Dr.WEB

Server Security Suite (Windows)

Руководство администратора

Dr.Web Server Security Suite (Windows)
Версия 12.0
Руководство администратора
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 Dr.Web Server Security Suite, а также рекомендации по его использованию и решению типичных проблем, связанных с компьютерными угрозами. В основном рассматриваются стандартные режимы работы компонентов программы Dr.Web Server Security Suite (с настройками по умолчанию).

В Приложениях содержится общая справочная информация, а также дополнительные параметры для настройки программы Dr.Web Server Security Suite.

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 — Dr.Web Server Security Suite;
- FTP — (от англ. File Transfer Protocol) протокол передачи файлов;
- HTTP — (от англ. Hypertext Transfer Protocol) протокол передачи гипертекста;

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

2. О продукте

Dr.Web Server Security Suite 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.

Dr.Web Server Security Suite 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 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.

Dr.Web Server Security Suite 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.

Dr.Web Server Security Suite 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 Dr.Web Server Security Suite обеспечивает защиту от вредоносных действий, направленных на работу антивирусных программ.

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

2.1. Компоненты защиты и модули управления

Dr.Web Server Security Suite включает в состав следующие компоненты защиты и модули управления:

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

Компонент/модуль	Описание
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 или по расписанию и производит антивирусную проверку компьютера.
Консольный сканер Dr.Web	Версия Сканера с интерфейсом командной строки.
Модуль обновления	Позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов Dr.Web, а также производит их автоматическую установку.
SpIDer Agent	Модуль, с помощью которого осуществляется настройка и управление работой компонентов продукта.

2.2. Методы обнаружения угроз

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

Сигнатурный анализ

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

Origins Tracing

Это уникальная технология Dr.Web, которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы заражения или вредоносное поведение. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения Dr.Web, от таких угроз, как троянская программа-вымогатель Trojan.Encoder.18 (также известная под названием «gpcode»). Кроме того, использование технологии Origins Tracing позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing, добавляется постфикс `.Origin`.

Эмуляция исполнения

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

Эвристический анализ

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

Эвристический анализатор также использует технологию FLY-CODE — универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке упакованных объектов также используется технология анализа их структурной энтропии,

которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

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

Поведенческий анализ

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

Dr.Web Process Heuristic

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

Dr.Web Process Heuristic анализирует поведение каждой запущенной программы, сверяясь с постоянно обновляемым облачным сервисом Dr.Web, и на основе актуальных знаний о том, как ведут себя вредоносные программы, делает вывод о ее опасности, после чего принимаются необходимые меры по нейтрализации угрозы. К названиям угроз, обнаруженных при помощи Dr.Web Process Heuristic, добавляется префикс `DPH`.

Данная технология защиты данных позволяет свести к минимуму потери от действий 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.

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

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

Защита от инжектов

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

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

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

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

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

Защита от вымогателей

Защита от вымогателей — один из компонентов Превентивной защиты, обеспечивающий защиту файлов пользователей от троянцев-шифровальщиков. Данные

вредоносные программы, попадая на компьютер пользователя, блокируют доступ к данным путем шифрования, после чего вымогают деньги за расшифровку. К названиям угроз, обнаруженных при помощи Защиты от вымогателей, добавляется префикс `DPH:Trojan.Encoder`.

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

Также проверяются следующие характеристики приложения:

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

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

Метод машинного обучения

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

Обнаружение угроз строится на классификации вредоносных объектов согласно определенным признакам. С помощью технологии машинного обучения, основанной на методе опорных векторов, происходит классификация и запись в базу фрагментов кода сценарных языков. Затем проверяемые объекты анализируются на основе соответствия признакам вредоносного кода. Технология машинного обучения автоматизирует обновление списка данных признаков и пополнение вирусных баз. Благодаря подключению к облачному сервису обработка больших объемов данных происходит быстрее, а постоянное обучение системы обеспечивает превентивную защиту от новейших угроз. При этом технология может функционировать и без постоянного обращения к облаку.

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

Облачные технологии обнаружения угроз

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

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

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

2.3. Системные требования

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

Параметр	**Требования**
Процессор	С поддержкой системы команд i686
Операционная система	Для 32-разрядных операционных систем: • Windows Server 2003 с пакетом обновлений SP1; • Windows Server 2008 с пакетом обновлений SP2 или более поздними. Для 64-разрядных операционных систем: • 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

Параметр	Требования
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; • Xen; • KVM

Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой программы Dr.Web Server Security Suite на 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».

Dr.Web Server Security Suite версии 12.0 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.

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

Назначение	Направление	Номера портов
Для обновления (если включена опция обновления по https)	исходящий	443
Для обновления	исходящий	80
Для отправки почтовых уведомлений		25 или 465 (либо в зависимости от настроек почтовых уведомлений)
Для соединения с облачным сервисом Dr.Web Cloud	исходящий	443 (TCP), 2075 (в том числе для UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

3. Установка, изменение и удаление программы

Перед началом установки Dr.Web Server Security Suite 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 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;
- 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.

Установка Dr.Web возможна в одном из следующих режимов:

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

3.1. Установка программы

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

Установка в режиме мастера установки

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

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

Чтобы установить программу

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

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

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

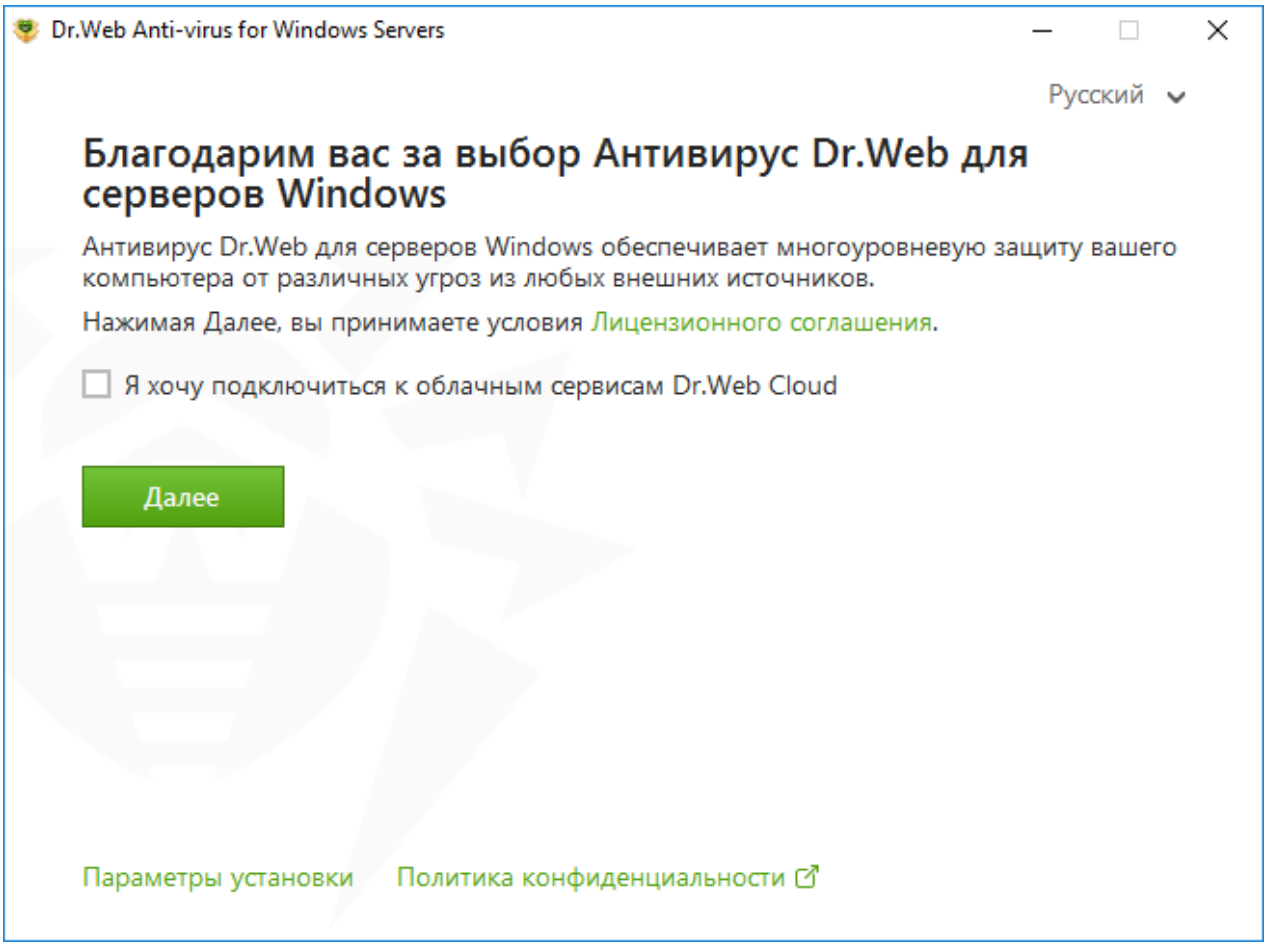

Рисунок 1. Мастер установки

3. Если вы хотите произвести установку с параметрами по умолчанию, перейдите к следующему пункту. Чтобы выбрать устанавливаемые компоненты, указать путь

установки и некоторые дополнительные параметры, нажмите ссылку **Параметры установки**.

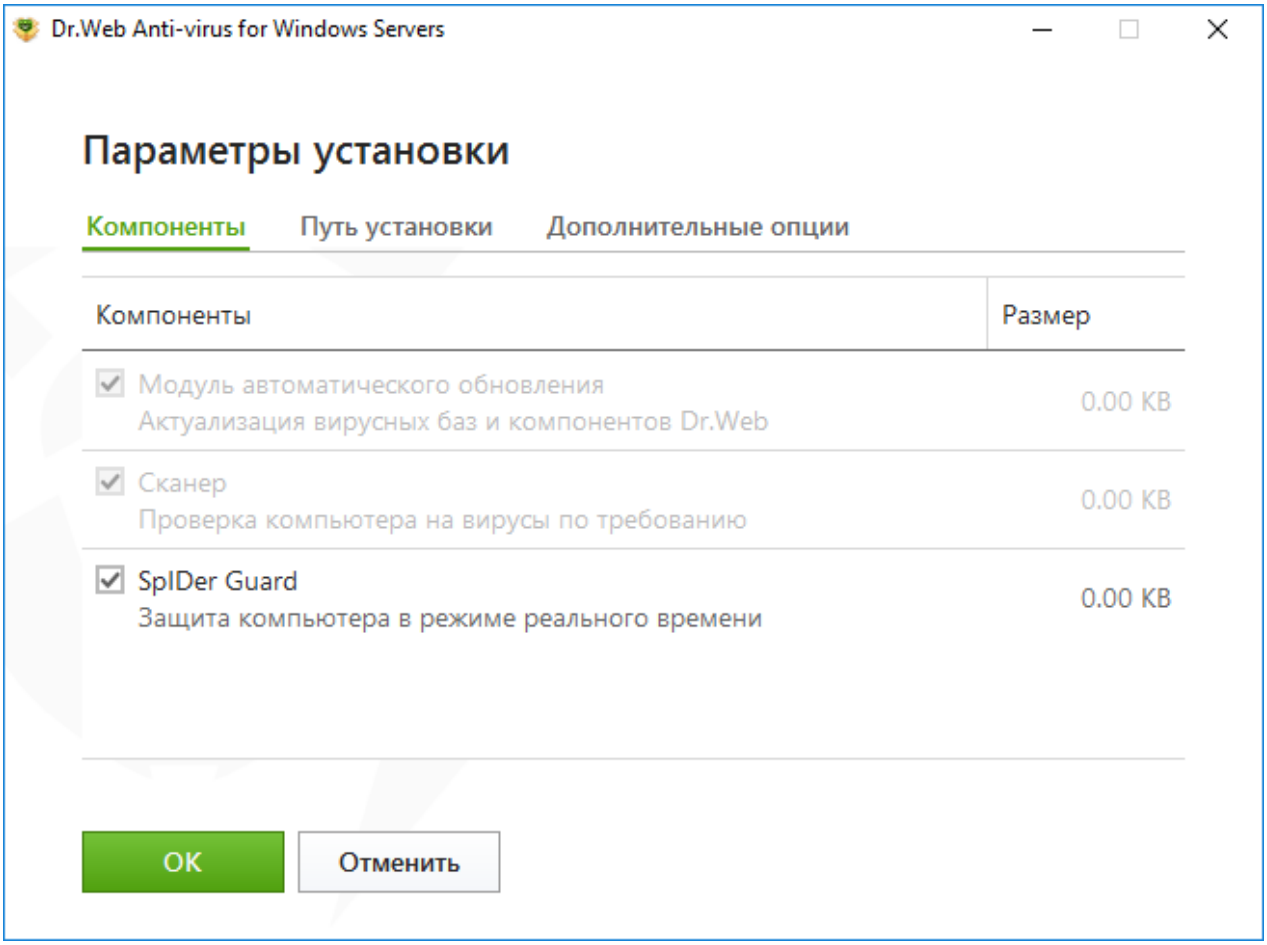

Рисунок 2. Параметры установки

Данная опция предназначена для опытных пользователей.

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

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

4. Нажмите кнопку **Далее**. Обратите внимание, что тем самым вы принимаете условия лицензионного соглашения.
5. В окне **Мастер регистрации** необходимо выбрать одну из следующих опций:
   - если у вас есть ключевой файл и он находится на жестком диске или съемном носителе, выберите **Указать путь к действующему ключевому файлу**. Нажмите кнопку **Обзор** и выберите нужный ключевой файл в открывшемся окне. Подробнее вы можете прочитать в инструкции Активация при помощи ключевого файла;
   - для продолжения установки без ключевого файла выберите **Получить лицензию позднее**. В этом случае ни один компонент программы не будет работать до тех пор, пока вы не укажете действительный ключевой файл. Вы сможете приобрести лицензию и получить действующий ключевой файл после установки продукта.

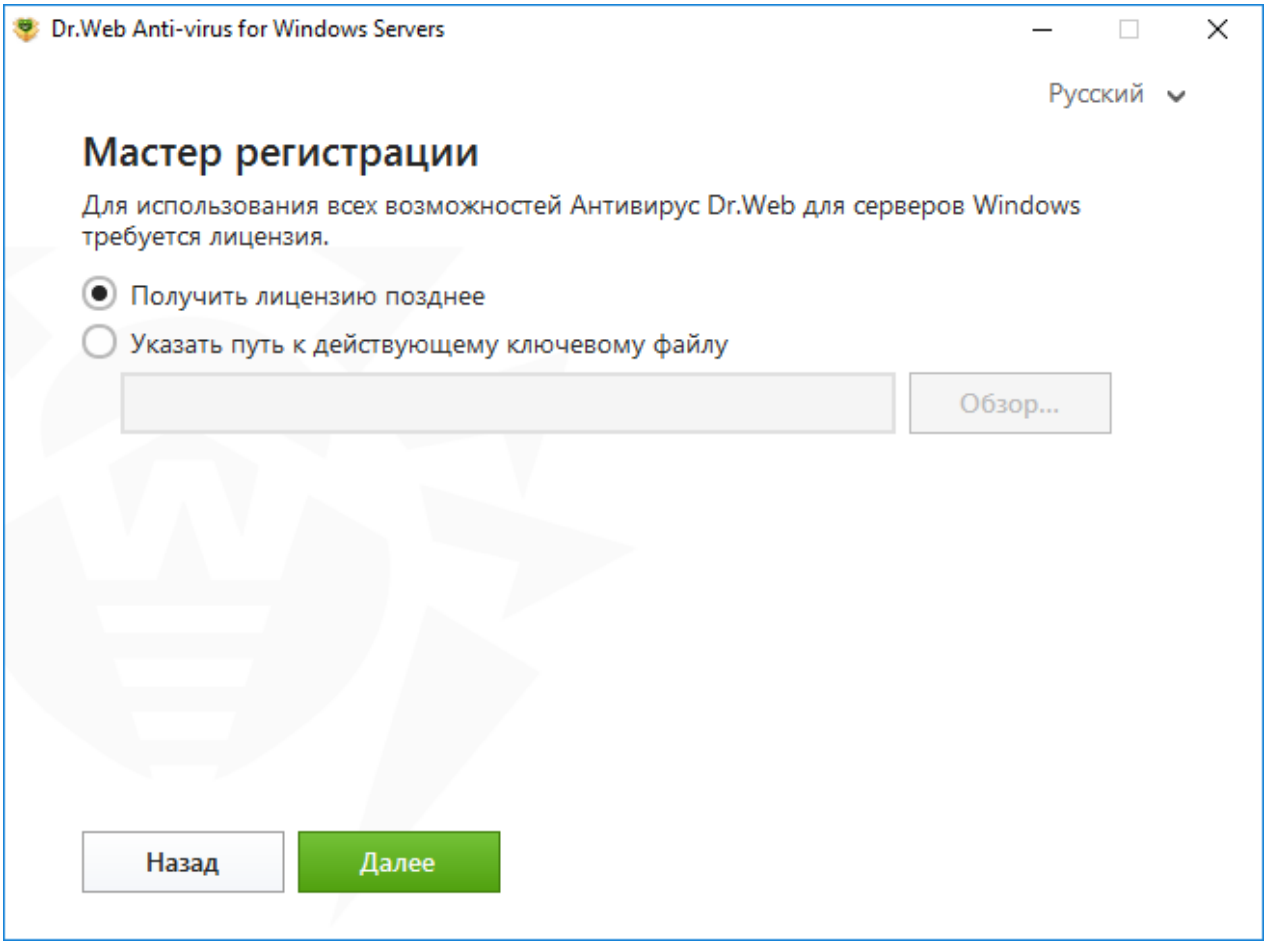

Рисунок 3. Мастер регистрации

Нажмите кнопку **Далее**.

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

Установка в режиме командной строки

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

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

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

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

Ошибка службы BFE при установке программы Dr.Web

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

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

1. Просканируйте систему при помощи лечащей утилиты CureIt! от компании «Доктор Веб». Скачать утилиту вы можете на сайте: https://free.drweb.com/download+cureit+free/.
2. 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».

3.2. Изменение компонентов программы

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

- при наличии установочного файла запустите его;
- из Панели управления Windows:
  1. Перейдите в раздел Панели управления Windows, посвященный установке и удалению программ.
  2. В списке установленных программ выберите строку **Dr.Web Anti-virus for Windows Servers**.
  3. Нажмите кнопку **Изменить**.

Чтобы удалить или добавить компоненты

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

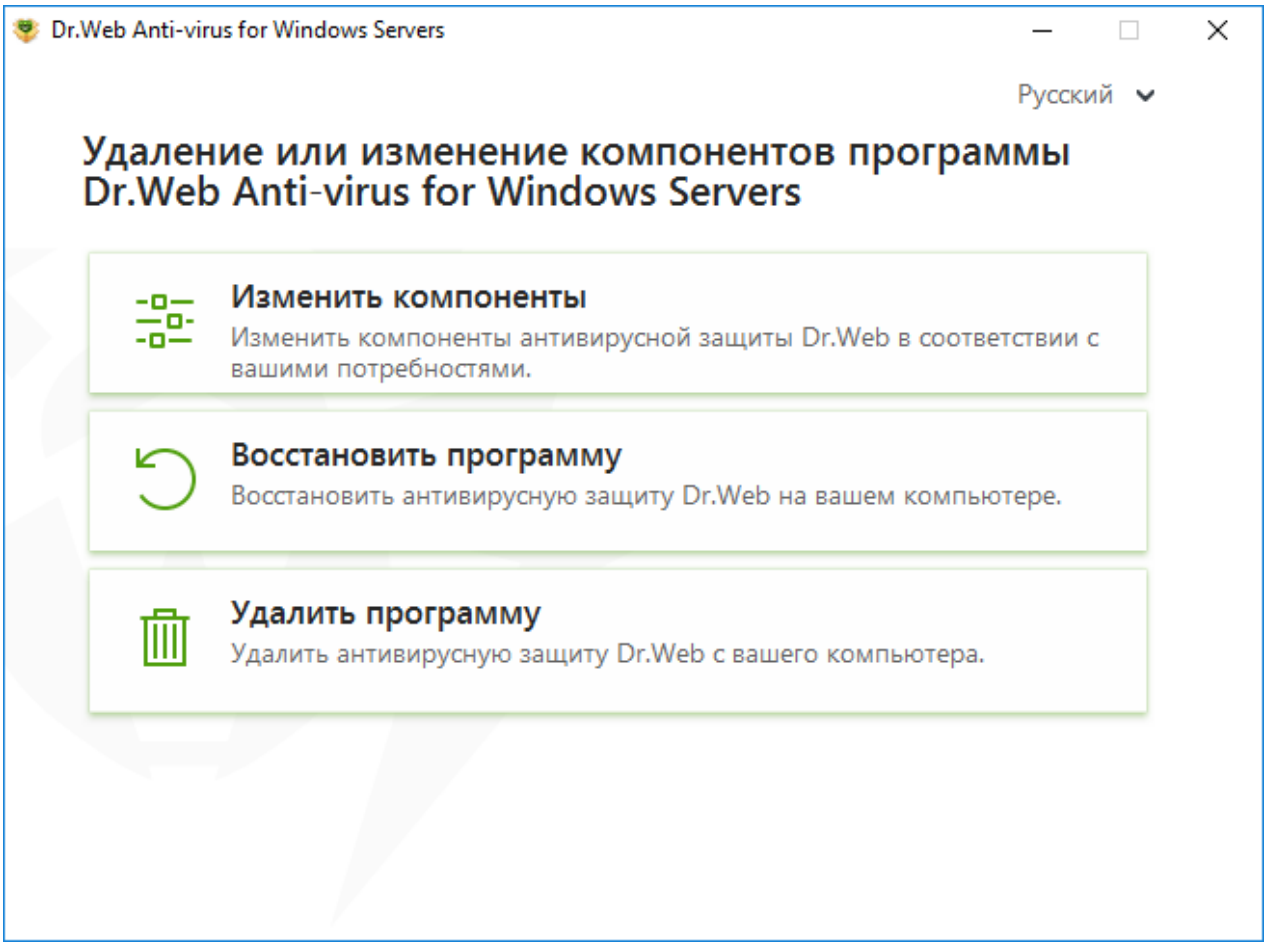

Рисунок 4. Мастер удаления/изменения компонентов

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

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

- **Восстановить программу**, если необходимо восстановить антивирусную защиту на вашем компьютере. Эта функция применяется в том случае, когда некоторые из компонентов программы Dr.Web были повреждены.
- **Удалить программу**, чтобы удалить все установленные компоненты.

3.3. Удаление и переустановка программы

Удаление Dr.Web

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

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

1. Для удаления Dr.Web Server Security Suite 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** и **Настройки Dr.Web Anti-virus for Windows Servers**. Нажмите кнопку **Далее**.
5. Откроется окно **Отключение Самозащиты**, в котором необходимо ввести изображенный код подтверждения, после чего нажать кнопку **Удалить программу**.
6. Изменения вступят в силу после перезагрузки компьютера. Процесс перезагрузки можно отложить, нажав кнопку **Перезагрузить позже**. Нажмите кнопку **Перезагрузить сейчас** для немедленного завершения процедуры удаления или изменения состава компонентов Dr.Web.

Переустановка Dr.Web

1. Загрузите актуальный дистрибутив программы с официального сайта компании «Доктор Веб». Для этого необходимо ввести действительный серийный номер в соответствующее поле.
2. Удалите продукт, как описано выше.
3. Перезагрузите компьютер.
4. Заново установите программу, используя загруженный дистрибутив (`drweb-12.0-av-win-server.exe`). 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 с помощью файла CloudCar

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

Проверка работы Dr.Web Cloud

1. Убедитесь, что у вас включено использование облачного сервиса Dr.Web Cloud.
2. Загрузите тестовый файл по адресу https://download.geo.drweb.com/pub/drweb/tools/cloudcar.exe (EXE, 7 КБ).
3. Если у вас установлен и включен компонент SplDer Guard, при попадании файла на компьютер он автоматически будет перемещен в карантин. Если компонент SplDer Guard не установлен или отключен, просканируйте загруженный файл. Для этого вызовите контекстное меню нажатием правой кнопки мыши по имени файла и выберите пункт **Проверить с Dr.Web**.
4. Проверьте, что тестовый файл обработан Dr.Web как `CLOUD:AMTSO.Test.Virus`. Префикс `CLOUD` в названии угрозы будет свидетельствовать о корректной работе Dr.Web Cloud.

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.
- Модуль обновления 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. Лицензирование

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

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

Способы активации лицензии

Активировать коммерческую лицензию вы можете одним из следующих способов:

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

Активация лицензии в Мастере регистрации возможна только при помощи ключевого файла. Активация лицензии в Менеджере лицензий возможна при помощи серийного номера или ключевого файла.

Подробнее об активации лицензии см. в разделах Активация при помощи серийного номера и Активация при помощи ключевого файла.

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

Возможные вопросы

Как я могу перенести лицензию на другой компьютер?

Вы можете перенести вашу коммерческую лицензию на другой компьютер при помощи ключевого файла или серийного номера.

Чтобы перенести лицензию на другой компьютер

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

Я забыл регистрационный email. Как я могу его восстановить?

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

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

Как я могу изменить регистрационный email?

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

Почему в моем продукте отсутствует часть компонентов?

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

  Чтобы включить недостающие компоненты

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

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

5.1. Активация лицензии

Чтобы использовать все функции и компоненты программы, необходимо активировать лицензию. Активация лицензии возможна при помощи:

- серийного номера,
- ключевого файла.

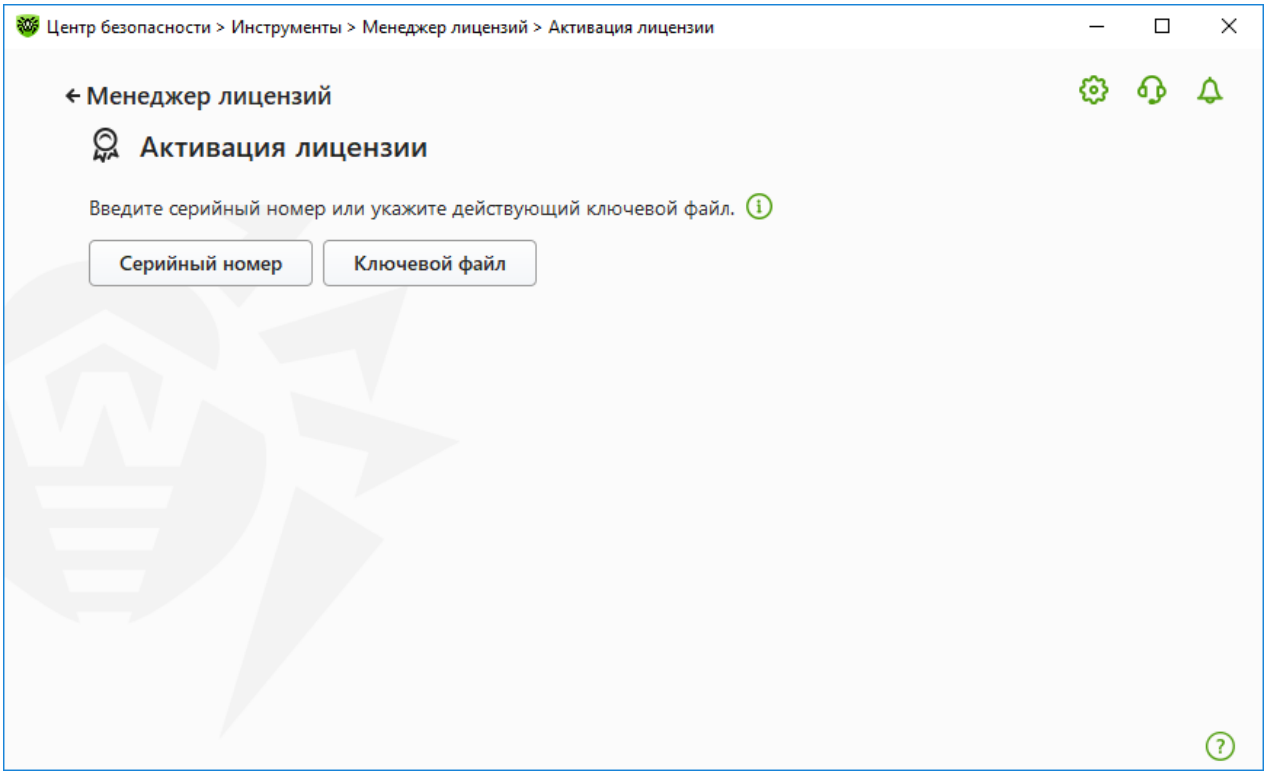

Рисунок 5. Активация лицензии

Пользователи Windows Server 2003 могут активировать лицензию только при помощи ключевого файла.

> Если вы уже являлись пользователем Dr.Web, то вы сможете продлить действие приобретенной лицензии.

Активация лицензии на Windows Server 2003

Пользователи Windows Server 2003 могут активировать лицензию только при помощи ключевого файла. Если ключевого файла нет, но есть серийный номер, его необходимо зарегистрировать на сайте компании «Доктор Веб». После завершения процесса регистрации вам будет предоставлена ссылка для скачивания ключевого файла. Используйте этот ключевой файл для активации лицензии во время установки или в любое время работы продукта при помощи Мастера регистрации, который входит в состав Менеджера лицензий:

1. В меню Dr.Web выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать**.
2. В открывшемся окне нажмите кнопку **Обзор**, чтобы указать путь к ключевому файлу.
3. Нажмите кнопку **ОК**, чтобы закрыть окно и вернуться к Менеджеру лицензий.

Повторная активация

Повторная активация лицензии может потребоваться в случае утраты ключевого файла.

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

При переустановке продукта или если лицензия предоставляет право установки продукта на несколько компьютеров, повторная активация серийного номера не требуется.

Получить лицензионный ключевой файл через Менеджер лицензий можно ограниченное количество раз. Если это число превышено, то ключевой файл можно получить, подтвердив регистрацию своего серийного номера на сайте https://products.drweb.com/register/. Ключевой файл будет выслан на адрес электронной почты, который был указан при первой регистрации.

5.1.1. Активация при помощи серийного номера

Если у вас есть серийный номер, вы можете:

- активировать лицензию в любое время работы продукта при помощи Менеджера лицензий:
  1. В меню Dr.Web выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать**.
  2. Откроется окно Активации лицензии. Нажмите кнопку **Серийный номер**.

