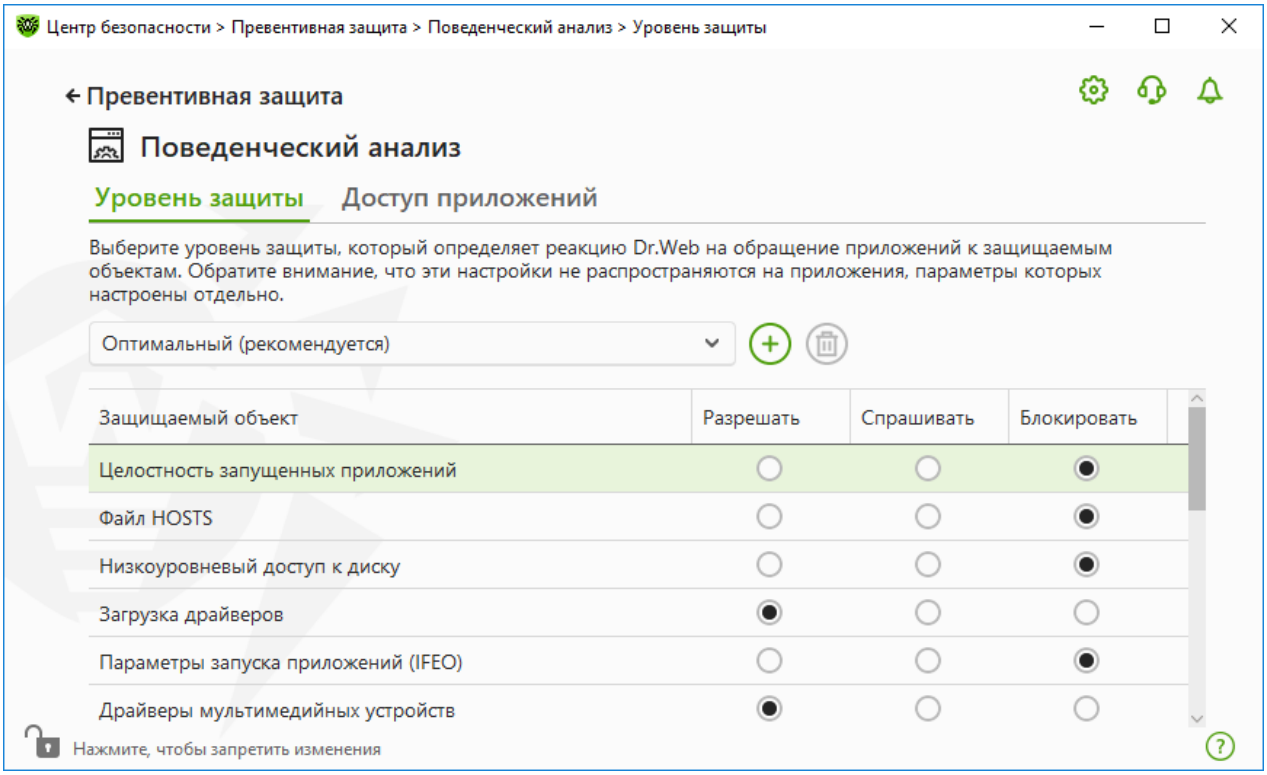

Рисунок 62. Параметры Поведенческого анализа

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)	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.

Уровень защиты	Описание
	 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:

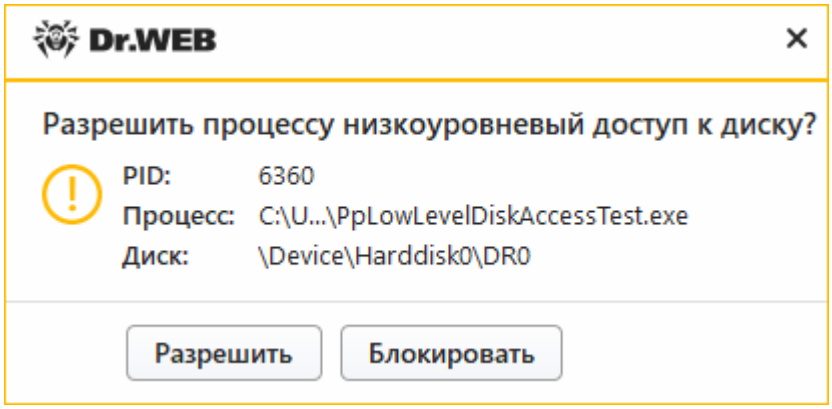

Рисунок 63. Пример уведомления с запросом доступа к защищаемому объекту

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

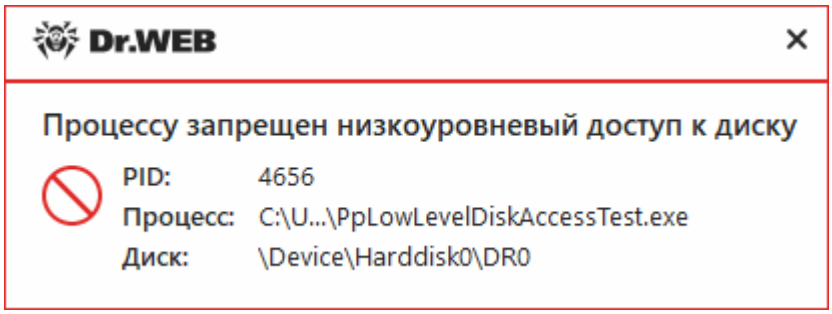

Рисунок 64. Пример уведомления о запрете доступа к защищаемому объекту

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 **ОК**.

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 **ОК**, чтобы подтвердить удаление.

Получение уведомлений

Вы можете настроить вывод уведомлений о действиях компонента Поведенческий анализ на экран.

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.

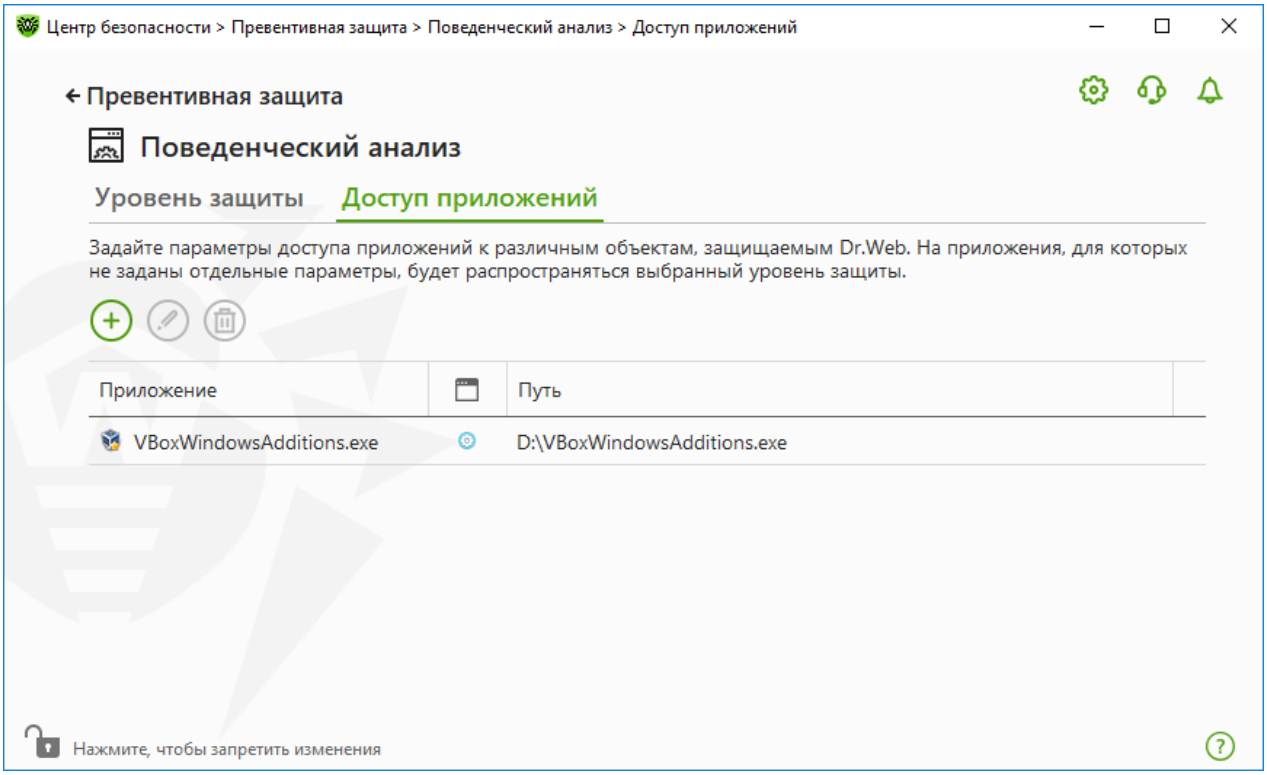

Рисунок 65. Параметры доступа для приложений

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.

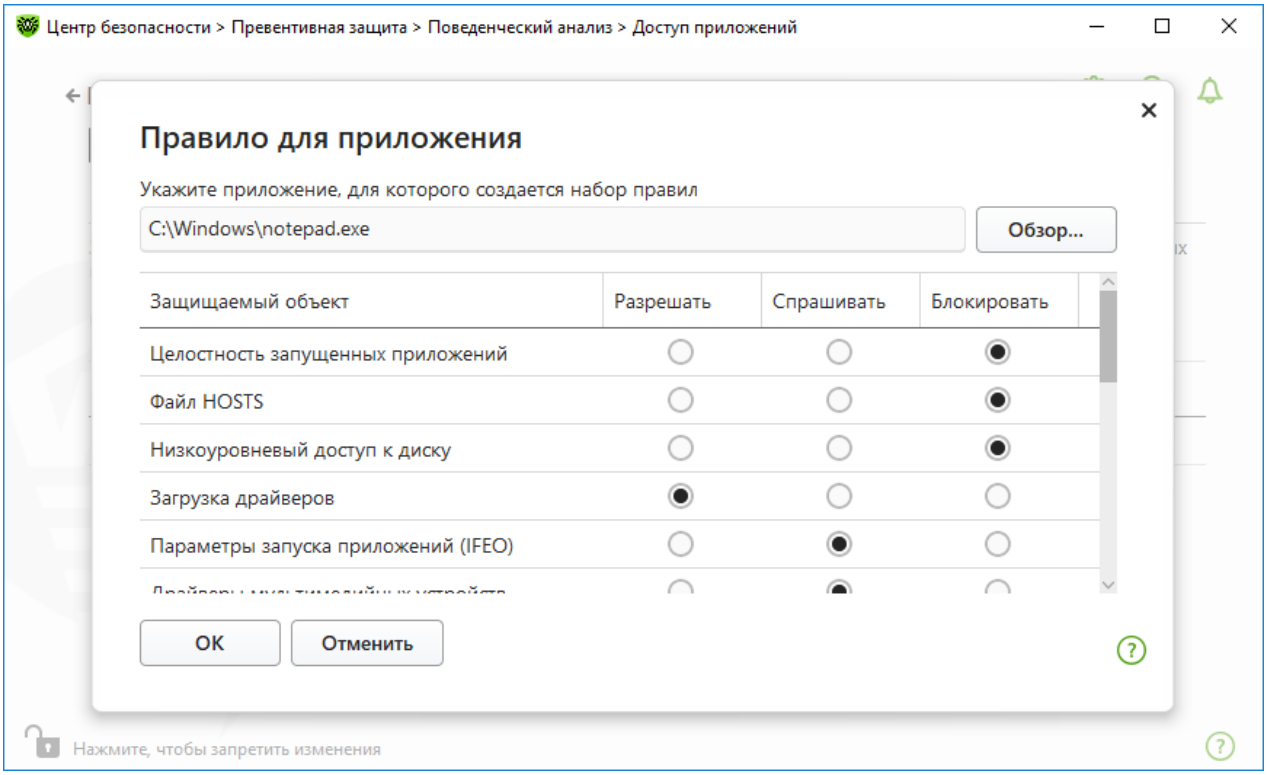

Рисунок 66. Добавление набора правил для приложения

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.

Защищаемый объект	Описание
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.

Прочие настройки позволяют защищать от модификации ветки реестра (как в системном профиле, так и в профилях всех пользователей).

Защищаемый объект	Описание
Параметры запуска приложений (IFEO)	• `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\Microsoft\Windows\CurrentVersion\Group Policy Objects\*\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers` • `Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\*\Software\Policies\Microsoft\Windows\SrpV2` • `Software\Policies\Microsoft\Windows\Safer` • `Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers` • `Software\Policies\Microsoft\Windows\SrpV2`
Плагины Internet Explorer (BHO)	• `Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects`

Защищаемый объект	Описание
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	• 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.

10.3. Защита от эксплойтов

Компонент Защита от эксплойтов позволяет блокировать вредоносные объекты, которые используют уязвимости в популярных приложениях.

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 .

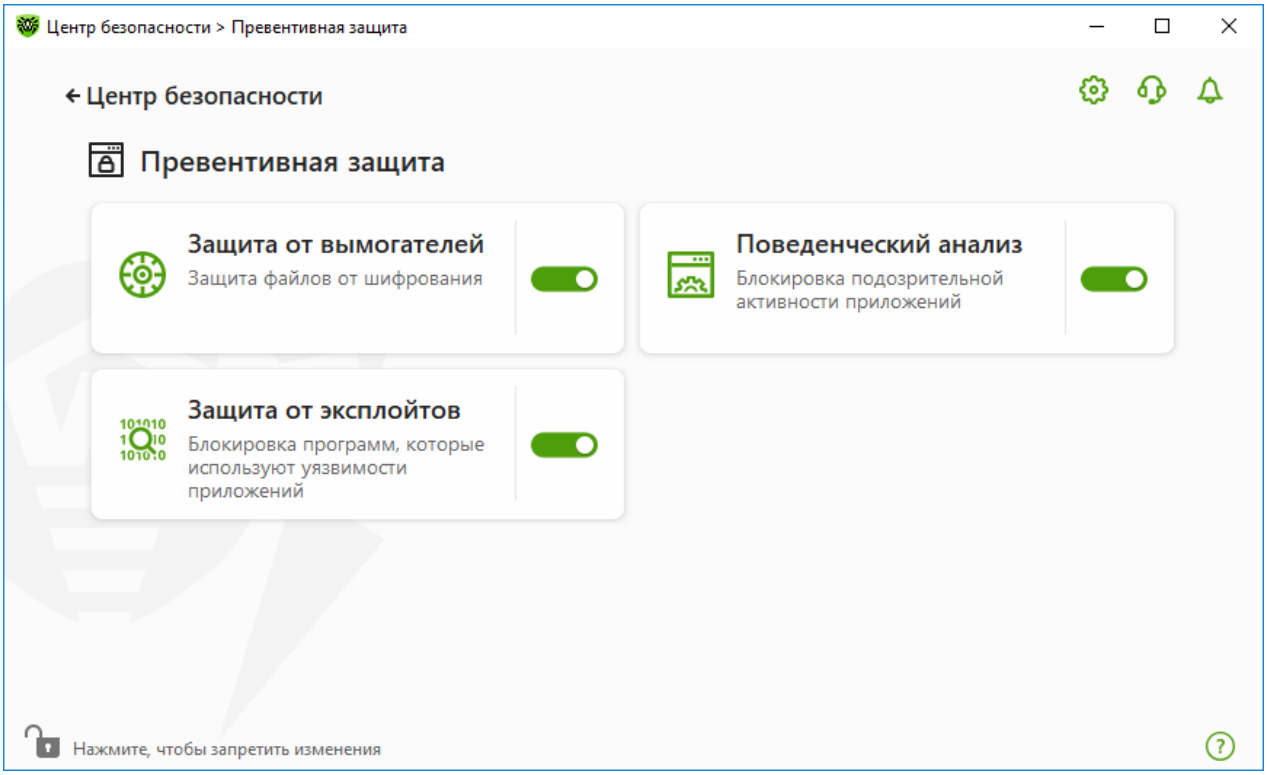

Рисунок 67. Включение/отключение компонента Защита от эксплойтов

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.

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

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

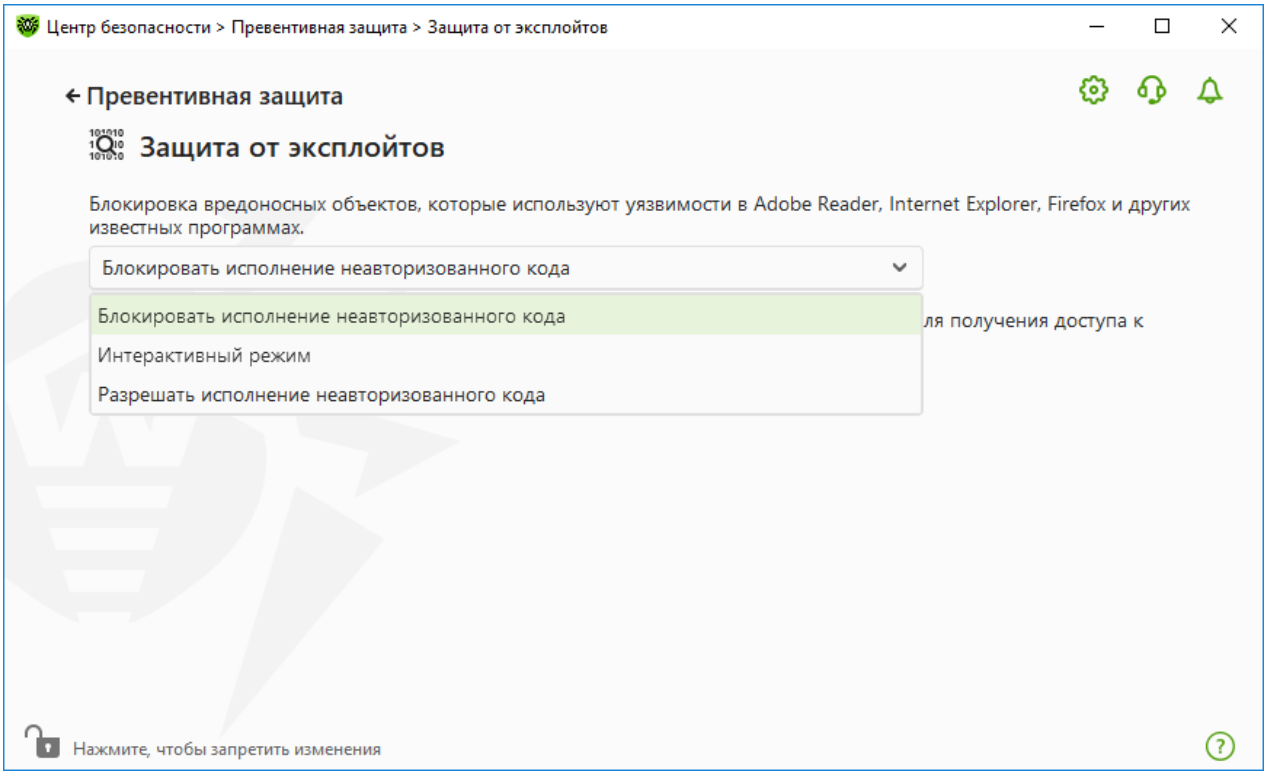

Рисунок 68. Выбор уровня защиты

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.

См. также:

- Уведомления

11. Устройства

В окне **Устройства** вы можете ограничить доступ к определенным устройствам или шинам устройств и настроить список разрешенных устройств.

> Параметры доступа к устройствам применяются для всех учетных записей Windows.

Чтобы перейти в окно Устройства

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. Нажмите плитку **Устройства**.

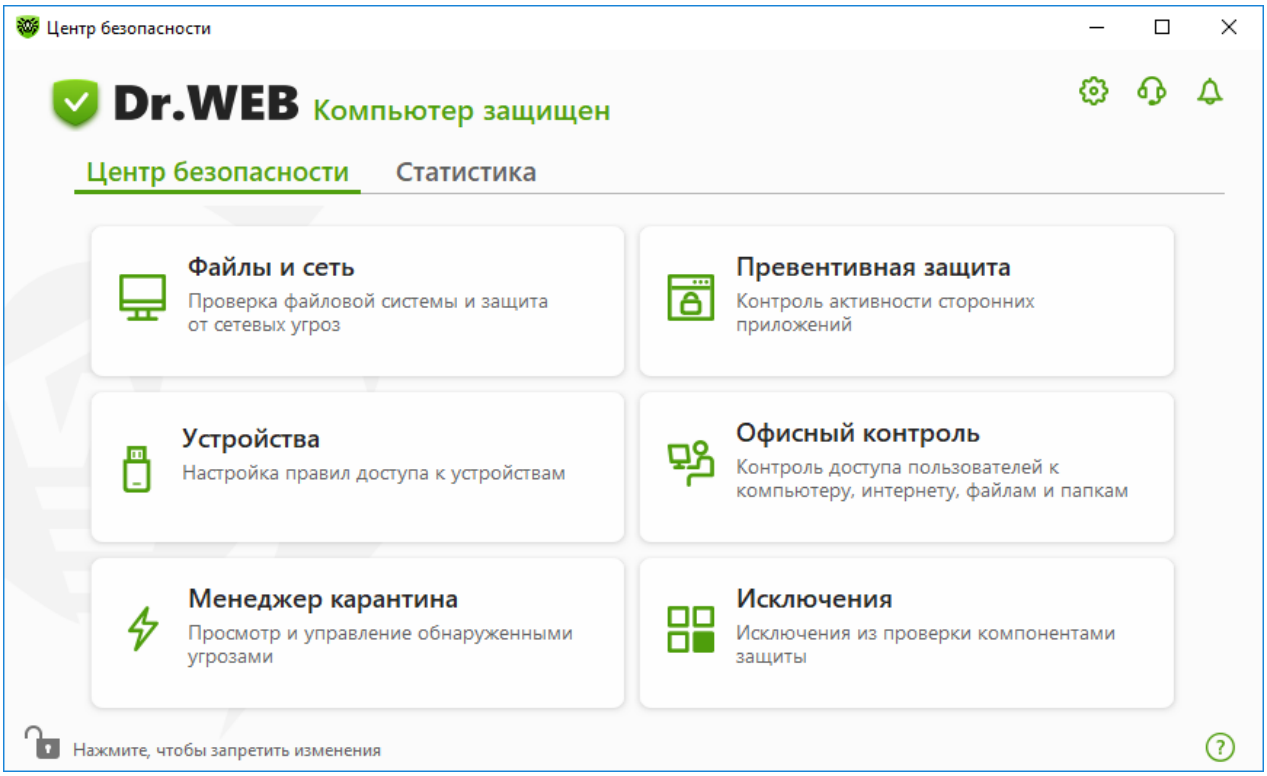

Рисунок 69. Доступ к окну Устройства

В этом разделе:

- Основные параметры блокировки
- Блокировка шин и классов устройств
- Формирование списка разрешенных устройств

Основные параметры

Вы можете включить соответствующие опции, чтобы:

- блокировать передачу заданий на печать;
- блокировать передачу данных по локальным сетям и интернету.

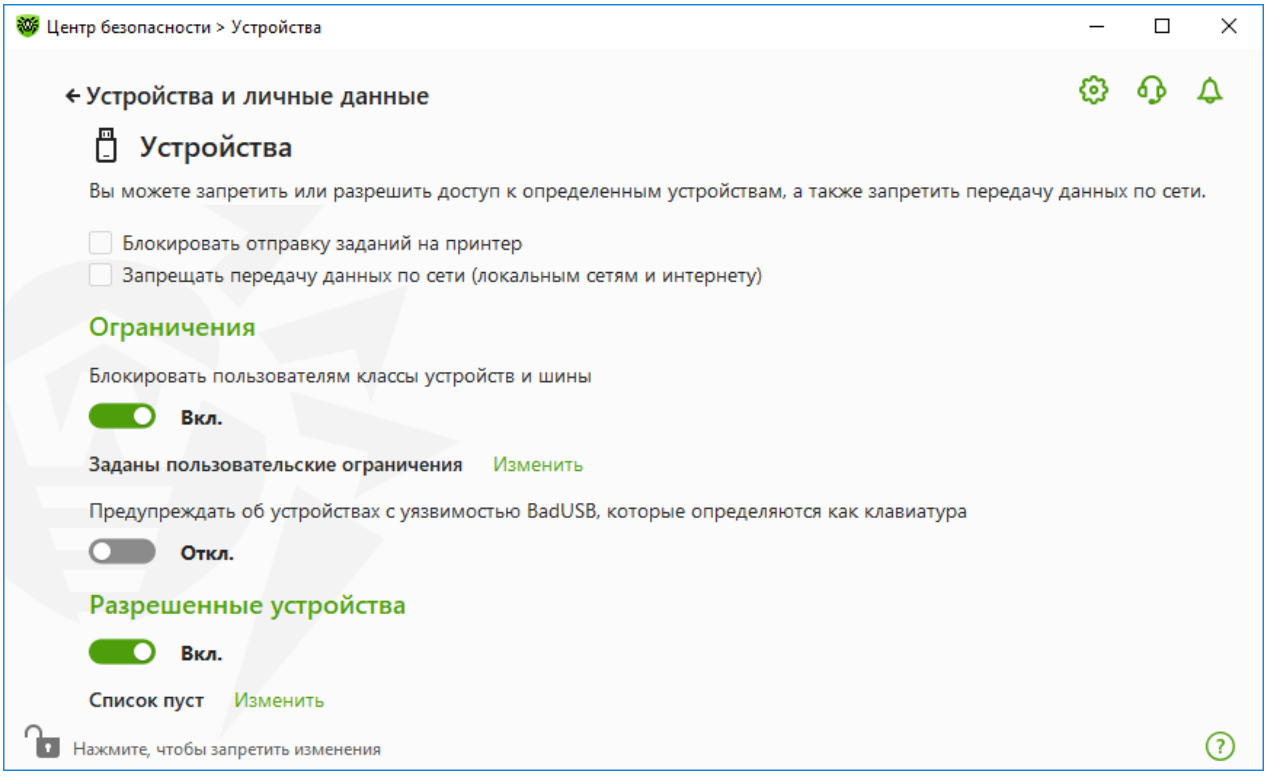

Рисунок 70. Параметры блокировки устройств

По умолчанию все опции отключены.

Опция **Блокировать съемные носители** доступна только тем пользователям, у которых она была включена до обновления компонентов продукта от 02.02.2022. Если вы не пользовались этой опцией или устанавливаете продукт впервые, воспользуйтесь опцией **Блокировать пользователям классы и шины устройств**, чтобы запретить доступ к данным на съемных носителях.

Ограничения

Параметры блокировки устройств

Функция блокировки устройств позволяет как заблокировать один или несколько классов устройств на всех шинах, так и заблокировать все устройства, подключенные к

одной или нескольким шинам. Под *классами устройств* понимаются устройства, выполняющие одинаковые функции (например, устройства для печати). Под *шинами* — подсистемы передачи данных между функциональными блоками компьютера (например, шина USB).

Чтобы заблокировать доступ к выбранным классам устройств и шинам

1. Включите опцию **Блокировать пользователям классы и шины устройств** при помощи соответствующего переключателя .
2. Нажмите ссылку **Изменить**.
3. В открывшемся окне вы можете выбрать классы устройств или шины, доступ к которым хотите заблокировать.

Предупреждение об устройствах с уязвимостью BadUSB

Некоторые инфицированные USB-устройства могут опознаваться компьютером как клавиатура. Чтобы программа Dr.Web проверяла, действительно ли подключенное устройство является клавиатурой, включите опцию **Предупреждать об устройствах с уязвимостью BadUSB, которые определяются как клавиатура**. В этом случае при подключении клавиатуры откроется окно разблокировки. Вам нужно нажать указанные кнопки на клавиатуре.

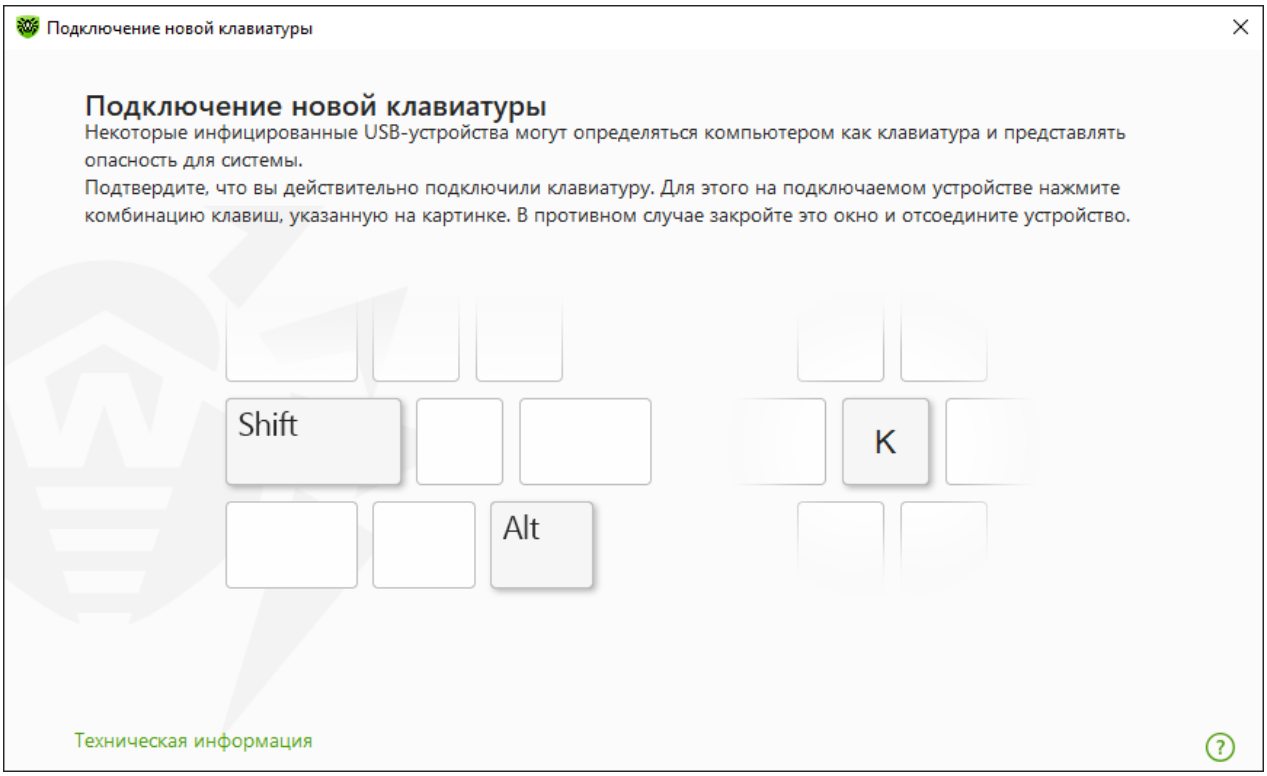

Рисунок 71. Окно разблокировки клавиатуры

При нажатии ссылки **Техническая информация** откроется окно с подробной информацией об устройстве.

Разрешенные устройства

Если вы ограничили доступ к каким-либо классам устройств или шинам, вы можете отдельно разрешить доступ к определенным устройствам, добавив их в список разрешенных устройств. Также в список можно добавить конкретное устройство, чтобы не проверять его на наличие BadUSB-уязвимости.

Чтобы добавить устройства в список разрешенных

1. Включите опцию **Разрешенные устройства** при помощи соответствующего переключателя.
2. Нажмите кнопку **Изменить** (кнопка становится активна, если заданы ограничения).
3. В открывшемся окне вы можете сформировать список устройств, на которые не будут распространяться ограничения доступа.

11.1. Блокировка шин и классов

Чтобы перейти в окно Классы и шины устройств

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Устройства**.
3. В группе настроек **Ограничения** включите опцию **Блокировать пользователям классы и шины устройств** при помощи переключателя.
4. Нажмите ссылку **Изменить**.
5. В открывшемся окне вы можете выбрать шины или классы устройств, доступ к которым хотите заблокировать.

Окно содержит таблицу с информацией о заблокированных шинах и классах устройств. По умолчанию таблица пустая. В ней будут отображаться шины и классы при добавлении их в список заблокированных. При этом в строке с заблокированной шиной отображаются все заблокированные на ней классы устройств.

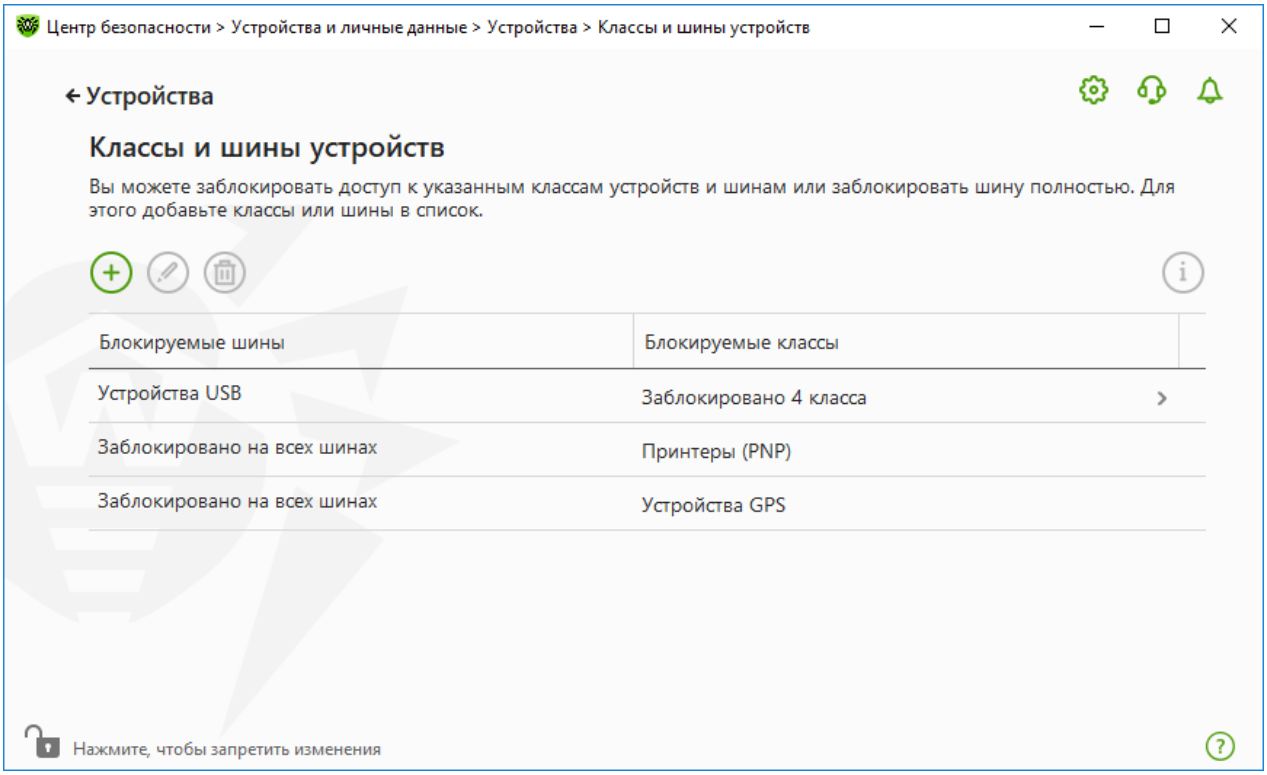

Рисунок 72. Заблокированные шины и классы

В столбце **Блокируемые классы** отображается количество заблокированных классов на соответствующей шине. Если на одной шине заблокировано несколько классов, они отображаются в выпадающем списке.

Серым цветом выделен класс, заблокированный на всех шинах.

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление объекта в список заблокированных.
- Кнопка ✎ — редактирование настроек блокировки для выбранного объекта в таблице.
- Кнопка 🗑 — удаление выбранного объекта из списка заблокированных.

Вы можете просмотреть подробную информацию о заблокированной шине и заблокированных на ней классах устройств. Для этого выберите необходимую строку и нажмите ⓘ.

Блокировка шины

1. Чтобы заблокировать шину полностью или некоторые устройства на определенной шине, нажмите кнопку ⊕.
2. Из выпадающего списка выберите объект, который вы хотите заблокировать: **Шина**. Нажмите **Далее**.

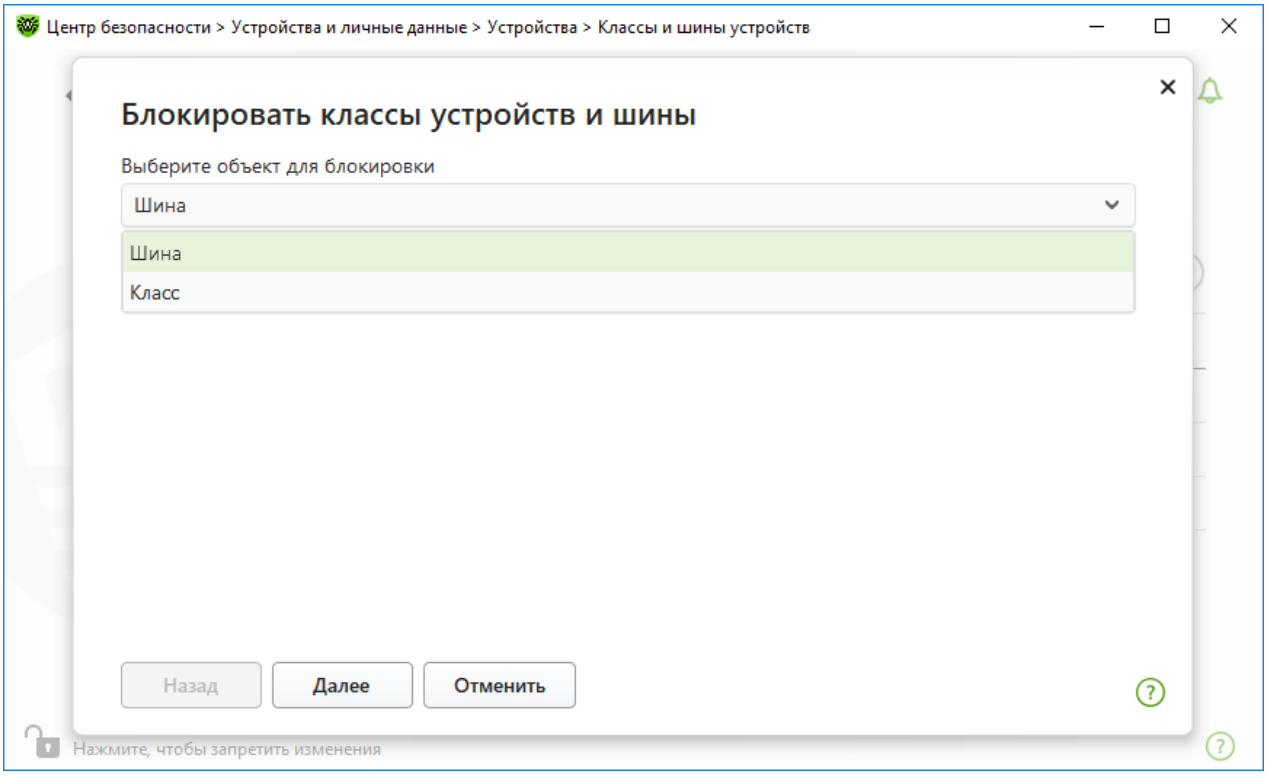

Рисунок 73. Выбор объекта для блокировки

3. Выберите тип шины. Нажмите **Далее**.

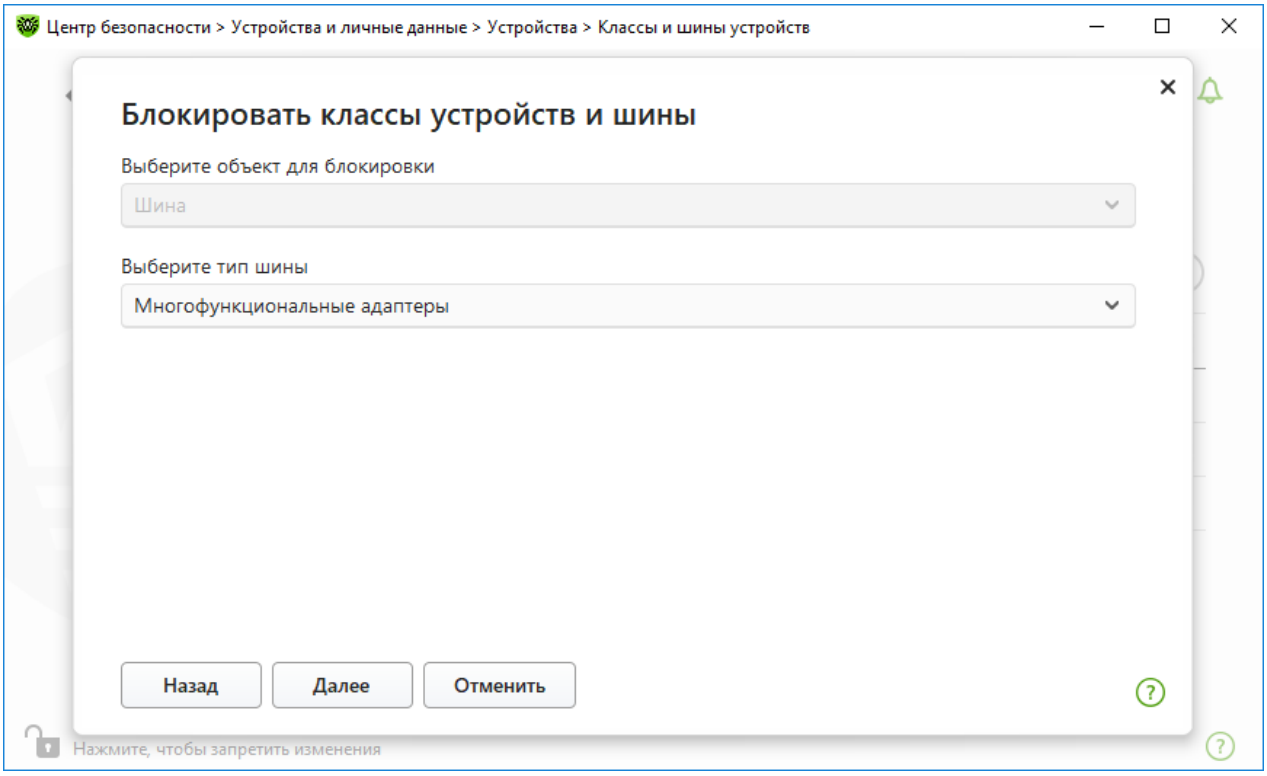

Рисунок 74. Выбор типа шины

4. Выберите тип блокировки и нажмите **Далее**:
   - **Полностью** — будут заблокированы все классы устройств на данной шине;

- **Частично** — откроется окно выбора классов устройств для блокировки на данной шине.

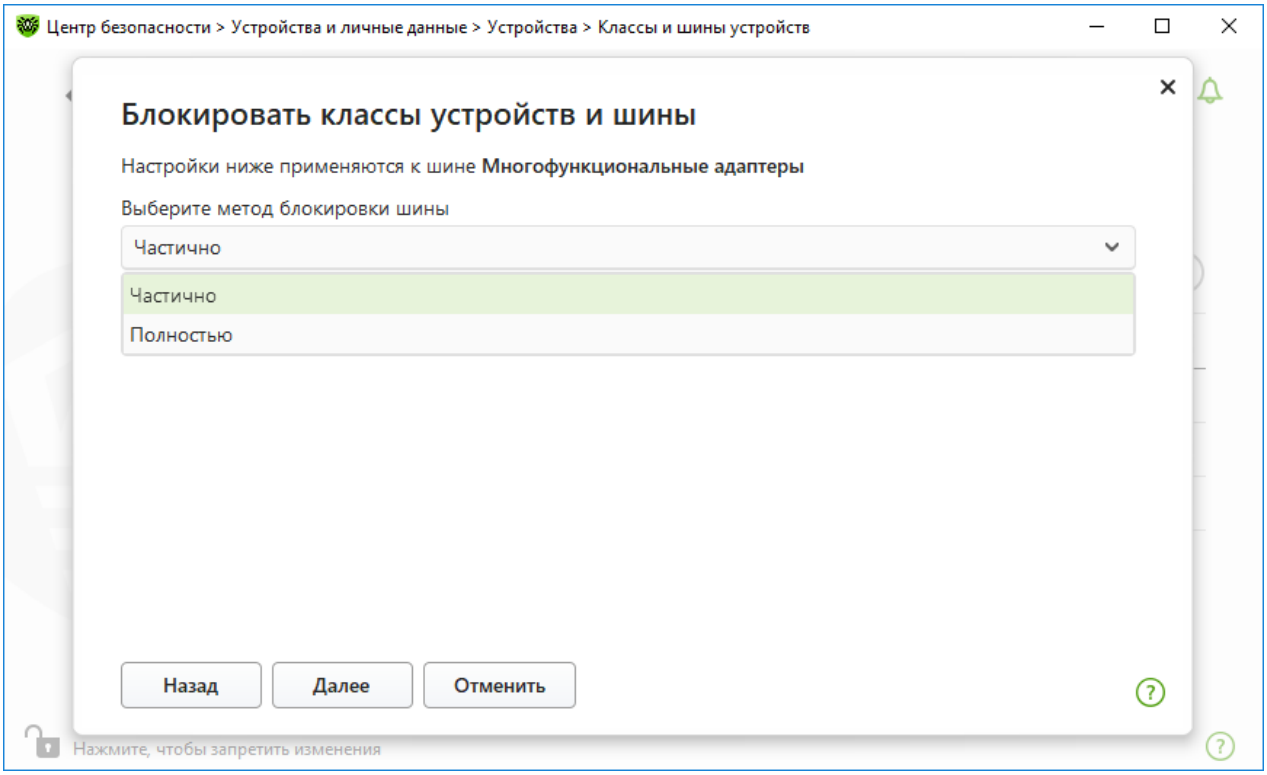

Рисунок 75. Выбор метода блокировки шины

5. Если вы выбрали опцию **Частично**, в открывшемся окне отметьте флажками те классы из списка, которые вы хотите заблокировать. Нажмите **Блокировать**.