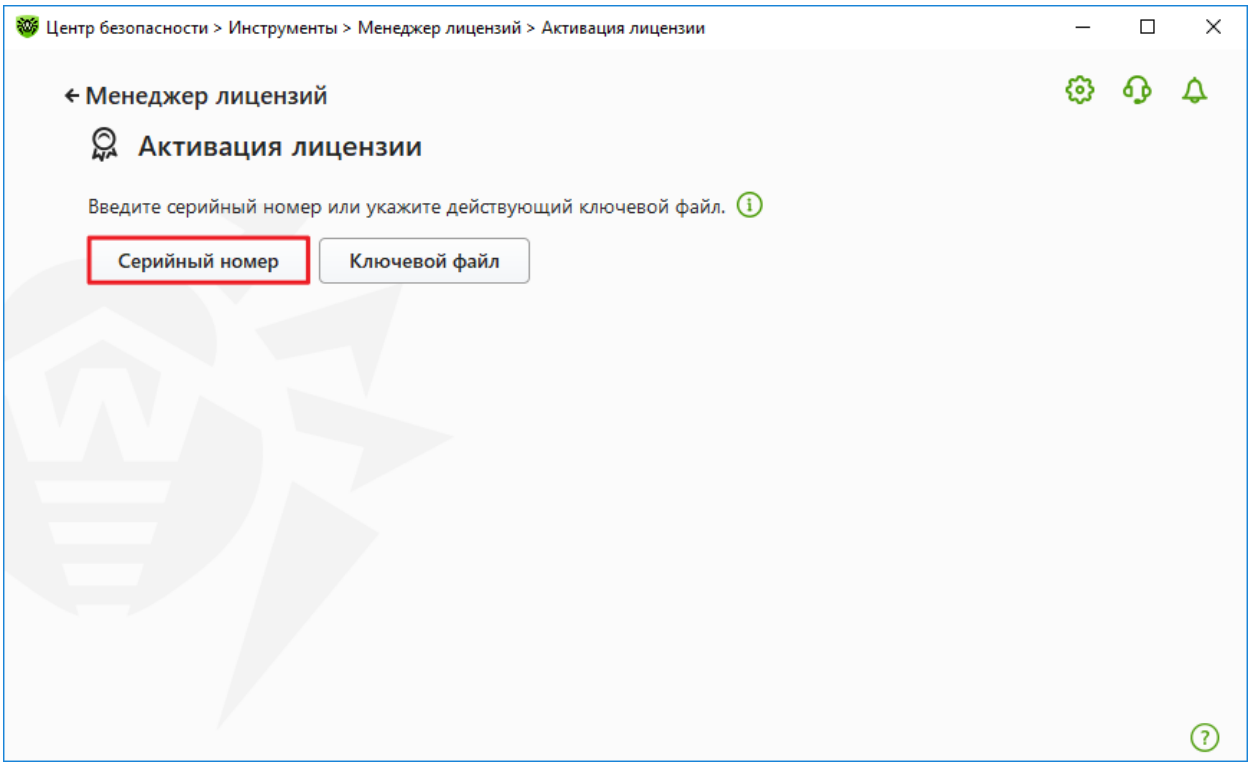

Рисунок 6. Доступ к окну ввода серийного номера

3. В новом окне введите серийный номер и нажмите **Активировать**.

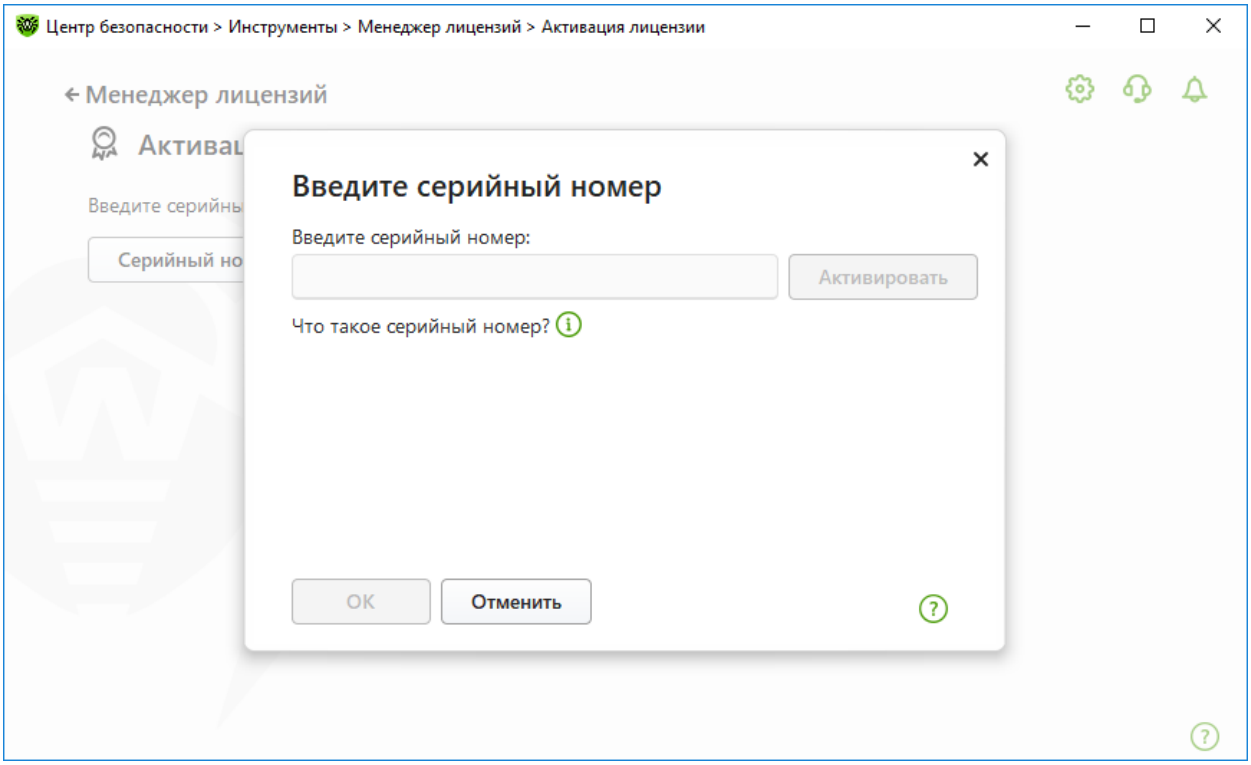

Рисунок 7. Активация при помощи серийного номера

4. Откроется страница сайта компании «Доктор Веб», на которой нужно ввести свои регистрационные данные. Следуйте инструкциям на сайте для завершения регистрации.

При длительном ожидании окно активации автоматически закроется с выведением сообщения об ошибке.

Не закрывайте окно активации до завершения регистрации серийного номера. Если по какой-либо причине окно было закрыто, лицензию можно будет активировать только с помощью ключевого файла.

5. На указанный вами электронный адрес будет отправлена ссылка для регистрации серийного номера. Перейдите по ней, чтобы завершить активацию лицензии.
6. При успешной активации в окне программы появится подробная информация о лицензии. Нажмите кнопку **ОК**, чтобы закрыть окно и вернуться к Менеджеру лицензий.

Если активация лицензии завершилась неудачно, выводится сообщение об ошибке. Проверьте подключение к интернету и нажмите кнопку **Повторить**.

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

5.1.2. Активация при помощи ключевого файла

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

- во время установки продукта при помощи Мастера регистрации:
  1. Запустите установку продукта. На 5 шаге установки выберите пункт **Указать путь к действующему ключевому файлу**. Нажмите **Далее**.

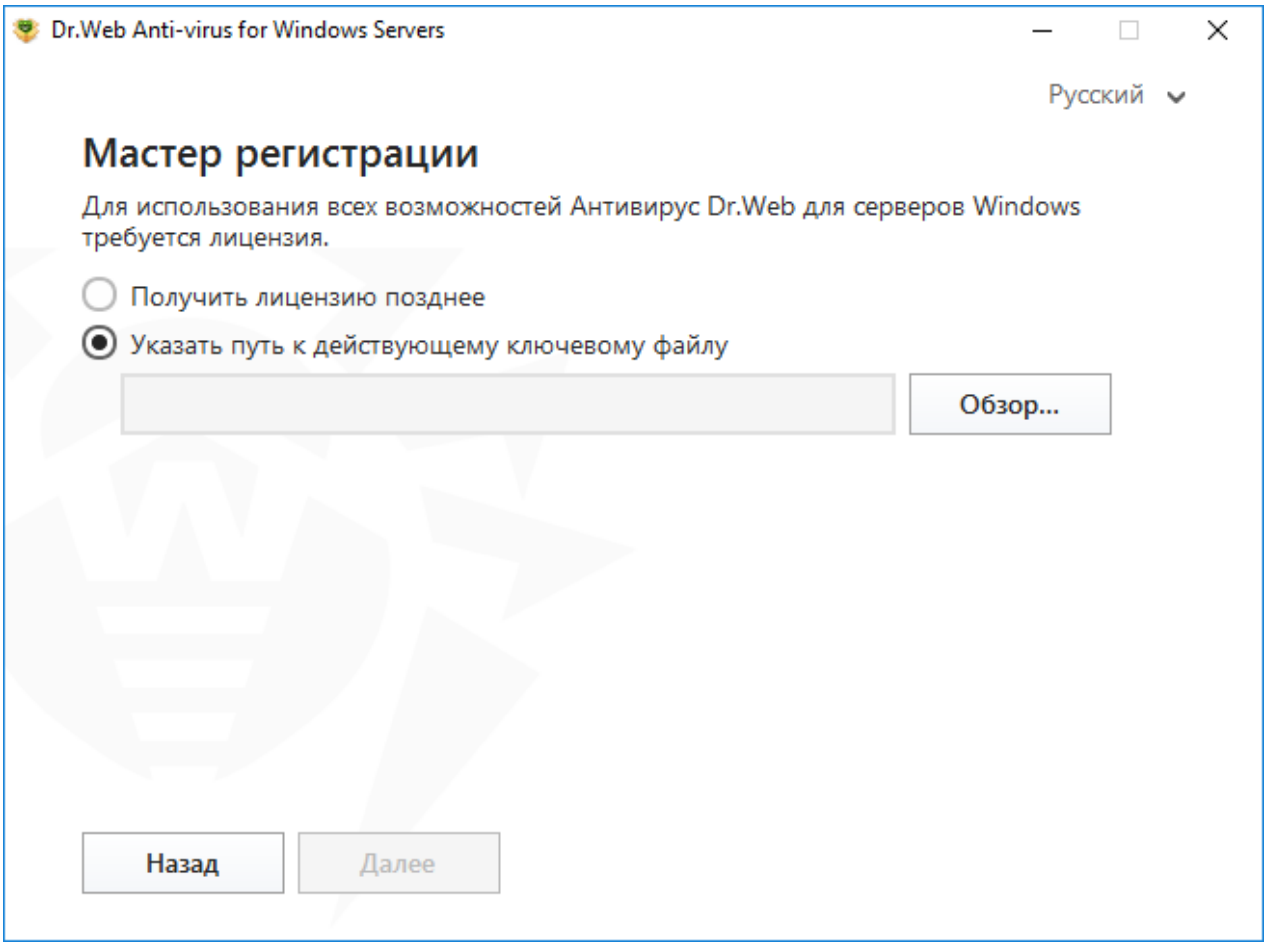

Рисунок 8. Установка. Мастер регистрации

2. Продолжите установку продукта, следуя инструкциям Мастера установки.

- в любое время работы продукта при помощи Менеджера лицензий:

1. В меню Dr.Web выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать**.
2. Откроется окно Активации лицензии. Нажмите кнопку **Ключевой файл**.

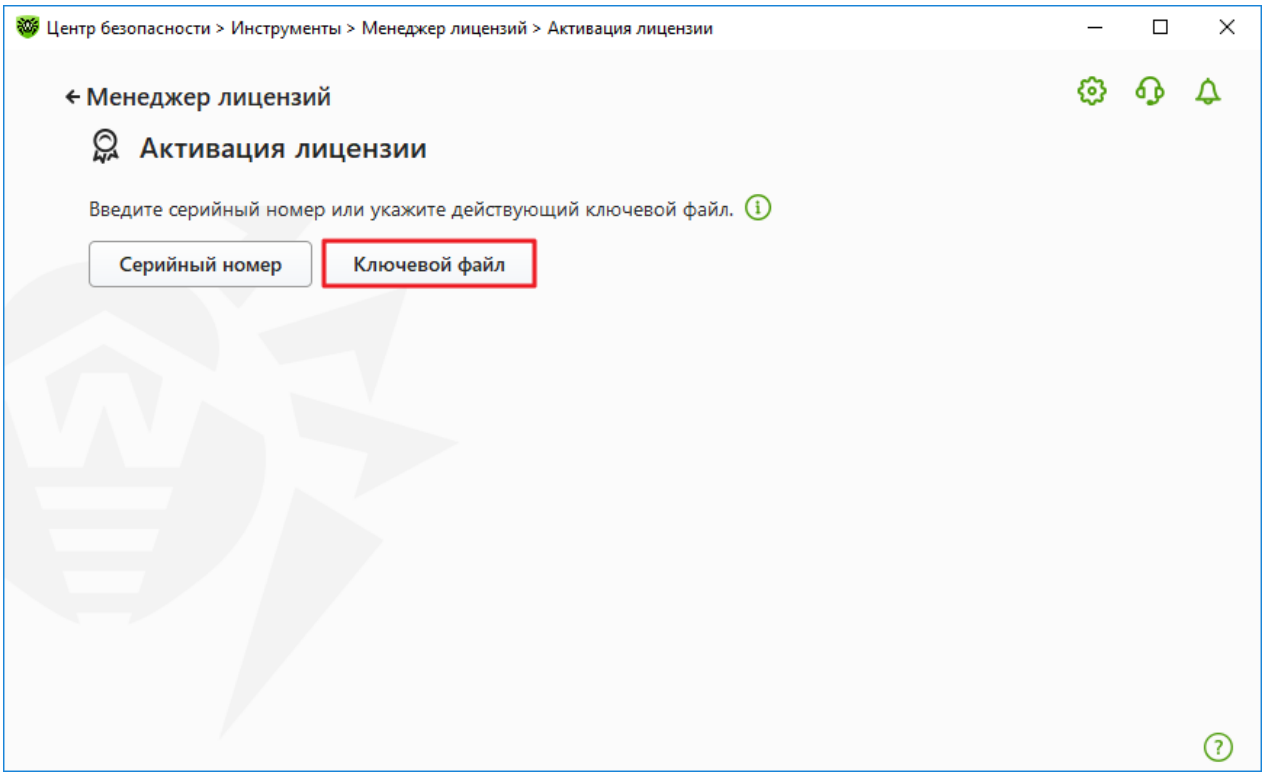

Рисунок 9. Доступ к окну ввода ключевого файла

3. В открывшемся окне нажмите кнопку **Обзор**, чтобы указать путь к ключевому файлу.

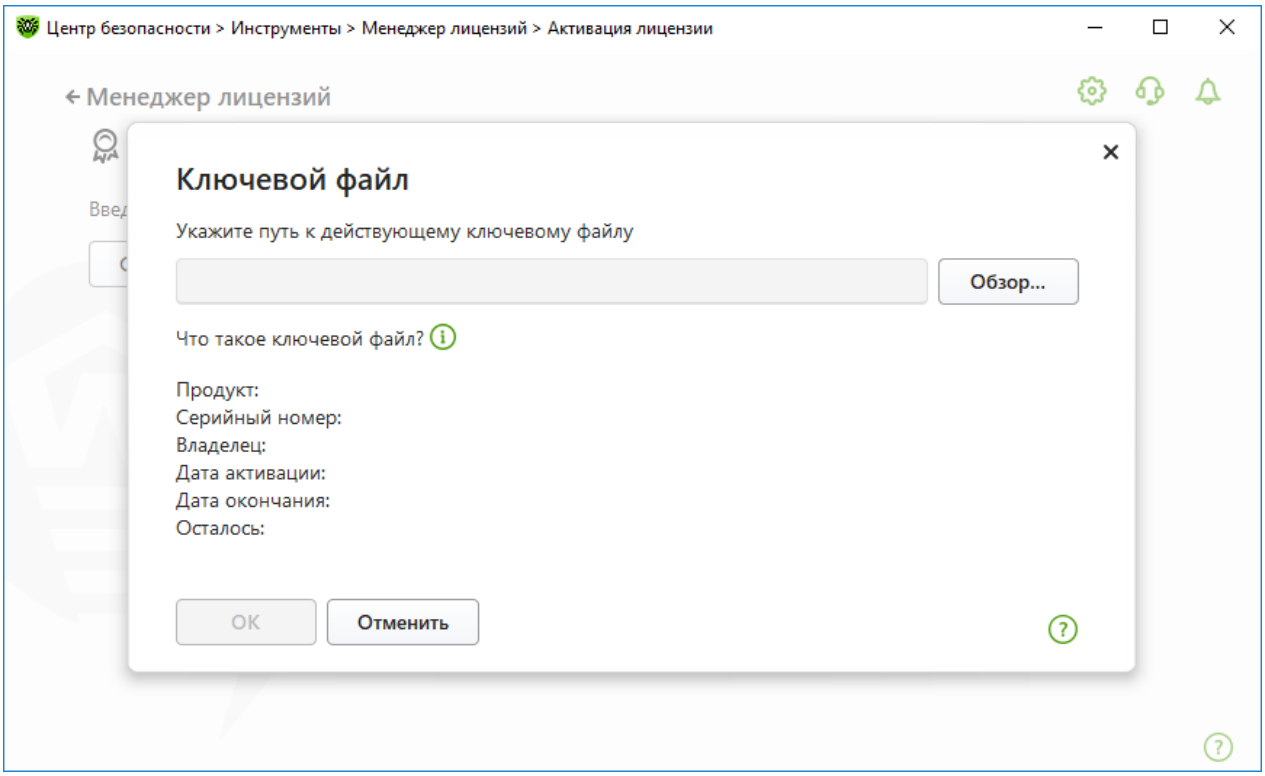

Рисунок 10. Активация при помощи ключевого файла

4. Нажмите кнопку **OK**, чтобы закрыть окно и вернуться к Менеджеру лицензий.

5.2. Продление лицензии

Вы можете продлить текущую лицензию с помощью Мастера продлений на сайте компании «Доктор Веб».

Чтобы продлить текущую лицензию при помощи Менеджера лицензий

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

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

При длительном ожидании окно активации автоматически закроется с выведением сообщения об ошибке.

Не закрывайте окно активации до завершения продления. Если по какой-либо причине окно было закрыто, лицензию можно будет активировать только с помощью ключевого файла.

Если продление лицензии завершилось неудачно, выводится сообщение об ошибке. Проверьте подключение к интернету и нажмите кнопку **Повторить**.

Чтобы активировать лицензию

1. Откройте окно Менеджера лицензий, выбрав пункт **Лицензия** в меню Dr.Web. Нажмите кнопку **Активировать**.
2. В открывшемся окне нажмите кнопку **Серийный номер** или **Ключевой файл**. Введите серийный номер или укажите путь к ключевому файлу. Пользователи Windows Server 2003 могут активировать лицензию только при помощи ключевого файла.

Подробные инструкции по активации лицензии доступны в разделах Активация при помощи серийного номера и Активация при помощи ключевого файла.

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

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

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

Возможные вопросы

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

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

Рекомендуется удалить старую лицензию из продукта. Для этого:

1. В режиме администратора в меню Dr.Web выберите пункт **Лицензия**. Откроется окно Менеджера лицензий.
2. Нажмите кнопку **Подробнее**, при этом откроется окно Сведений о лицензии.
3. В выпадающем списке выберите лицензию, на основе которой было сделано продление, и нажмите кнопку .

5.3. Ключевой файл

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

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

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

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

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

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

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

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

Рекомендуется сохранять ключевой файл до истечения срока действия лицензии.

6. Меню программы

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

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

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

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

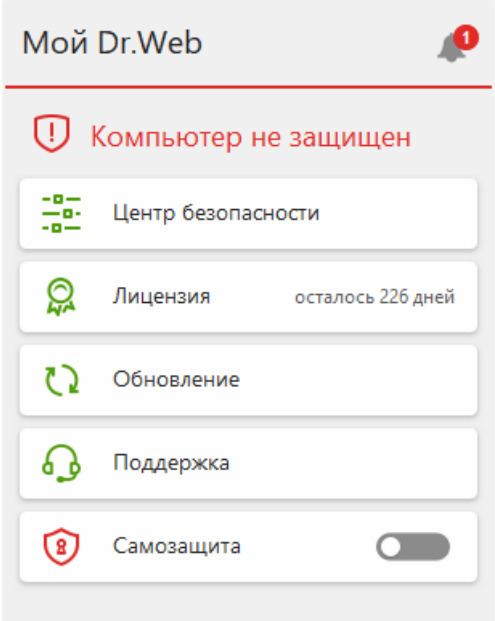

Рисунок 11. Меню программы

Пункты меню программы

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

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

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

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

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

Поддержка. Открывает окно поддержки.

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

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

Возможные состояния программы

Значок Dr.Web отражает текущее состояние программы:

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

7. 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**.

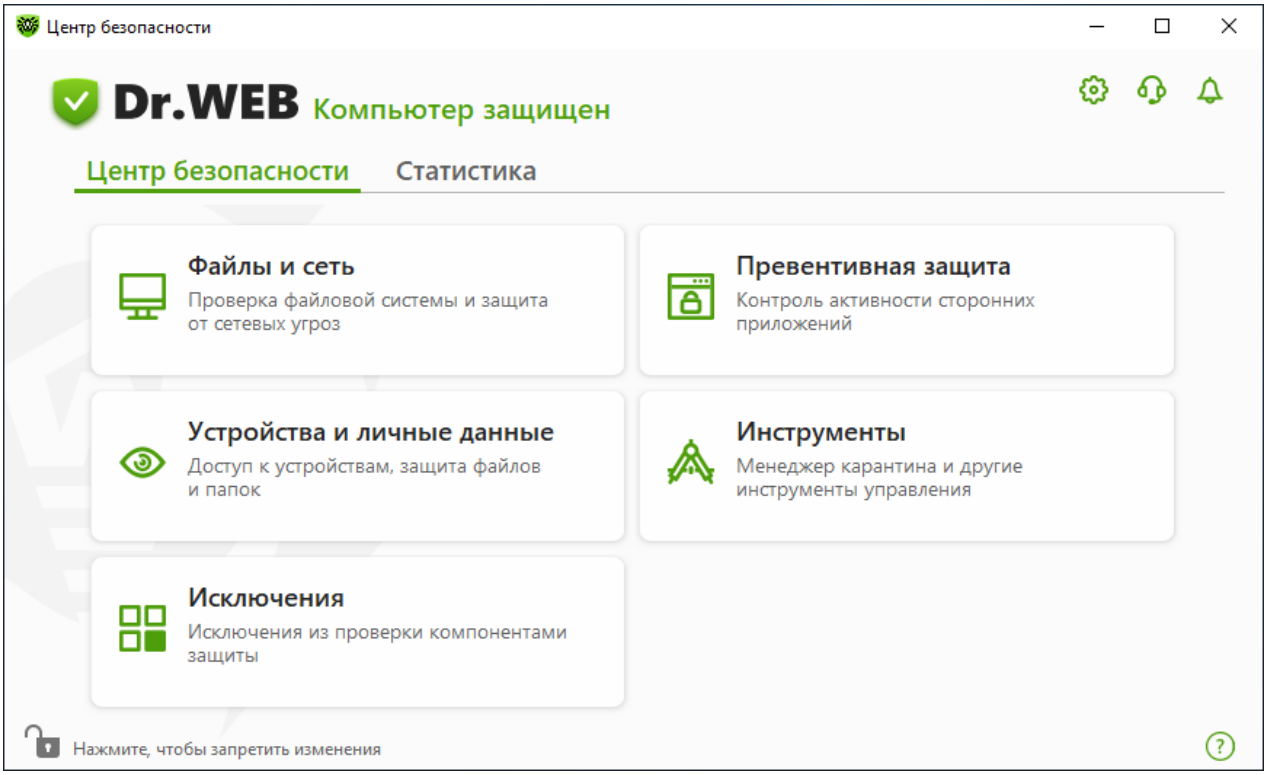

Рисунок 12. Окно Центр безопасности

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 и личные данные;
- Инструменты;
- Исключения;

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

Режим администратора

Для 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 группе настроек **Инструменты**. 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.

Статусы защиты

В верхней части окна отображается статус защищенности системы.

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

8. Обновление баз и программных модулей

Для обнаружения вредоносных объектов продукты Dr.Web используют вирусные базы, в которых содержится информация обо всех известных вредоносных программах. Регулярное обновление позволяет обнаруживать ранее неизвестные угрозы, блокировать их распространение, а в ряде случаев излечивать ранее неизлечимые зараженные файлы. Вирусные базы считаются устаревшими по истечении 24 часов с момента последнего успешного обновления. Помимо вирусных баз обновляются также программные модули Dr.Web и справка продукта.

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

Проверка актуальности обновлений

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

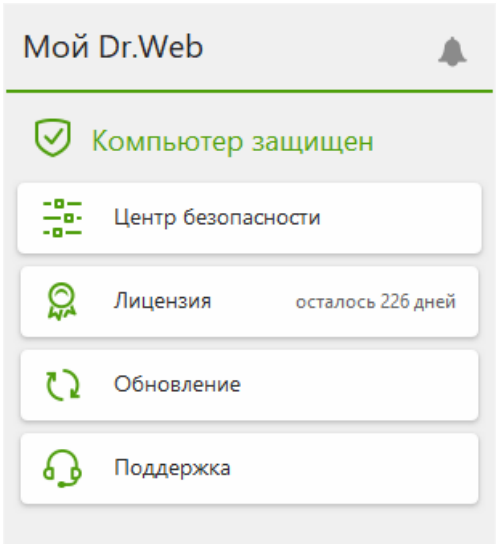

Рисунок 13. Меню Dr.Web

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

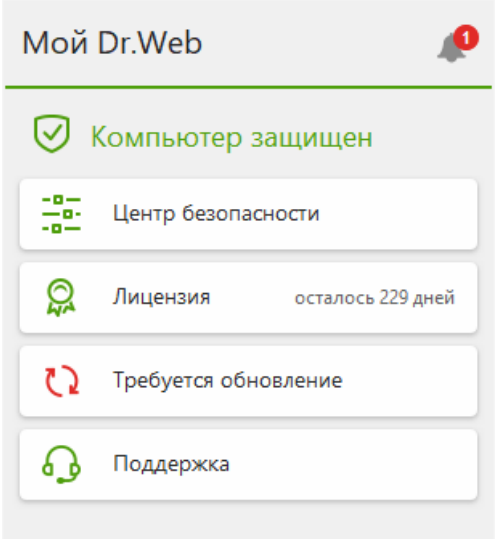

Рисунок 14. Необходимость обновления

Запуск процесса обновления

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

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

Чтобы запустить обновления из меню Dr.Web

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

Чтобы запустить обновления из командной строки

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

Отчеты и журнал статистики

Чтобы посмотреть историю обновлений во вкладке Статистика

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

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

Как настроить обновление баз и компонентов без доступа к интернету?