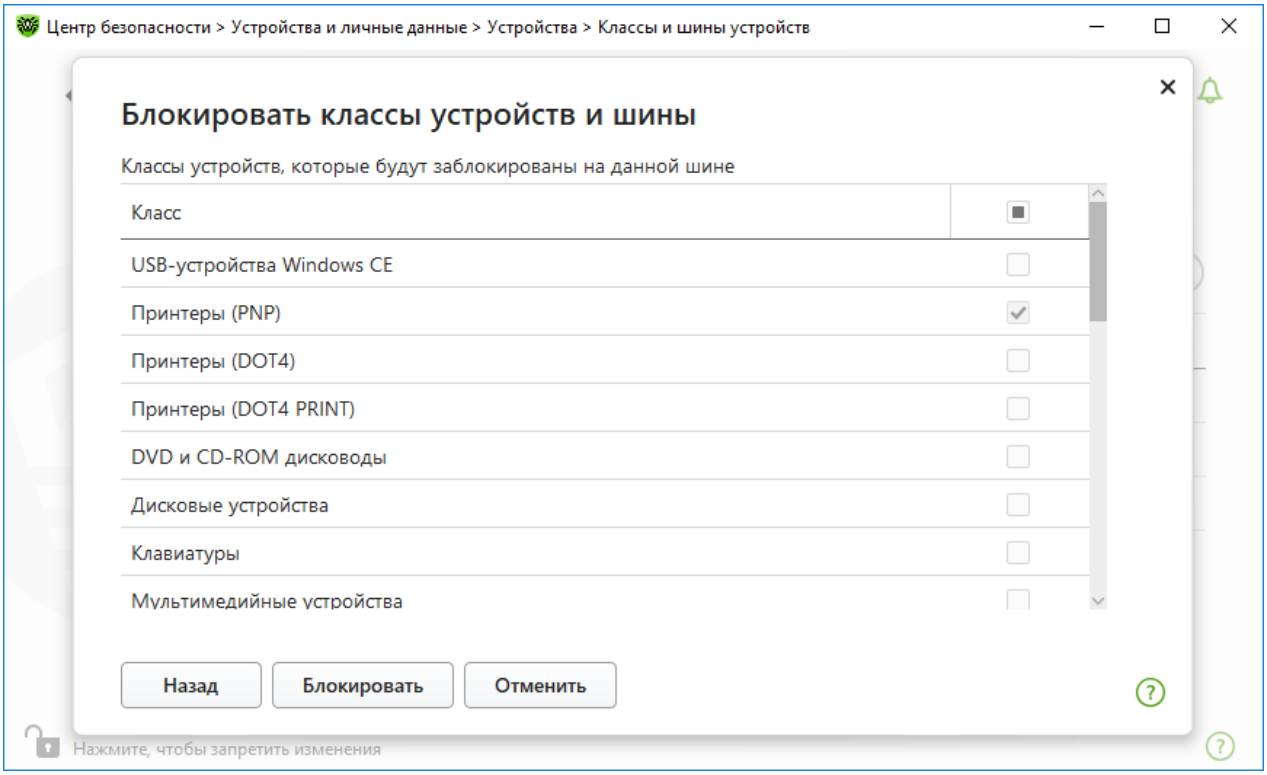

Рисунок 76. Выбор классов устройств на шине

Блокировка класса устройств

1. Чтобы заблокировать один или несколько классов устройств, нажмите кнопку ⊕.
2. Из выпадающего списка выберите объект, который вы хотите заблокировать: **Класс**. Нажмите **Далее**.

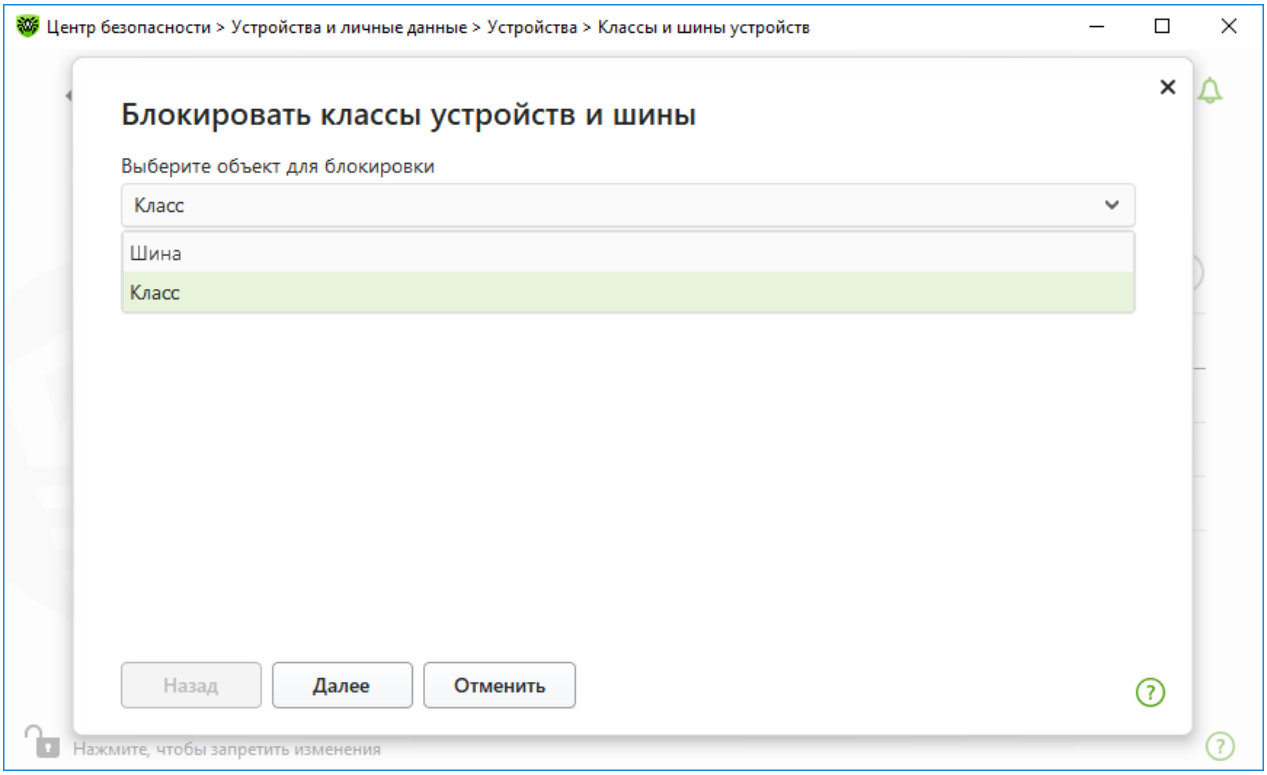

Рисунок 77. Выбор объекта для блокировки

3. Отметьте флажками те классы из списка, которые вы хотите заблокировать. Нажмите **Блокировать**.

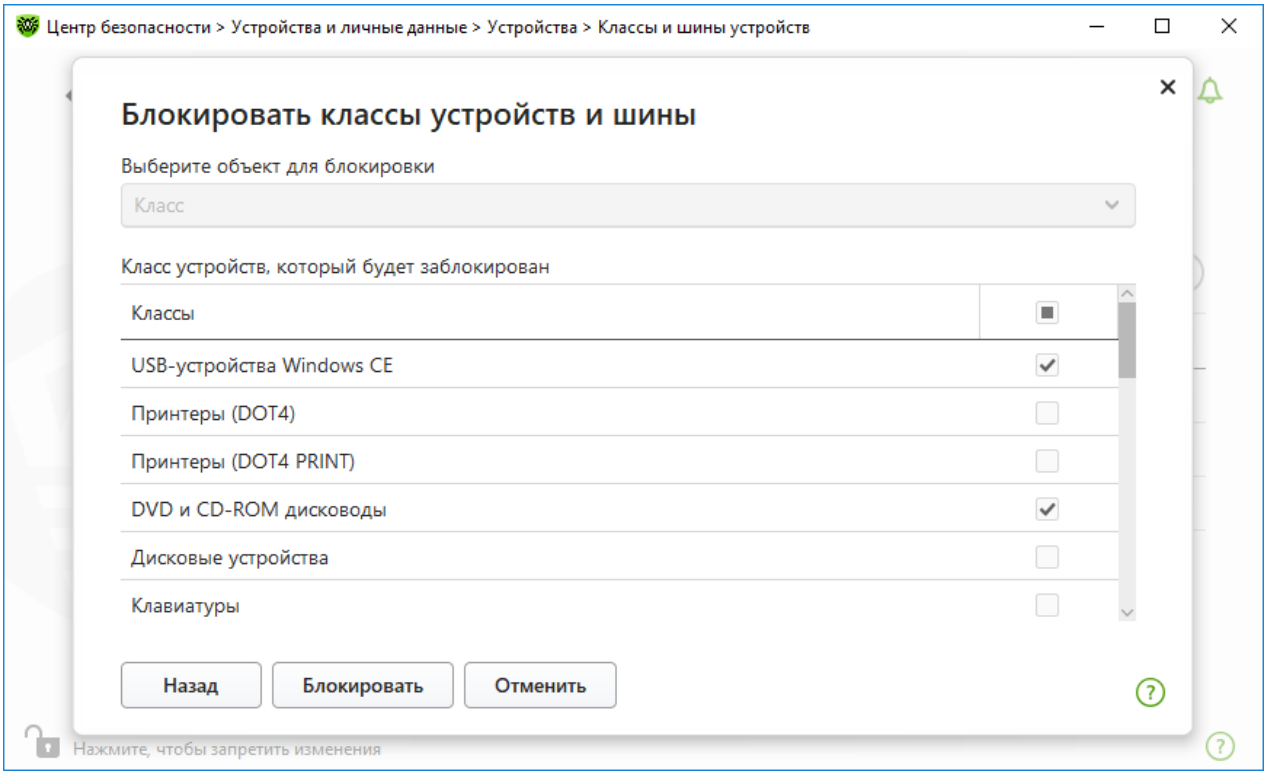

Рисунок 78. Выбор классов устройств

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

При блокировке шины USB клавиатура и мышь вносятся в исключения.

Получение уведомлений

Вы можете настроить вывод уведомлений о блокировке устройств на экран.

11.2. Разрешенные устройства

Чтобы перейти в окно Разрешенные устройства

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Устройства**.
3. В группе настроек **Разрешенные устройства** нажмите ссылку **Изменить**.

Окно **Разрешенные устройства** содержит информацию обо всех устройствах, добавленных в список разрешенных. Эта информация представлена в таблице:

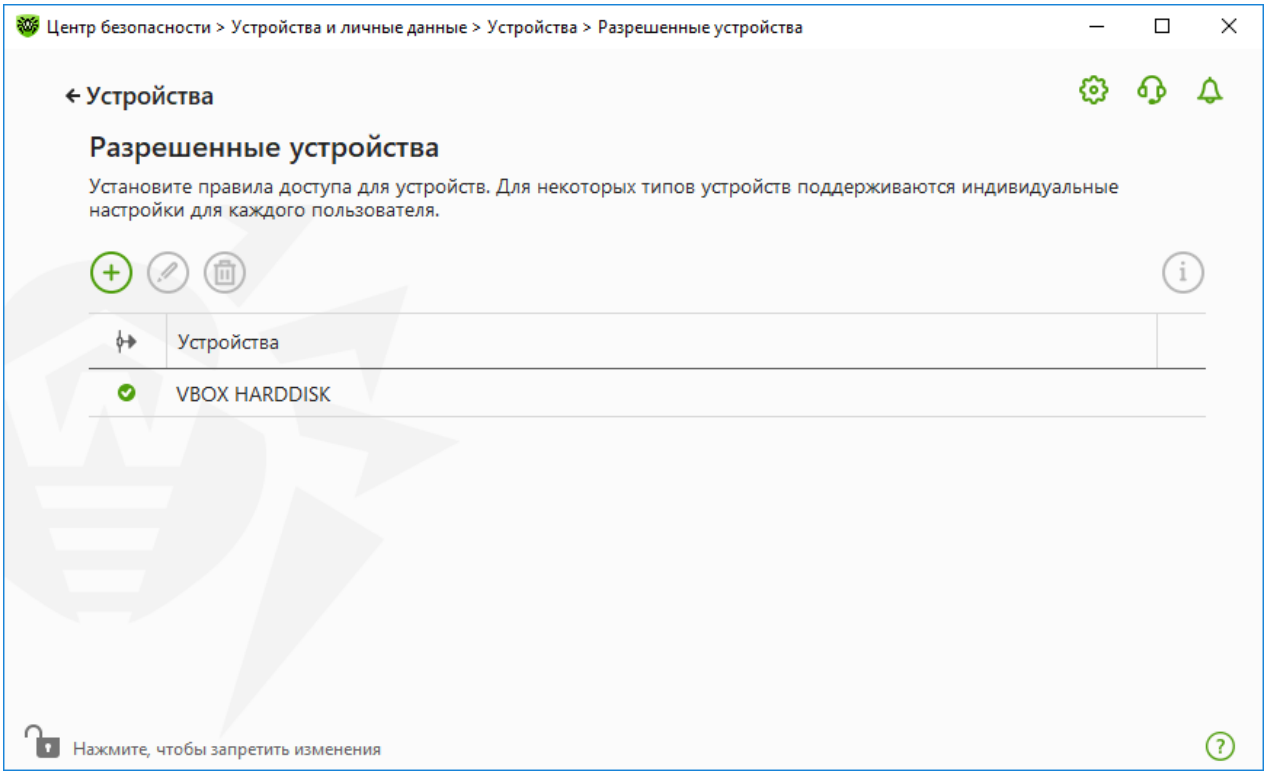

Рисунок 79. Разрешенные устройства

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление набора правил для устройства;
- Кнопка ✎ — редактирование набора правил для устройства;
- Кнопка 🗑 — удаление набора правил для устройства.

Вы можете просмотреть подробную информацию об устройстве, добавленном в список разрешенных. Для этого выберите необходимую строку и нажмите ⓘ.

В столбце ⇹ (**Тип правила**) отображается два типа правил:

- ✔ — задано правило **Разрешать все**.
- ⚙ — задано правило **Только чтение**.

Чтобы добавить устройство в список разрешенных

1. Убедитесь, что устройство подключено к компьютеру.
2. Нажмите кнопку ⊕. В открывшемся окне нажмите кнопку **Обзор** и выберите нужное устройство. Воспользуйтесь фильтром, чтобы в таблице отобразились только подключенные или только отключенные устройства. Нажмите кнопку **ОК**.

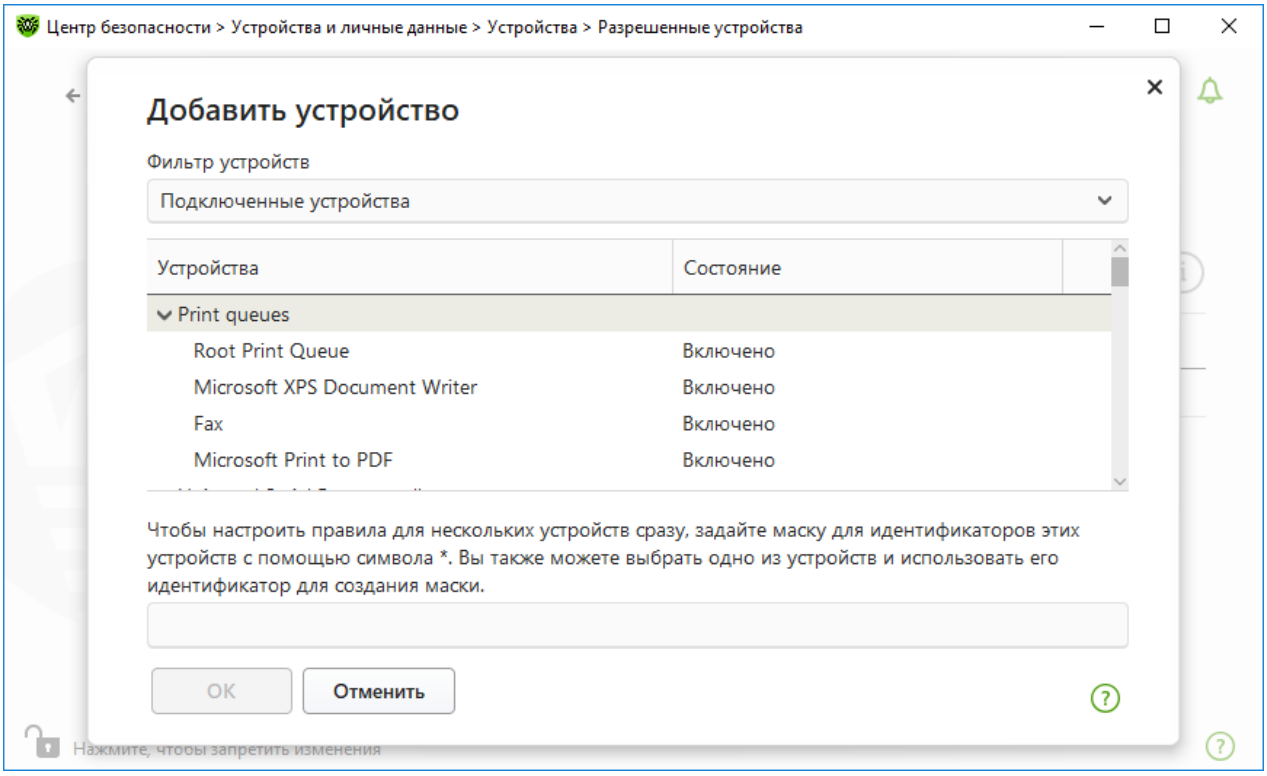

Рисунок 80. Добавление устройства в список разрешенных

3. Для устройств с файловой системой вы можете настроить правила доступа. Для этого в столбце **Правило** выберите один из режимов: **Разрешать все** или **Только чтение**. Чтобы добавить новое правило для конкретного пользователя, нажмите ⊕. Чтобы удалить правило, нажмите 🗑.

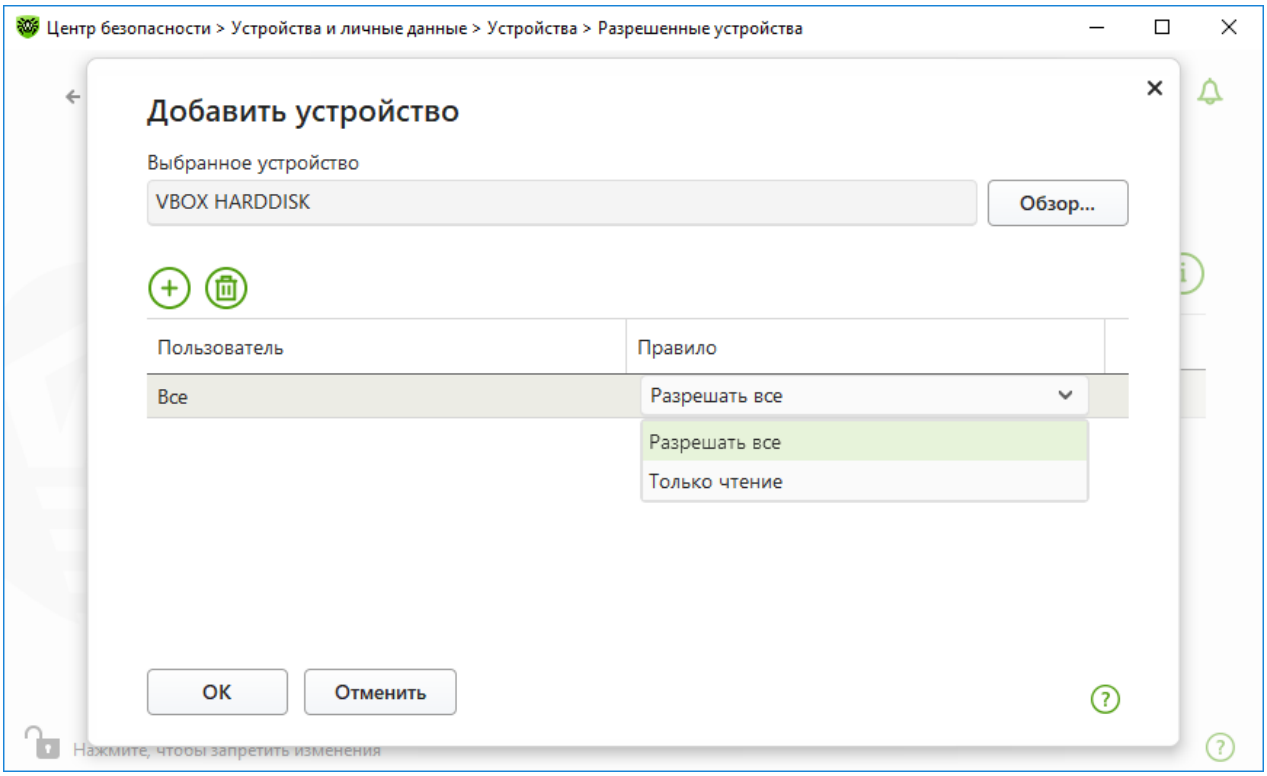

Рисунок 81. Выбор правила для конкретного пользователя

4. Чтобы сохранить изменения, нажмите **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите **Отменить**. Вы вернетесь к списку разрешенных устройств.