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

Подробнее о том, как настроить зеркало обновлений

Вы можете настроить обновление с зеркала обновлений двумя способами:

Чтобы настроить получение обновлений при подключении к антивирусной сети

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

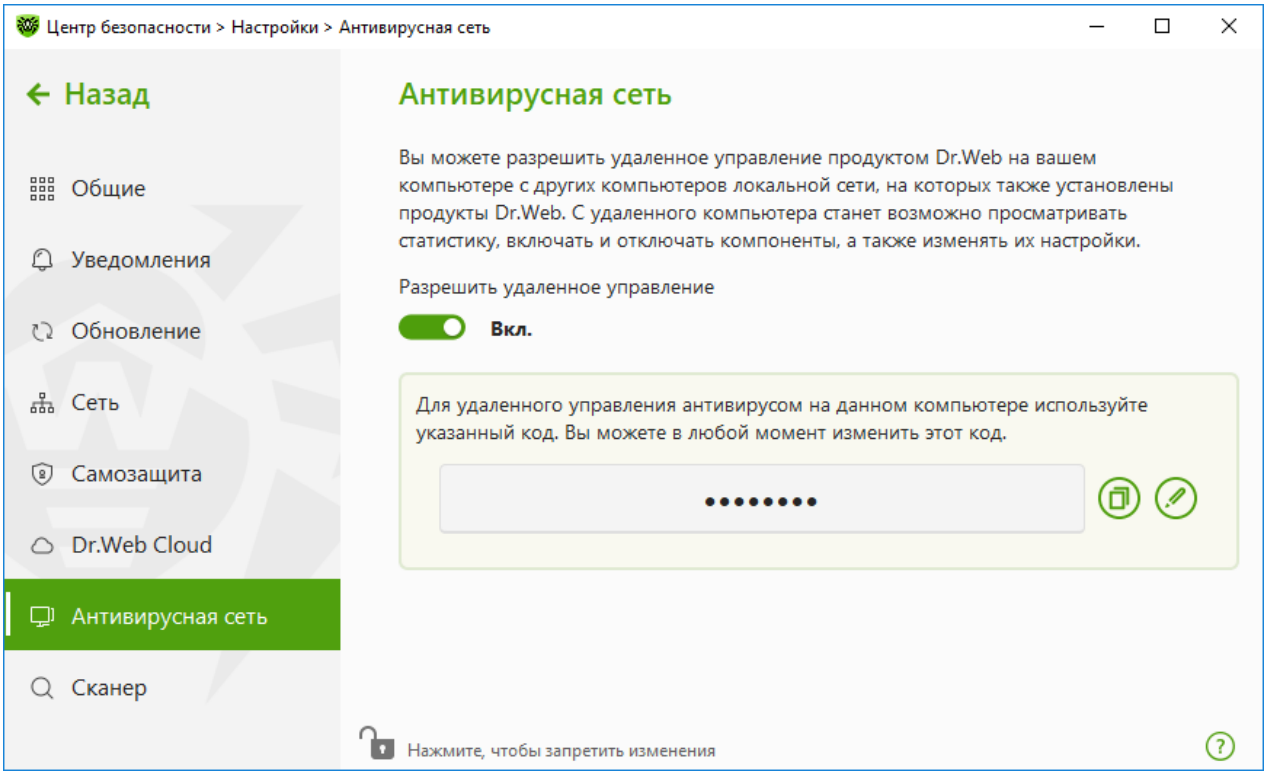

Рисунок 15. Включение удаленного доступа

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

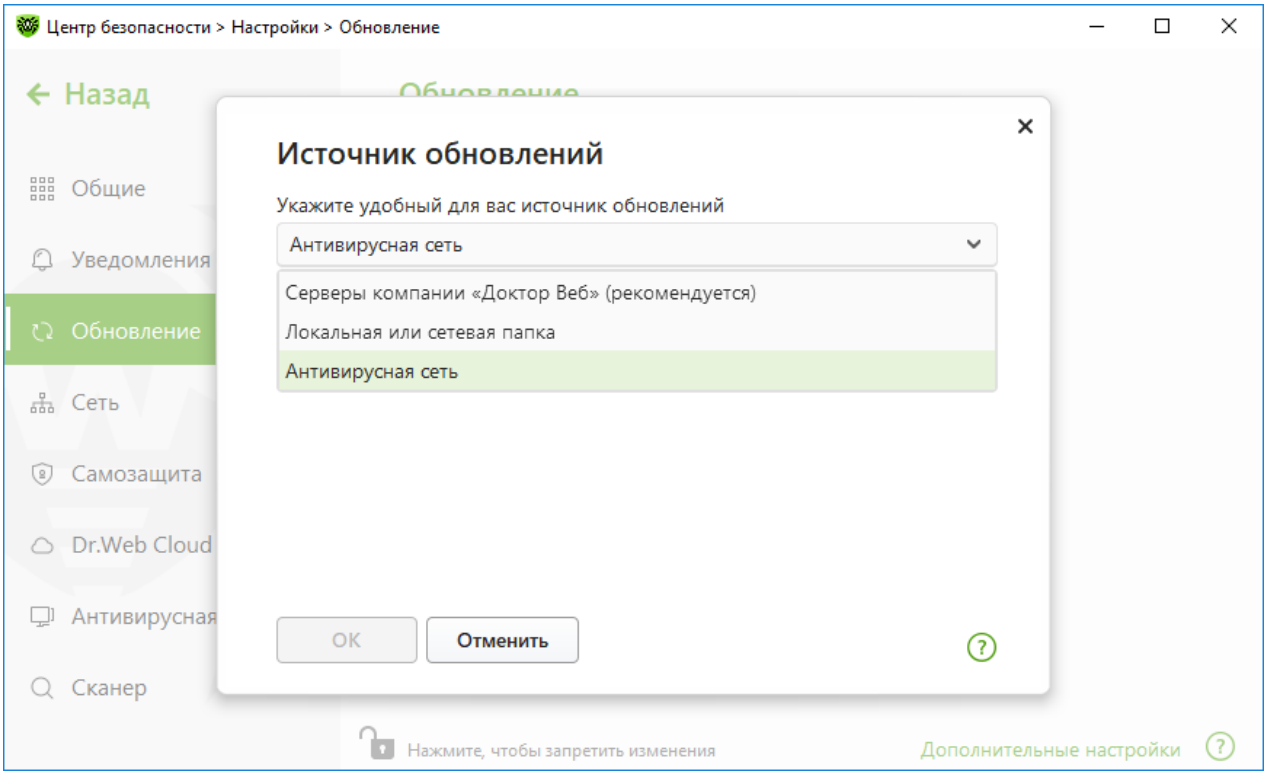

Рисунок 16. Выбор источника обновлений

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

Чтобы настроить получение обновлений из локальной или сетевой папки

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

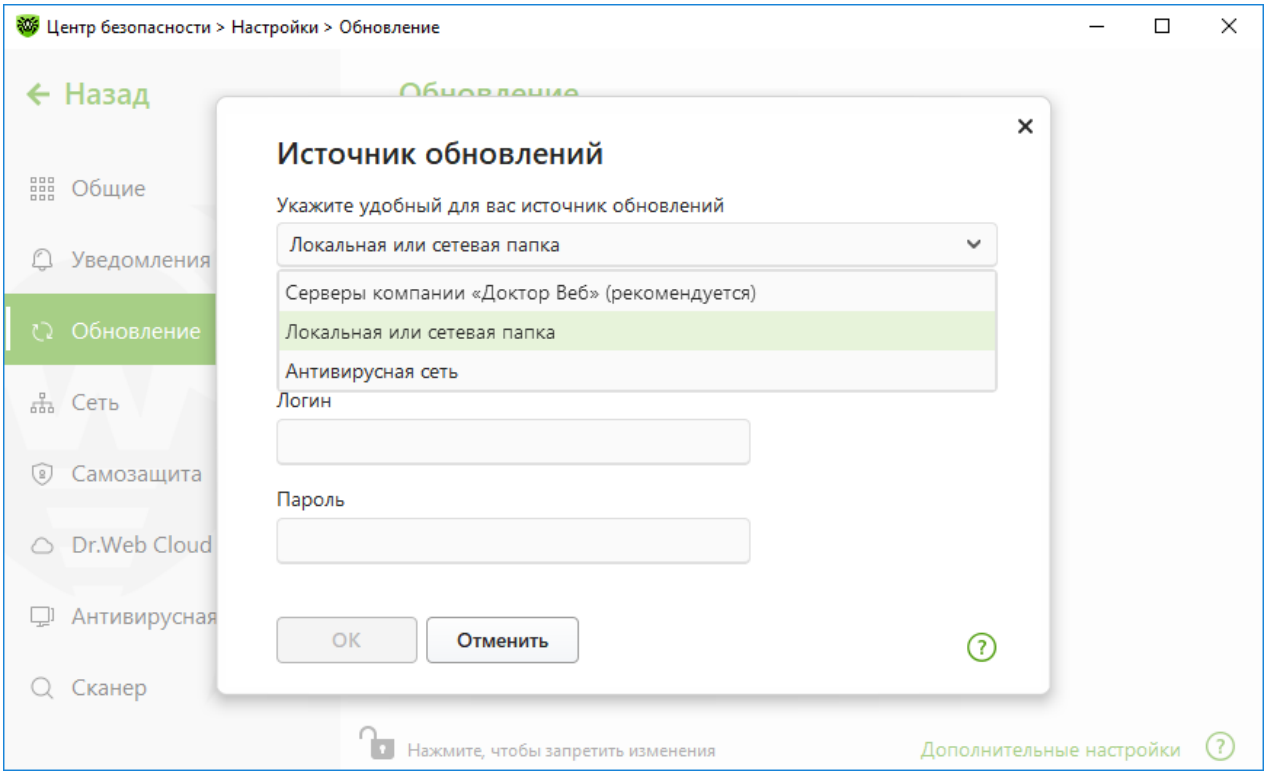

Рисунок 17. Выбор источника обновлений

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

9. 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.

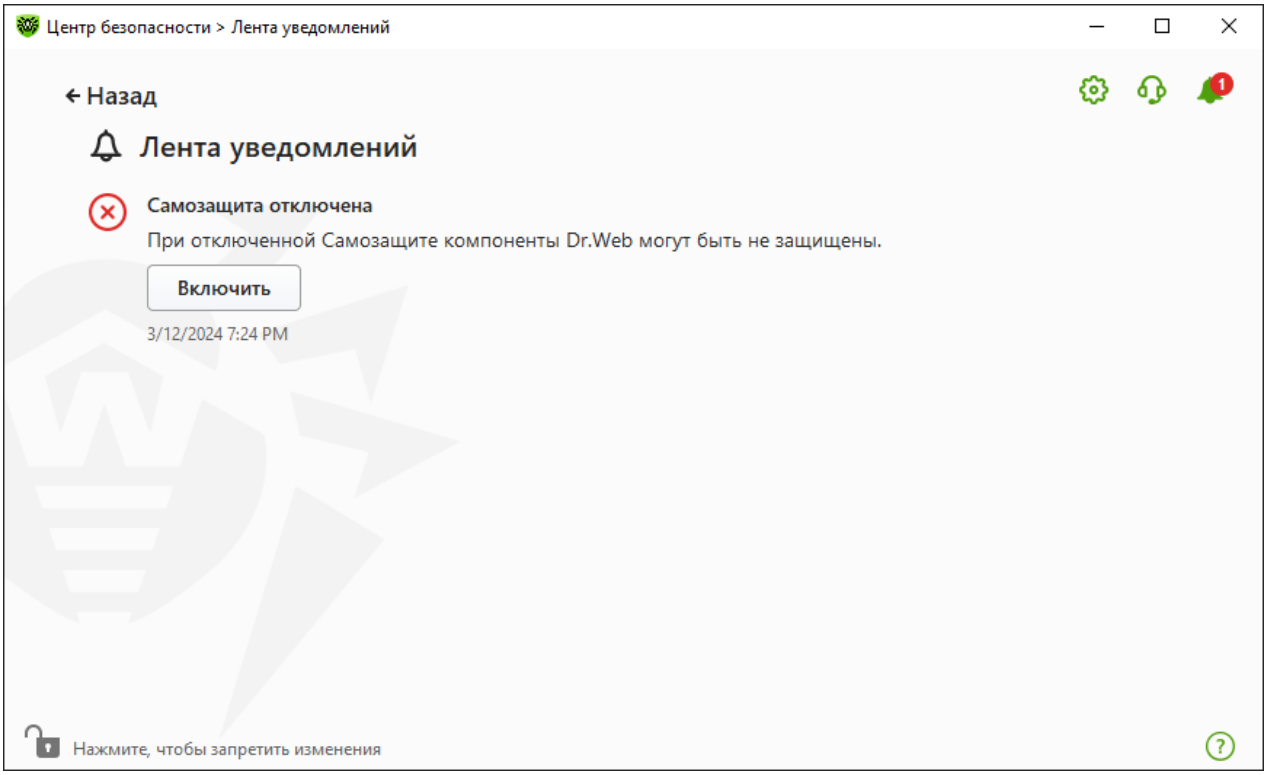

Рисунок 18. Окно ленты уведомлений

Срок хранения уведомлений

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

Типы уведомлений

Критические уведомления	
Лицензия	• Действующая лицензия не найдена. • Текущая лицензия заблокирована.
Угрозы	• Обнаружена угроза. • Требуется перезагрузка для обезвреживания угроз. • Вирусные базы устарели.
Запрет доступа к объектам и устройствам	• Устройство заблокировано в соответствии с настройками.
Важные уведомления	
Лицензия	• Срок действия лицензии истекает. • Текущая лицензия заблокирована.
Обновление	• Требуется перезагрузка, чтобы обновления вступили в силу.
Маловажные информационные уведомления	
Новая версия	• Доступна новая версия продукта.

Настройки отображения

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

10. Настройки программы

Чтобы перейти к изменению настроек программы

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

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

В этом разделе:

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

10.1. Общие настройки

К общим настройкам относятся следующие:

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

Чтобы открыть общие настройки

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

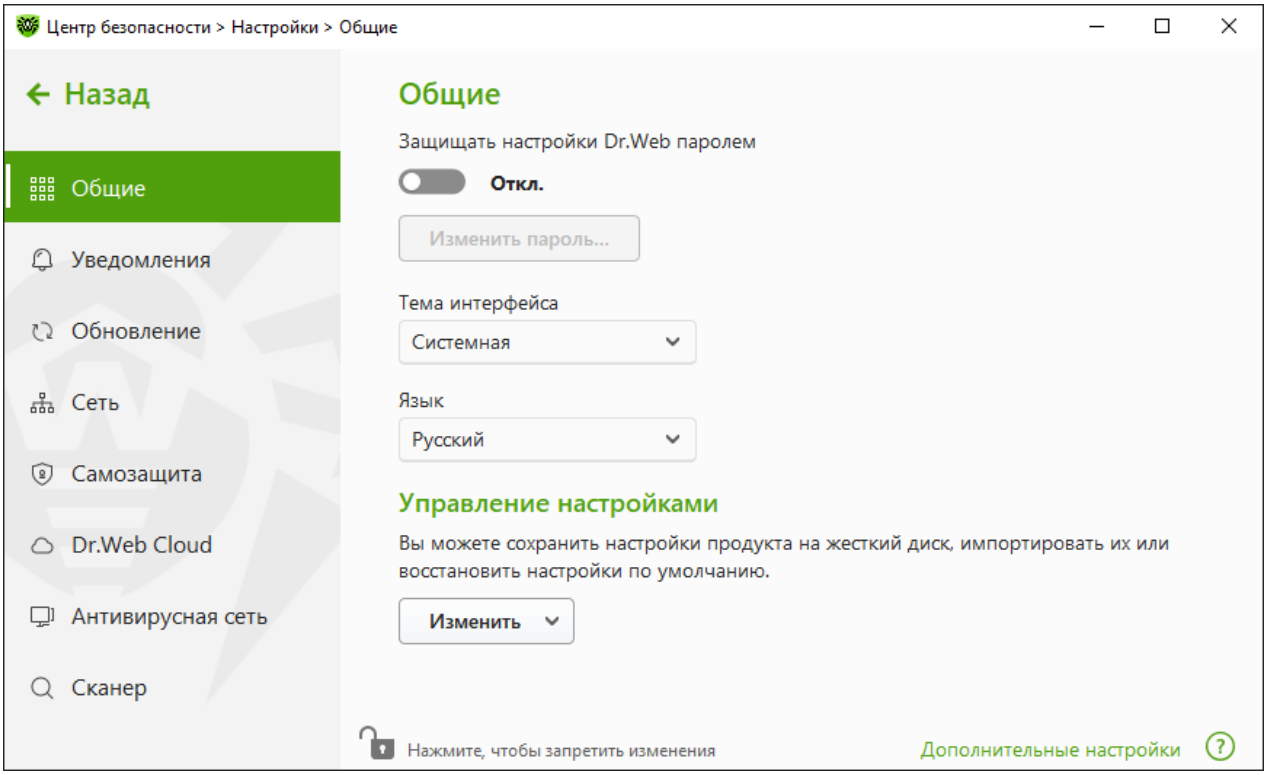

Рисунок 19. Общие настройки

10.1.1. Защита настроек программы паролем

Вы можете ограничить доступ к настройкам Dr.Web на вашем компьютере при помощи пароля. Пароль не ограничен по длине и может включать в себя любую комбинацию букв, цифр и специальных символов. Для более надежной защиты используйте пароль, состоящий из 10 или более различных знаков. 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 .

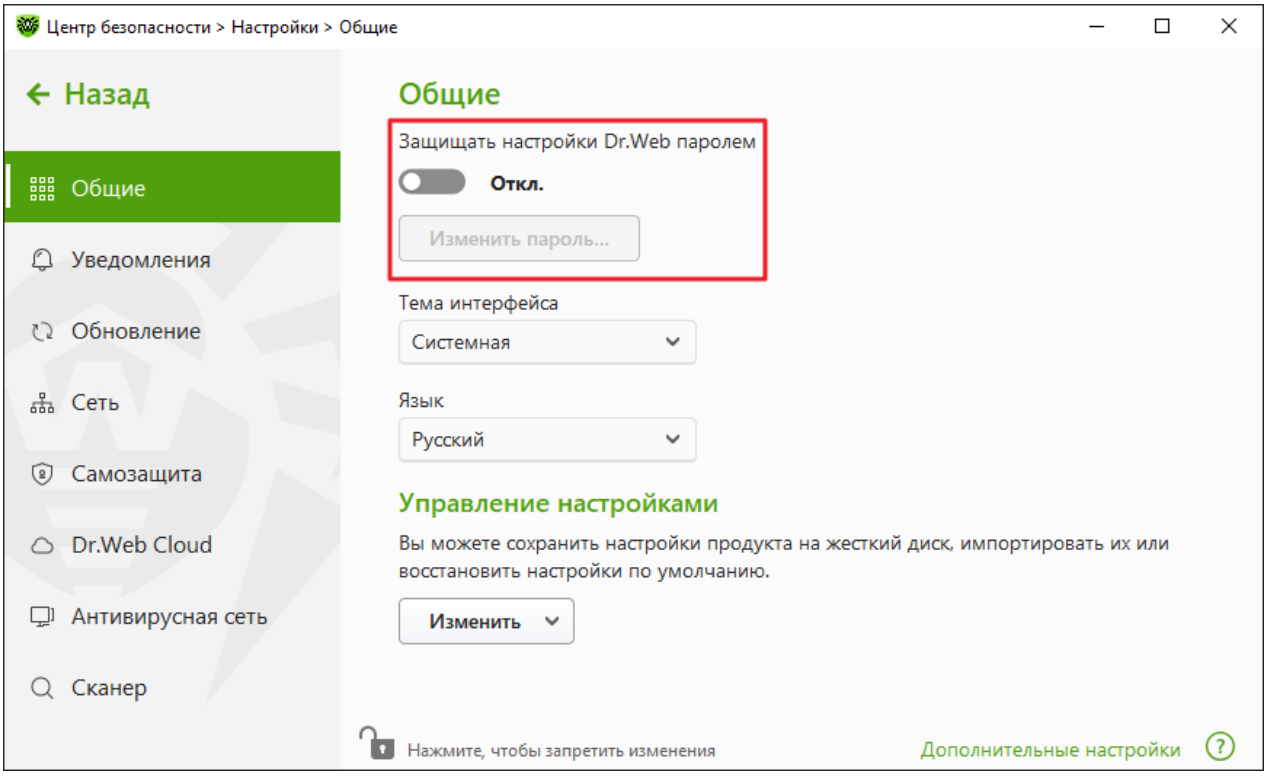

Рисунок 20. Защита настроек паролем

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

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

10.1.2. 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.

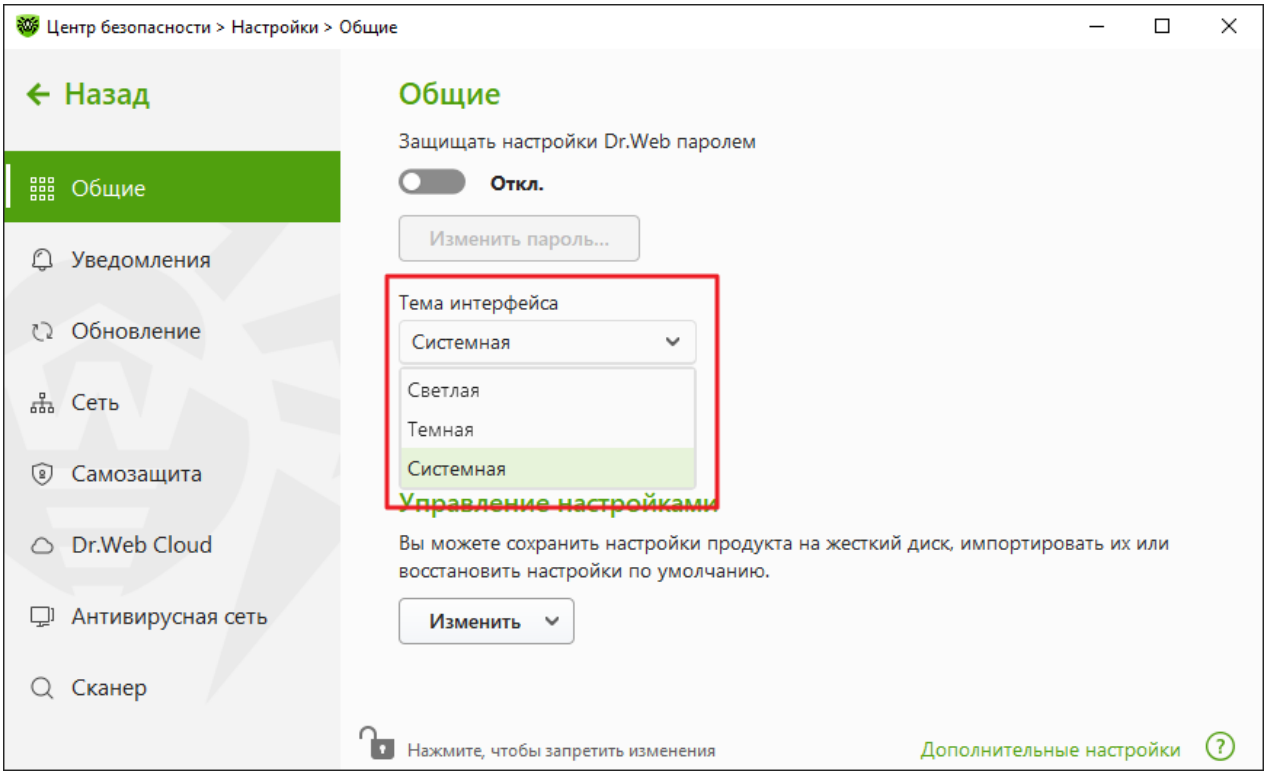

Рисунок 21. Выбор цвета темы интерфейса

Темная тема доступна только на компьютерах с операционной системой 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.

10.1.3. 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.

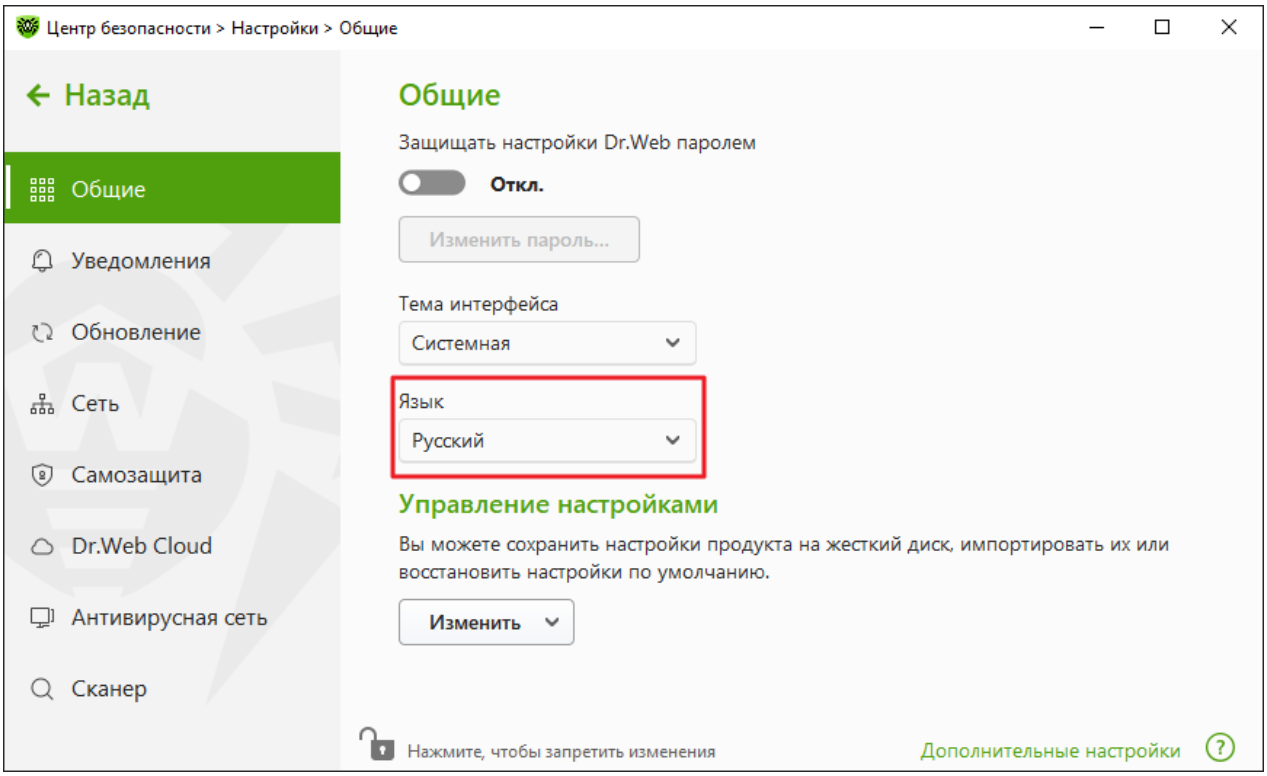

Рисунок 22. Выбор языка программы

10.1.4. Управление настройками Dr.Web

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

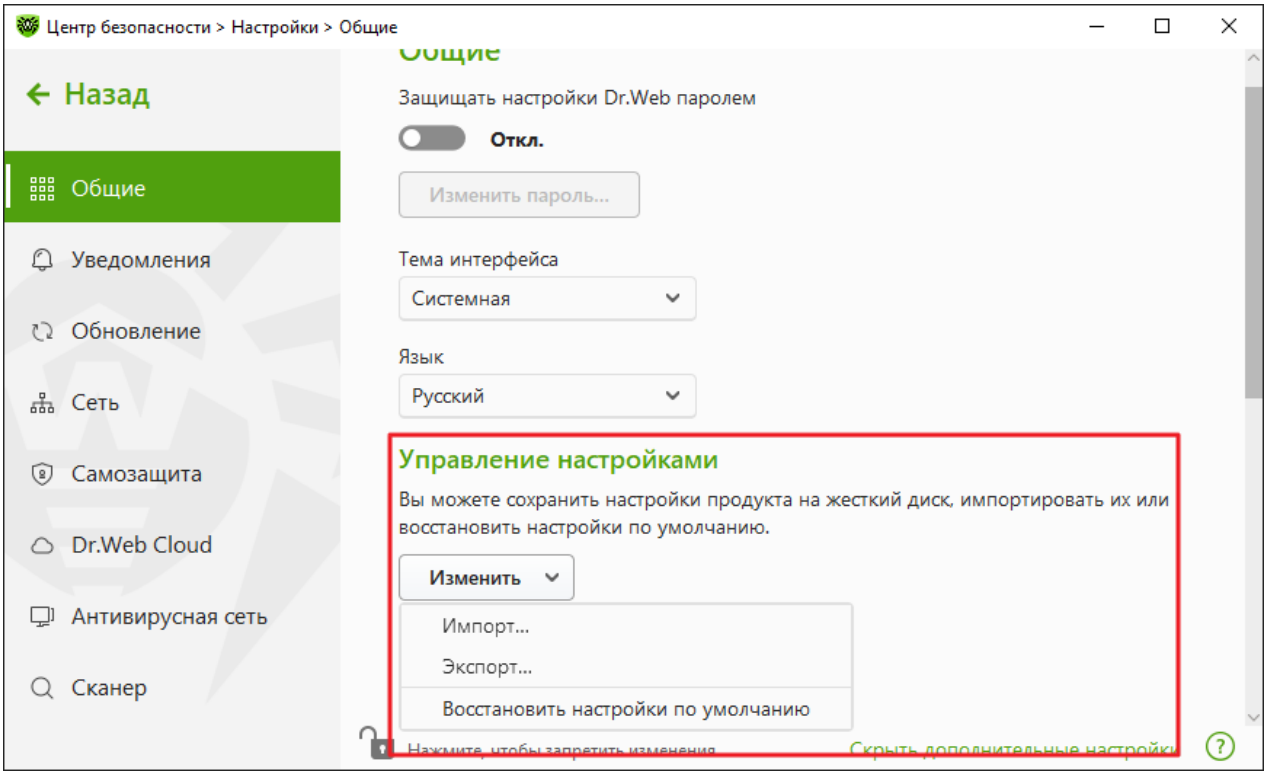

Рисунок 23. Управление настройками

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

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

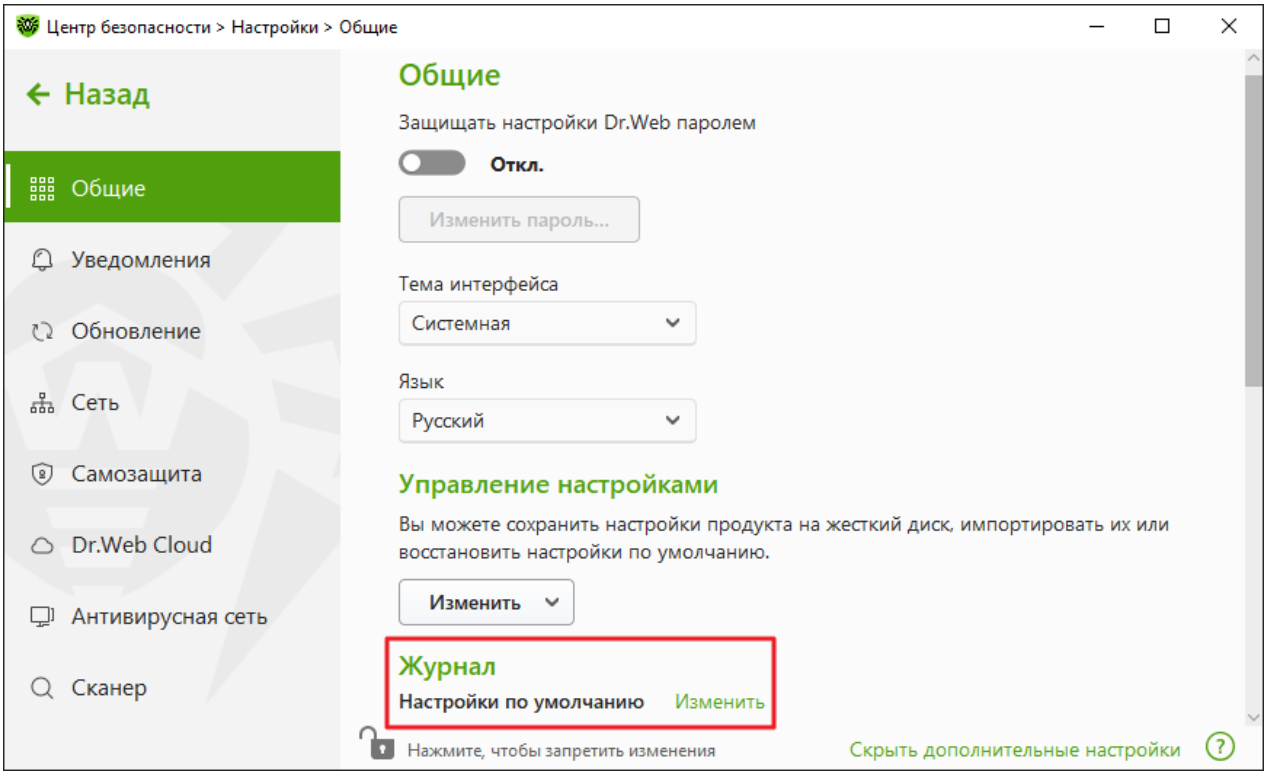

Рисунок 24. Общие настройки. Журнал

Откроется окно настроек ведения подробного журнала:

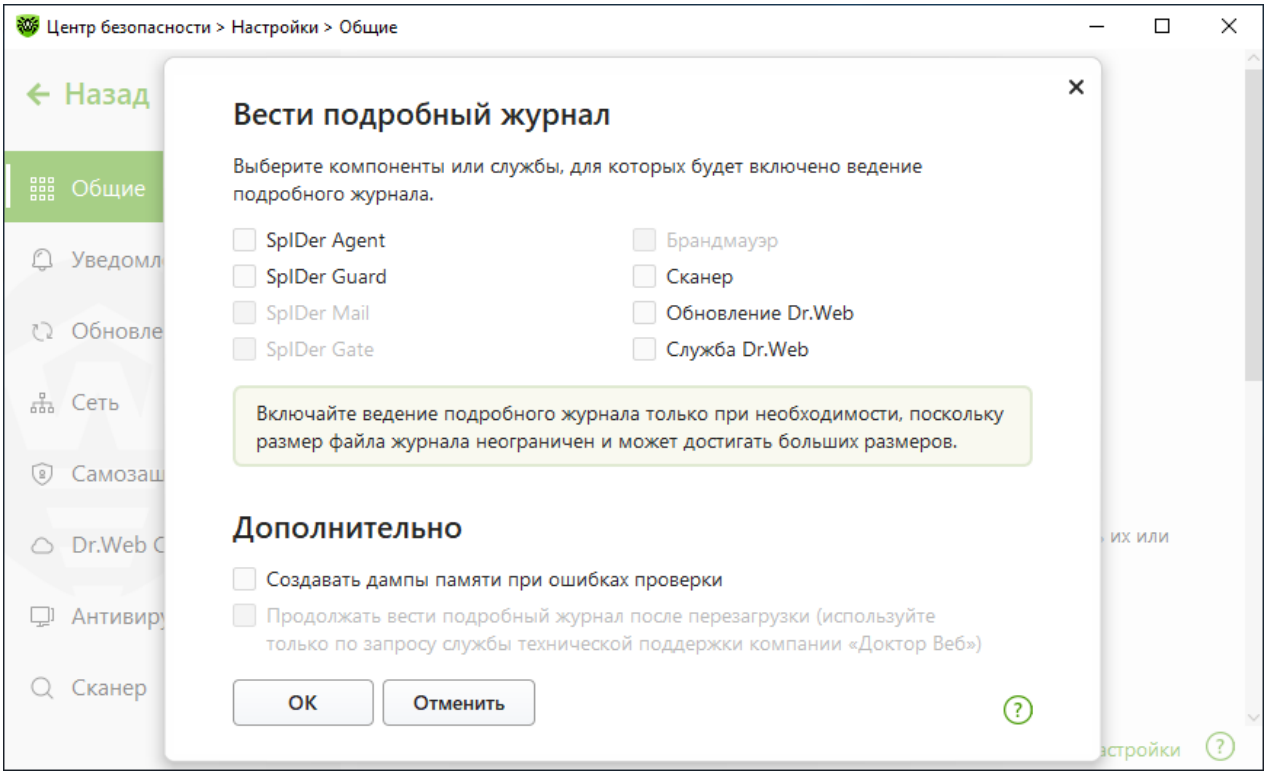

Рисунок 25. Настройки ведения журнала работы

3. Выберите компоненты, 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 антивирусной сетью, лицензионные события, состояние работы компонентов Dr.Web, управление настройками (импорт, экспорт), 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.
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.
Обновление Dr.Web	Список обновленных файлов Dr.Web и статусы их загрузки, информация о работе вспомогательных скриптов, дата и время проведения обновления, информация о перезапуске компонентов Dr.Web после обновления.
Служба Dr.Web	Информация о компонентах Dr.Web, изменение настроек компонентов, включение и выключение компонентов, события превентивной защиты, подключение к антивирусной сети.

Создание дампов памяти

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

Включение подробных журналов

При включении подробных журналов фиксируется максимальное количество информации о работе компонентов Dr.Web. Это приведет к отключению ограничения на размер файлов журнала и снизит производительность работы Dr.Web и

операционной системы. Использовать этот режим следует только при возникновении проблем в работе компонентов или по просьбе службы технической поддержки компании «Доктор Веб».

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

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

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

10.1.6. Настройки карантина

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

Чтобы изменить настройки хранения обнаруженных угроз

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

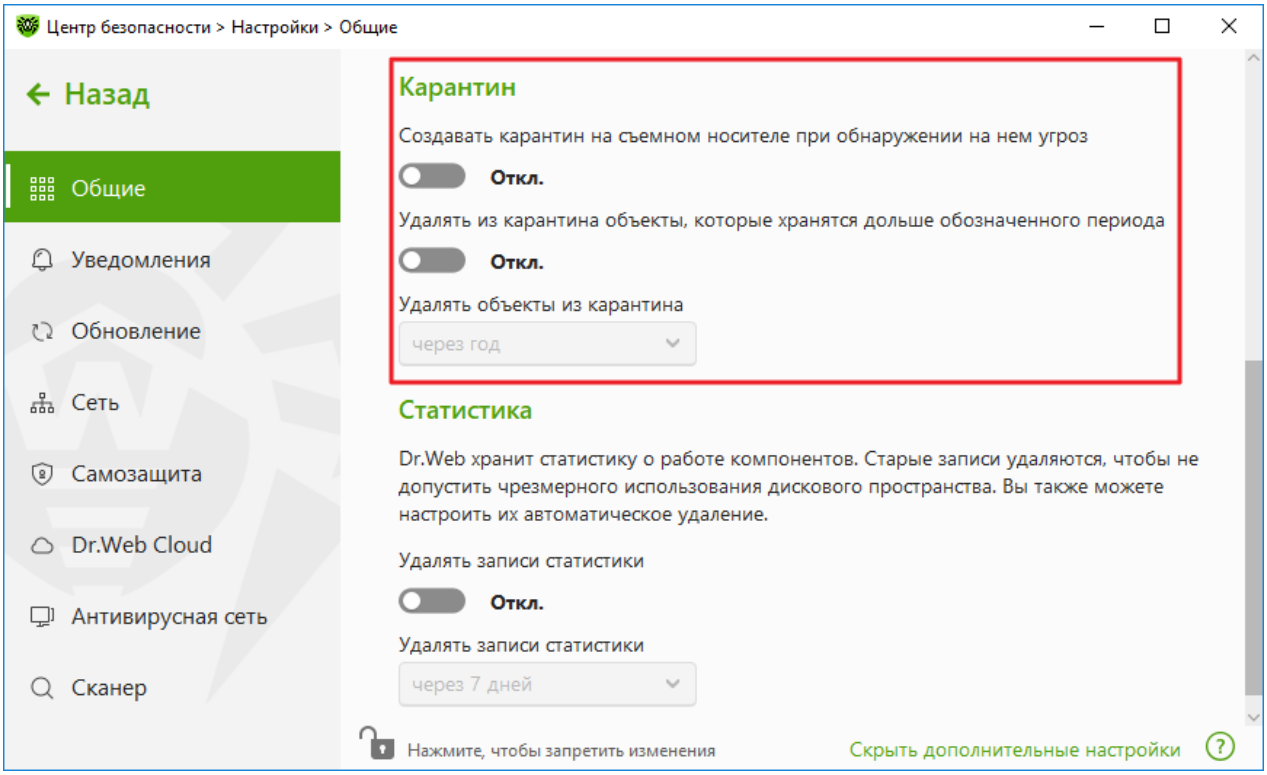

Рисунок 26. Настройки карантина

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

Создание карантина на съемном носителе

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

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

Автоматическое удаление объектов из карантина

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

10.1.7. Автоматическое удаление записей статистики

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

Чтобы включить или отключить автоматическое удаление записей статистики

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

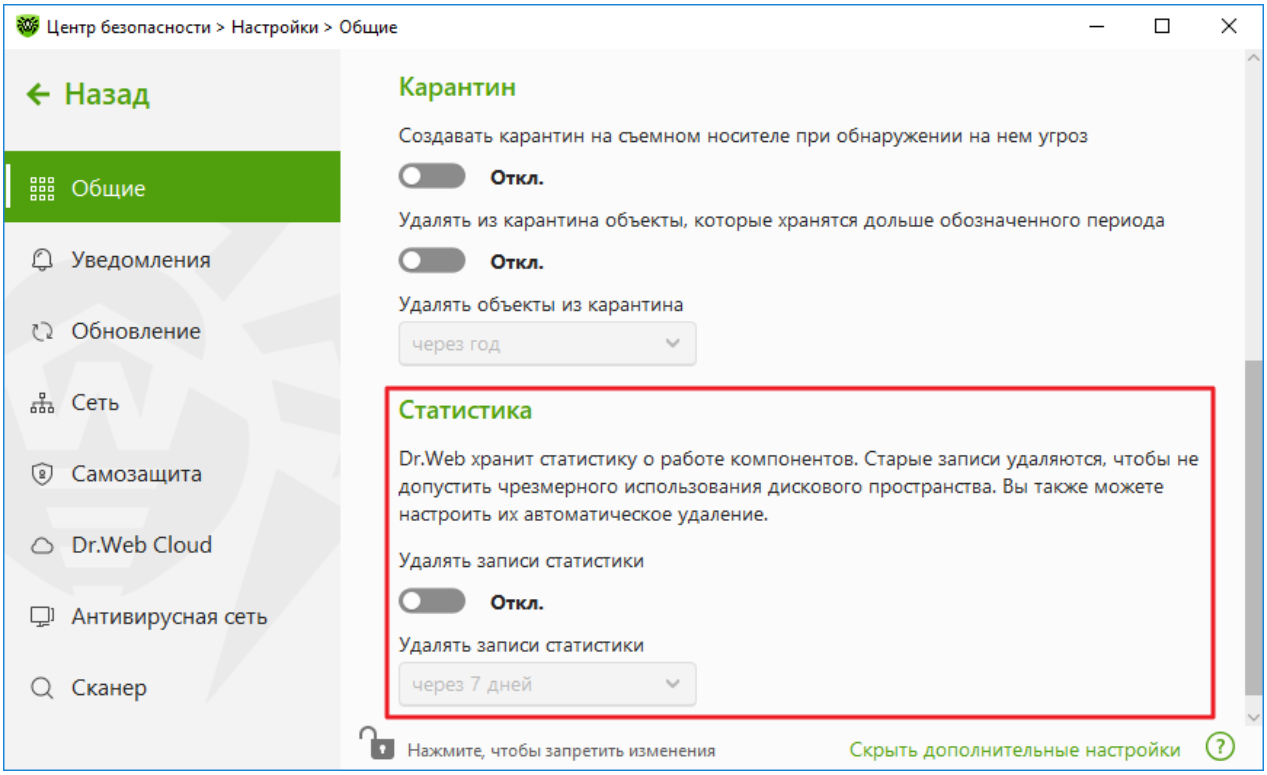

Рисунок 27. Настройки статистики

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

10.2. Настройки уведомлений

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

В этом разделе:

- Настройка параметров уведомлений
- Настройка вывода уведомлений на экран

- Настройка отправки уведомлений по почте

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

Чтобы открыть настройки уведомлений

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

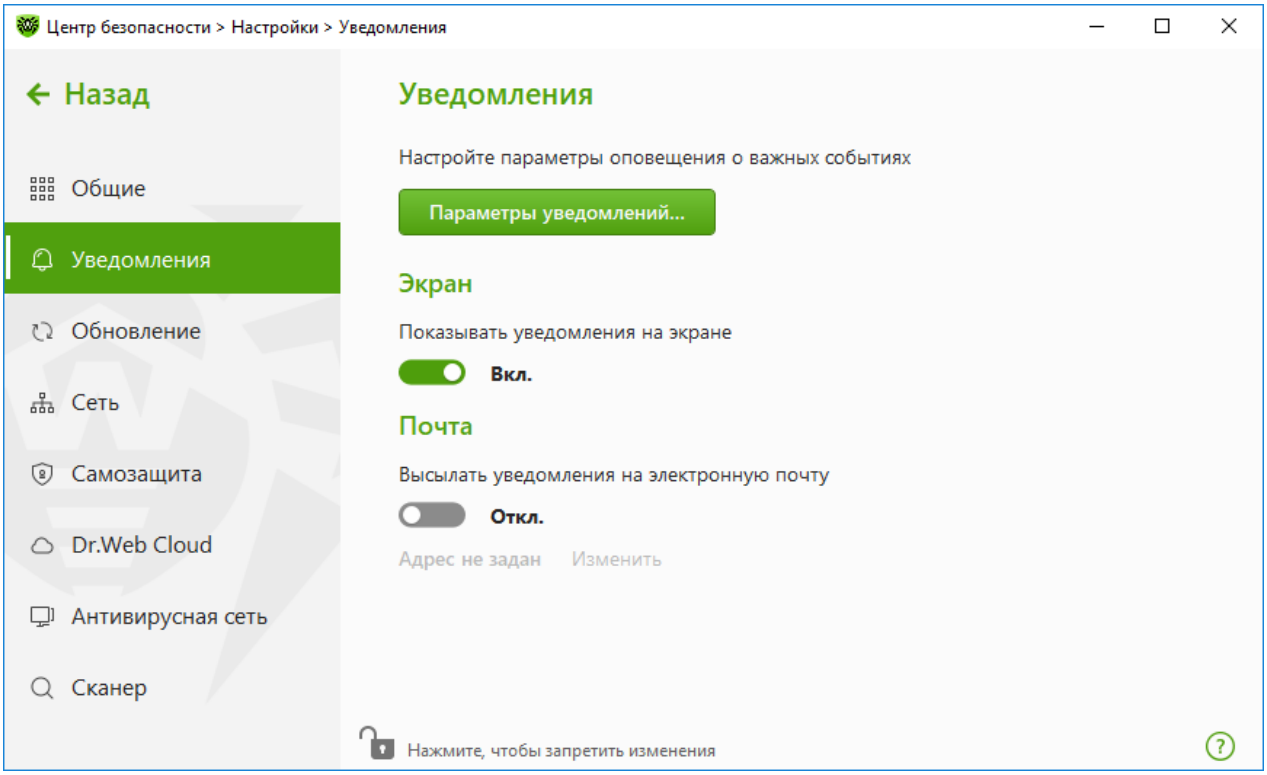

Рисунок 28. Настройки уведомлений

Чтобы настроить параметры уведомлений

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

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

Тип уведомления	Описание
Обнаружена угроза	Уведомления об угрозах, обнаруженных SpIDer Guard. По умолчанию уведомления включены.
Важные уведомления	Важные уведомления о следующих событиях: • Вирусные базы устарели. • 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. • Информация об обновлениях и поддержке продукта. По умолчанию уведомления включены.
Малозначительные уведомления	Малозначительные уведомления о следующих событиях: • Успешное обновление. • Ошибка обновления. • Процессу запрещено изменение содержимого папки. По умолчанию уведомления выключены, кроме уведомления о запрещении процессу изменения содержимого папки.
Лицензия	Уведомления о следующих событиях: • Срок действия лицензии истекает. • Действующая лицензия не найдена. • Текущая лицензия заблокирована.

3. При необходимости задайте дополнительные параметры отображения экранных оповещений:

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

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

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

- установка приоритетных обновлений, для которых требуется перезагрузка;
- перезагрузка для завершения обезвреживания угроз;
- автоматическая перезагрузка;
- запрос на разрешение процессу модификации объекта;
- успешное подключение к удаленному компьютеру в Антивирусной сети;
- подключена новая клавиатура.

Уведомления, которые выводятся на экран

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

Уведомления по почте

Чтобы получать уведомления о событиях по почте

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

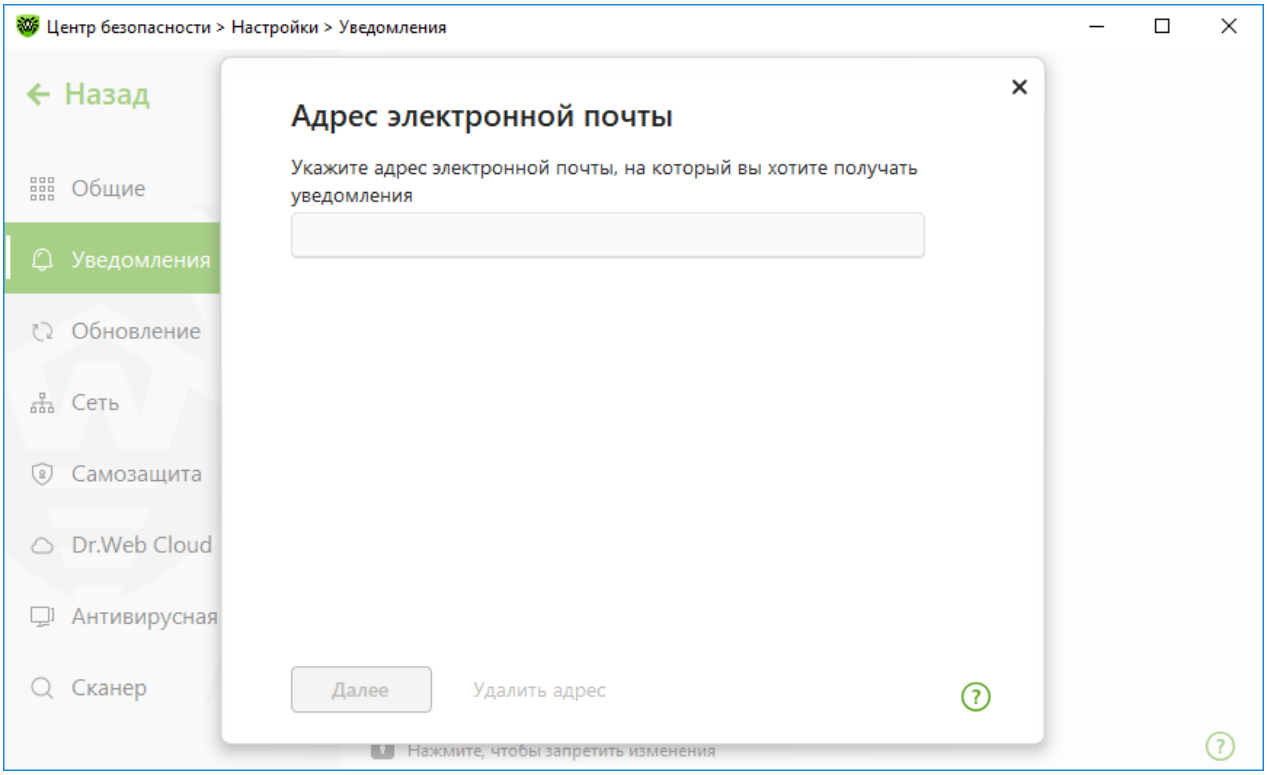

Рисунок 29. Указание адреса для почтовых уведомлений

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

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

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

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

10.3. Настройки обновления

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

Вы можете настроить следующие параметры обновления Dr.Web:

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

Чтобы открыть настройки обновления

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

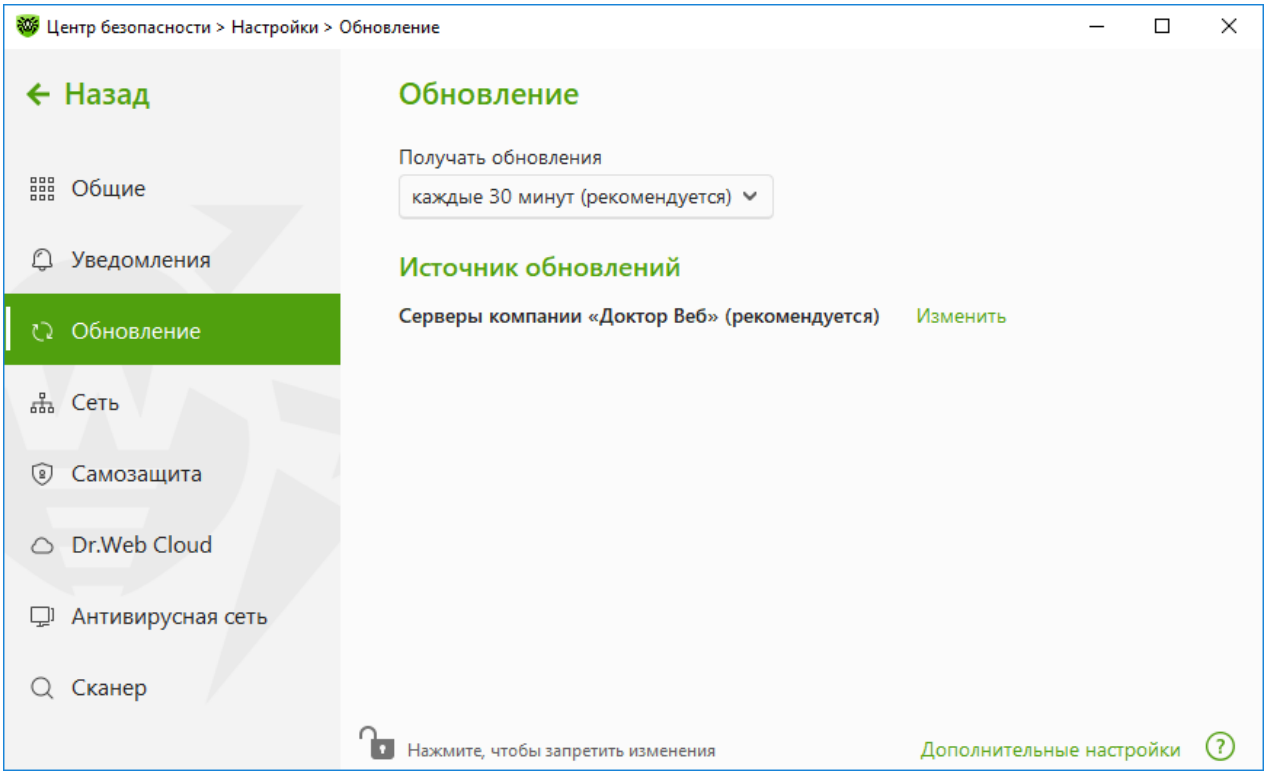

Рисунок 30. Настройки обновления

Периодичность обновлений

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

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

Настройка источника обновлений

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

Чтобы настроить удобный для вас источник обновлений

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

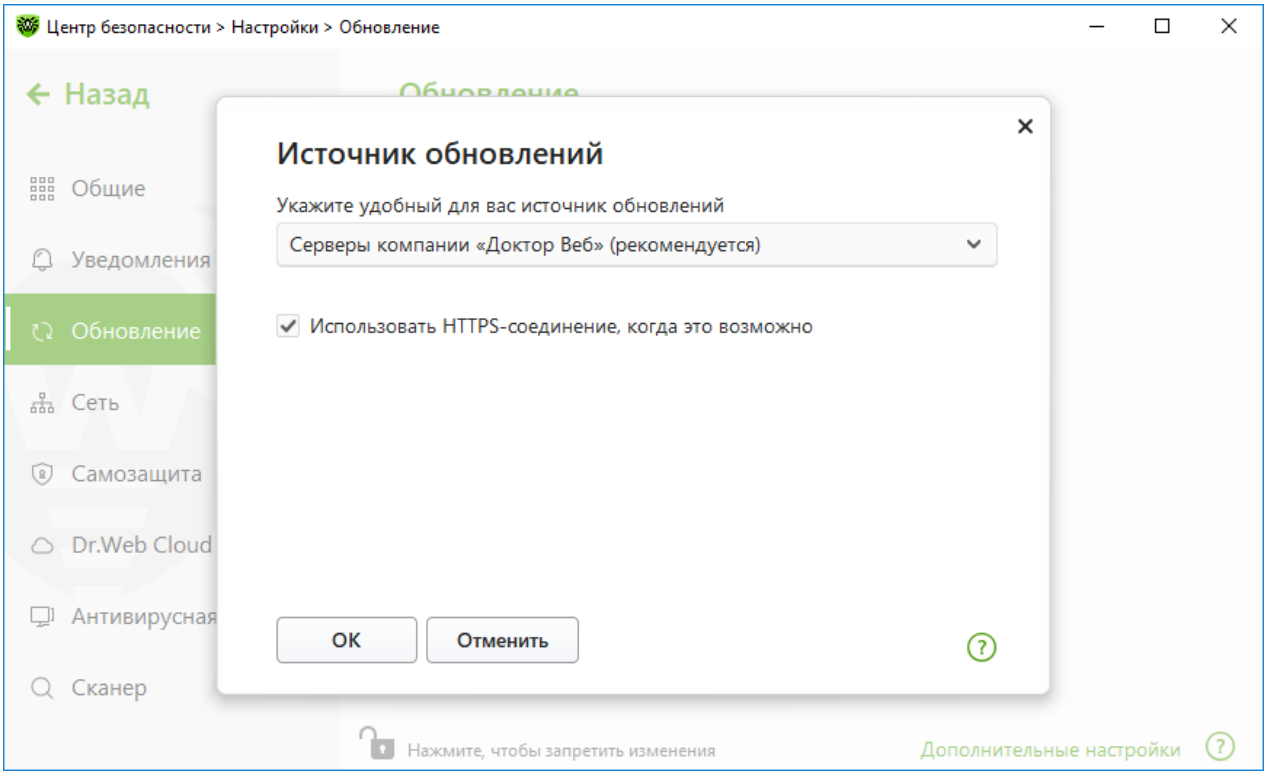

Рисунок 31. Настройка источника обновлений

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

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

Дополнительные настройки

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

Настройка обновляемых компонентов

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

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

Создание зеркала обновлений

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

Чтобы настроить ваш компьютер в качестве зеркала обновлений

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

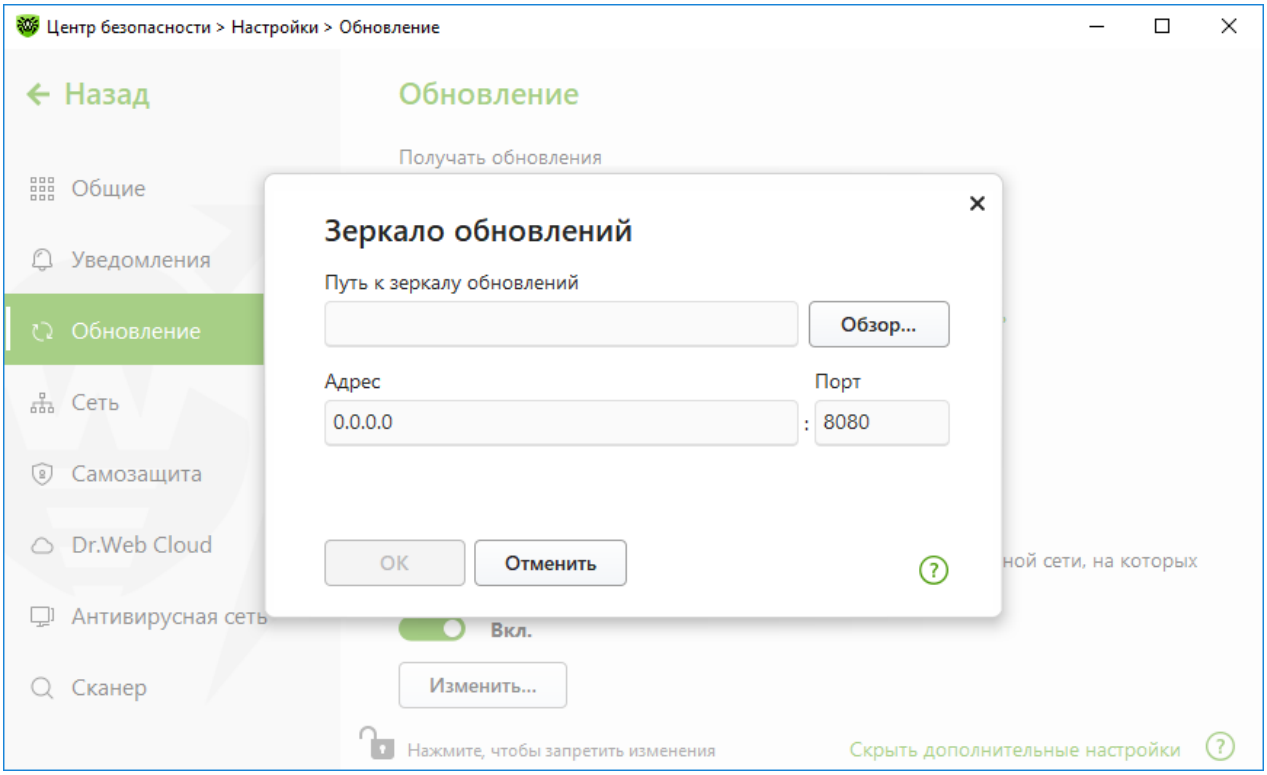

Рисунок 32. Настройка зеркала обновлений

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

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

10.4. Сеть

Вы можете настроить параметры соединения с прокси-сервером.

В этом разделе:

- Настройка соединения с прокси-сервером

Чтобы открыть настройки сети

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

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

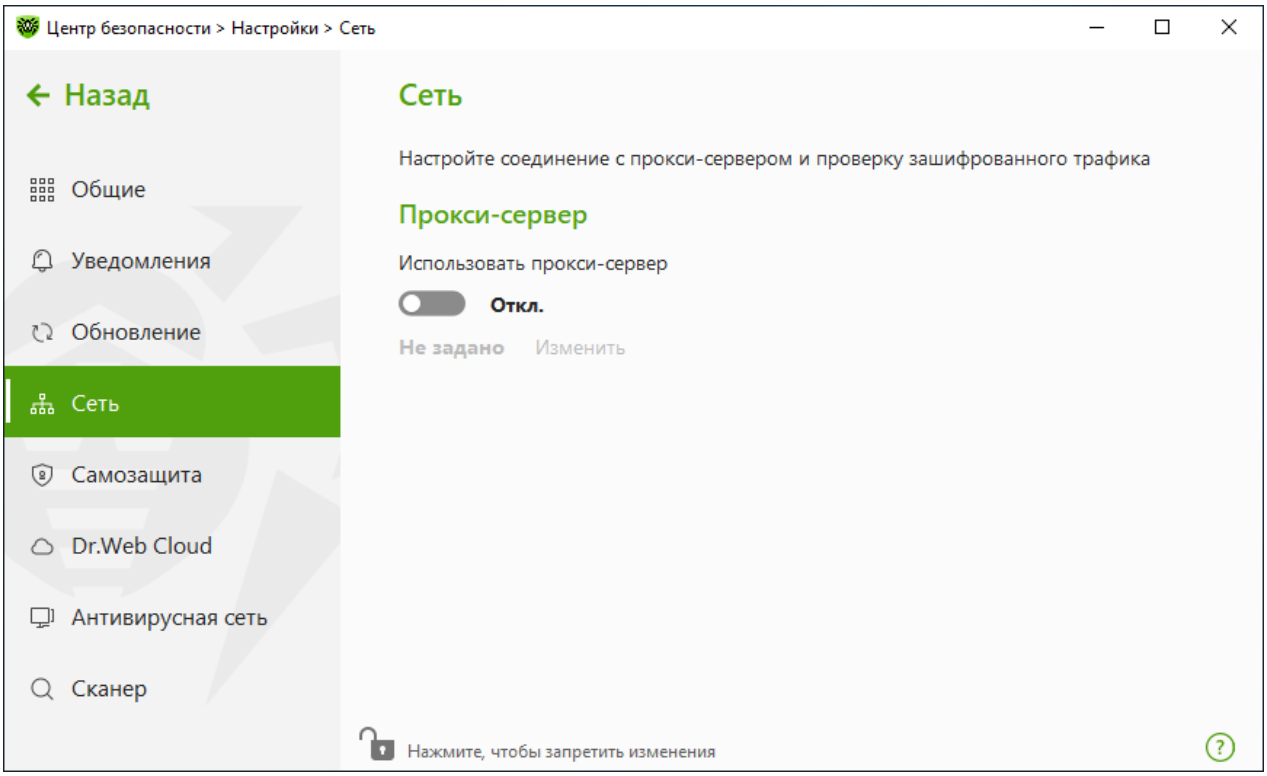

Рисунок 33. Подключение к прокси-серверу

Использование прокси-сервера

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

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

Настройка	Описание
Тип	Выберите протокол для подключения к прокси-серверу.
Адрес	Укажите адрес прокси-сервера.
Порт	Укажите порт прокси-сервера.
Логин	Укажите имя учетной записи для подключения к прокси-серверу.

Настройка	Описание
Пароль	Укажите пароль учетной записи, используемой для подключения к прокси-серверу.
Тип авторизации	Выберите тип авторизации, требуемый для подключения к прокси-серверу (только для HTTP).