12. Офисный контроль

При помощи компонента Офисный контроль вы можете управлять доступом пользователей к сайтам, файлам и папкам, а также контролировать время работы в интернете и за компьютером.

По умолчанию Офисный контроль включен и работает в режиме **Без ограничений**.

Чтобы включить или отключить Офисный контроль

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Офисный контроль**. Откроется окно **Офисный контроль**.

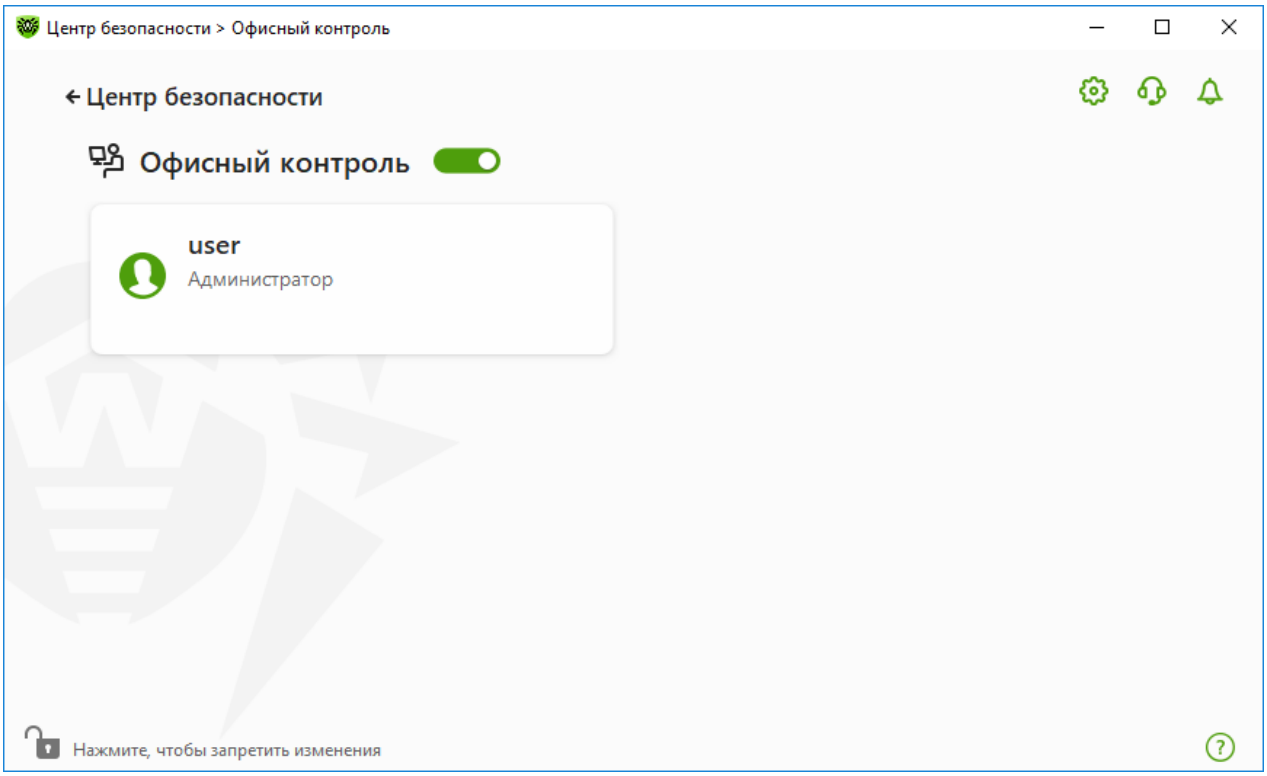

Рисунок 82. Офисный контроль

3. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
4. Включите или отключите Офисный контроль при помощи соответствующего переключателя .

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

Параметры Офисного контроля для отдельного пользователя

Перед настройкой ограничений для пользователя убедитесь, что данный пользователь не обладает правами администратора. В противном случае пользователь сможет изменять параметры компонента Офисный контроль и отключить ограничения доступа.

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

Чтобы перейти к параметрам Офисного контроля

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. В окне Офисного контроля (см. рисунок Офисный контроль) нажмите плитку с именем пользователя, для которого вы хотите настроить Офисный контроль. Откроется окно параметров Офисного контроля для выбранного пользователя.

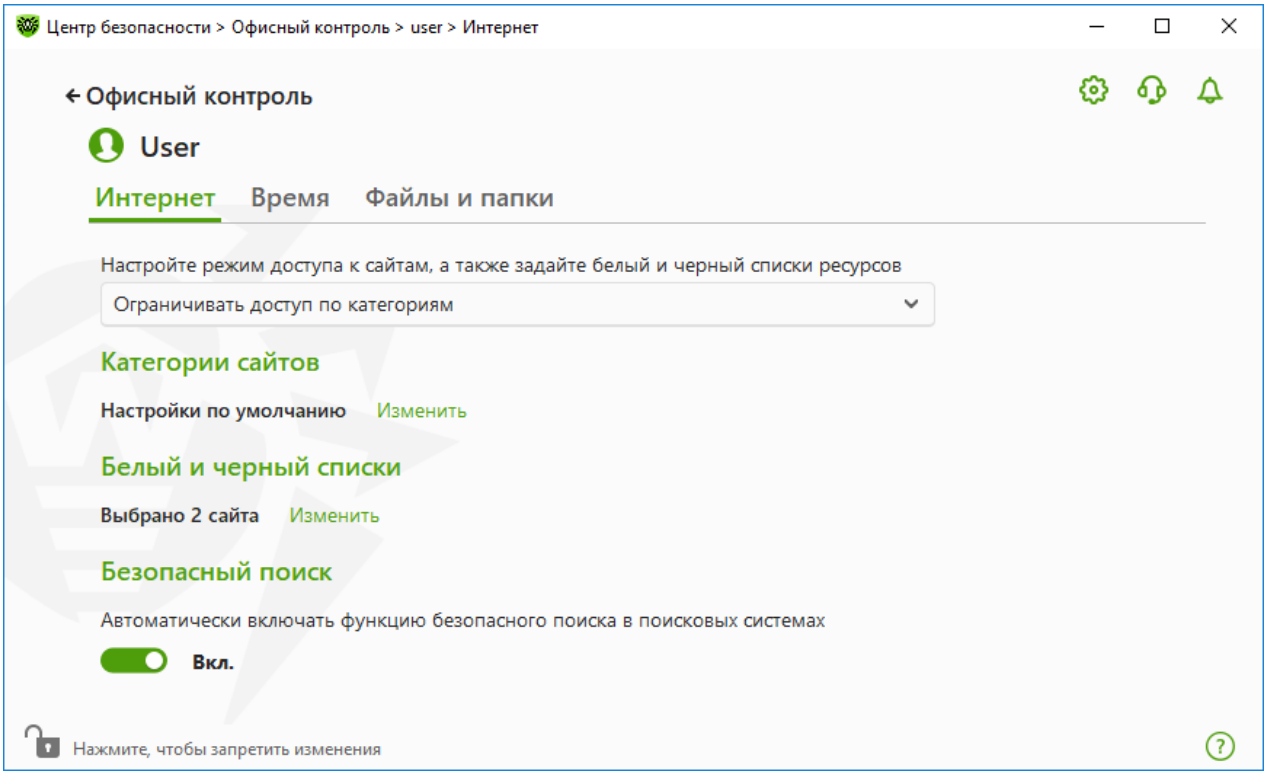

Рисунок 83. Параметры Офисного контроля

3. Выберите нужную вкладку для изменения параметров Офисного контроля:
   - **Интернет** — параметры доступа к интернет-ресурсам. Позволяет оградить пользователей от посещения нежелательных сайтов (сайтов, посвященных насилию, азартным играм и т. п.), а также разрешить посещение указанных сайтов. См. раздел Доступ к интернет-ресурсам.

- **Время** — параметры доступа к компьютеру и интернету. Позволяет ограничить время работы пользователя в определенные часы и дни недели. См. раздел Ограничение по времени.
- **Файлы и папки** — параметры доступа к ресурсам файловой системы. Позволяет ограничить доступ к отдельным файлам и папкам целиком (на локальных дисках и на съемных носителях). См. раздел Доступ к файлам и папкам.

Если пользователь использует учетную запись Windows с правами администратора, ее тип необходимо изменить на стандартный.

Изменение типа учетной записи пользователя

На Windows XP

1. Откройте меню **Пуск**, далее нажмите кнопку **Панель управления** и выберите **Учетные записи пользователей**.
2. Выберите учетную запись, тип которой вы хотите изменить, и нажмите **Изменить тип учетной записи**.
3. Выберите тип учетной записи пользователя — **Ограниченная**.
4. Нажмите **Изменить тип учетной записи**, чтобы сохранить изменения.

На Windows Vista и Windows 7

1. Откройте меню **Пуск**, далее нажмите кнопку **Панель управления** и выберите **Учетные записи пользователей**.
2. Для изменения типа учетной записи нажмите **Управление другой учетной записью**.
3. Выберите учетную запись, тип которой вы хотите изменить, и нажмите **Изменить тип учетной записи**.
4. Выберите тип учетной записи пользователя — **Стандартная**.
5. Нажмите **Изменить тип учетной записи**, чтобы сохранить изменения.

На Windows 8

1. Откройте **Панель управления** и выберите **Учетные записи пользователей и семейная безопасность**.
2. Нажмите кнопку **Управление другой учетной записью**.
3. Выберите учетную запись, тип которой вы хотите изменить, и нажмите **Изменить тип учетной записи**.
4. Выберите тип учетной записи пользователя — **Стандартная**.

5. Нажмите **Изменить тип учетной записи**, чтобы сохранить изменения.

На Windows 8.1

1. Переместите указатель мыши в правый нижний угол экрана, затем вверх и нажмите кнопку **Параметры**, затем выберите **Изменение параметров компьютера**.
2. Выберите элемент **Учетные записи**, затем — **Другие учетные записи**.
3. Выберите учетную запись, тип которой вы хотите изменить, и нажмите **Изменить тип учетной записи**.
4. Выберите тип учетной записи пользователя — **Стандартная**.
5. Нажмите **Ок**.

На Windows 10

1. Нажмите кнопку **Пуск**, далее нажмите кнопку **Параметры**.
2. В открывшемся окне выберите **Учетные записи**.
3. В левой части окна выберите **Другие пользователи**.
4. Нажмите иконку учетной записи, тип которой вы хотите изменить, и нажмите **Изменить тип учетной записи**.
5. Выберите тип учетной записи пользователя — **Стандартная**.
6. Нажмите **Ок**.

На Windows 11

1. Нажмите кнопку **Пуск**, далее нажмите кнопку **Параметры**.
2. В открывшемся окне выберите **Учетные записи**.
3. В центральной части окна выберите **Другие пользователи**.
4. Нажмите иконку учетной записи, тип которой вы хотите изменить, и нажмите **Изменить тип учетной записи**.
5. Выберите тип учетной записи пользователя — **Стандартная**.
6. Нажмите **Ок**.

При наличии на компьютере только одной учетной записи вы не сможете изменить ее тип на стандартный. Более подробную информацию вы можете найти на сайте службы технической поддержки компании Microsoft.

Получение уведомлений

Вы можете настроить вывод уведомлений о действиях компонента Офисный контроль на экран.

12.1. Доступ к интернет-ресурсам

На вкладке **Интернет** вы можете ограничить пользователю посещение нежелательных сайтов (сайтов, посвященных насилию, азартным играм и т. п.), а также разрешить посещение указанных сайтов. По умолчанию для всех пользователей установлен режим **Без ограничений**. Также доступны следующие режимы:

- **Ограничивать доступ по категориям**
- **Разрешать доступ только к сайтам из белого списка**

> Зашифрованный трафик не контролируется. Блокировка ресурсов в браузерах возможна только по имени хоста.

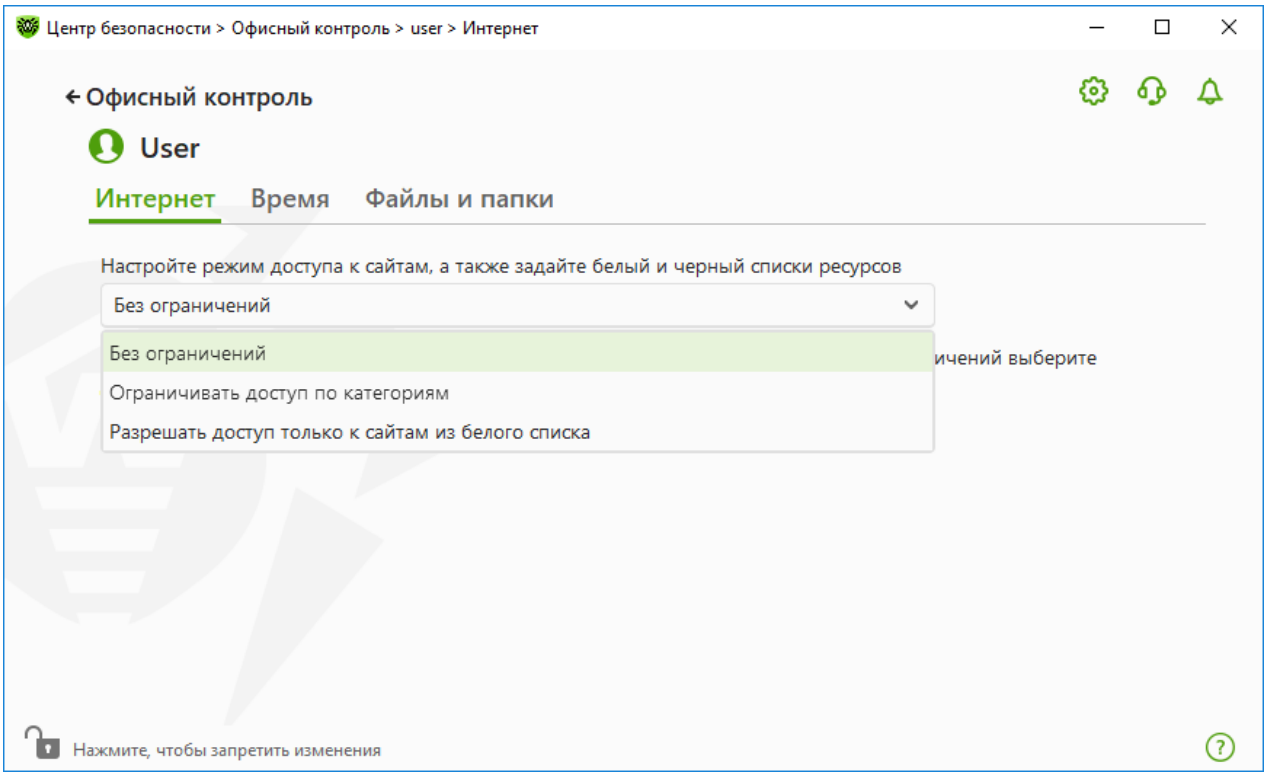

Рисунок 84. Выбор режима работы Офисного контроля

Режим Ограничивать доступ по категориям

В этом режиме вы можете указать категории ресурсов, доступ к которым хотите ограничить. Один и тот же сайт может быть отнесен сразу к нескольким различным категориям. В этом случае Офисный контроль блокирует доступ к сайту, если он попадает хотя бы в одну из запрещенных категорий.

Также в этом режиме вы можете самостоятельно указывать сайты, доступ к которым будет запрещен или разрешен вне зависимости от других ограничений. Для этого используйте белый и черный списки сайтов.

Перед включением ограничений по категориям необходимо очистить кеш браузера.

Чтобы запретить или разрешить доступ к веб-ресурсам требуемой категории

1. В группе настроек **Категории сайтов** нажмите ссылку **Изменить**. Откроется окно параметров блокируемых категорий.

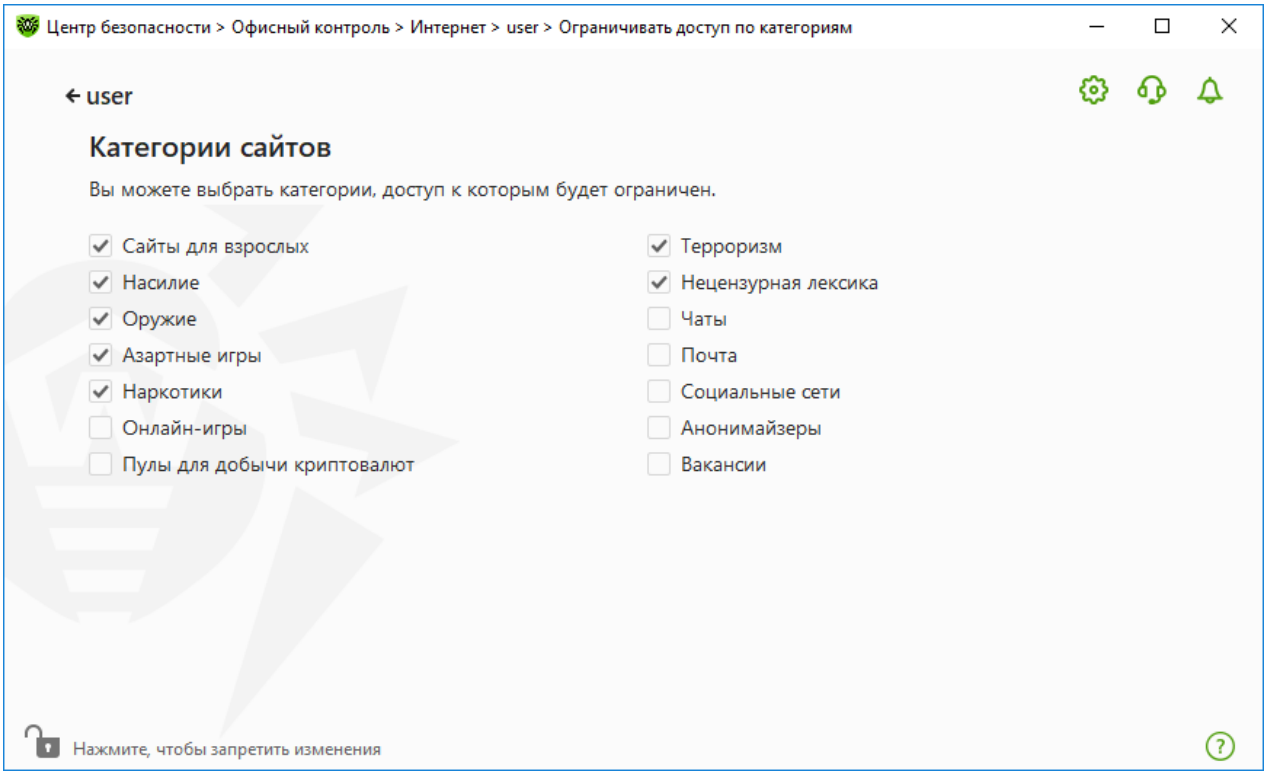

Рисунок 85. Категории блокируемых сайтов

2. Установите или снимите флажок, чтобы запретить или разрешить доступ к веб-ресурсам требуемой категории.

Категории интернет-ресурсов

Категория	Описание
Сайты для взрослых	Сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.
Насилие	Сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
Оружие	Сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
Азартные игры	Сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.
Наркотики	Сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
Онлайн-игры	Сайты, на которых размещены игры, использующие постоянное соединение с интернетом.
Терроризм	Сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
Нецензурная лексика	Сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
Чаты	Сайты для обмена сообщениями в режиме реального времени.
Электронная почта	Сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика.
Социальные сети	Социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств.
Анонимайзеры	Сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам.
Пулы для добычи криптовалют	Сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют.
Вакансии	Сайты, которые используются для размещения вакансий и поиска работы.

Режим Разрешать доступ только к сайтам из белого списка

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

При выборе режима **Разрешать доступ только к сайтам из белого списка** такие сайты могут отображаться некорректно. Баннеры и другие элементы сайта, интегрированные с внешними ресурсами, отображаться не будут.

Белый и черный списки сайтов

Вы можете задать белый и черный список сайтов, доступ к которым разрешается или блокируется вне зависимости от остальных параметров Офисного контроля.

Перед добавлением сайта в черный или белый список необходимо очистить кеш браузера, если сайт ранее открывался в этом браузере.

Настройка белого и черного списков сайтов Офисного контроля

1. В группе настроек **Белый и черный списки** нажмите ссылку **Изменить**. Откроется окно настройки белого и черного списков.