10.5. Самозащита

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

В этом разделе:

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

Чтобы перейти к настройкам Самозащиты

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

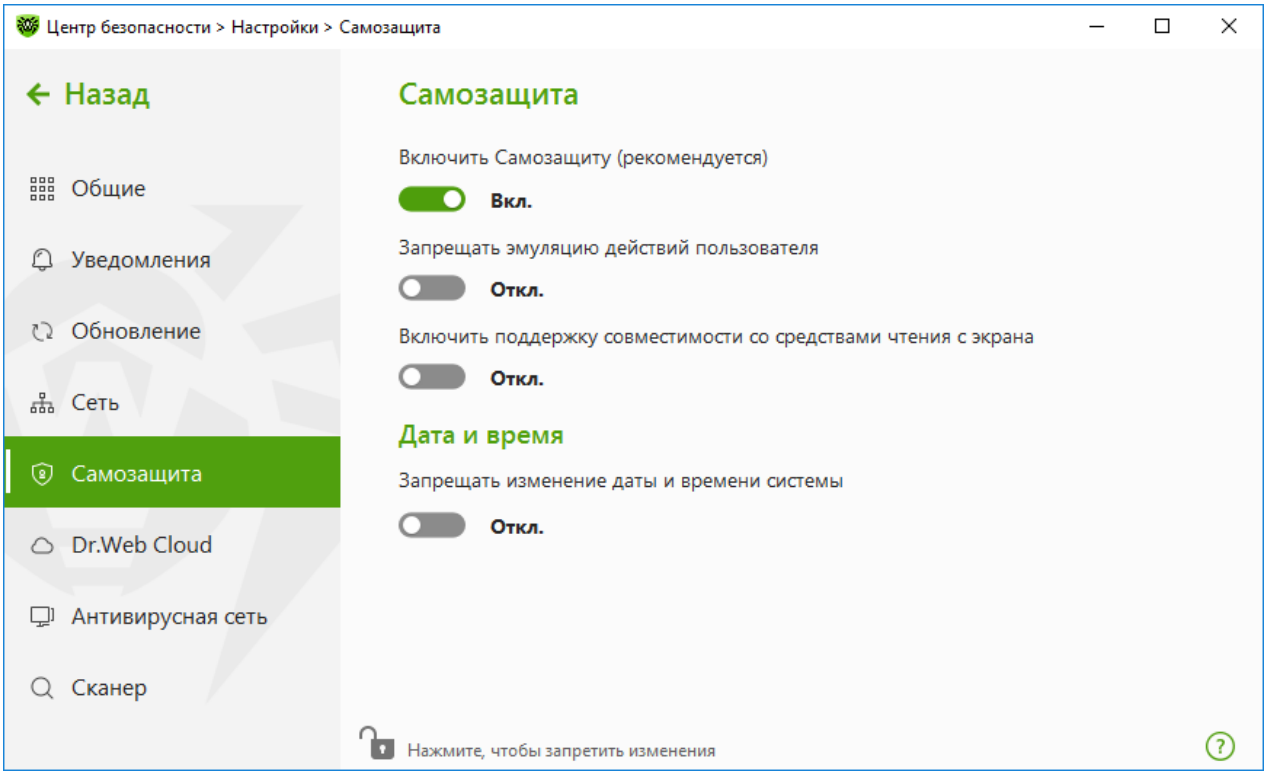

Рисунок 34. Параметры защиты Dr.Web

Настройки Самозащиты

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

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

Чтобы произвести возврат к точке восстановления системы, необходимо отключить модуль Самозащиты.

Настройка **Запрещать эмуляцию действий пользователя** позволяет предотвратить изменения в настройках Dr.Web, производимые сторонними программными средствами. В том числе будет запрещено исполнение скриптов, эмулирующих работу клавиатуры и мыши в окнах Dr.Web (например, скриптов для изменения настроек Dr.Web, удаления лицензии и других действий, направленных на изменение работы Dr.Web).

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

Дата и время

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

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

10.6. Dr.Web Cloud

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

В этом разделе:

- Облачный сервис
- Программа улучшения качества ПО

Чтобы включить или отключить Dr.Web Cloud

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

Рисунок 35. Подключение к Dr.Web Cloud

Облачный сервис

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

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

Программа улучшения качества ПО

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

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

10.7. Удаленный доступ к Dr.Web

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

Чтобы разрешить или запретить удаленное управление продуктом Dr.Web

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

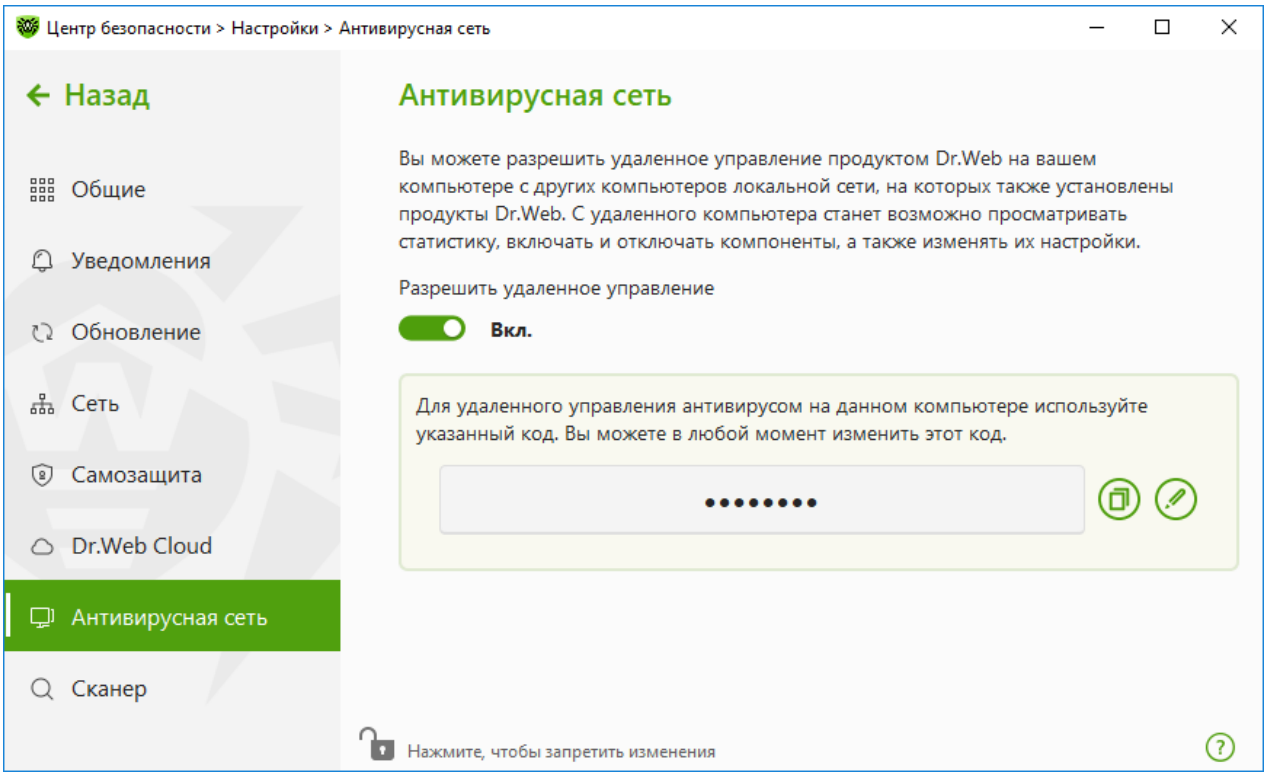

Рисунок 36. Включение удаленного управления антивирусом

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

Удаленное управление позволяет просматривать статистику, включать и отключать модули, а также изменять их настройки. Компоненты Карантин, Сканер, Защита от потери данных и Антивирусная сеть недоступны.

10.8. Параметры проверки файлов

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

Чтобы перейти к параметрам проверки файлов

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

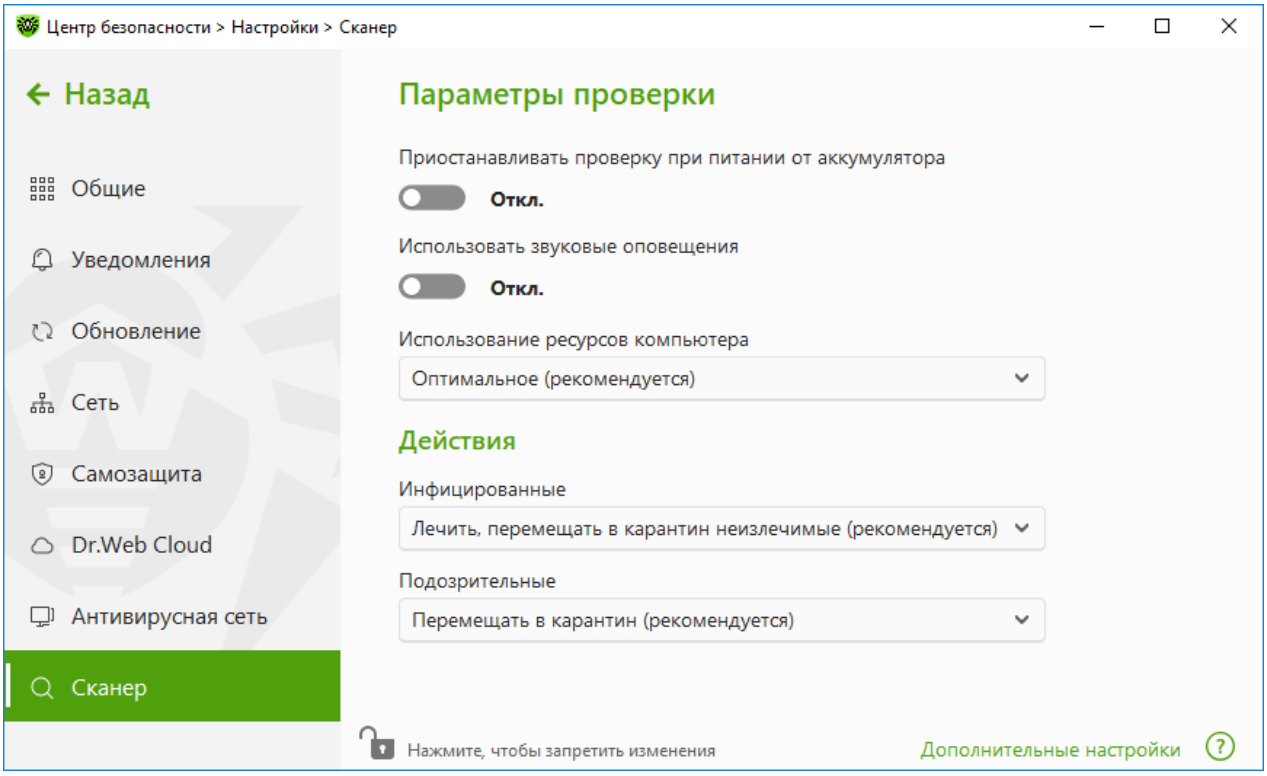

Рисунок 37. Настройка Сканера

Параметры проверки

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

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

Действие	Описание
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.

11. Файлы и сеть

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

Чтобы перейти в группу настроек Файлы и сеть

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

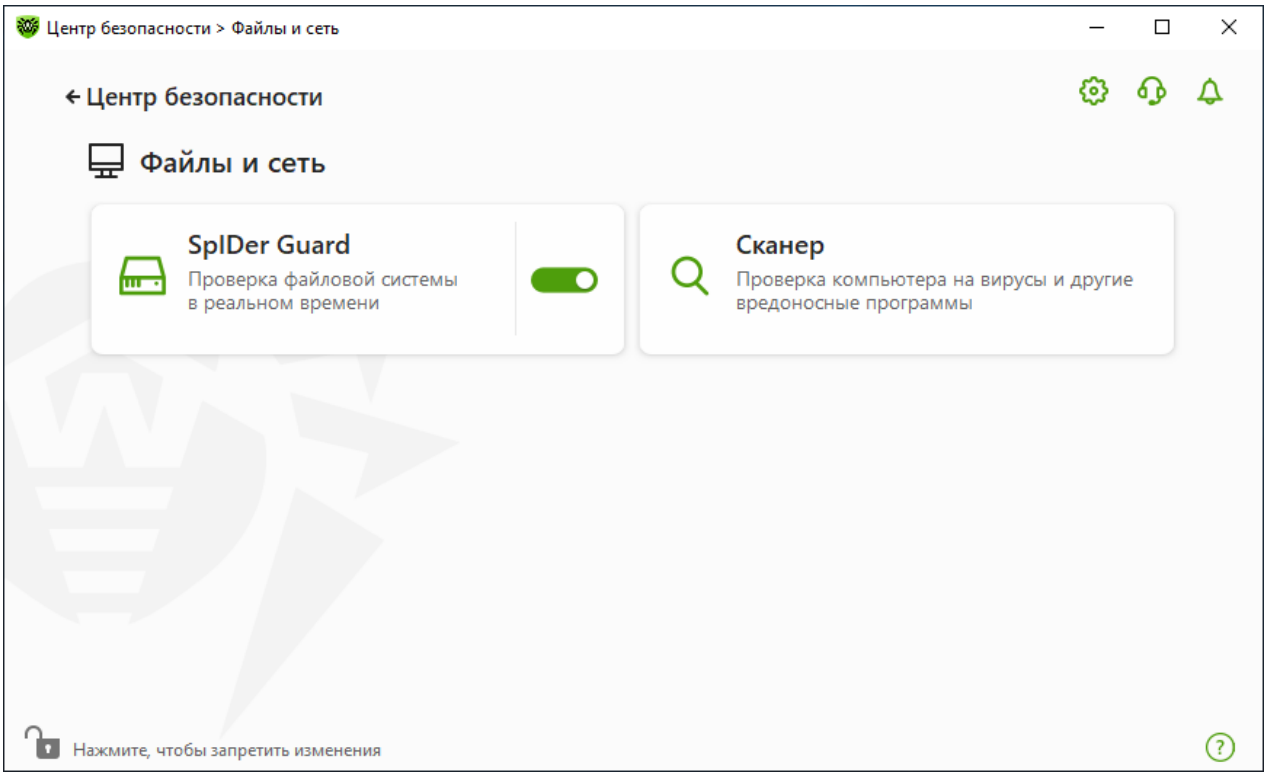

Рисунок 38. Окно Файлы и сеть

Включение и отключение компонентов защиты

Включите или отключите необходимый компонент при помощи переключателя .

Чтобы перейти к параметрам компонентов

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

В этом разделе:

- Монитор файловой системы SplDer Guard — компонент, проверяющий файлы во время их открытия, запуска или изменения, а также запускаемые процессы в режиме реального времени.
- Сканер — компонент, проверяющий объекты по запросу или по расписанию.

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

11.1. 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 .

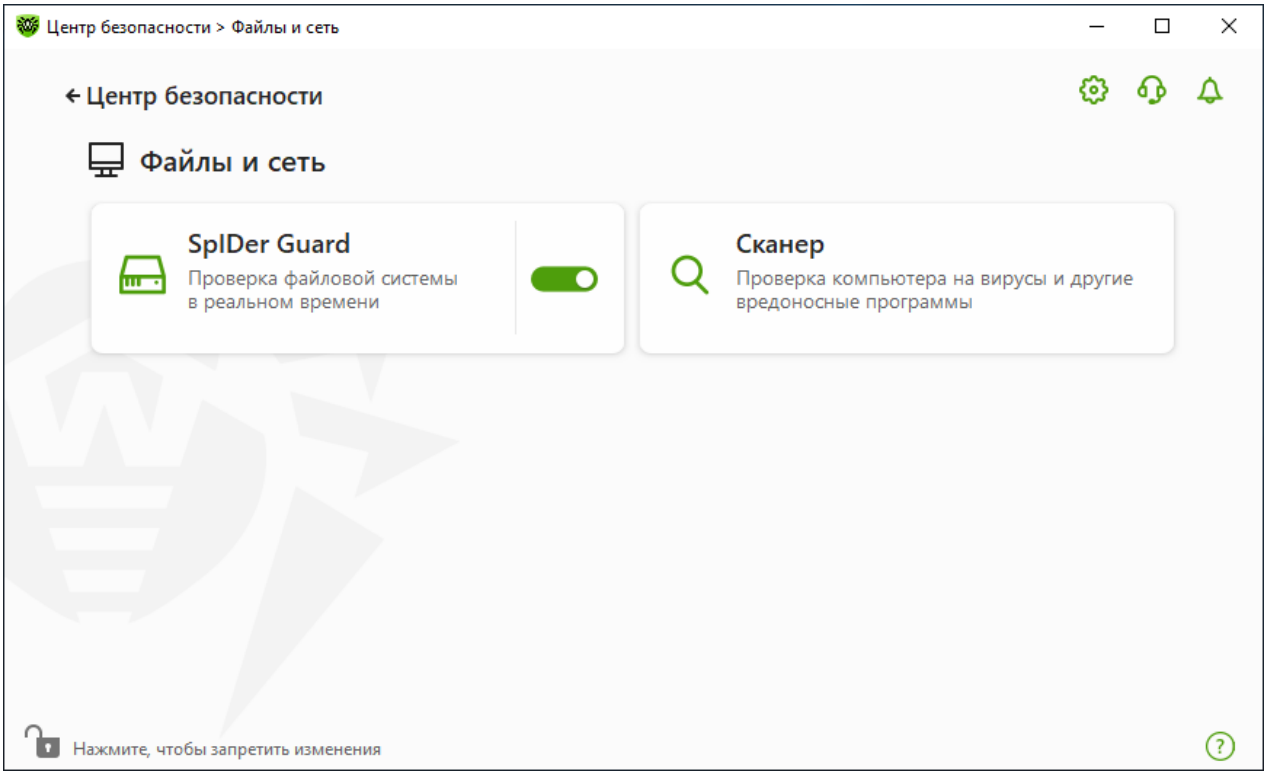

Рисунок 39. Включение/отключение SplDer Guard

В этом разделе:

См. также:

Особенности работы SplDer Guard

При настройках по умолчанию SplDer Guard на лету проверяет на жестком диске только создаваемые или изменяемые файлы, на съемных носителях — все открываемые файлы. Кроме того, SplDer Guard постоянно отслеживает действия всех запущенных процессов и блокирует процессы с поведением, характерным для вредоносных программ.

> ⚠ Компонент SplDer 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 SplDer Guard запускается автоматически при каждой загрузке операционной системы, при этом запущенный монитор файловой системы SplDer 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 SplDer Guard.

Параметры монитора файловой системы SplDer Guard

При обнаружении зараженных объектов SplDer 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 SplDer Guard

1. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт» 🔓). В противном случае нажмите на замок 🔒.

2. Нажмите плитку **SpIDer Guard**. Откроется окно параметров компонента.

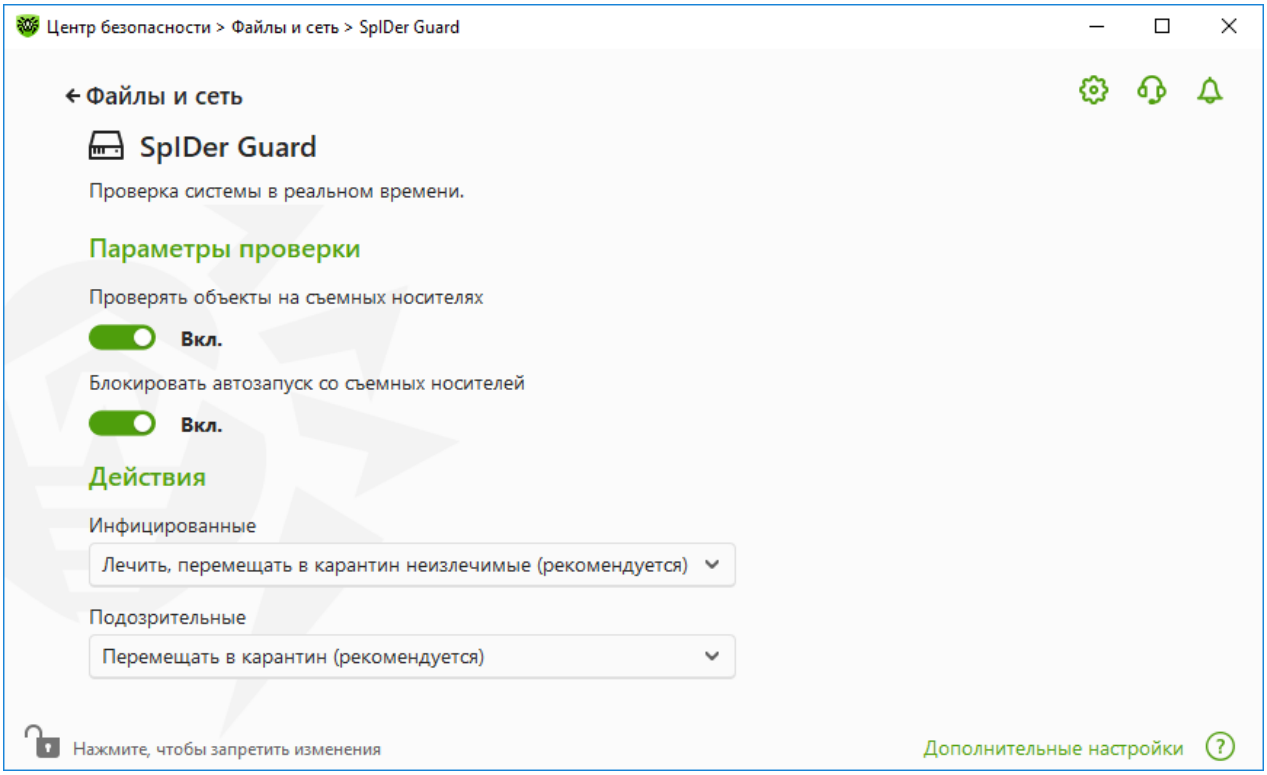

Рисунок 40. Параметры монитора файловой системы

Проверка съемных носителей

SpIDer Guard по умолчанию проверяет 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 SplDer Guard.

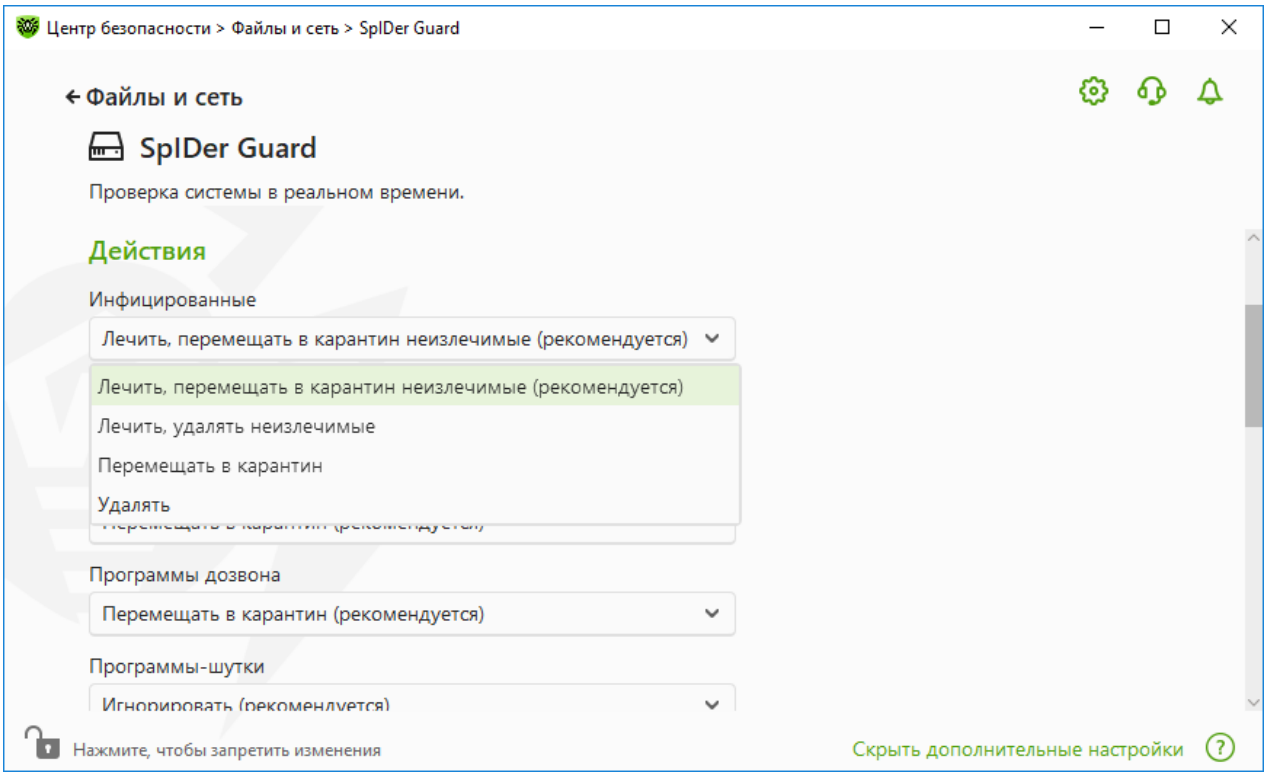

Рисунок 41. Настройка действий, применяемых к угрозам

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

Возможные действия

К угрозам могут быть применены следующие действия:

Действие	Описание
Лечить, перемещать в	Восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин.

Действие	Описание
карантин неизлечимые	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).
Удалять	Удалить объект. Для загрузочных секторов никаких действий производиться не будет.
Перемещать в карантин	Переместить объект в специальную папку Карантина. Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропустить объект без выполнения каких-либо действий и не выводить оповещения. Данное действие возможно только для вредоносных программ: рекламных программ, программ дозвона, программ-шуток, потенциально опасных программ и программ взлома.

Режим проверки компонентом SpIDer Guard

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

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

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

Режим	Описание
	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 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 Server 2016 и более поздних).

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.

11.2. 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

11.2.1. Запуск и режимы проверки

Сканер можно запустить при загрузке Windows в безопасном режиме. При этом остальные компоненты Dr.Web работать не будут.

Чтобы запустить проверку файлов

При работе под управлением операционных систем Windows Server 2008 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.

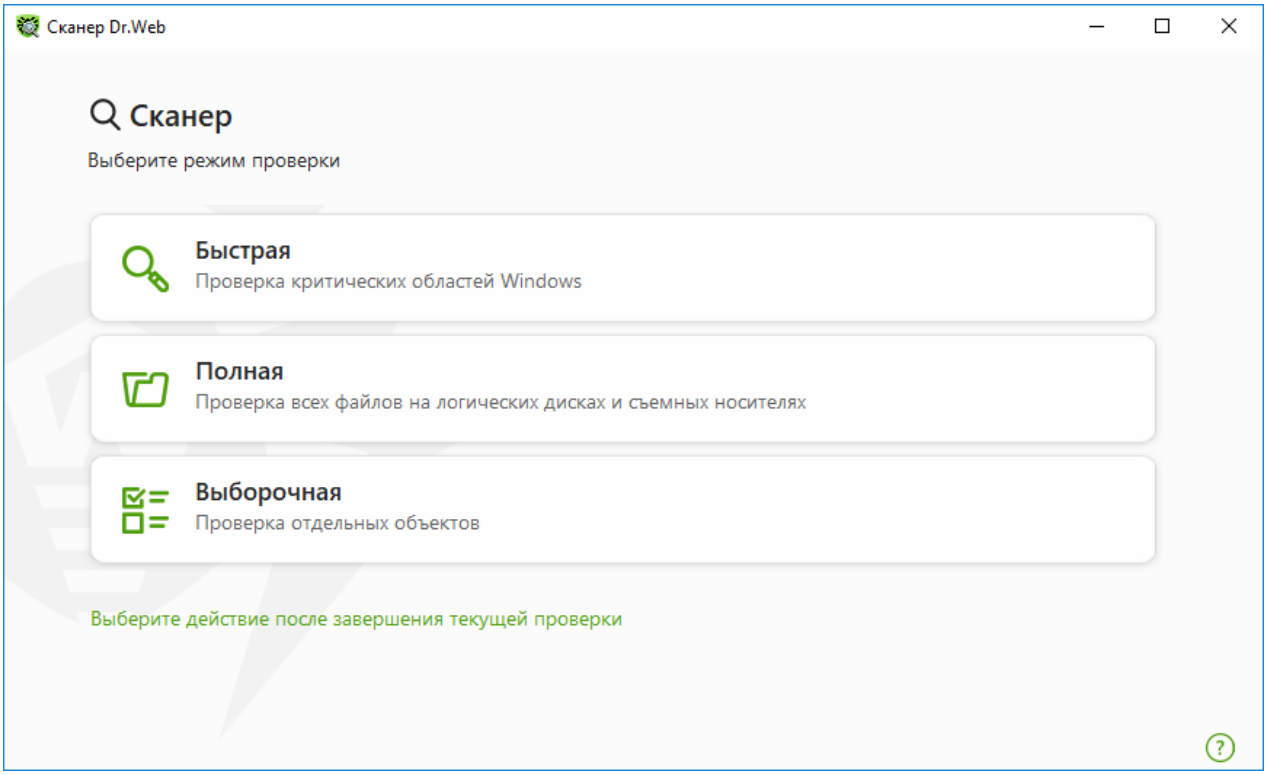

Рисунок 42. Выбор режима проверки

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

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

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

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

Чтобы проверить конкретный файл или папку

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

Описание режимов проверки

Режим проверки	Описание
Быстрая	В данном режиме проверяются: • загрузочные секторы всех дисков; • оперативная память; • корневая папка загрузочного диска; • системная папка Windows; • папка «Мои документы»; • временные файлы; • точки восстановления системы; • наличие руткитов (если процесс проверки запущен от имени администратора).  Архивы и почтовые файлы в этом режиме не проверяются.
Полная	В данном режиме производится полная проверка оперативной памяти и всех жестких дисков (включая загрузочные секторы), а также осуществляется проверка на наличие руткитов.
Выборочная	В данном режиме могут быть проверены любые файлы и папки, а также такие объекты, как оперативная память, загрузочные секторы и т. п. Чтобы добавить объекты в список проверки, нажмите кнопку  .

11.2.2. 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.

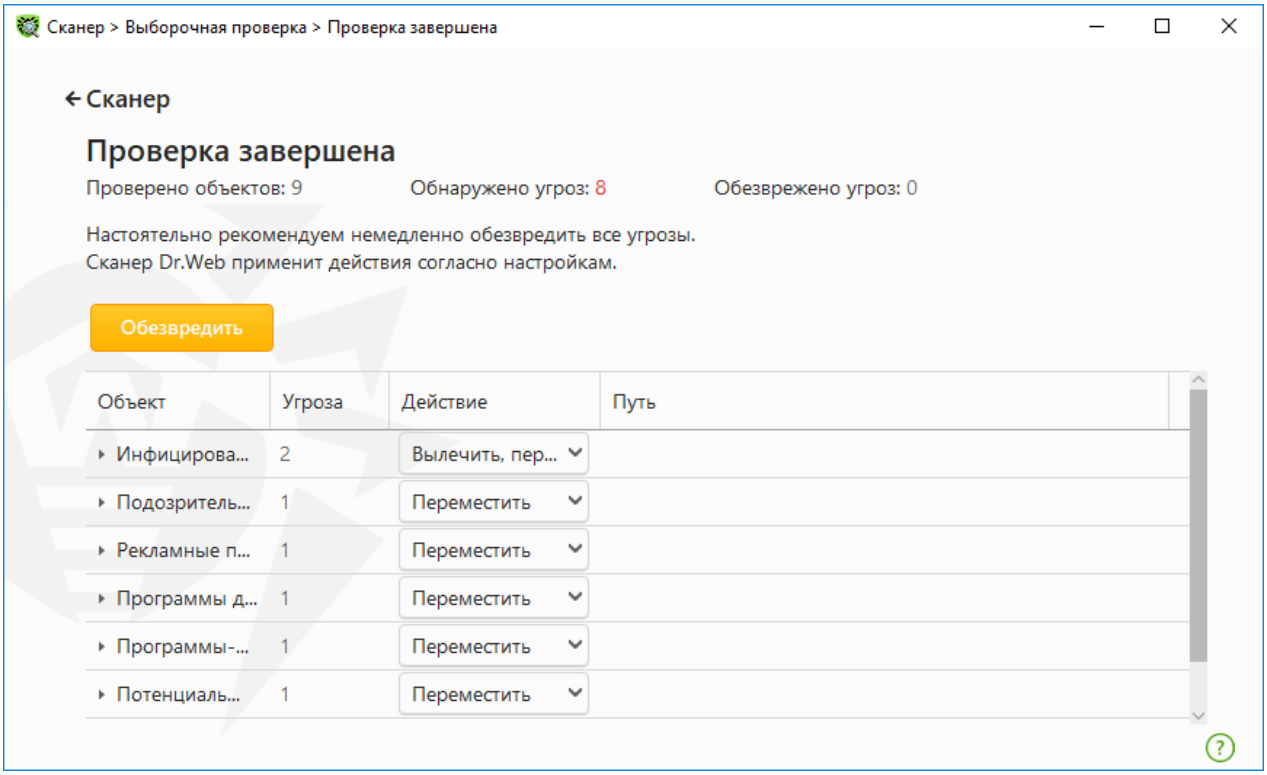

Рисунок 43. Выбор действия по окончании проверки

Таблица с результатами проверки содержит следующую информацию:

Столбец	Описание
Объект	В этом столбце указано наименование зараженного или подозрительного объекта (имя файла — если заражен файл, **Boot sector** в случае зараженного загрузочного сектора, **Master Boot Record** в случае зараженного MBR жесткого диска).
Угроза	В этом столбце указано наименование 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`.

11.2.3. Дополнительные возможности

В этом разделе содержится информация о дополнительных возможностях работы Сканера:

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

Запуск Сканера с параметрами командной строки

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

Синтаксис команды запуска следующий:

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

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

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

Чаще употребляются следующие варианты указания объектов проверки:

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

Консольный сканер

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

Консольный сканер помещает подозрительные объекты в Карантин.

Чтобы запустить Консольный сканер, воспользуйтесь следующей командой:

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

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

Список ключей Консольного сканера содержится в Приложении А.

Коды возврата:

0 — проверка успешно завершена, инфицированные объекты не найдены

1 — проверка успешно завершена, найдены инфицированные объекты

10 — указаны некорректные ключи

11 — ключевой файл не найден либо не поддерживает Консольный сканер

12 — не запущен Scanning Engine

255 — проверка прервана пользователем

Запуск проверки в Планировщике заданий Windows

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

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

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

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

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

12. 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**.

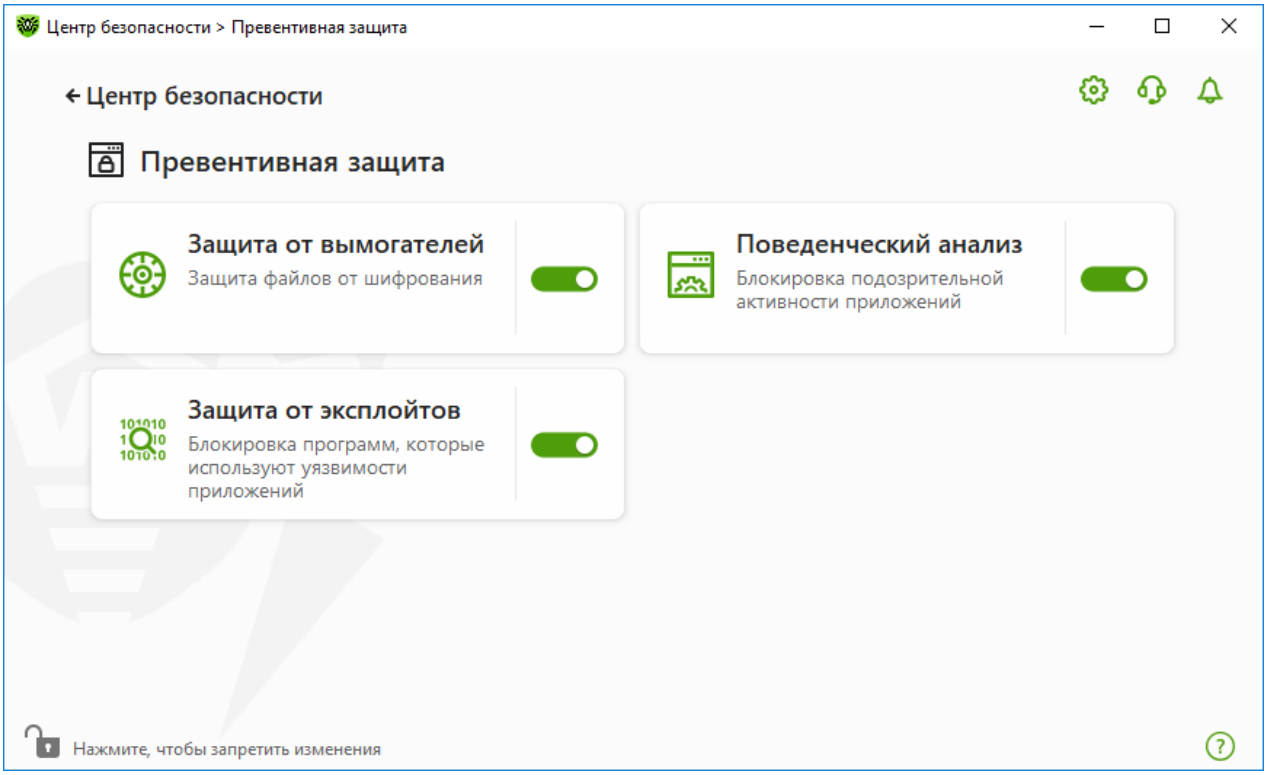

Рисунок 44. Окно Превентивная защита

Включение и отключение компонентов защиты

Включите или отключите необходимый компонент при помощи переключателя .

Чтобы перейти к параметрам компонентов

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

В этом разделе:

- 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.

12.1. 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.

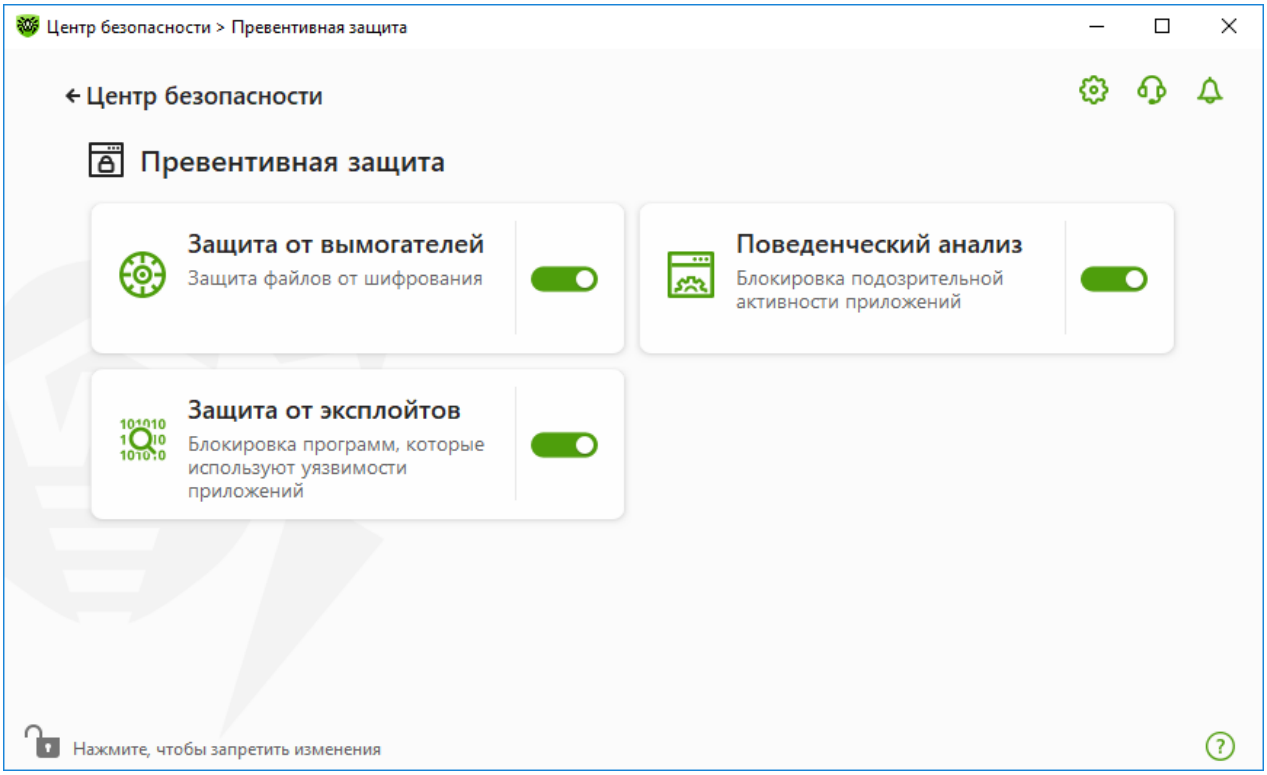

Рисунок 45. Включение/отключение компонента Защита от вымогателей

В этом разделе:

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

Реакция Dr.Web на попытки приложений зашифровать файл

Чтобы настроить параметры компонента Защита от вымогателей

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

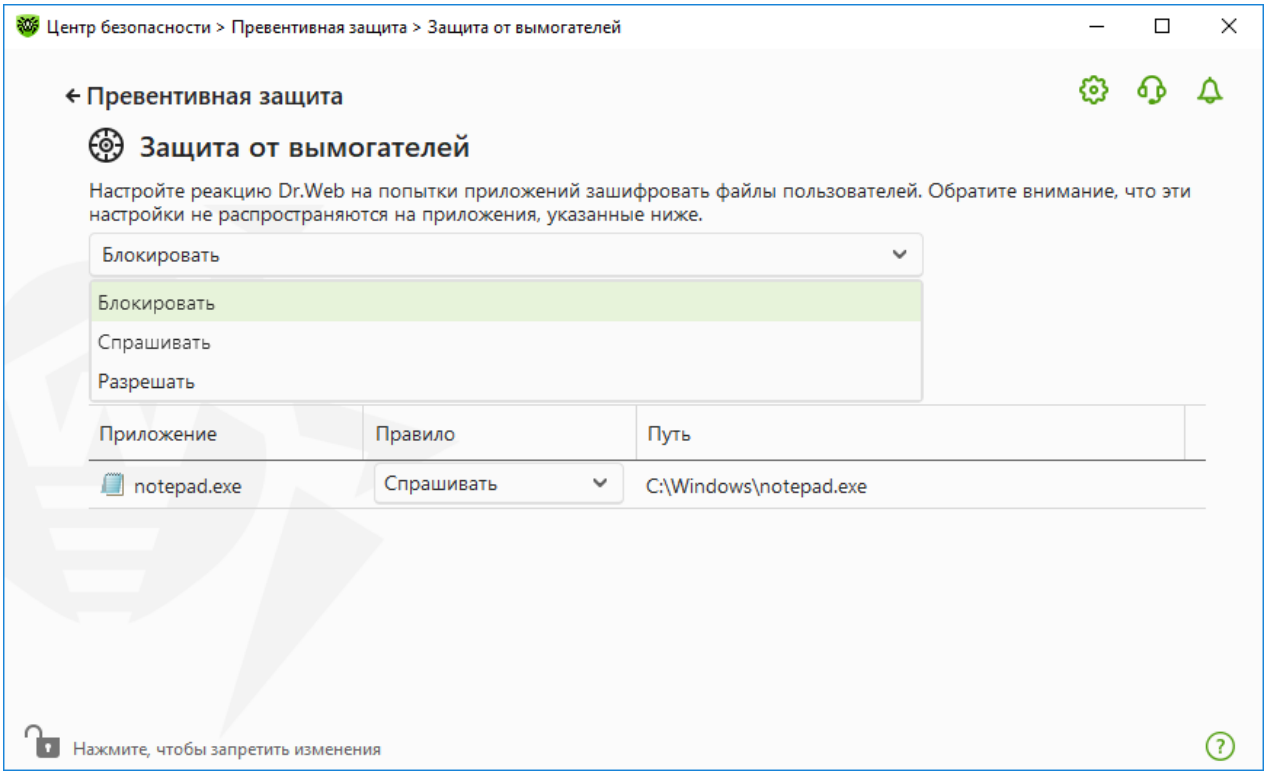

Рисунок 46. Выбор реакции Dr.Web

- **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:

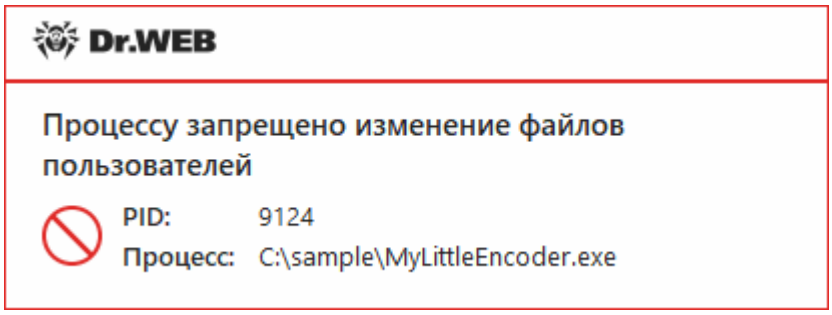

Рисунок 47. Пример уведомления о запрете изменения файлов пользователя

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

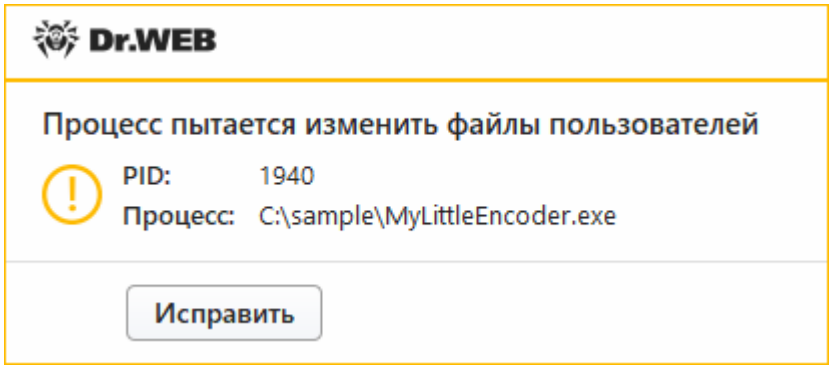

Рисунок 48. Пример уведомления о попытке изменения файлов пользователя

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

Получение уведомлений

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

См. также:

- Уведомления

Список приложений, исключенных из проверки

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

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

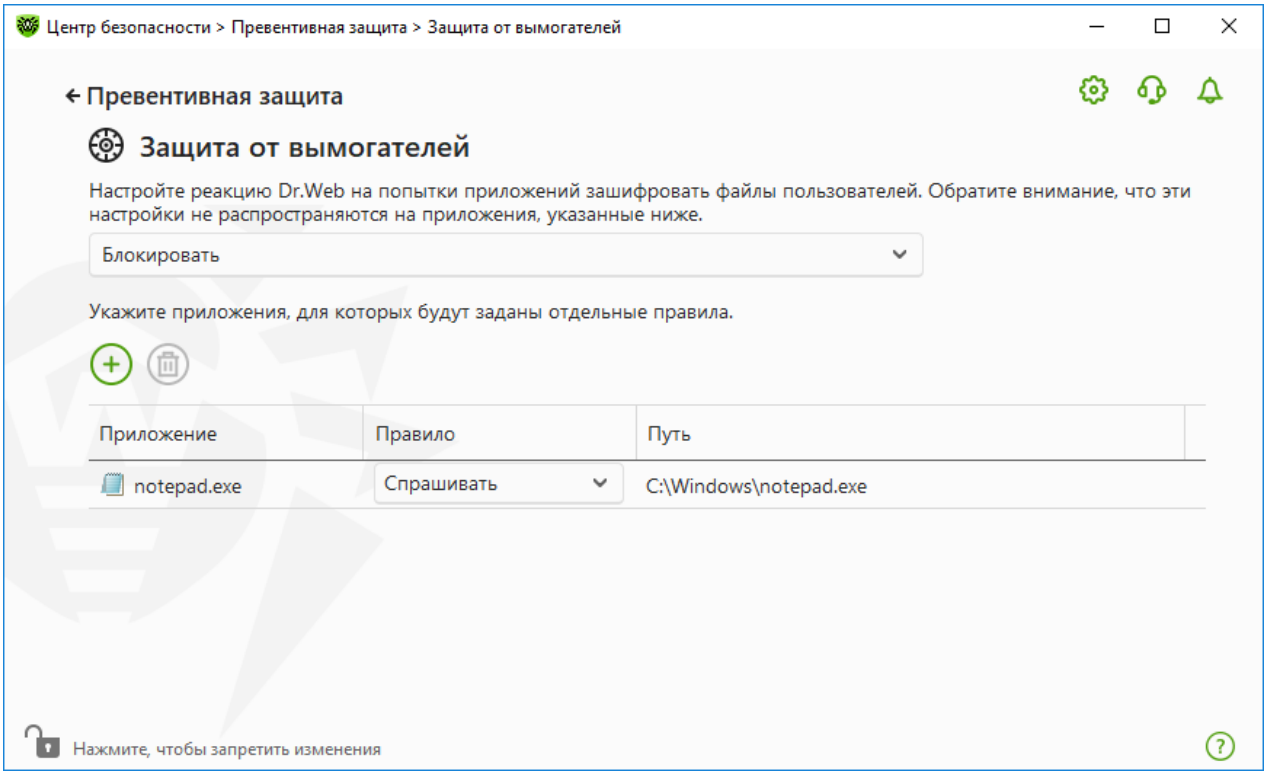

Рисунок 49. Исключения из проверки Защитой от вымогателей

Чтобы добавить приложение в список

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

Чтобы защитить свои данные от несанкционированных изменений, вы можете также добавить файлы в список защищенных.

12.2. 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. Для определения вредоносности приложений используются наиболее актуальные данные облачного сервиса Dr.Web.

Чтобы включить или отключить компонент Поведенческий анализ

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

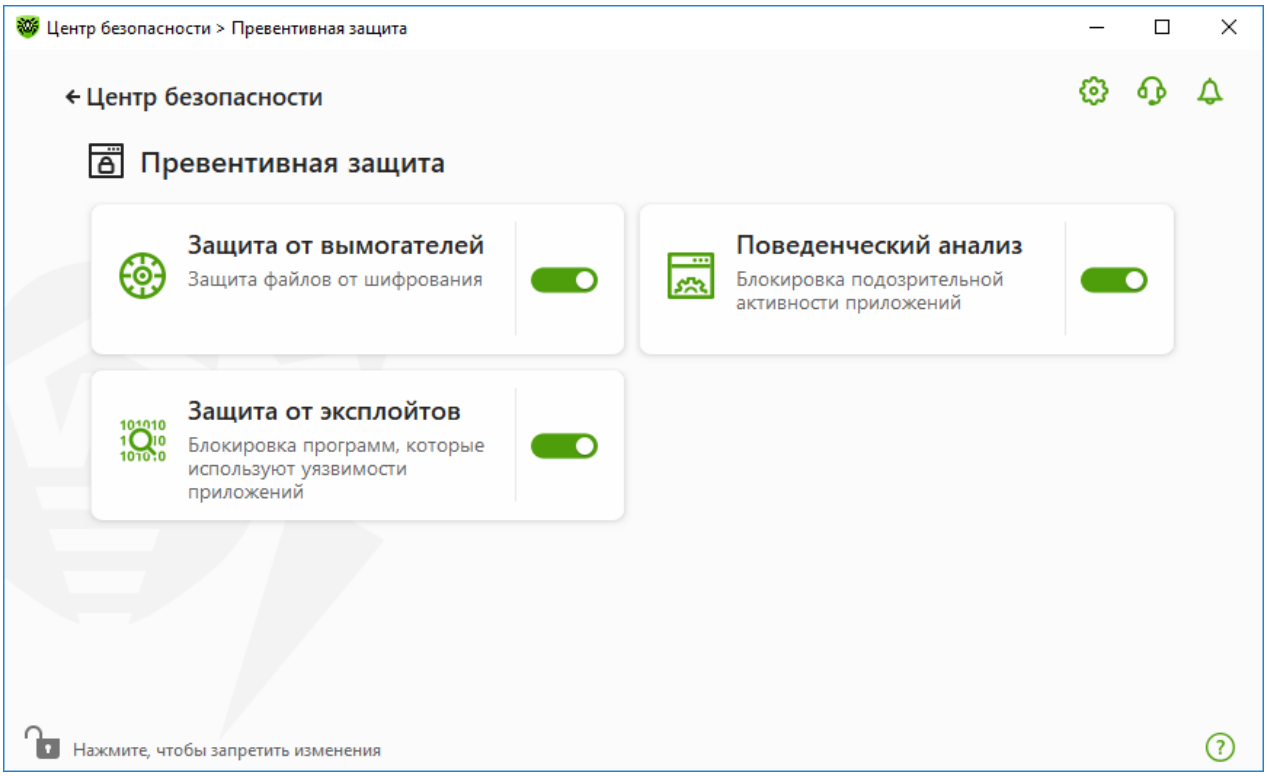

Рисунок 50. Включение/отключение компонента Поведенческий анализ

В этом разделе:

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

Параметры Поведенческого анализа

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

Чтобы перейти к параметрам компонента Поведенческий анализ

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

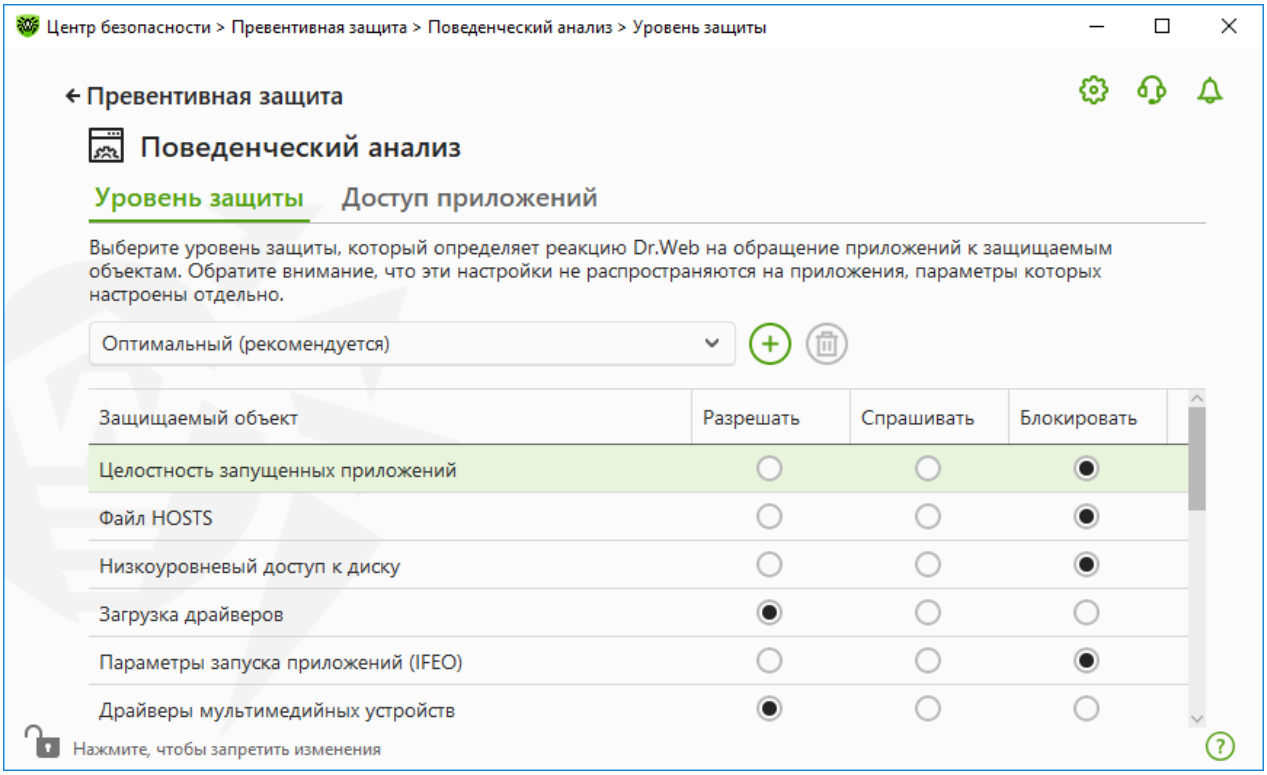

Рисунок 51. Параметры Поведенческого анализа

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

Уровни защиты

Уровень защиты	Описание
Оптимальный (рекомендуется)	Используется по умолчанию. Dr.Web запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему. Также запрещаются низкоуровневый доступ к диску и модификация файла HOSTS приложениям, действия которых однозначно определяются как попытка вредоносного воздействия на операционную систему. ⚠ Блокируются только действия приложений, которые не являются доверенными.
Средний	Этот уровень защиты можно установить при повышенной опасности заражения. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.

Уровень защиты	Описание
	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:

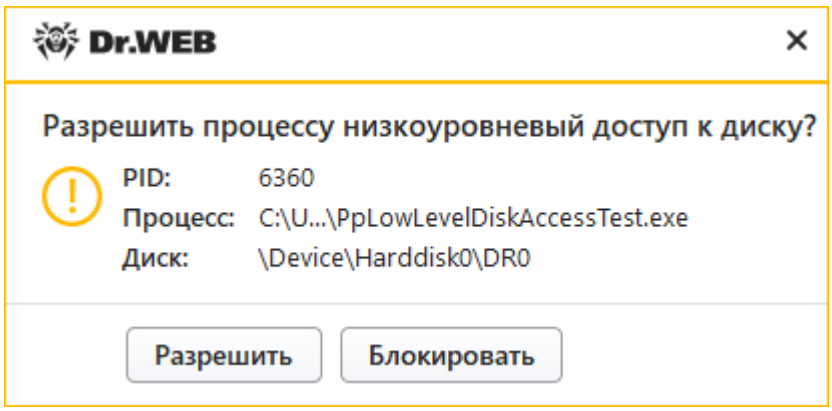

Рисунок 52. Пример уведомления с запросом доступа к защищаемому объекту

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

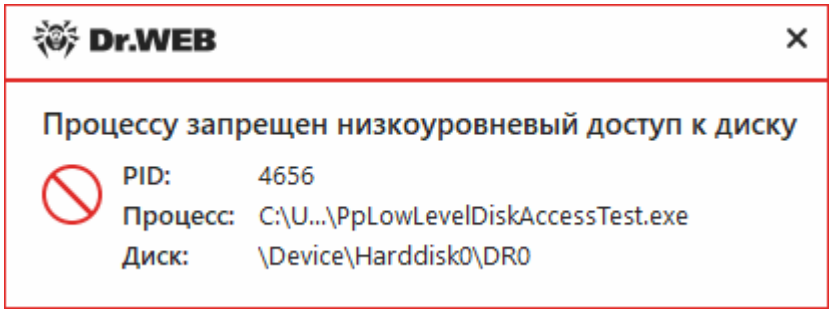

Рисунок 53. Пример уведомления о запрете доступа к защищаемому объекту

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 и отправку этих уведомлений на электронную почту.

См. также:

- Уведомления

Доступ приложений

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

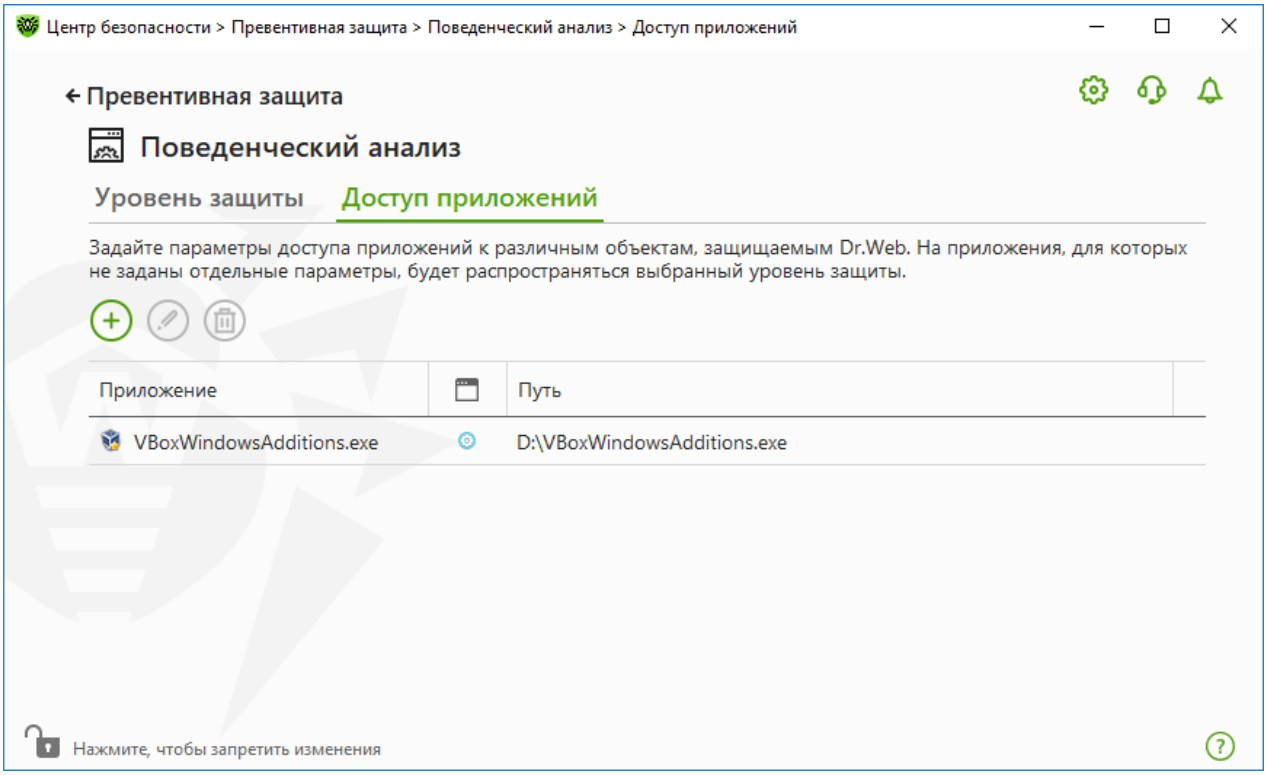

Рисунок 54. Параметры доступа для приложений

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.