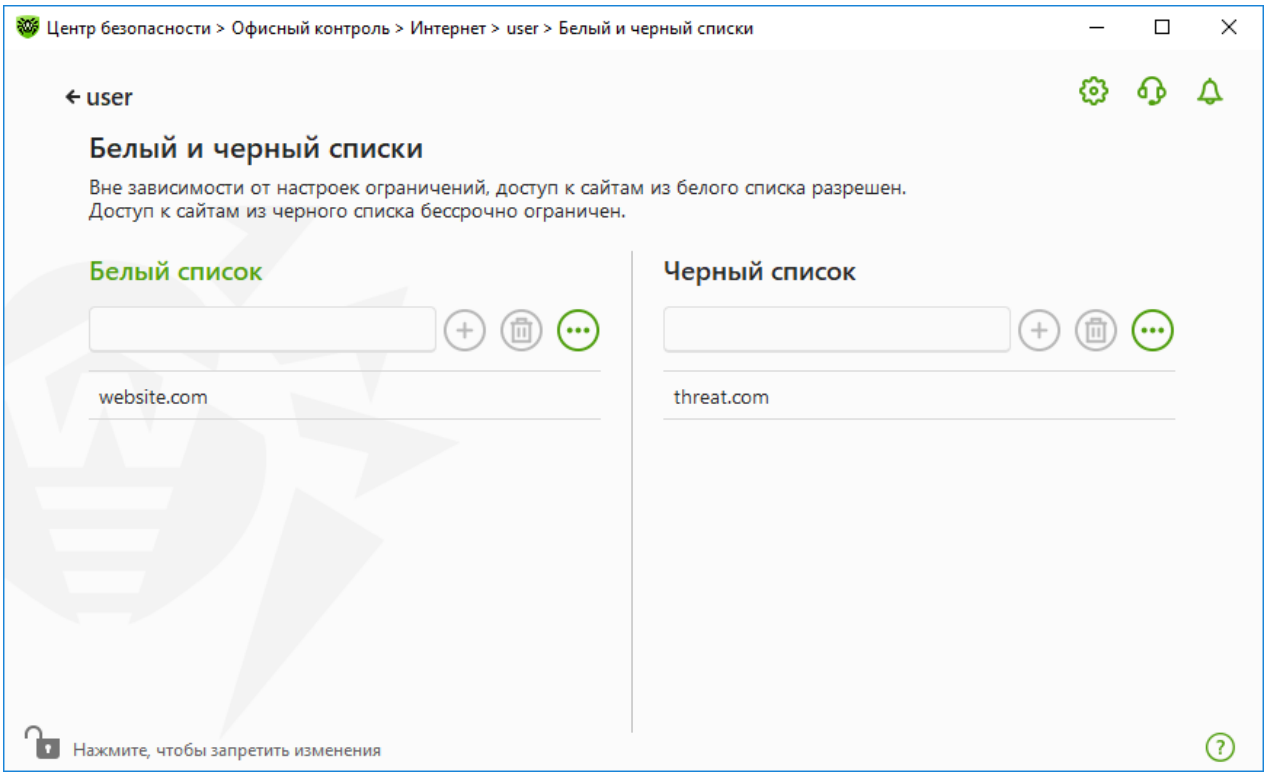

Рисунок 86. Настройка белого и черного списков Офисного контроля

2. Внесите объект в поле **Белый список**, чтобы разрешить доступ к веб-ресурсу. Внесите объект в поле **Черный список**, чтобы запретить доступ к веб-ресурсу. Внесение объекта в белый или черный список возможно в формате маски, домена или адреса (на уровне URL):
   - Чтобы добавить в список определенные сайты, введите определяющую их маску в поле ввода. Допускается использование букв, цифр, символов «:», «/», «-», «?»

и «*». Маски добавляются в формате: `mask://...`

Маска задает общую часть имени объекта, при этом:

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

Примеры:

- `mask://*.ru/` — будут обрабатываться все сайты в зоне `.ru`;
- `mask://mail` — будут обрабатываться все сайты, в которых содержится слово «mail»;
- `mask://ma?l.ru/` — будут обрабатываться все сайты, в именах которых содержатся подстроки «ma» и «l.ru» с любым символом между ними.

При использовании символа «?» в начале маски учитывается только минимальное количество символов перед введенной подстрокой. Например, если задать маску `mask://???.ru`, будут обрабатываться такие адреса как `pro.ru`, `example.ru`, `example.com/test.run`.

- Чтобы добавить в список определенный домен, укажите имя домена с символом «.» или без него в конце адреса. Допускается использование букв, цифр и символа «/».

  Примеры:

  - `example.com` — будет обрабатываться сам `example.com`, а также его поддомены `*example.com`;
  - `example.` — будут обрабатываться поддомены `*example.com`, но не сам `example.com`;
  - `ru.` — будут обрабатываться все поддомены зоны `.ru` (например, `example.ru` или `www.test.ru`).
- Чтобы добавить в список те сайты, в адресе которых содержится определенный текст, введите в поле этот текст. Допускается использование букв, цифр, символов «/» и «-».

  Примеры:

  - `example.com/test` — будут обрабатываться такие адреса как `example.com/test11`, `template.example.com/test22` и т. п.;
  - `example` — будут обрабатываться такие адреса как `example.com`, `example.test.com`, `test.com/example`, `test.example222.com` и т. п.

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

При вводе маски, домена и адреса не учитывается регистр символов. Это означает, что

записи `example.com` и `ExAMple.COM` будут обрабатываться одинаково.

3. Нажмите кнопку ⊕, чтобы добавить адрес в список.
4. Чтобы удалить адрес из списка, выберите его в списке и нажмите кнопку 🗑.
5. При нажатии кнопки ⋯ доступны следующие действия:
   - **Изменить** — эта опция позволяет отредактировать выбранный из списка адрес.
   - **Экспорт** — эта опция позволяет сохранить созданный список адресов, чтобы использовать его на другом компьютере, на котором установлен Dr.Web.
   - **Импорт** — эта опция позволяет использовать список адресов, созданный на другом компьютере.
   - **Очистить все** — эта опция позволяет удалить все объекты из списка адресов.
6. При необходимости повторите шаги 2 и 3 для добавления других ресурсов.

Безопасный поиск

Опция **Безопасный поиск** влияет на выдачу результатов поисковых систем. Эта функция позволяет исключить нежелательные ресурсы из результатов поиска, используя средства поисковых систем.

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

12.2. Ограничение времени работы за компьютером и в интернете

На вкладке **Время** вы можете ограничить время работы пользователей за компьютером и в интернете. По умолчанию для всех пользователей установлен режим **Без ограничений**.

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

⚠ При включении ограничений времени работы за компьютером или в интернете, автоматически включается опция **Запрещать изменение даты и времени системы** в окне Самозащита основных настроек.

Таблица ограничения времени работы за компьютером и в интернете

Таблица доступна в режиме Офисного контроля **Без ограничений**. При внесении изменений в таблицу профиль **Без ограничений** будет автоматически заменен на **Пользовательский**.

С помощью таблицы можно указать дни недели и часы, когда пользователь может работать за компьютером, а также в интернете. При наступлении времени ограничения доступа к компьютеру будет произведен автоматический выход из системы. Пока действуют ограничения для определенной учетной записи, войти в эту учетную запись нельзя. Во время действия ограничений на работу в интернете весь интернет-контент перестанет загружаться.

Время, оставшееся до включения ограничений доступа, можно посмотреть в меню Dr.Web, нажав на плитку **Ограничение времени**.

Чтобы ограничить время работы в режиме таблицы

1. Выберите дни недели и часы, когда требуется запретить пользователю выход в интернет, и выделите соответствующие временные ячейки синим цветом:
   - чтобы выделить одну ячейку, нажмите на нее один раз левой кнопкой мыши;
   - чтобы одновременно выделить несколько расположенных рядом ячеек, один раз нажмите левой кнопкой мыши на первую ячейку и, удерживая кнопку нажатой, выделите весь необходимый период.
   - чтобы удалить все ячейки, нажмите правой кнопкой мыши в любом месте внутри таблицы и выберите **Очистить все**.
2. Выберите дни недели и часы, когда требуется запретить пользователю работу за компьютером, и выделите соответствующие временные ячейки красным цветом:
   - чтобы выделить одну ячейку, дважды нажмите на нее левой кнопкой мыши;
   - чтобы одновременно выделить несколько расположенных рядом ячеек, дважды нажмите левой кнопкой мыши на первую ячейку и, удерживая кнопку нажатой, выделите весь необходимый период.
   - чтобы удалить все ячейки, нажмите правой кнопкой мыши в любом месте внутри таблицы и выберите **Очистить все**.

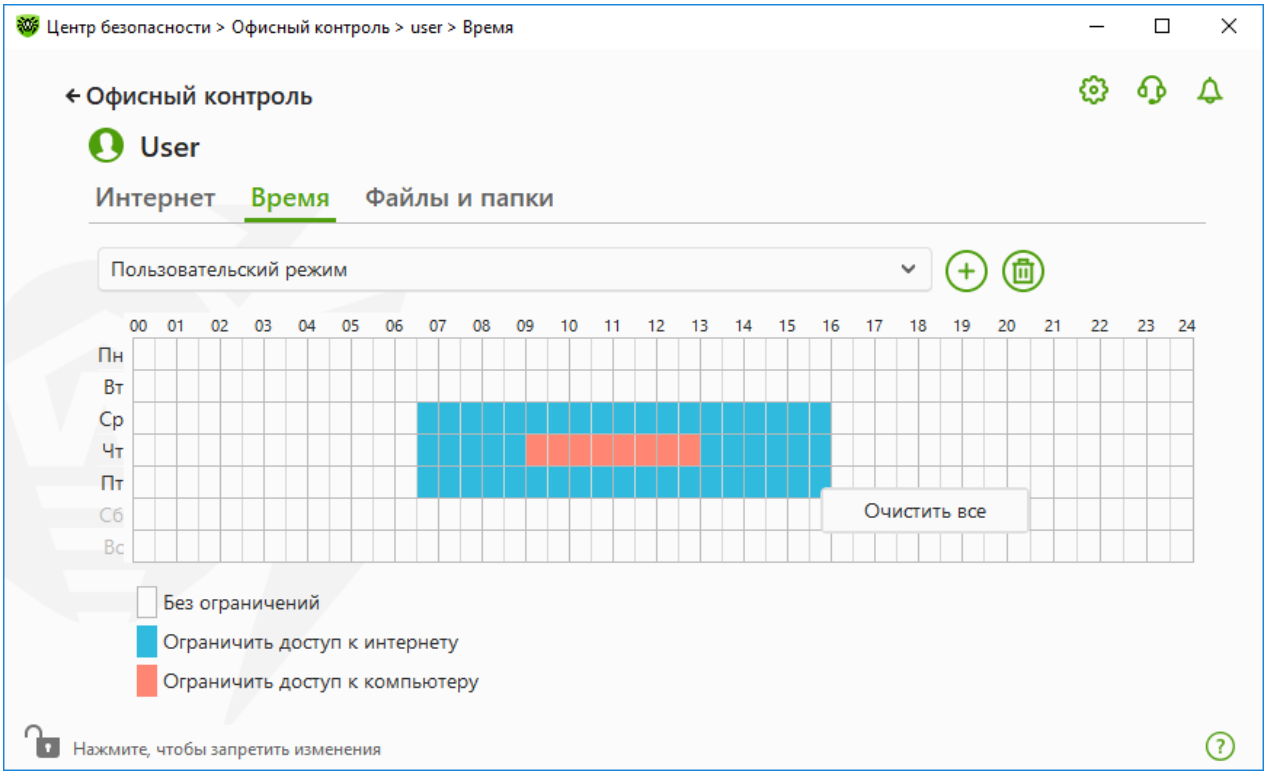

Рисунок 87. Таблица времени работы за компьютером и в интернете

Вы можете также создавать разные настройки для одного пользователя, сохраняя их в профили. Данная опция будет удобна, если вам понадобится периодически менять настройки на другие предопределенные значения.

Добавление и удаление профиля настроек

- Чтобы создать профиль настроек, нажмите кнопку ⊕. При этом в профиле сохранятся настоящие настройки таблицы. В дальнейшем при изменении настроек профиля они будут автоматически сохраняться.
- Чтобы удалить профиль настроек, нажмите кнопку 🗑.

12.3. Доступ к файлам и папкам

На вкладке **Файлы и папки** вы можете ограничить пользователям доступ к файлам и папкам. По умолчанию ограничения на доступ к файлам и папкам отсутствуют.

Чтобы включить или отключить ограничение доступа к файлам и папкам для пользователя, используйте переключатель ⬤.

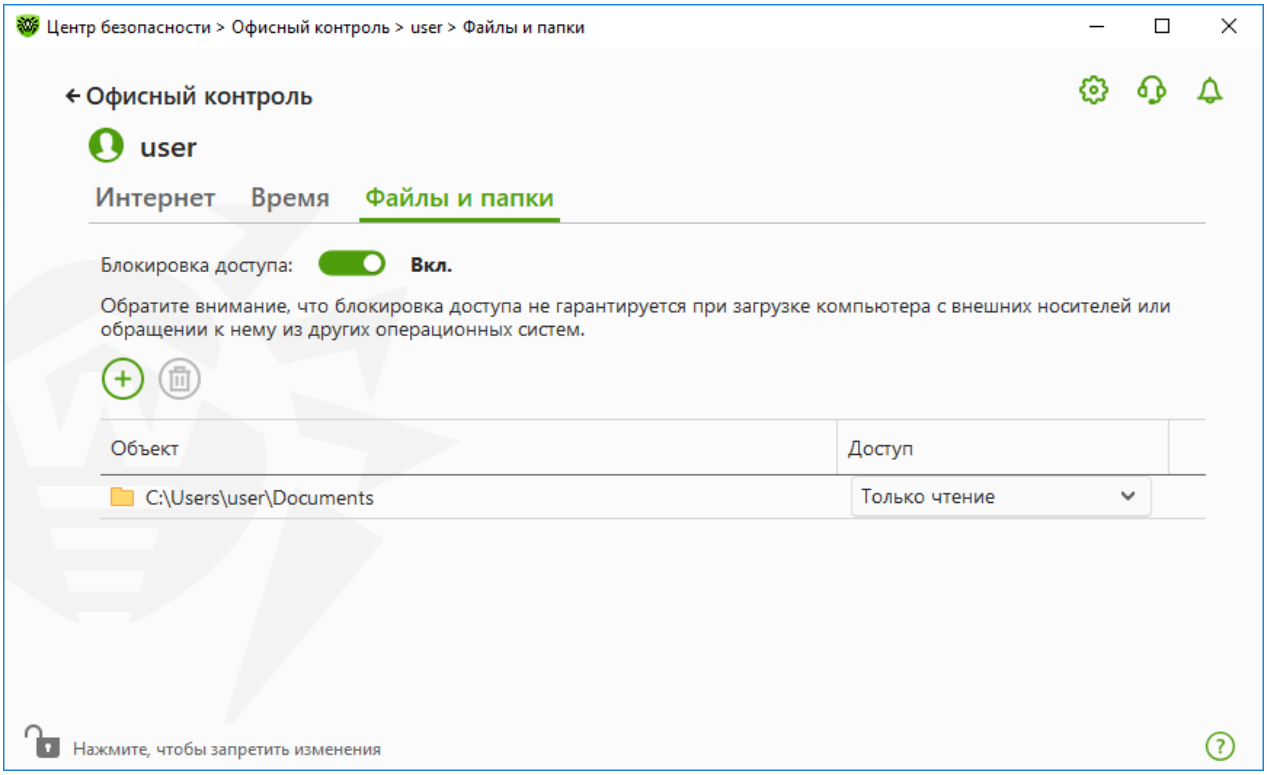

Рисунок 88. Управление доступом к файлам и папкам

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

Не допускается блокировка доступа к системным папкам, поскольку это может привести к критическим ошибкам в работе системы.

Чтобы ограничить доступ к файлам и папкам

1. Включите блокировку доступа к файлам и папкам, используя переключатель .
2. Чтобы добавить объект в список, нажмите кнопку и выберите нужный файл или папку.
3. Выберите режим доступа для добавленного объекта:
   - **Заблокирован**, чтобы полностью заблокировать доступ к выбранному объекту.
   - **Только чтение** (выбрано по умолчанию), чтобы разрешить чтение выбранного объекта (например, просмотр документа, изображения, запуск исполняемого файла), при этом выбранный объект нельзя будет переместить, удалить, а также изменить его содержимое.

Чтобы удалить объект, выберите его в списке и нажмите кнопку .

13. 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. Нажмите плитку **Менеджер карантина**.

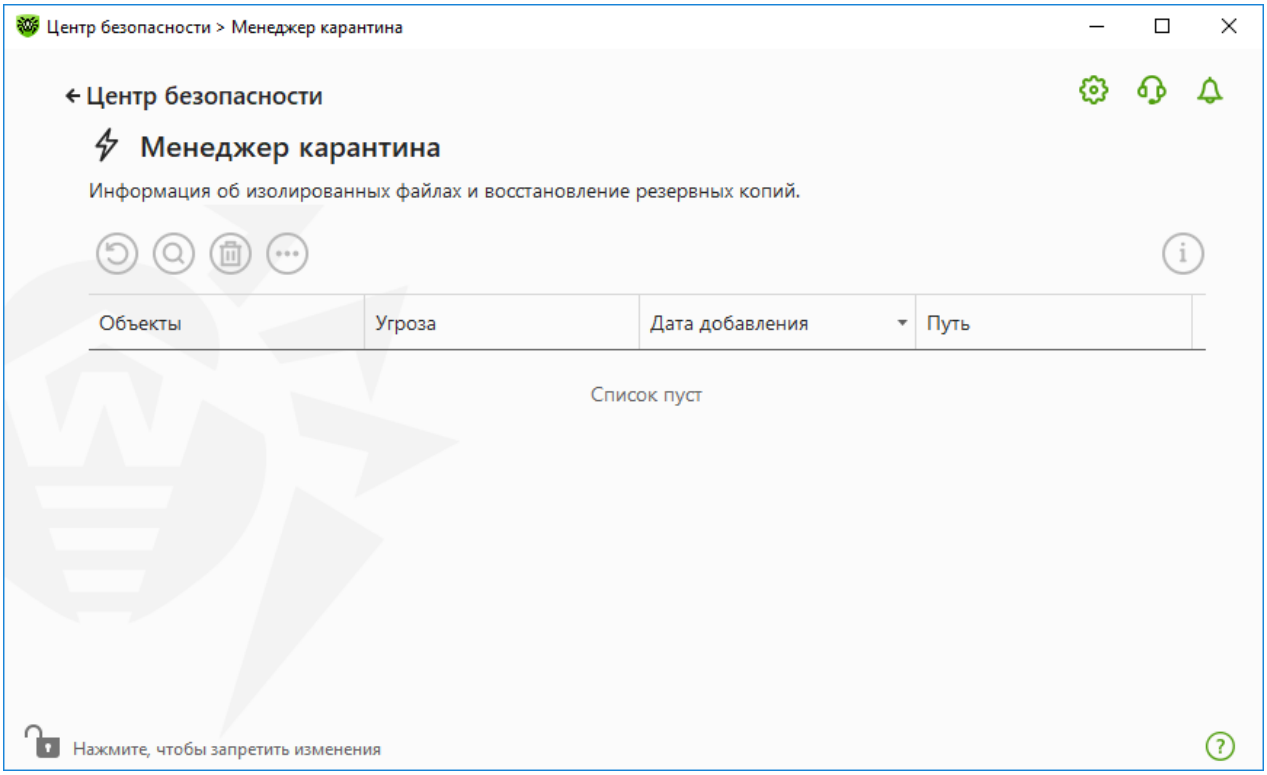

Рисунок 89. Объекты в карантине

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**.

Вы можете просмотреть подробную информацию об объекте, добавленном в карантин. Для этого выберите необходимую строку и нажмите  .

Дополнительно

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

14. Исключения

В данной группе настроек вы можете настроить исключения из проверок компонентами SpIDer Guard, SpIDer Gate, SpIDer Mail и Сканер, а также добавить адреса отправителей в черный или белый списки, чтобы письма от них не проверялись на спам.

Чтобы перейти в группу настроек Исключения

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

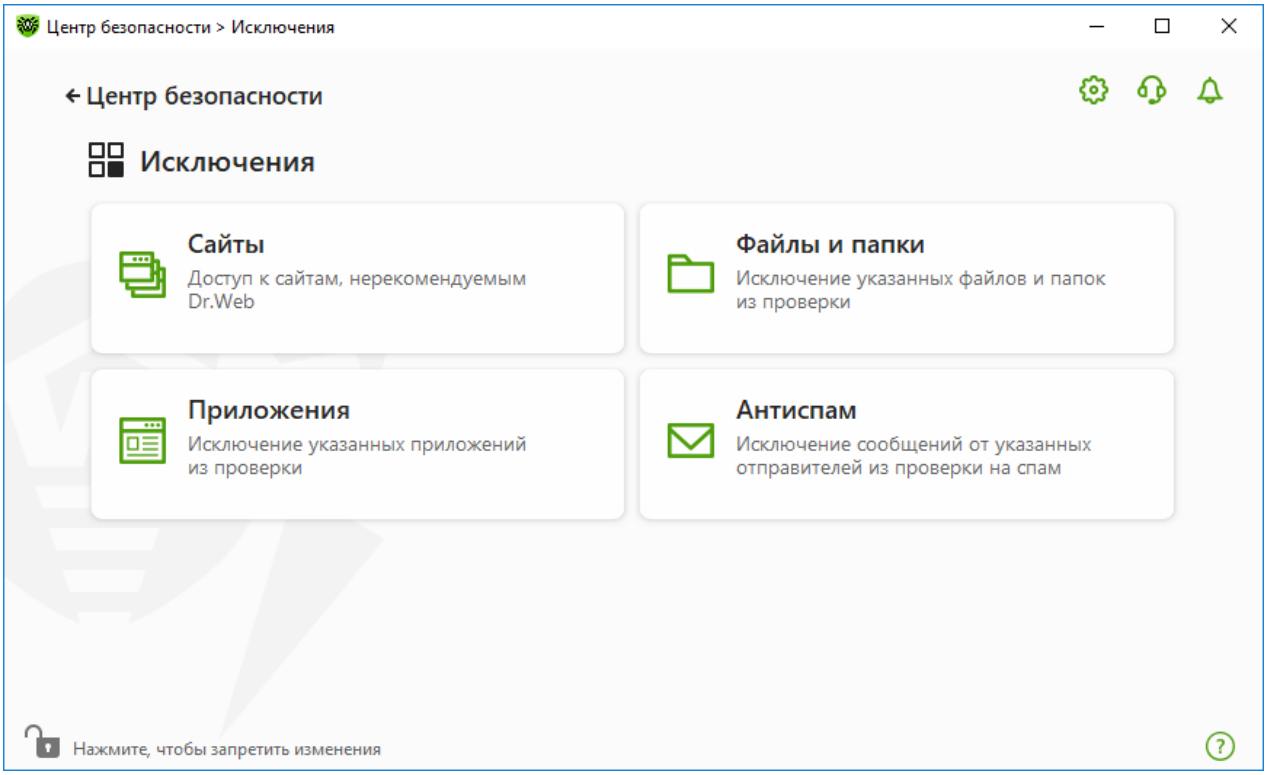

Рисунок 90. Окно Исключения

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.

> Обратите внимание, что изменения в этой группе настроек могут быть заблокированы со стороны администратора вашей антивирусной сети.

В этом разделе:

- Сайты — параметры доступа к сайтам, которые не рекомендуются к посещению компанией «Доктор Веб».
- Файлы и папки — исключение определенных файлов и папок из проверки компонентами SpIDer Guard и Сканер.
- Приложения — исключение определенных процессов из проверки компонентами SpIDer Guard, SpIDer Gate и SpIDer Mail.
- Антиспам — параметры проверки писем на спам компонентом SpIDer Mail.

14.1. Сайты

Вы можете задать список сайтов, доступ к которым будет разрешен вне зависимости от параметров проверки HTTP-трафика компонентом SpIDer Gate. Если в параметрах SpIDer Gate включена опция **Блокировать нерекомендуемые сайты**, вы можете разрешить доступ к определенным сайтам, добавив их в список исключений. Доступ к сайтам из списка будет разрешен, однако антивирусная проверка этих сайтов будет сохранена.