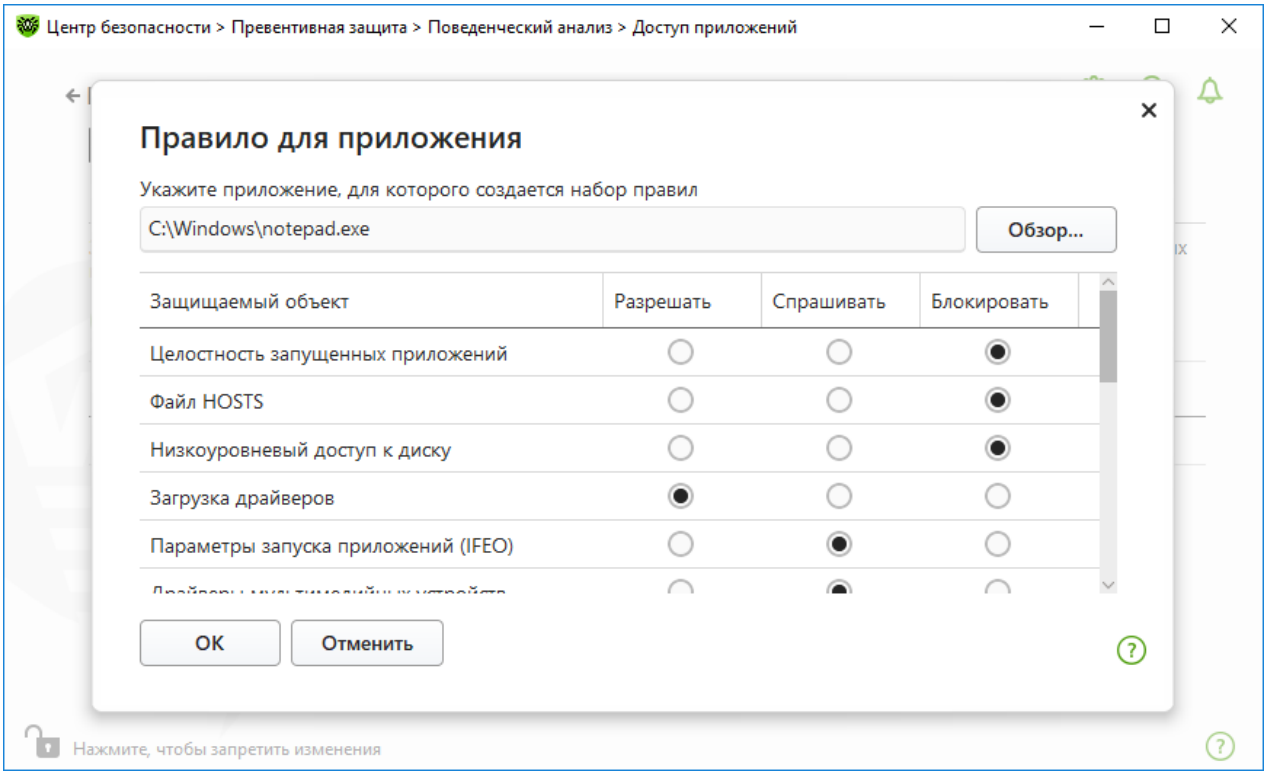

Рисунок 55. Добавление набора правил для приложения

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

Защищаемые объекты

Защищаемый объект	**Описание**
Целостность запущенных приложений	Данная настройка позволяет отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера.
Файл HOSTS	Файл HOSTS используется операционной системой для упрощения доступа к интернету. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
Низкоуровневый доступ к диску	Данная настройка позволяет запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
Загрузка драйверов	Данная настройка позволяет запрещать приложениям загрузку новых или неизвестных драйверов.

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
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

Защищаемый объект	Описание
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.

12.3. Защита от эксплойтов

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

Чтобы включить или отключить компонент Защита от эксплойтов

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

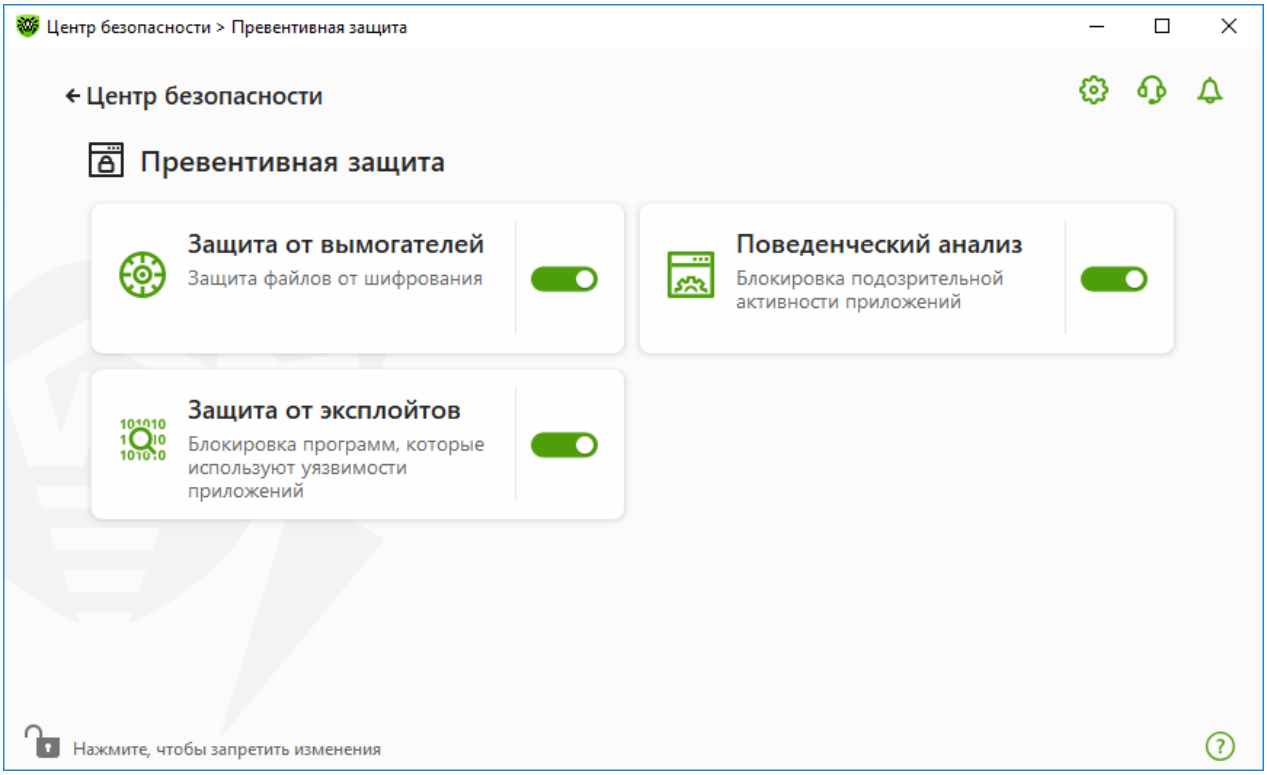

Рисунок 56. Включение/отключение компонента Защита от эксплойтов

Чтобы перейти к параметрам компонента Защита от эксплойтов

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

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

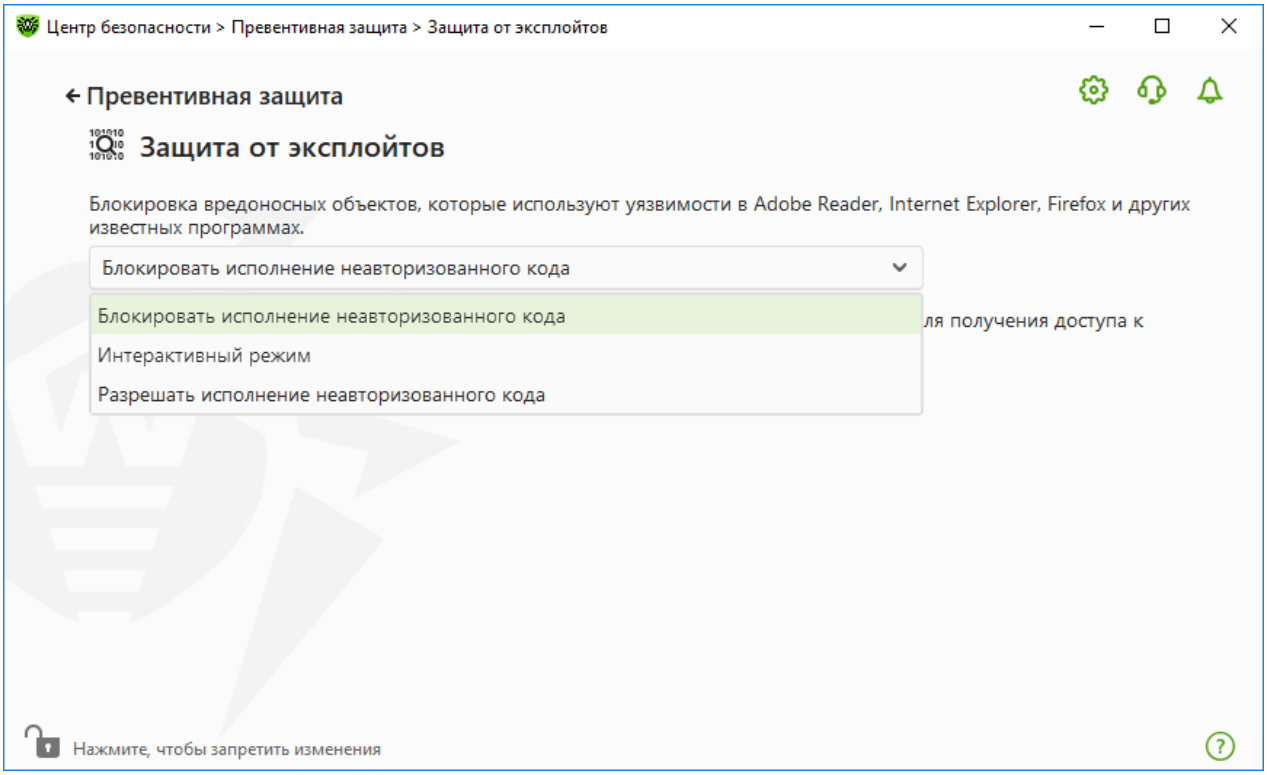

Рисунок 57. Выбор уровня защиты

Уровни защиты

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

Получение уведомлений

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

См. также:

- Уведомления

13. Устройства и личные данные

Данная группа настроек позволяет настроить защиту для важных папок, а также заблокировать доступ к определенным классам и шинам устройств.

Чтобы перейти в группу настроек Устройства и личные данные

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

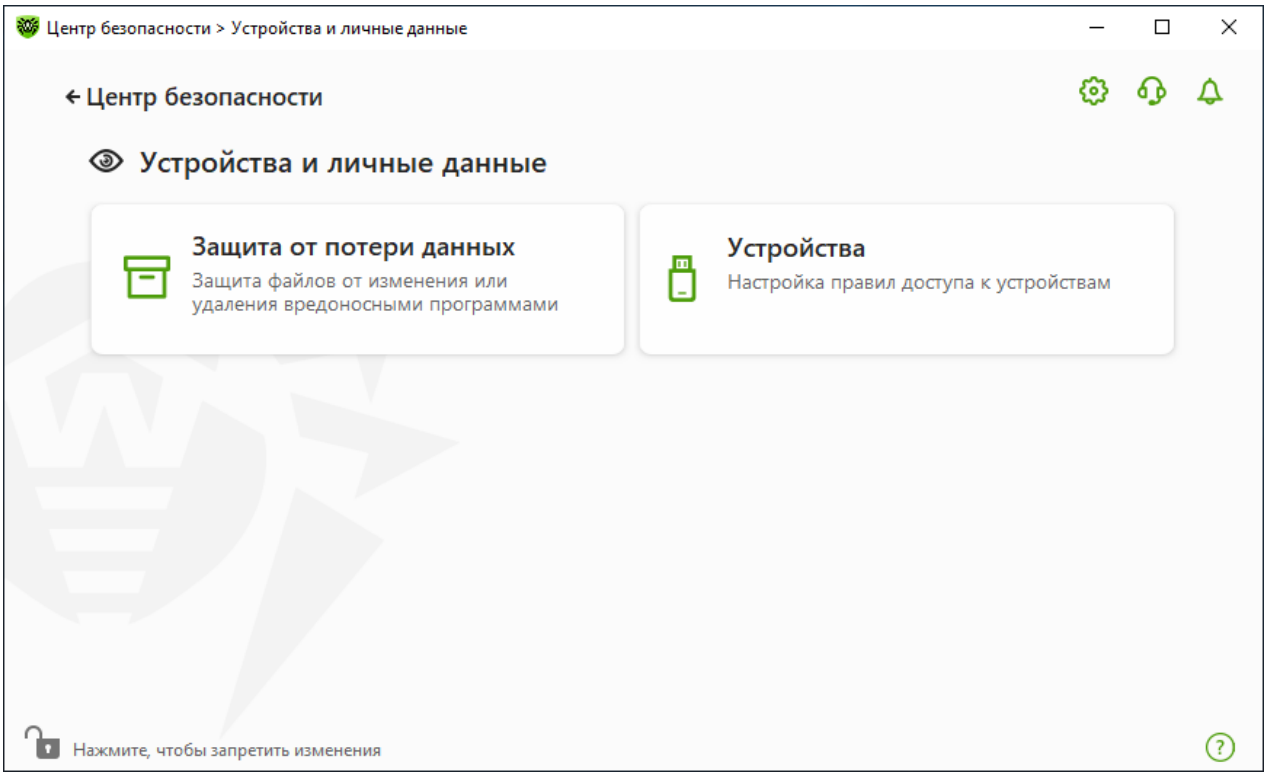

Рисунок 58. Окно Устройства и личные данные

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 окне:

- Защита от потери данных — дополнительная защита для важных файлов и папок.
- Устройства — управление блокировкой устройств.

13.1. Защита от потери данных

Защита от потери данных — функция, которая обеспечивает защиту содержимого важных папок от изменений вредоносным программным обеспечением. Вы можете свободно просматривать и добавлять файлы в защищенную папку, однако любая модификация файлов в ней или удаление запрещены. Чтобы разрешить приложениям доступ к папке, можно добавить необходимые приложения в исключения. Также вы можете восстановить ранее сохраненные копии.

Чтобы перейти в окно Защита от потери данных

1. Откройте меню Dr.Web и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Устройства и личные данные**.
3. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
4. Нажмите плитку **Защита от потери данных**.

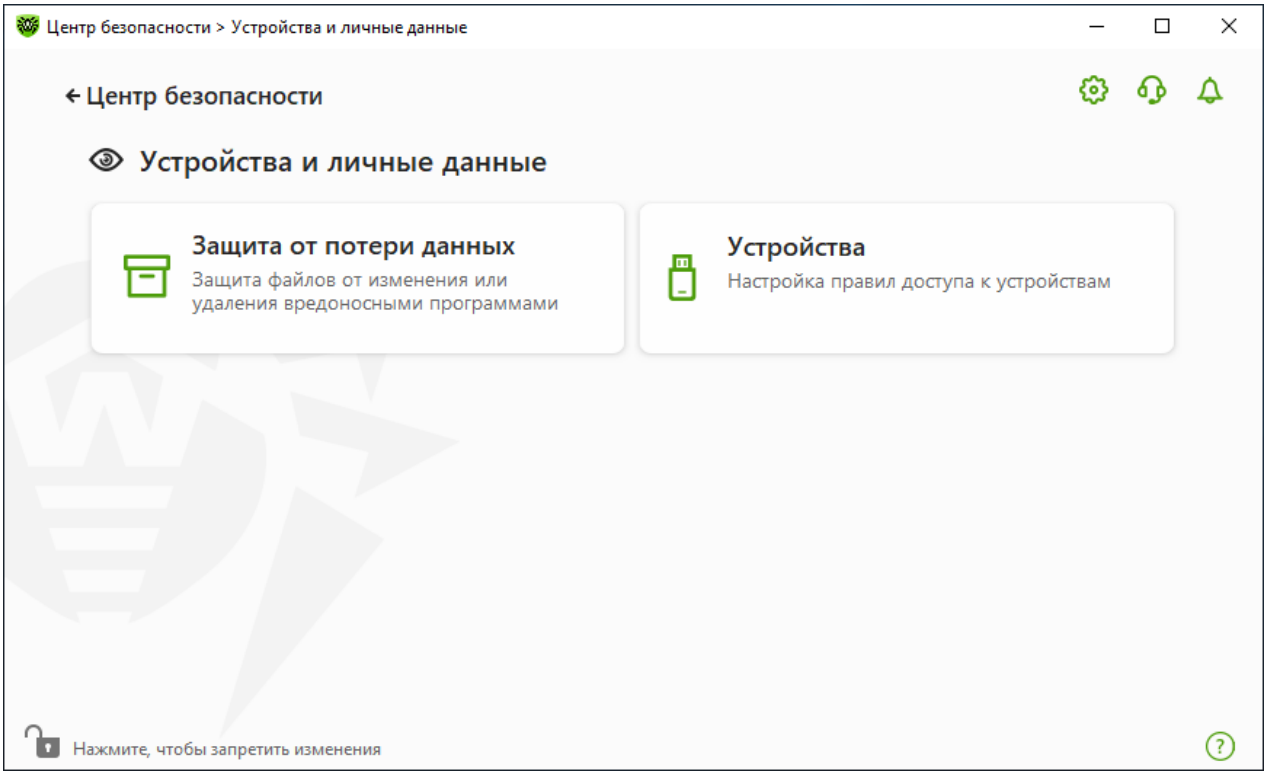

Рисунок 59. Доступ к окну Защита от потери данных

В этом разделе:

- Особенности работы при наличии сохраненных копий файлов
- Управление защищаемыми папками
- Исключения
- Восстановление и удаление сохраненных копий

Особенности работы при наличии сохраненных копий файлов

Начиная с версии 12.0 программа не позволяет сохранять копии файлов. Вместо сохранения копий теперь используется опция добавления папок в список защищенных.

Поскольку принцип работы компонента изменился, необходимо настроить защиту папок заново. Папки, для которых была включена защита в предыдущих версиях программы, копируются в список защищенных папок вне зависимости от наличия сохраненных копий этих папок. При первом запуске программы после обновления до версии 12.0 появляется уведомление о переходе от функции сохранения копий файлов к защите выбранных папок:

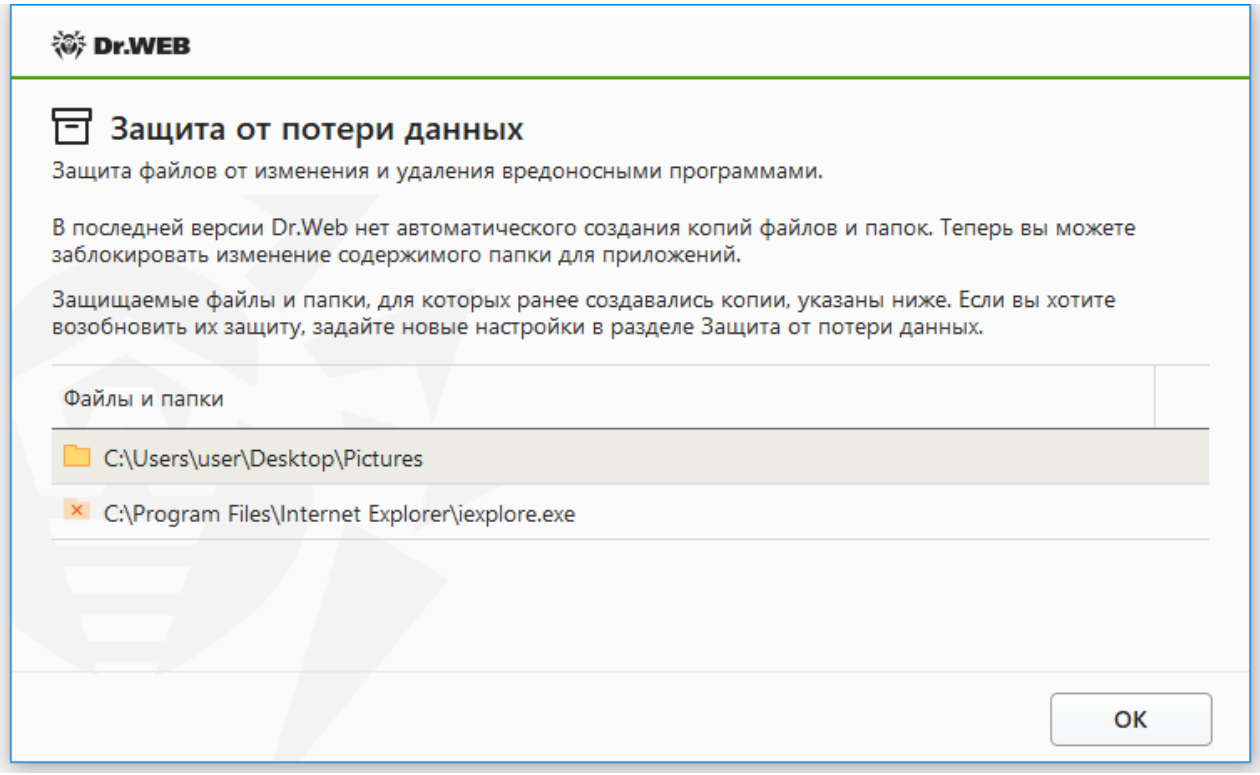

Рисунок 60. Уведомление об изменении принципа работы компонента

Там же указан список всех найденных папок и файлов, для которых была включена защита. Если папка не может быть добавлена в защищенные, она будет отображаться в списке со значком . Не могут быть добавлены под защиту системные каталоги, а также отдельные файлы.

По умолчанию защита папок, перенесенных в список защищаемых из предыдущих версий, отключена. Чтобы включить защиту, перейдите в окно **Защита от потери данных** и отметьте нужные папки в столбце **Включить защиту**.

Сохраненные в предыдущих версиях копии файлов доступны для восстановления.

Уведомления

После обновления продукта до версии 12.0 программа информирует пользователя об изменении принципа работы компонента Защита от потери данных:

- Сразу после перезагрузки в середине экрана показывается уведомление об изменении принципа работы компонента. См. рисунок 60.
- В Ленте уведомлений отображается уведомление об изменении метода защиты папок. Чтобы перейти к новым настройкам защиты папок, нажмите кнопку **Настроить защиту**. После перехода к настройкам защищенных папок данное уведомление исчезнет из ленты уведомлений.

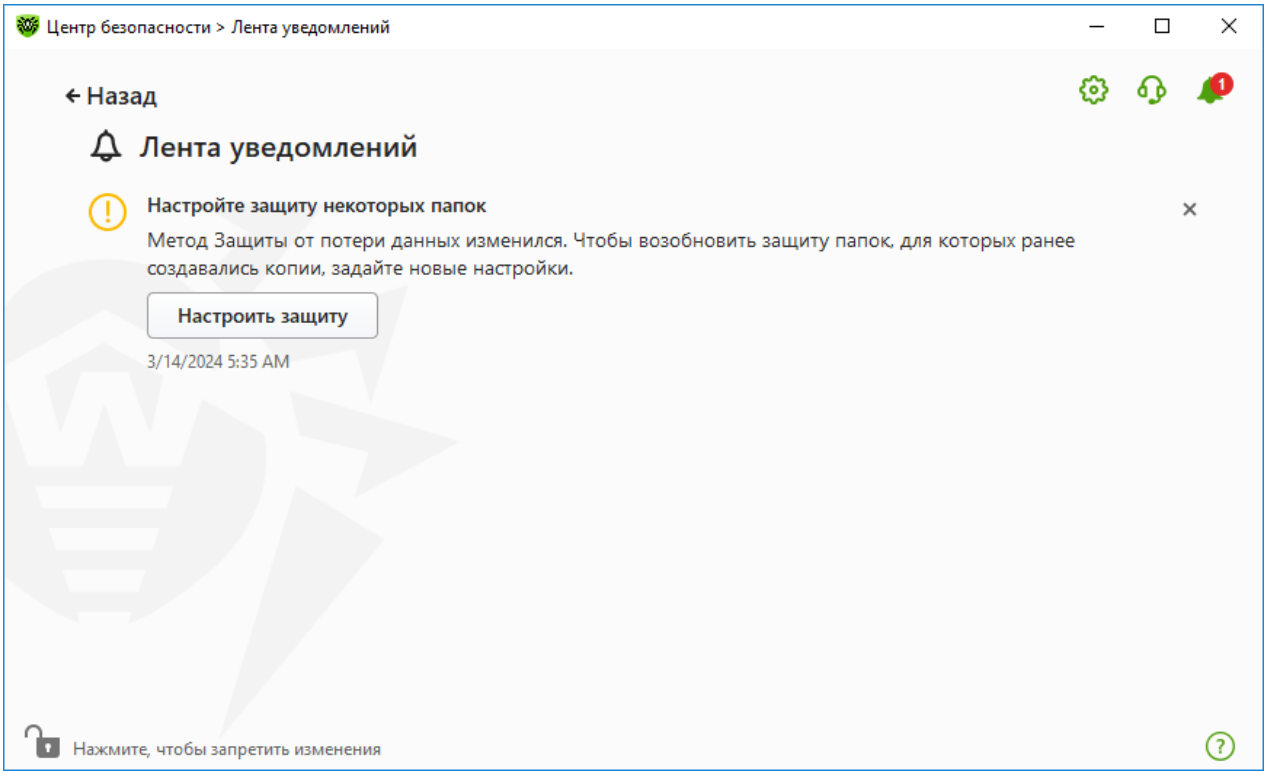

Рисунок 61. Уведомление в ленте уведомлений

- При первом открытии окна **Защита от потери данных** появляется уведомление со списком файлов и папок, которые не могут быть добавлены в список защищенных.

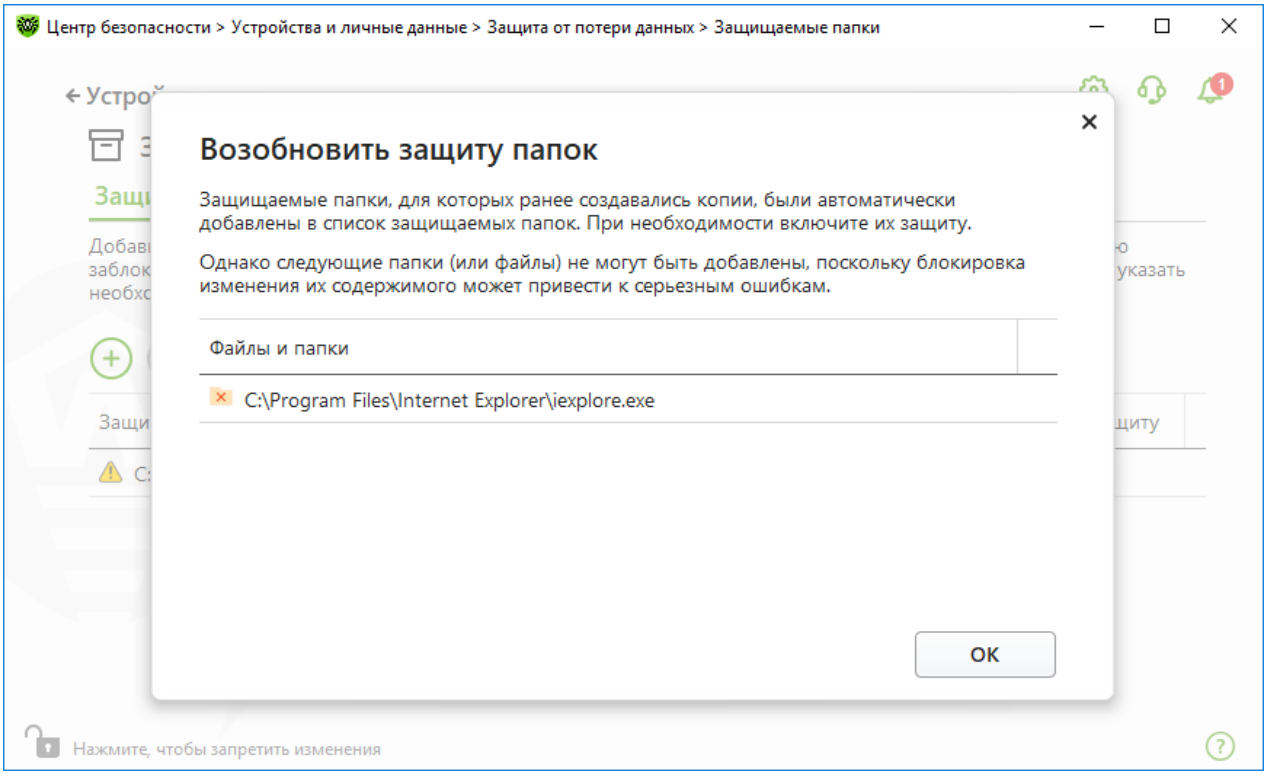

Рисунок 62. Уведомление при первом переходе в окно Защита от потери данных

Защищаемые папки

Для каждой папки вы можете настроить параметры доступа для приложений. Защищенная папка будет доступна для просмотра и копирования. Также будет доступно создание новых элементов в папке и их модификация процессами, создавшими новые элементы, до тех пор, пока эти процессы не завершены. При обращении приложений к папке будет показываться уведомление о запрете доступа.

В случае обнаружения угрозы доступ к удалению и модификации файлов в защищенных папках остается только у Dr.Web.

При добавлении папки в список защищенных действует правило по умолчанию — запрет на любые модификации и удаление содержимого папки всем приложениям, кроме приложений из списка доверенных. Со списком доверенных приложений можно ознакомиться на сайте https://products.drweb.com/services/data_protection/. Список включает наиболее популярные приложения, такие как некоторые приложения Microsoft и Adobe. Системные процессы, такие как `explorer.exe`, не входят в список доверенных, поскольку могут быть использованы вредоносными объектами для атак на систему.

Не допускается добавление системных папок в список защищаемых, поскольку это может привести к критическим ошибкам в работе системы.

Защита от потери данных распространяется только на локальные (расположенные физически на вашем устройстве) файлы и папки в рамках той же операционной системы, на которой настраивается защита. При наличии на одном компьютере нескольких операционных систем защиту от потери данных необходимо настраивать отдельно на каждой системе. Защита сетевых дисков и папок невозможна.