Чтобы настроить список сайтов, доступ к которым будет разрешен

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

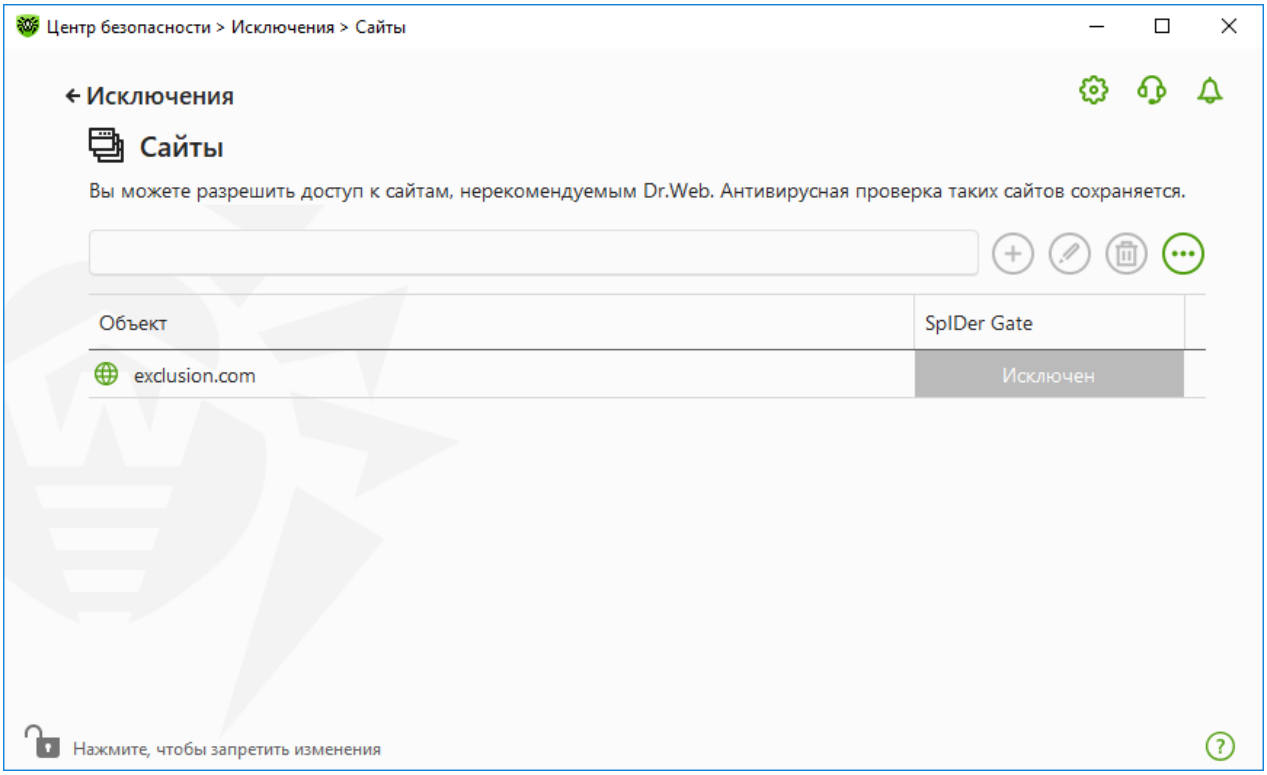

Рисунок 91. Список исключаемых сайтов

По умолчанию список пуст. Если адрес сайта добавлен в список исключений, то доступ к нему будет предоставляться вне зависимости от других параметров SpIDer Gate. Обратите внимание, если такой сайт добавлен одновременно и в черный список модуля Офисный контроль, и в исключения, доступ к нему будет заблокирован.

Чтобы добавить доменные адреса в список исключений

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

     Маска задает общую часть имени объекта, при этом:

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

     Примеры:

     - `mask://*.ru/` — будут открываться все сайты в зоне `.ru`;
     - `mask://mail` — будут открываться все сайты, в которых содержится слово «mail»;
     - `mask://ma?l.ru/` — будут открываться все сайты, в именах которых содержатся подстроки «ma» и «l.ru» с любым символом между ними.

     

     При использовании символа «?» в начале маски учитывается только минимальное количество символов перед введенной подстрокой. Например, если задать маску `mask://???.ru`, будут открываться такие адреса как `pro.ru`, `example.ru`, `example.com/test.run`.

     Чтобы учитывалось указанное количество символов перед введенной подстрокой, используйте символ «/» в конце маски. Например, если задать маску `mask://???.ru/`, будут открываться адреса с тремя символами перед «.ru/».

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

2. Нажмите кнопку ⊕ или кнопку ENTER на клавиатуре. Указанный адрес появится в списке.
3. При необходимости повторите шаги 1 и 2 для добавления других адресов.

Работа с объектами в списке

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление адреса сайта в список исключений. Становится доступна, если в текстовое поле введено какое-либо значение.
- Кнопка ✎ — редактирование выбранного адреса сайта в списке исключений.
- Кнопка 🗑 — удаление выбранного адреса сайта из списка исключений.
- 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.

Действия удаления или редактирования объекта доступны также в контекстном меню при нажатии правой кнопкой мыши на один или несколько выбранных объектов.

14.2. 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. Вы также можете исключить из проверки Сканером файлы, находящиеся внутри архивов.

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**.

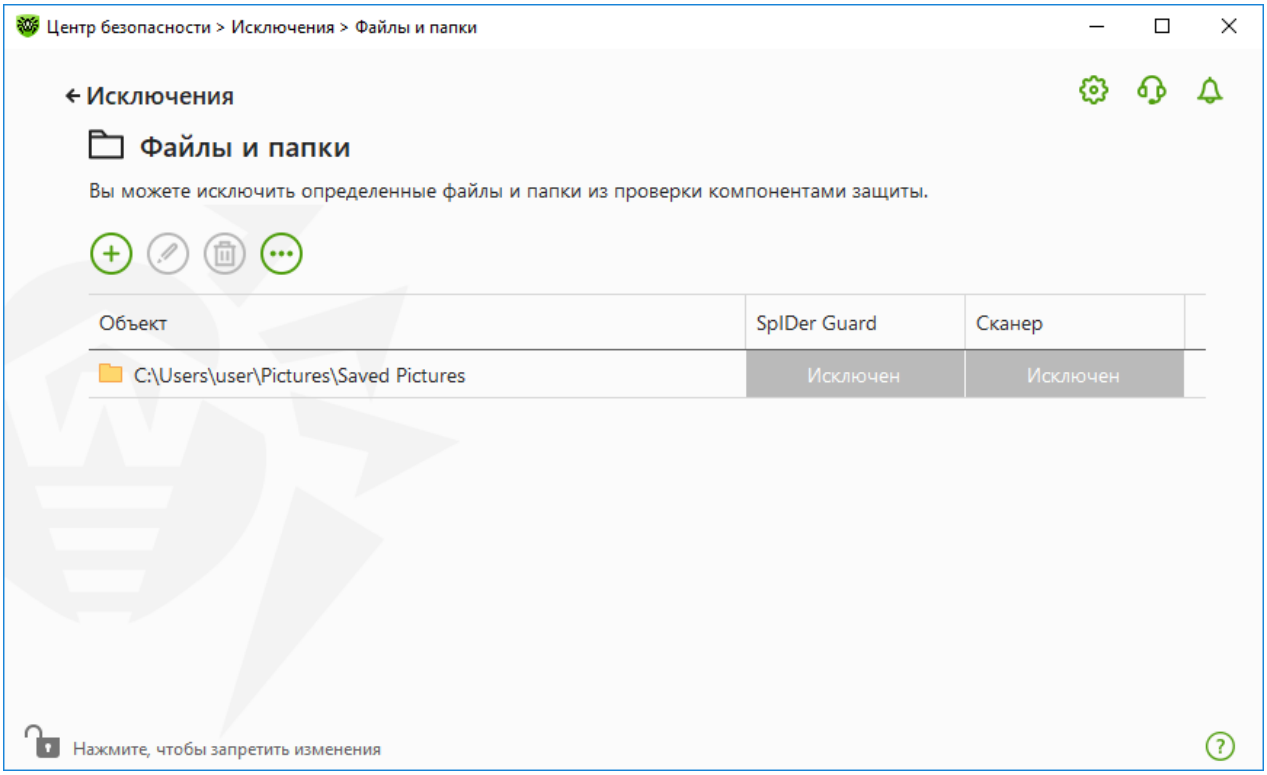

Рисунок 92. Список исключаемых файлов и папок

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 файлы в папке `C:\folder` и всех подпапках на любом уровне вложенности.
  - `C:\folder\*` — исключает из проверки файлы в папке `C:\folder`. В подпапках файлы будут проверяться.
  - `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.

- чтобы исключить из проверки Сканером файлы определенного вида внутри архивов, введите маску их пути или расширения в поле ввода. При этом необходимо использовать символ «/». Например:

  - `C:\folder.zip/file.*` — исключает из проверки все файлы с именем `file` в архиве `C:\folder.zip`.
  - `*/file.txt` — исключает из проверки все файлы `file.txt` во всех архивах.

2. В окне добавления файла или папки укажите, какие компоненты не должны проводить проверку выбранного объекта.
3. Нажмите кнопку **ОК**. 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.

14.3. Приложения

Вы можете задать список программ и процессов, активность которых исключается из проверки файловым монитором SpIDer Guard, интернет-монитором SpIDer Gate 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**.

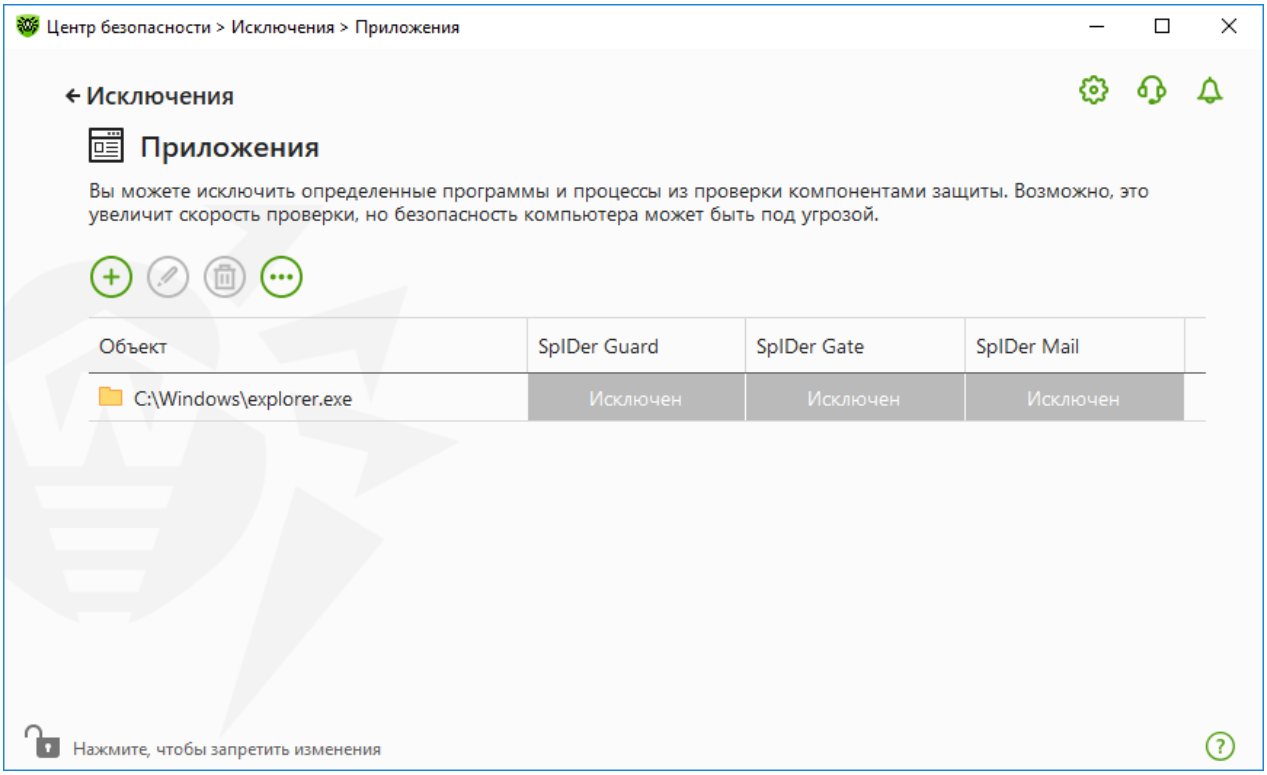

Рисунок 93. Список исключаемых приложений

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 или использовать переменные среды. Например:
     - `C:\Program Files\folder\example.exe`
     - `%PROGRAMFILES%\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 при необходимости 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.

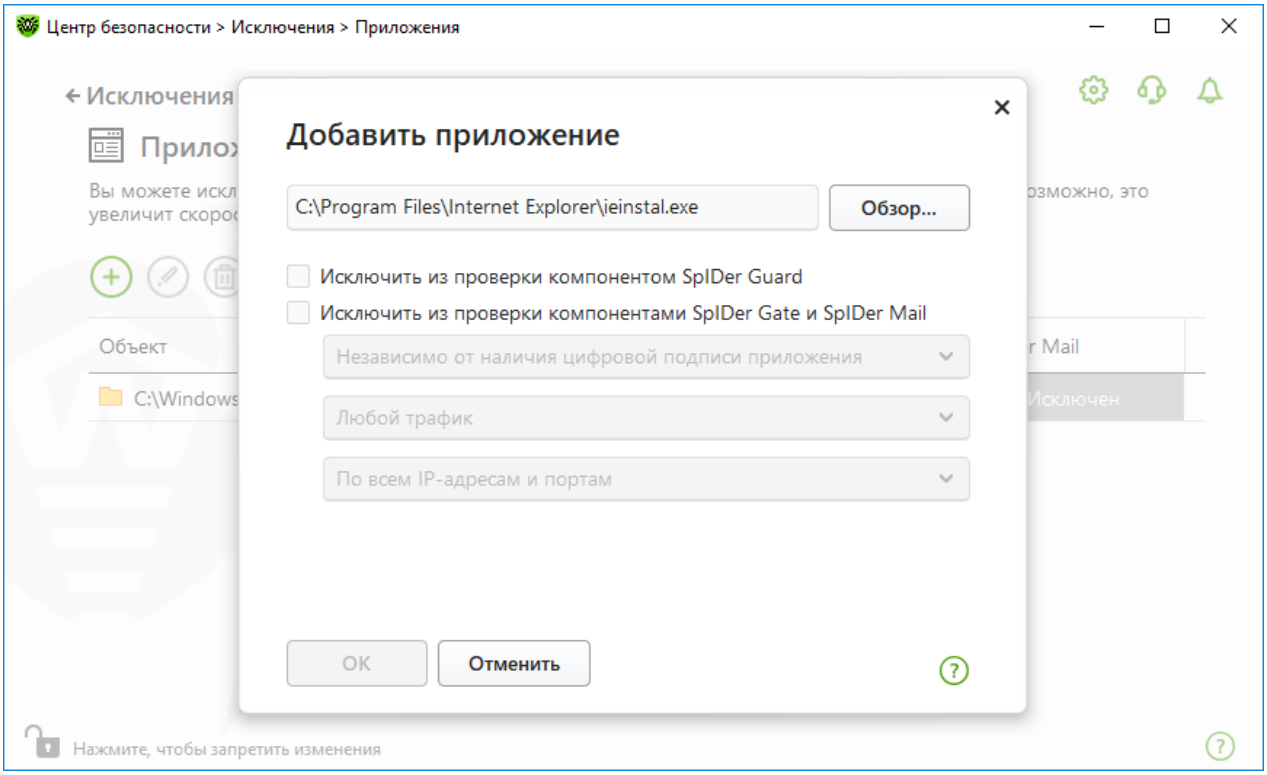

Рисунок 94. Добавление приложений в исключения

3. Для объектов, исключаемых из проверки компонентами SpIDer Gate и 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 **ОК**. 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.

14.4. Антиспам

Вы можете задать списки отправителей, письма которых будут исключены из проверки на спам. Антивирусная проверка таких писем сохраняется.

Чтобы настроить черный и белый списки адресов

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.

2. В открывшемся окне нажмите плитку **Исключения**.
3. Нажмите плитку **Антиспам**.

Реакция компонента SpIDer Mail на письма отправителей из черного и белого списков:

- Если адрес отправителя добавлен в белый список, то письмо считается безопасным и не подвергается анализу на содержание спама.
- Если адрес отправителя добавлен в черный список, то письму без дополнительного анализа присваивается статус спама.

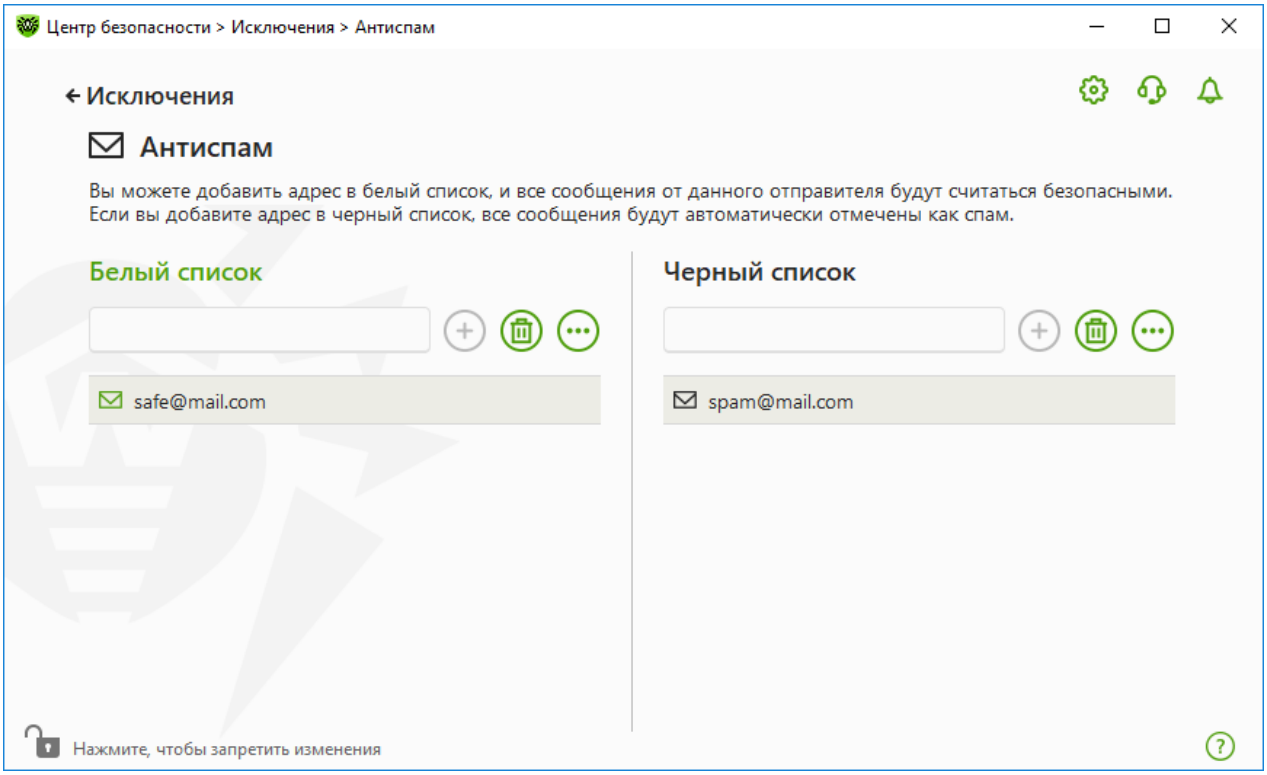

Рисунок 95. Черный и белый список адресов

По умолчанию оба списка пусты.

Чтобы добавить почтовые адреса в исключения

1. Введите в поле ввода почтовый адрес отправителя или маску, задающую почтовые адреса отправителей, чьи письма вы хотите обрабатывать автоматически без проведения анализа. Методы ввода:

- чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, `name@pochta.ru`). Все письма, полученные с этого адреса, будут обрабатываться без анализа;
- чтобы добавить в список отправителей, использующих похожие адреса электронной почты, используйте символы «`*`» и «`?`», чтобы заменить отличающуюся часть адреса. При этом символ «`*`» замещает любую последовательность символов, а символ «`?`» — один (любой) символ. Пример: если вы введете адрес `name*@pochta.ru`, то

письма от отправителей с адресами вида `name@pochta.ru`, `name1@pochta.ru`, `name_moj@pochta.ru` и т. п. будут обрабатываться без анализа;

- чтобы гарантированно получать или блокировать письма с почтовых адресов в конкретном домене, используйте символ «*» вместо имени пользователя. Пример: чтобы задать все письма от отправителей из домена pochta.ru, введите `*@pochta.ru`.

2. Чтобы добавить введенный адрес в список, нажмите кнопку ⊕ или кнопку ENTER на клавиатуре.
3. При необходимости повторите шаги 1 и 2 для добавления других адресов.

Работа с объектами в списке

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление почтового адреса в список. Становится доступна, если в текстовое поле введено какое-либо значение.
- Кнопка 🗑 — удаление выбранного почтового адреса из списка.
- При нажатии кнопки ⋯ доступны следующие действия:
  - **Изменить** — эта опция позволяет отредактировать выбранный из списка почтовый адрес.
  - **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.

Действия удаления или редактирования объекта доступны также в контекстном меню при нажатии правой кнопкой мыши на один или несколько выбранных объектов.

15. 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
   - Офисный контроль
   - Угрозы
   - Брандмауэр

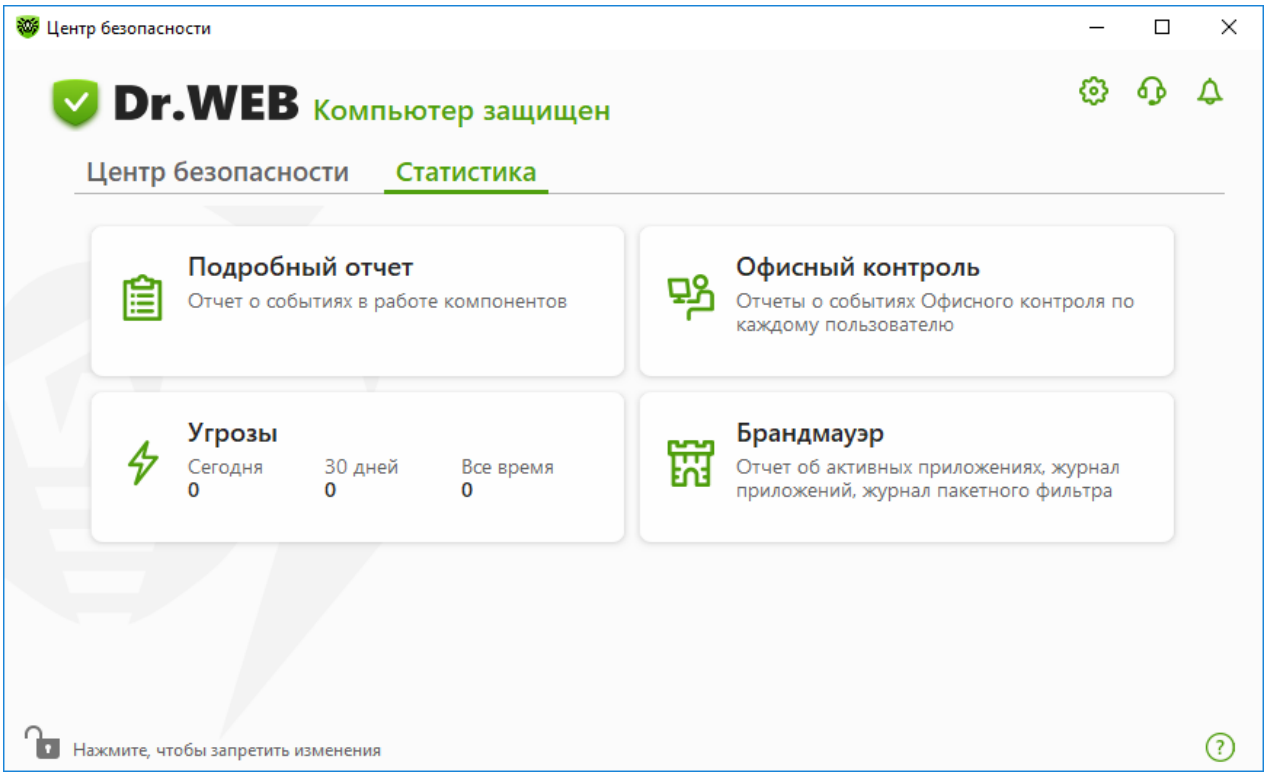

Рисунок 96. Статистика работы компонентов

4. Выберите группу для просмотра отчетов.

Подробный отчет

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

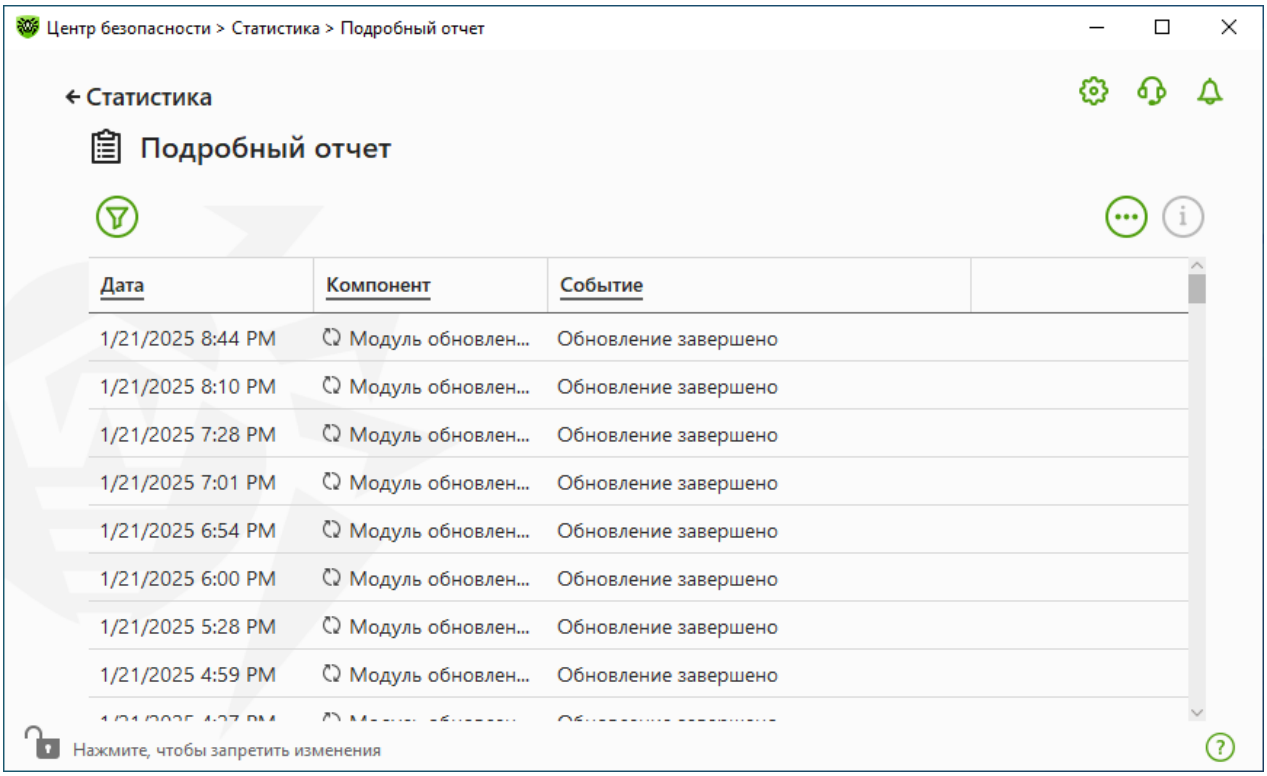

Рисунок 97. Окно подробного отчета

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.

Офисный контроль

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

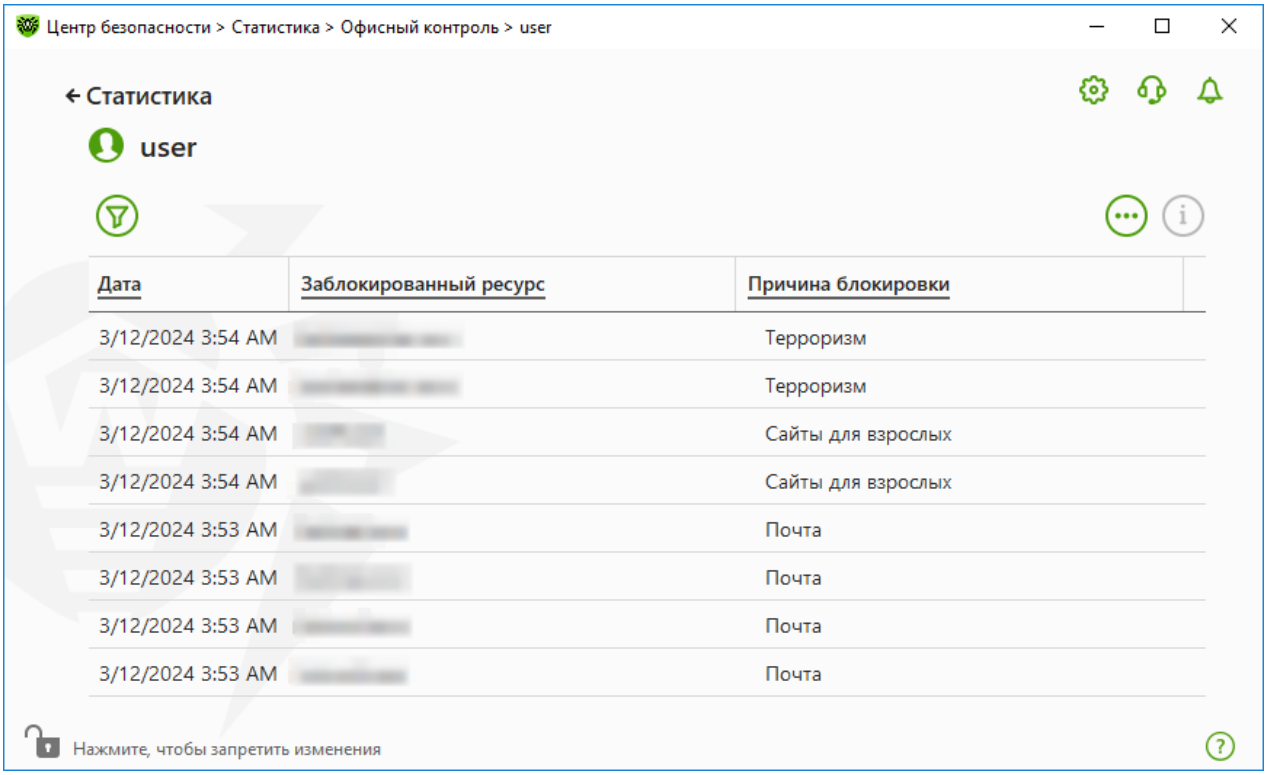

Рисунок 98. Окно статистики Офисного контроля

В отчете фиксируются следующие сведения:

- **Дата** — дата и время блокировки;
- **Заблокированный ресурс** — ссылка на заблокированный ресурс;
- **Причина блокировки** — категория или список исключений, к которым относится заблокированный ресурс.

По умолчанию отображаются все события за все время.

Для работы с объектами в таблице используются элементы управления.

Для отбора событий можно воспользоваться дополнительными фильтрами.

> В статистику попадают также интегрированные с другими страницами внешние ресурсы, например встроенные виджеты. Попадание их в статистику не означает, что пользователь намеренно пытался посетить данные сайты.

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.

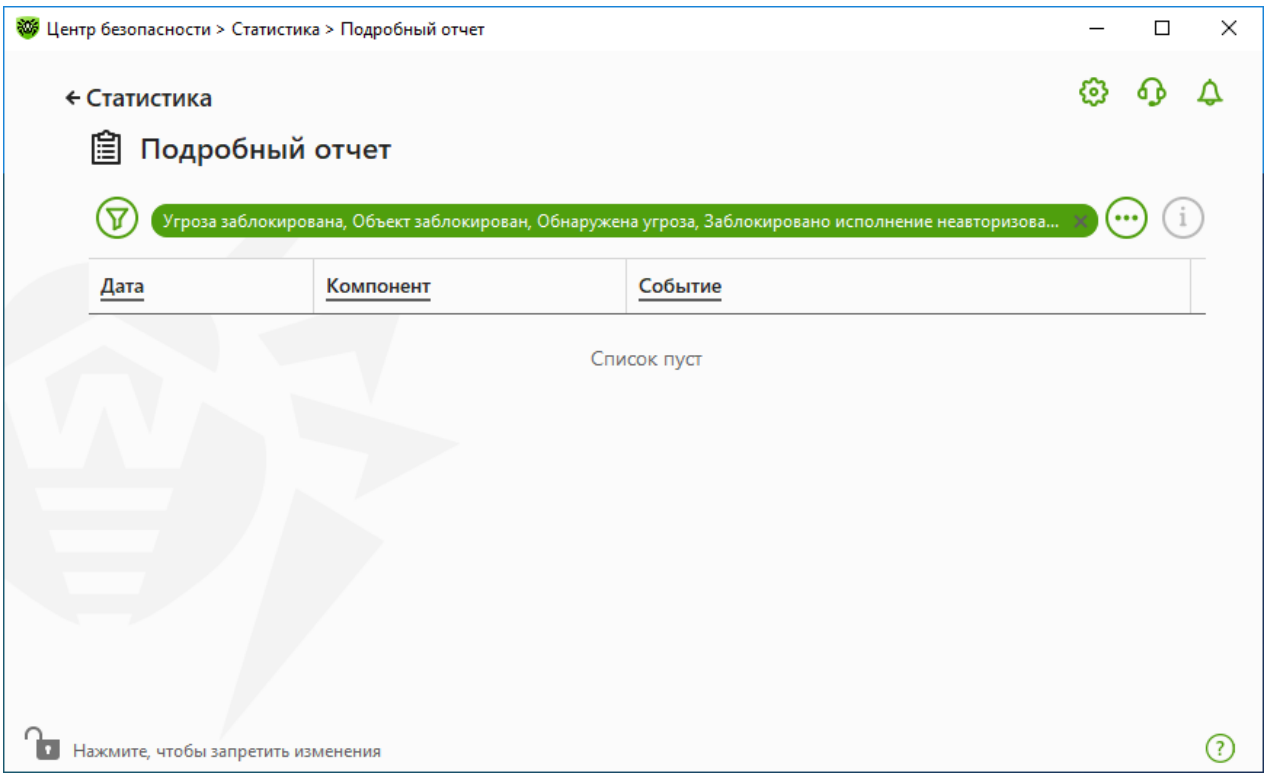

Рисунок 99. Окно статистики по угрозам

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.

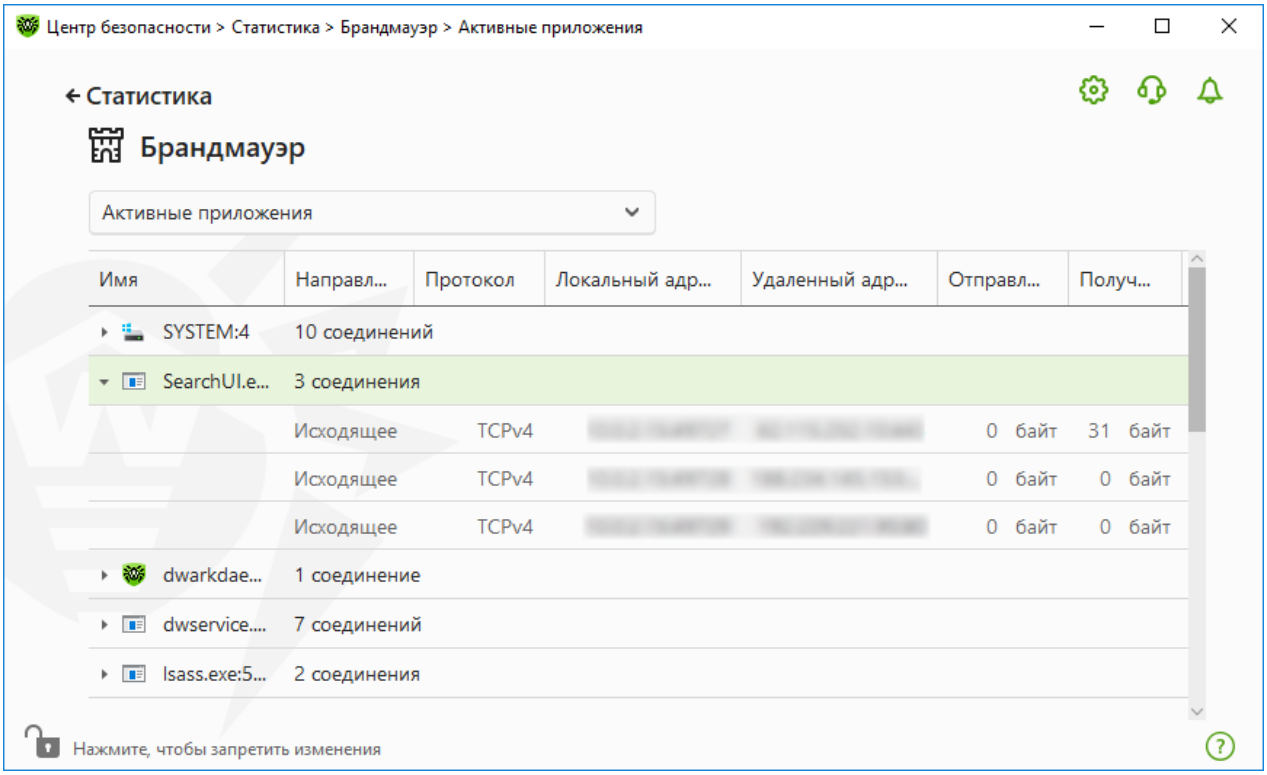

Рисунок 100. Окно статистики сетевой активности

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.

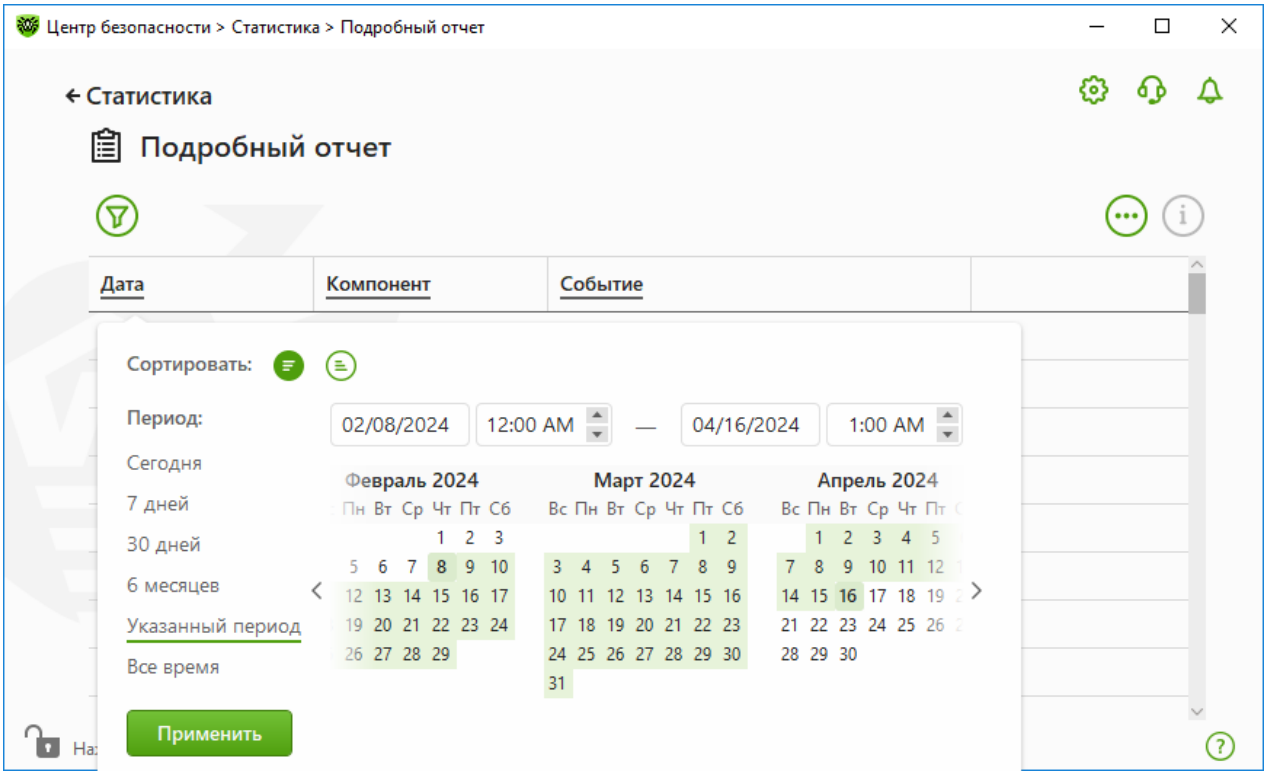

Рисунок 101. Сортировка по дате

   - 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.

   Для статистики Офисного контроля кроме сортировки по дате доступны следующие параметры:

   - Сортировка по заблокированному ресурсу. Вы можете отсортировать записи только по возрастанию или убыванию.

- Сортировка по причине блокировки. Вы можете отметить причины блокировки 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**.

16. Оповещения сервера

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

Чтобы перейти к окну Оповещения сервера

1. Откройте меню Dr.Web .
2. Выберите пункт **Оповещения сервера**.

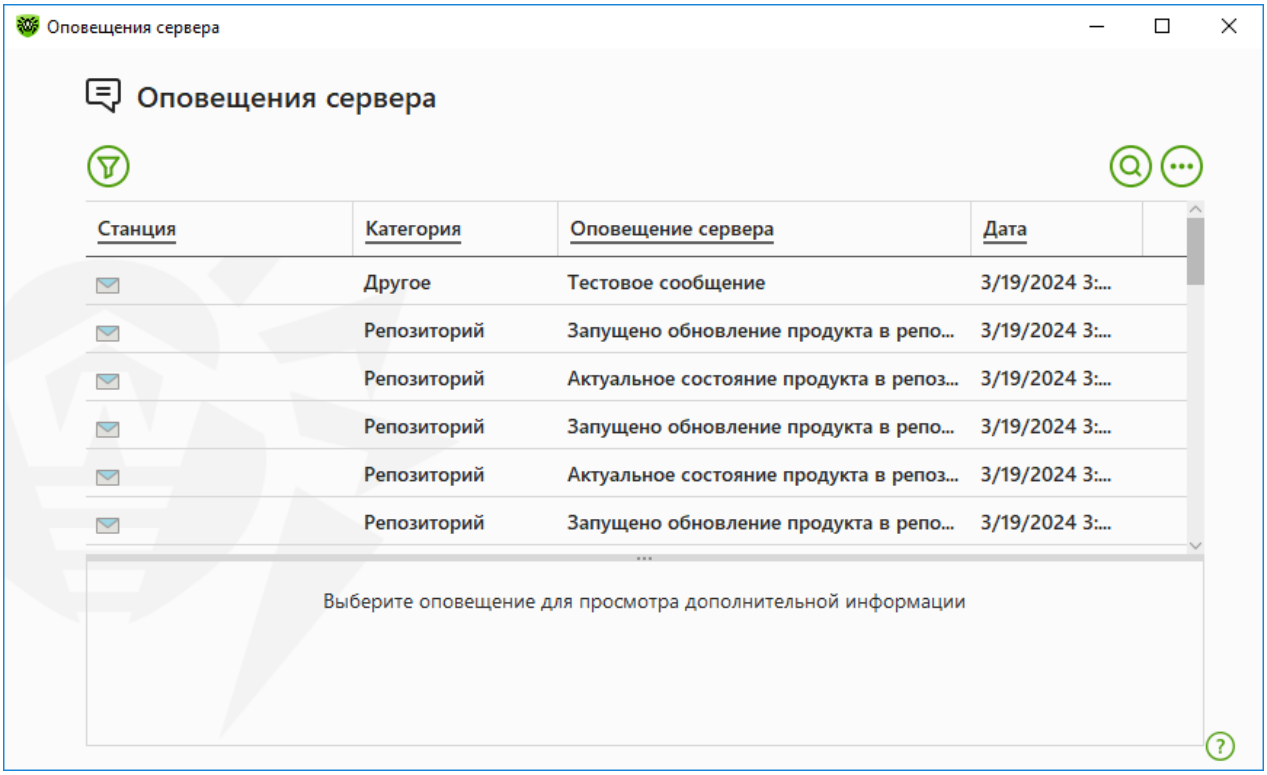

Рисунок 102. Окно Оповещения сервера

Все полученные оповещения выводятся списком в верхней части окна. Для просмотра дополнительной информации нажмите на соответствующее оповещение.

Фильтры

Чтобы посмотреть в списке только те оповещения, которые соответствуют определенным параметрам, воспользуйтесь фильтрами. По нажатию доступен фильтр по умолчанию. Его настройки дублируют настройки на сервере. Также вы можете создавать собственные фильтры оповещений.

Кнопки управления элементами в таблице:

- При нажатии кнопки  доступны следующие действия:
  - Выбор фильтра по умолчанию.
  - 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 оповещение (оповещения).
  - **Отметить как прочитанное** — позволяет отметить выделенные оповещения как прочитанные.
  - **Удалить все** — позволяет удалить все оповещения из таблицы.
- При нажатии кнопки  доступно окно поиска по всем оповещениям.

Чтобы задать пользовательский фильтр

1. Для сортировки по определенному параметру нажмите на заголовок необходимого столбца:
   - Сортировка по станции. Вы можете отсортировать записи только по возрастанию или убыванию.
   - Сортировка по категории. Вы можете отметить те категории, информация от которых будет отображаться в отчете, либо отсортировать записи по возрастанию или убыванию. Фильтровать оповещения можно по следующим категориям:
     - Администраторы;
     - Станции;
     - Лицензии;
     - Новички;
     - Репозиторий;
     - Установки;
     - Другое.
   - Сортировка по оповещению сервера. Вы можете отсортировать записи только по возрастанию или убыванию.

- 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.

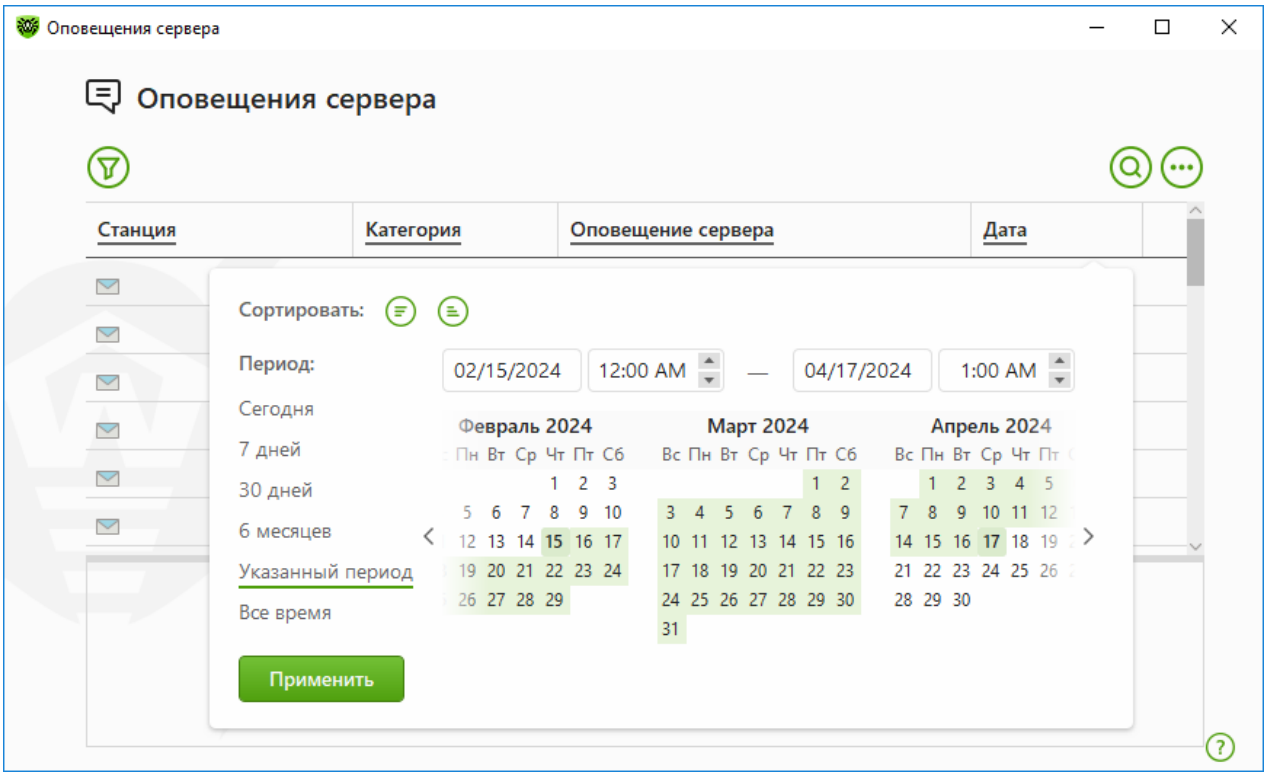

Рисунок 103. Сортировка по дате

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**.

17. 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:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. 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»:

1. Заполните веб-форму в соответствующей секции раздела https://support.drweb.com/.
2. 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/.

17.1. Помощь в решении проблем

При обращении к администратору вашей антивирусной сети 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**.

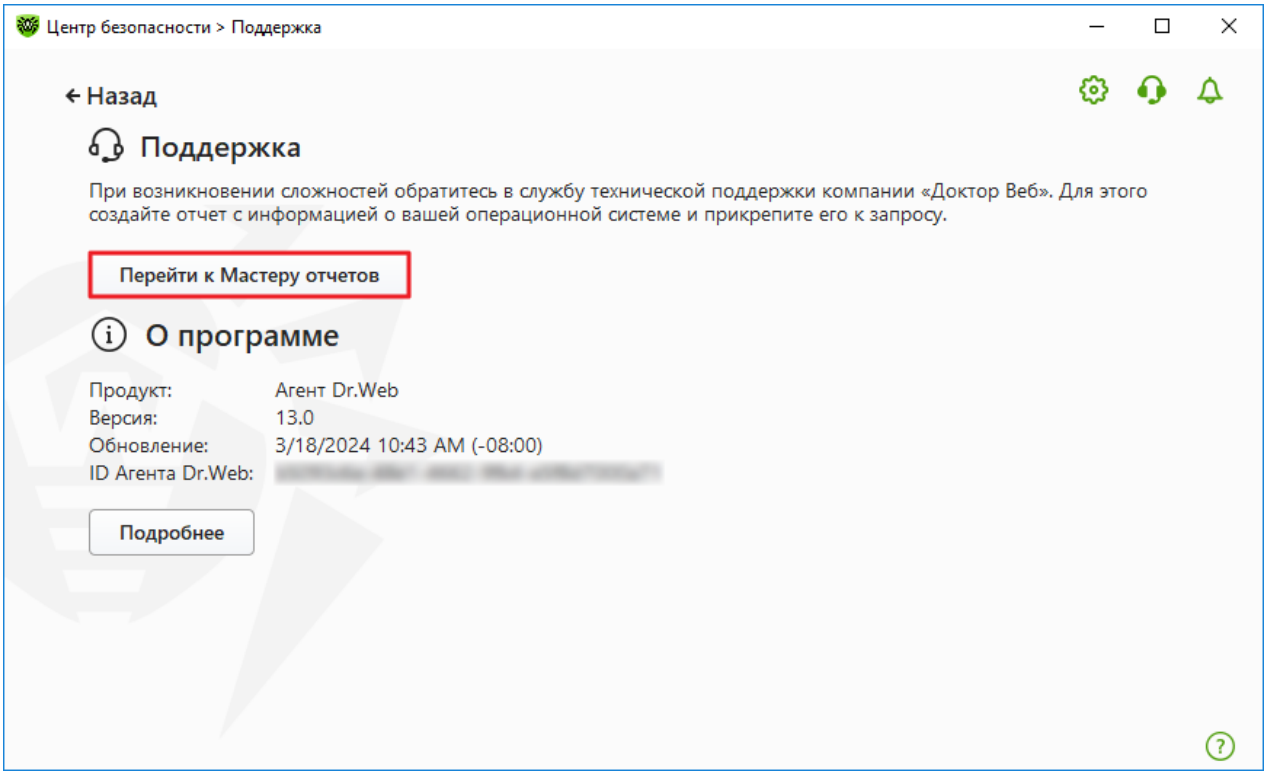

Рисунок 104. Поддержка

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

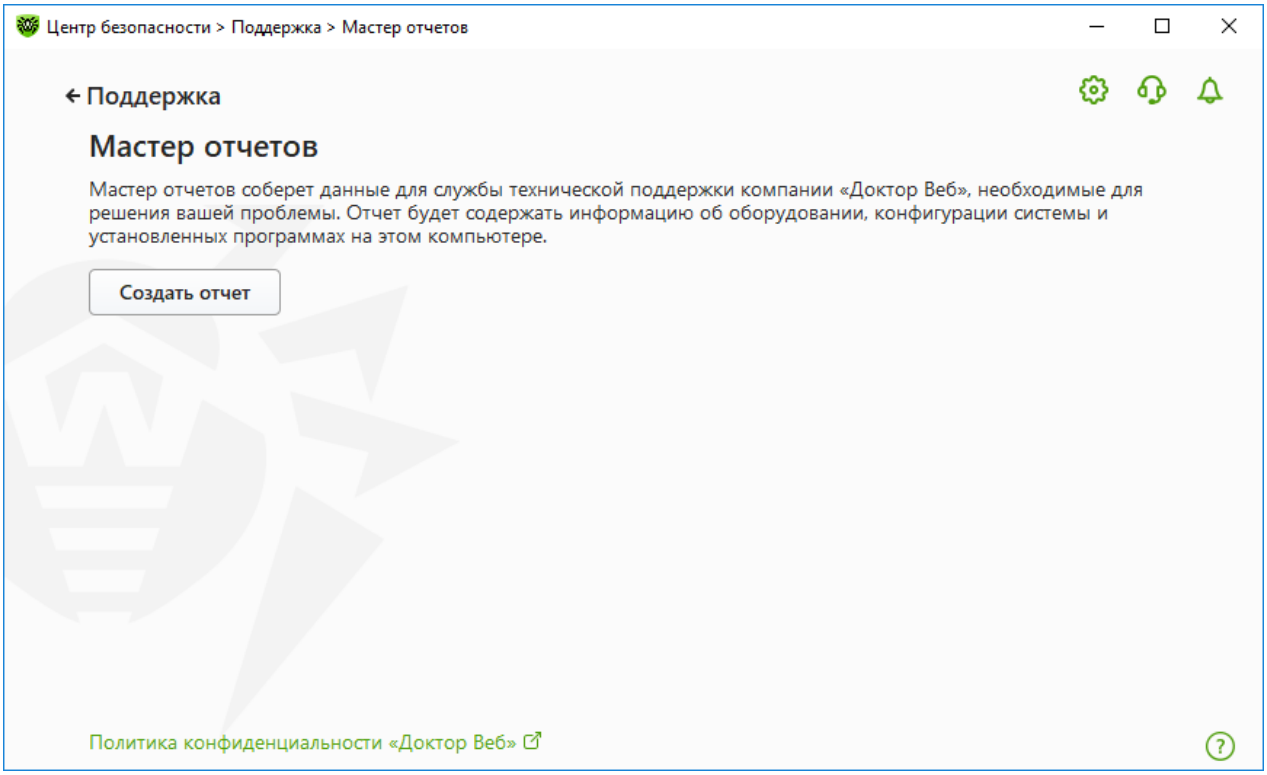

Рисунок 105. Создание отчета для технической поддержки

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. Отчет защищен паролем `virus`.

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**.

17.2. О программе

Блок **О программе** содержит информацию о:

- версии продукта;
- дате и времени последнего обновления;
- идентификационном номере Агента Dr.Web.

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**.

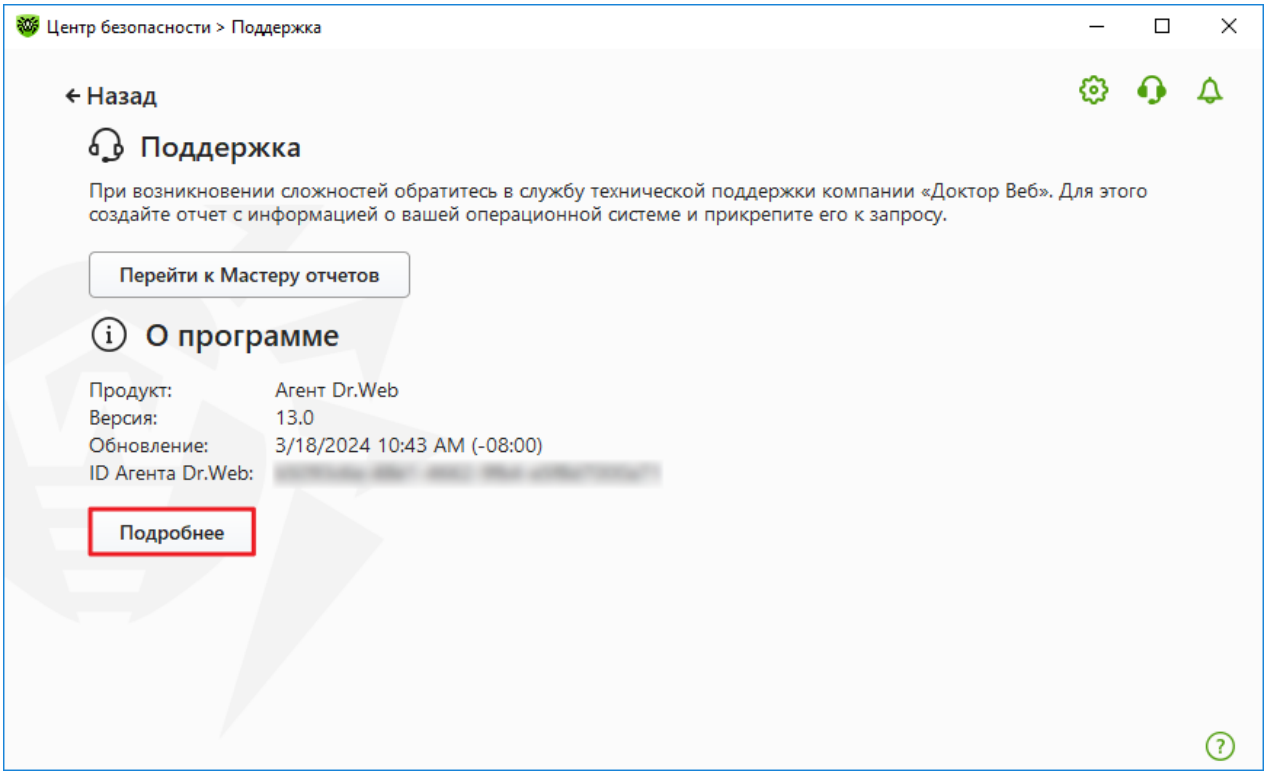

Рисунок 106. Доступ к окну О программе Dr.Web

18. 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 инсталляционным пакетам. 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.

18.1. Параметры для Сканера и Консольного сканера

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

Ключ	Описание
/HA	Производить эвристический анализ файлов и поиск в них неизвестных угроз. По умолчанию опция включена.
/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.
/NI[:X]	Уровень использования ресурсов системы, в процентах. Определяет количество памяти, используемой для проверки и системный приоритет проверки. По умолчанию — без ограничений.
/NOREBOOT	Отменяет перезагрузку и выключение после проверки. (Только для Сканера).
/NT	Проверять NTFS-потоки. По умолчанию опция включена.
/OK	Выводить полный список проверяемых объектов, сопровождая незараженные пометкой Ok. По умолчанию опция отключена.
/P:<*приоритет*>	Приоритет запущенной задачи проверки в общей очереди задач на проверку: 0 — низший. L — низкий. N — обычный. Приоритет по умолчанию. H — высокий. M — максимальный.
/PAL:<*уровень_вложенности*>	Максимальный уровень вложенности упаковщиков исполняемого файла. Если уровень вложенности превышает указанный, проверка будет производиться только до указанного уровня вложенности. По умолчанию — 1000.
/QL	Вывести список всех файлов, помещенных в карантин на всех дисках. (Только для Консольного сканера).

Ключ	Описание
/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).
/SCC	Выводить содержимое составных объектов. По умолчанию опция отключена.
/SCN	Выводить название контейнера. 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.

Ключ	Описание
/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 контейнерами (возможные действия: DQIR)
/ADL: <*действие*>	действия с программами дозвона (возможные действия: DQIR)
/AES: <*действие*>	действия с уязвимыми программами (возможные действия: IR)
/AHT: <*действие*>	действия с программами взлома (возможные действия: DQIR)
/AIC: <*действие*>	действия с неизлечимыми файлами (возможные действия: DQR)

Действие	Описание
/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, /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.

18.2. Параметры для инсталляционных пакетов

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

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

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

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

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

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

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

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

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

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

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

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

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

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

`/installdir` <*папка*> — папка установки.

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

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

- `remove` — удалить установленный продукт.

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

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

Если ключ не задан, по умолчанию используется системный язык.

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

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

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

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

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

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

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

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

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

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

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

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

`/silent` <*режим*> — определяет, будет ли инсталлятор запущен в фоновом режиме. Параметр <*режим*> может принимать следующие значения:

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

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

`/timeout` <*время*> — предельное время ожидания каждого ответа при поиске сервера. Задается в секундах. Прием ответных сообщений продолжается, пока время ожидания ответа не превышает значение тайм-аута.

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

18.3. Коды возврата для Консольного сканера

Возможные значения кода возврата и соответствующие им события следующие:

Код возврата	Событие
0	Угроз или подозрений на угрозы не обнаружено.
1	Обнаружены известные угрозы.
2	Обнаружены модификации известных угроз.
4	Обнаружены подозрительные объекты.
8	В архиве, контейнере или почтовом ящике обнаружены известные угрозы.
16	В архиве, контейнере или почтовом ящике обнаружены модификации известных угроз.
32	В архиве, контейнере или почтовом ящике обнаружены подозрительные объекты.
64	Успешно выполнено лечение хотя бы одного зараженного 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 угрозы (угроза), в том числе в архиве; обезвреживание не проводилось; больше никакой информации об угрозах не было.

18.4. Коды возврата для Модуля обновления

Возможные значения кода возврата и соответствующие им события следующие:

Код возврата	Событие
0	Ошибок нет.
4	Неверные параметры командной строки.
6	Необходим перезапуск обновления.
7	Обновление уже идет.

Код возврата	Событие
8	Обновления для указанных продуктов или компонентов не требуются.
9	Ошибка подключения к серверу.
10	Не удалось получить информацию о ревизии компонентов.
11	Список зон обновлений пуст.
12	Лицензия заблокирована.
13	Лицензия отсутствует.
16	Нет информации о лицензии.
25	Недоступно обновление в Мобильном режиме.

19. 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».

19.1. 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».

19.2. 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 вредоносным программам, 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.

20. Приложение В. Принципы именования угроз

При обнаружении вредоносного кода компоненты Dr.Web сообщают пользователю средствами интерфейса и заносят в файл отчета имя угрозы, присвоенное ей специалистами компании «Доктор Веб». Эти имена строятся по определенным принципам и отражают конструкцию угрозы, 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 угроз; более полная и постоянно обновляемая версия описания доступна по адресу https://vms.drweb.com/classification/.

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

Полное имя угрозы 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 вредоносных программ, 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 вредоносные программы 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 угроз, 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` — вредоносные программы, перезаписывающие код программы жертвы;
- `HLLP` — паразитические вредоносные программы;
- `HLLC` — вредоносные программы-спутники.

К группе префиксов языка разработки можно также отнести:

- `Java` — угрозы 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 вредоносные файлы, 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 вредоносной программы 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-угрозы

Префиксы угроз, 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 угроз. Такая угроза не обладает никакими характерными признаками (как текстовые строки, специальные эффекты и т. д.), которые позволили бы присвоить ей какое-то особенное название.

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

Суффиксы

Суффиксы используются для именования некоторых специфических вредоносных объектов:

- `generator` — объект является не вирусом, а вирусным генератором;
- `based` — вредоносный объект разработан с помощью указанного генератора или путем видоизменения указанной угрозы. В обоих случаях имена этого типа являются родовыми и могут обозначать сотни и иногда даже тысячи угроз;

- `dropper` — указывает, что объект является не вирусом, а контейнером указанного вируса.

21. Приложение Г. Основные термины и понятия

А

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

Архив — файл с упакованными в нем другими файлами и их метаданными. Возможные форматы: ARJ, GZIP, RAR, TAR, ZIP и т. п.

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.

И

Инсталляционный пакет — набор файлов, в котором содержатся все необходимые данные для установки продукта.

К

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

Контейнер — составной объект, который может быть распакован. Список форматов:

Проверяются всегда:

AUTOIT, BANGCLE, CHM, DOC1C, EMBEDOBJ, HTML, HTMLVBA, JAR, JSHTML, LNK, MSGVBA, ODEX, OLEEXPL, OPEN_XML, PDF, PPT, RC, RTF, SECSHELL, SWF, TENCENT, VISIO.

Проверяются при запуске:

NSIS, NSIS_as, PYINSTALL.

Проверяются при включенной опции **Проверять контейнеры**:

ADVINST, ASF, BCOMPILER, CLICKTEAM, CMTSCRIPT, CREATEINSTALL, DDS, DEB, DEPLOY, GKWARE, GTP, IJAMMER, INNO, ISHIELD, ISZ, JCOMPILER, LZMA, MACBIN, MSI, MSSE, MSXML, NETSTREAM, OCRA, PERL2EXE, PHP, PIMP, PYTHON, RPM, RSFX, SFACT, SFX74, SIM, SIS, SQUASH, TARMA, TCOMPR, THINST, UDF, UNIBIN, VISE, WIM, WISE, XAR, XENOCODE, XZ, ZLIB.

М

Модификация — код, полученный таким изменением известной угрозы, что при этом он опознается сканером, но алгоритмы лечения исходной угрозы к нему неприменимы.

П

Почтовый файл — файл почтового клиента, используемый для хранения различных данных электронной почты. Примеры форматов: DBX, MIME, PST, TBB, TNEF, UUE.

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 (запись об угрозе) — 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.