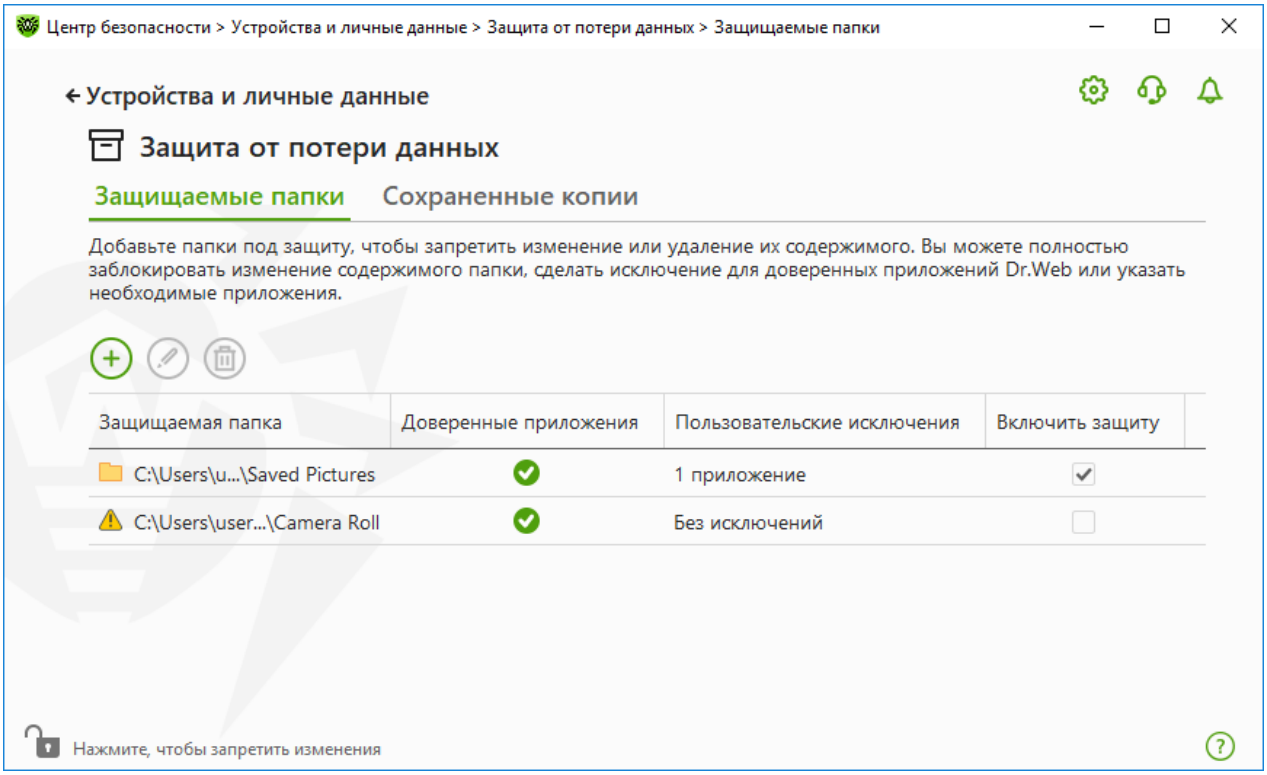

Рисунок 63. Защищаемые папки

В таблице выводится информация о:

- защищаемом объекте;
- количестве исключений из общего правила;
- статусе защиты.

Для активации функции защиты объекта установите флажок в столбце **Включить защиту** напротив необходимого объекта. При снятии флажка защита с папки полностью снимается и папка отображается со знаком ⚠.

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка ⊕ — добавление объекта в список защищенных;
- Кнопка ✎ — редактирование элементов в таблице;
- Кнопка 🗑 — удаление объекта из списка защищенных.

Чтобы добавить папку в список защищаемых

1. Нажмите кнопку ⊕. В открывшемся окне выберите необходимый объект, нажав кнопку **Обзор**.
2. При необходимости включите или выключите доступ к папке доверенным приложениям. По умолчанию опция включена.
3. Вы также можете указать приложения, которые будут иметь полный доступ к объекту вне зависимости от общих настроек.

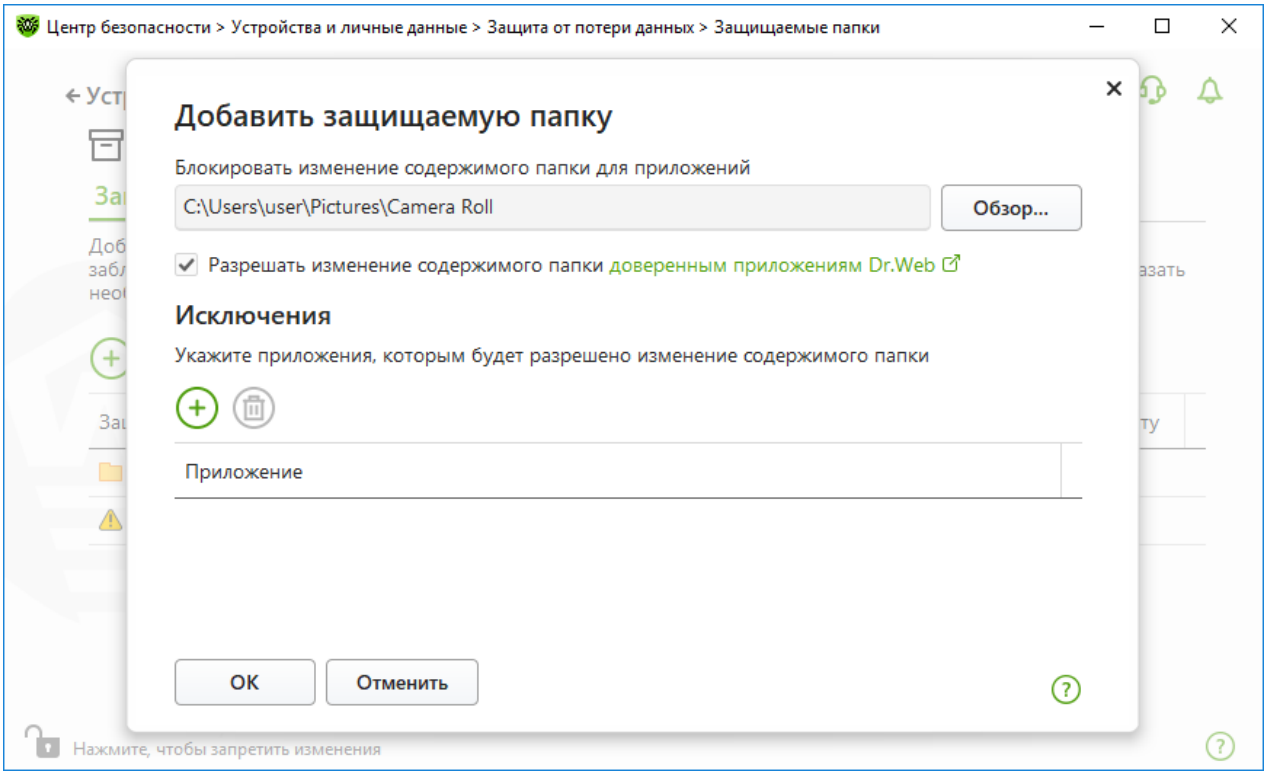

Рисунок 64. Добавление защищаемой папки

Исключения

Количество приложений, имеющих полный доступ к защищаемой папке, указано на главном окне Защиты от потери данных в столбце **Пользовательские исключения**.

Чтобы добавить приложение в исключения

1. В окне Защита от потери данных нажмите ⊕, чтобы добавить новую папку в список защищаемых.
2. В открывшемся окне нажмите ⊕. Выберите приложение, которое будет иметь полный доступ к объектам в защищаемой папке.
3. Нажмите **OK**.

Чтобы изменить список исключений для защищаемых папок

1. Выберите папку из списка и нажмите .
2. В нижней части открывшегося окна в таблице указаны все приложения, которые имеют полный доступ к выбранной папке.
   - Чтобы добавить новое приложение, нажмите .
   - Чтобы удалить приложение из списка исключений, нажмите .
3. Нажмите **OK**.

Сохраненные копии

Вкладка доступна, только если остались сохраненные в предыдущих версиях программы копии файлов. Функция позволяет восстановить или удалить сохраненные копии, но сохранение новых копий недоступно.

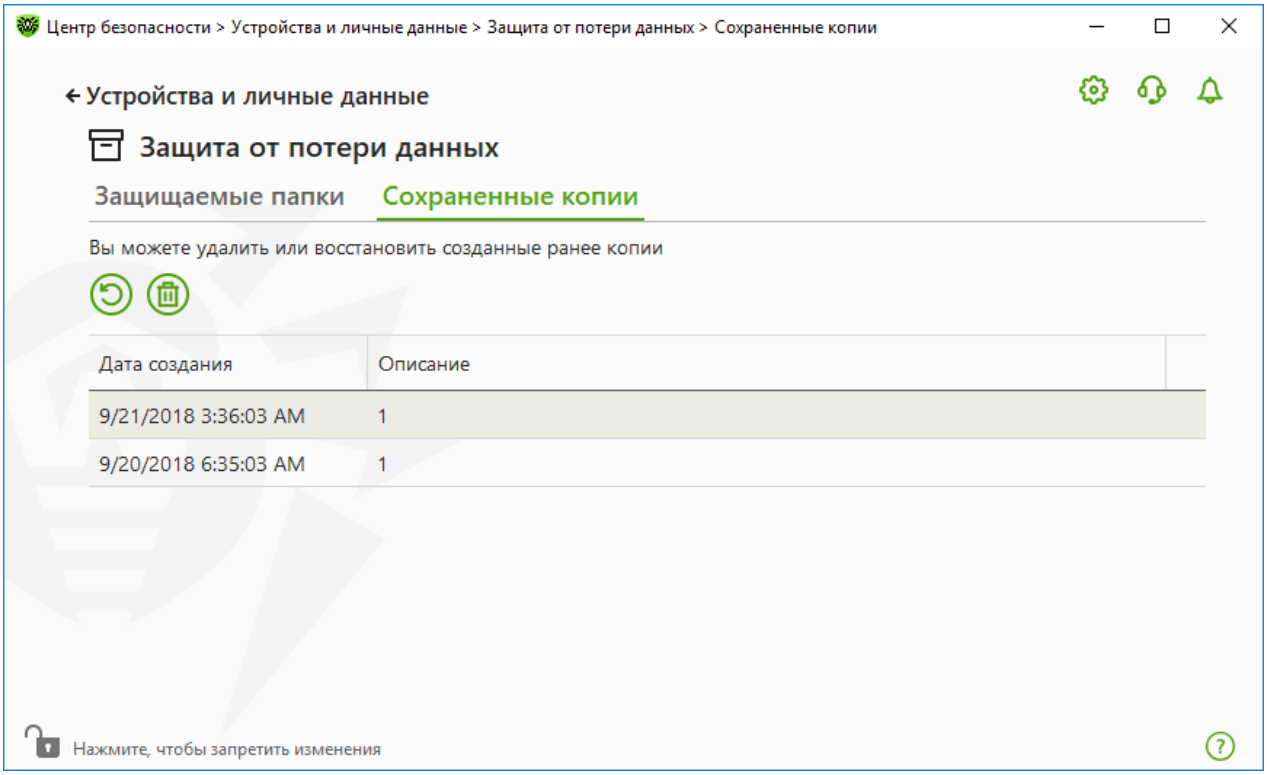

Рисунок 65. Список сохраненных копий

Удаление созданных копий

Вы можете удалить существующие копии, чтобы очистить место на диске (на самих файлах удаление копий не отразится). Для этого выберите необходимую копию и нажмите кнопку .

Восстановление файлов

В случае если ваши файлы были повреждены, вы можете восстановить их копии за определенную дату. Для этого:

1. Выберите необходимую копию (дата сохранения копии указана в столбце слева) и нажмите кнопку  .
2. В открывшемся окне укажите путь к папке, куда будут восстановлены файлы.

13.2. Блокировка устройств

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. В открывшемся окне нажмите плитку **Устройства и личные данные**.
3. Убедитесь, что Dr.Web работает в режиме администратора (замок в нижней части программы «открыт» ). В противном случае нажмите на замок  .
4. Нажмите плитку **Устройства**.

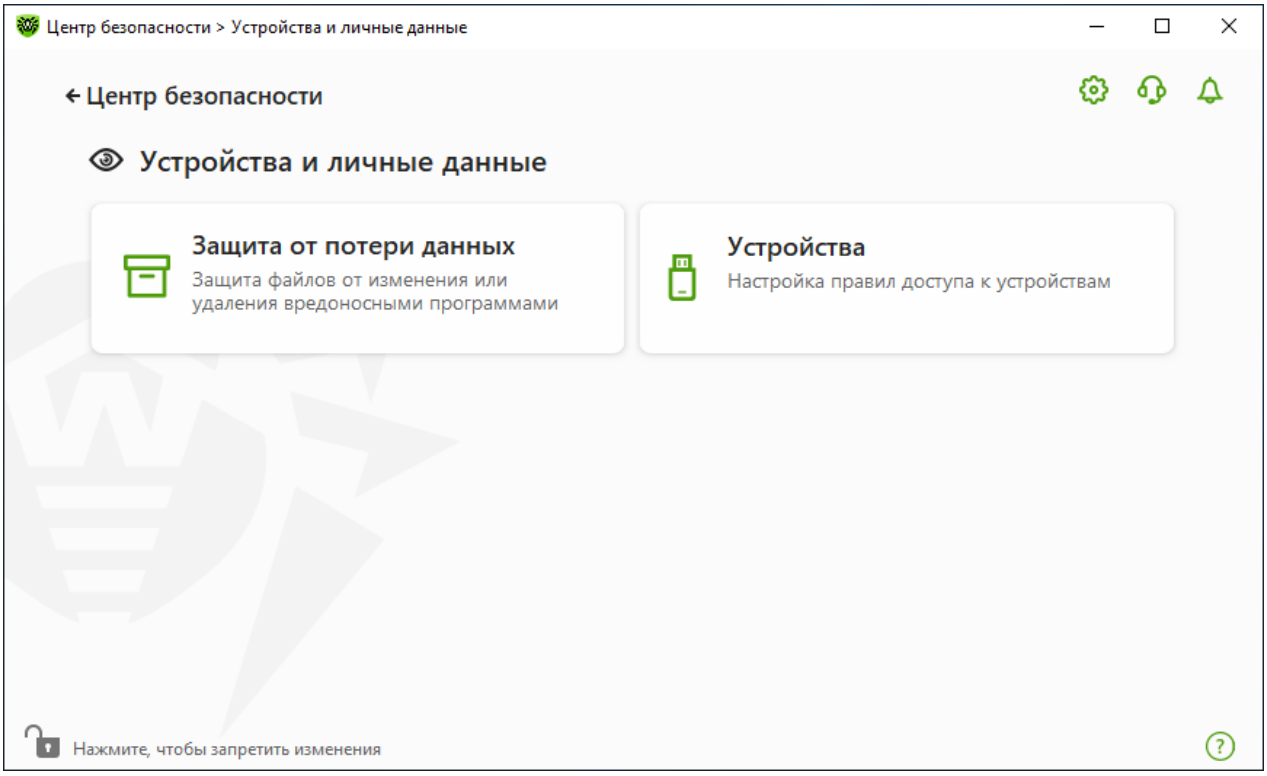

Рисунок 66. Доступ к окну Устройства

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.

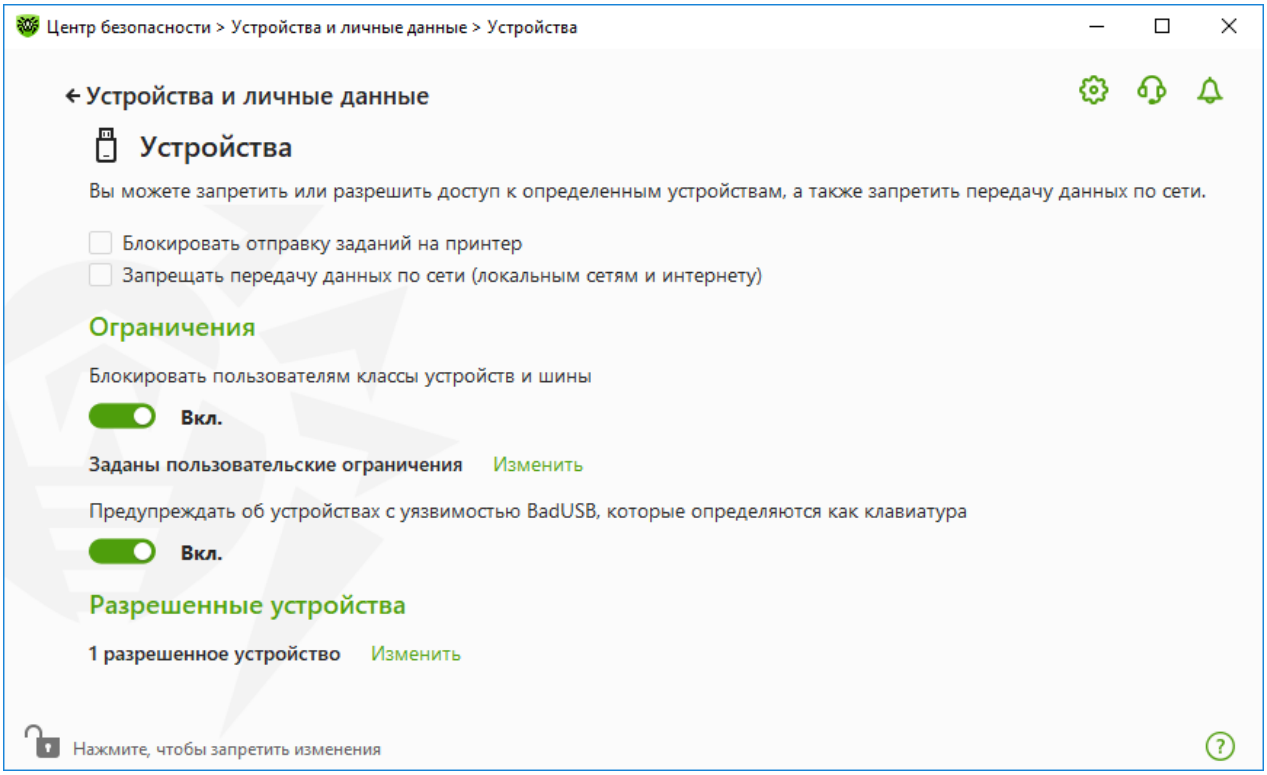

Рисунок 67. Параметры блокировки устройств

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.

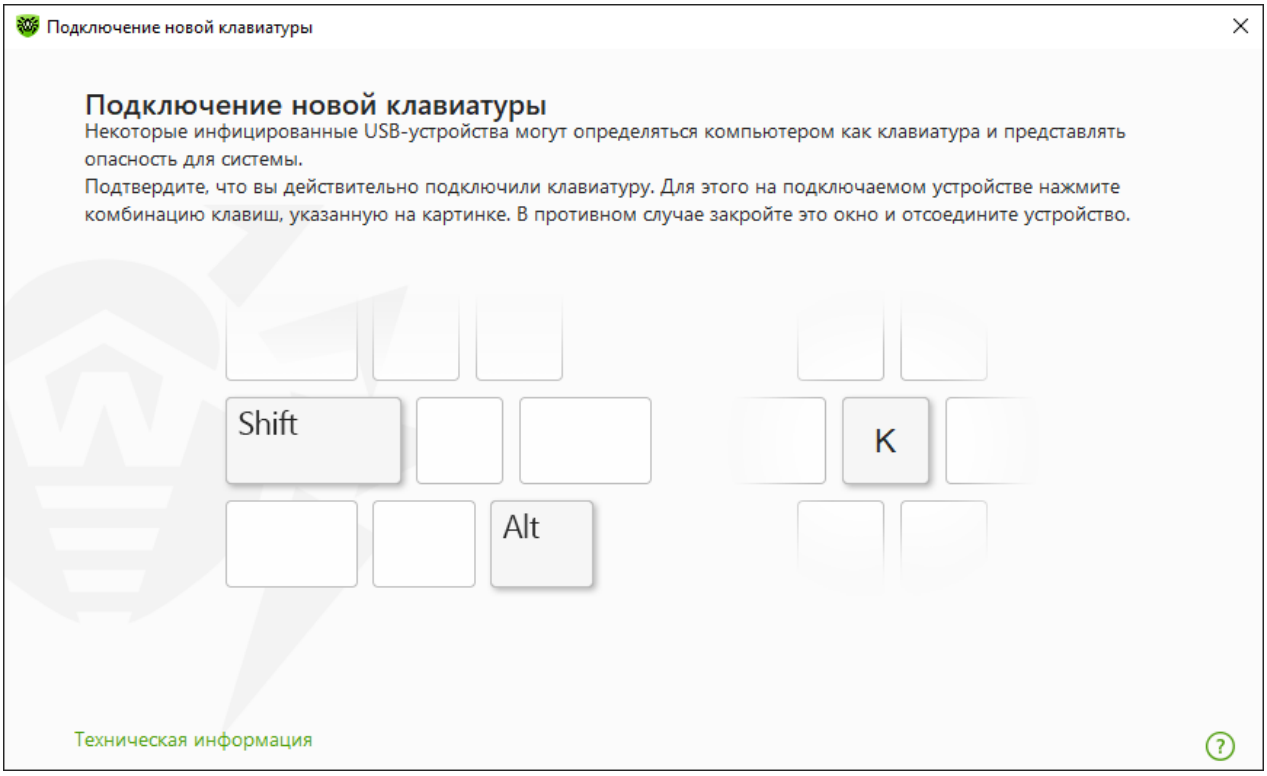

Рисунок 68. Окно разблокировки клавиатуры

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.

Для добавления устройств в список разрешенных в опции **Разрешенные устройства** нажмите **Изменить** (ссылка становится активна, если заданы ограничения). В открывшемся окне вы можете сформировать список устройств, на которые не будут распространяться ограничения доступа.

13.2.1. 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 и личные данные**.
3. В открывшемся окне нажмите плитку **Устройства**.
4. В группе настроек **Ограничения** включите опцию **Блокировать пользователям классы и шины устройств** при помощи переключателя .
5. Нажмите ссылку **Изменить**.
6. 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.

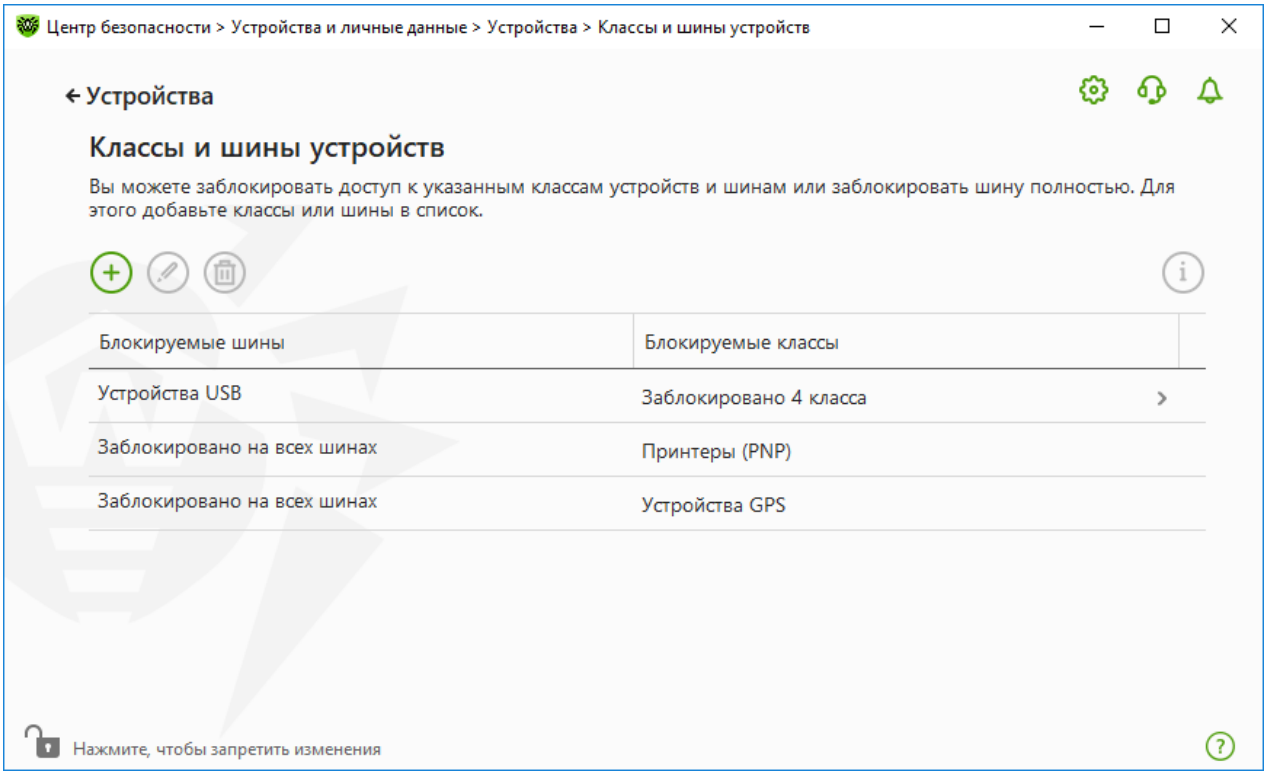

Рисунок 69. Заблокированные шины и классы

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**.

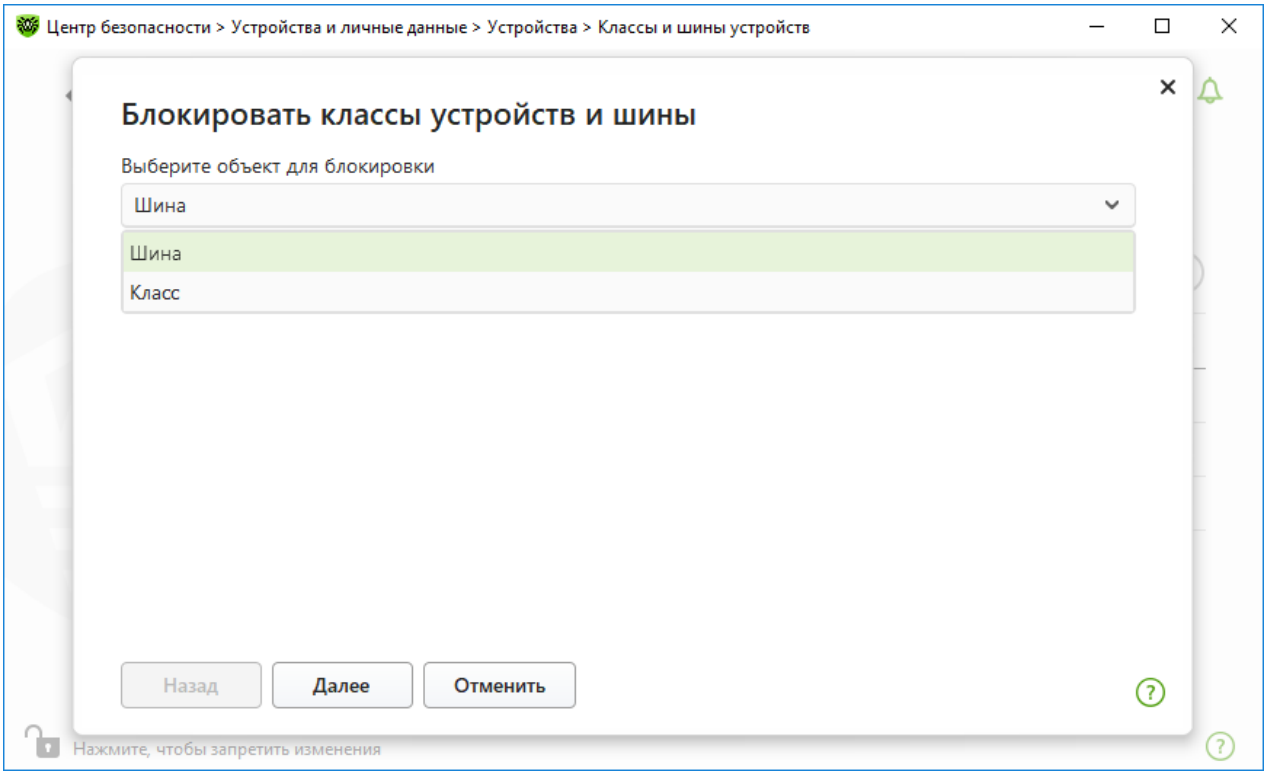

Рисунок 70. Выбор объекта для блокировки

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

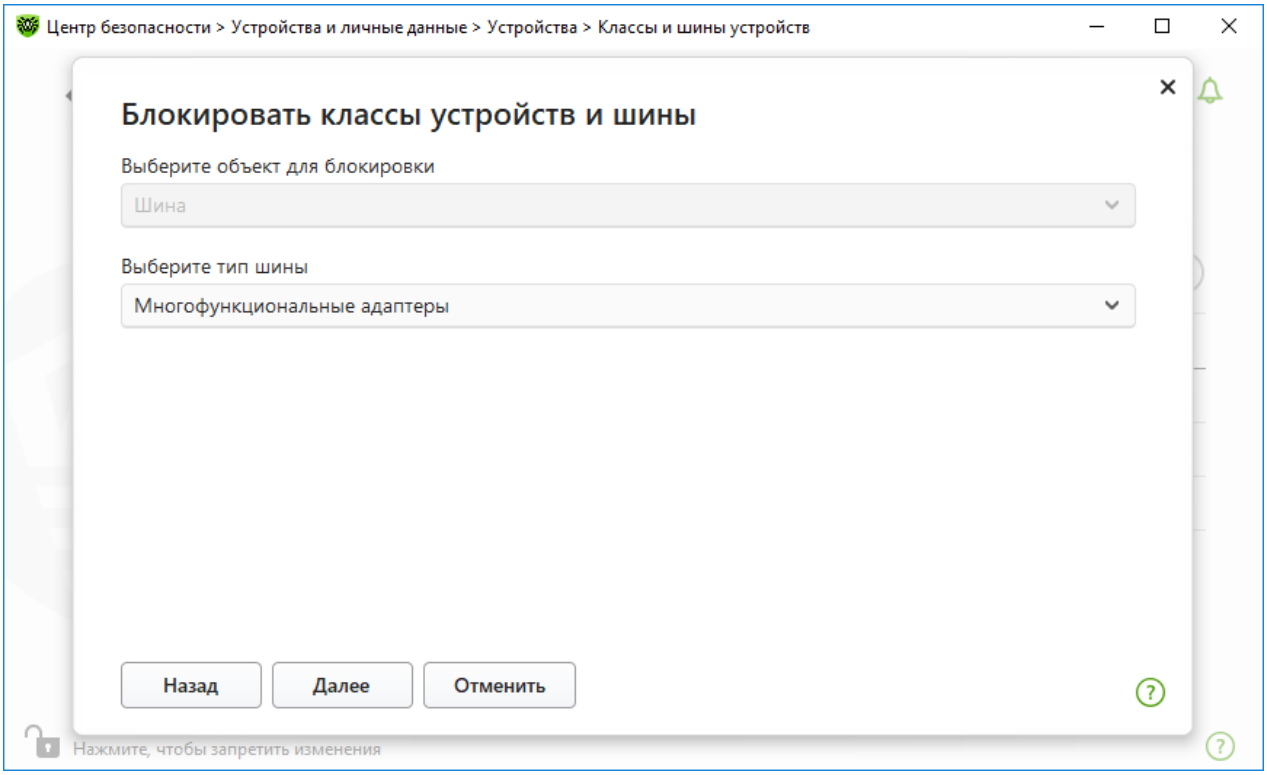

Рисунок 71. Выбор типа шины

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.

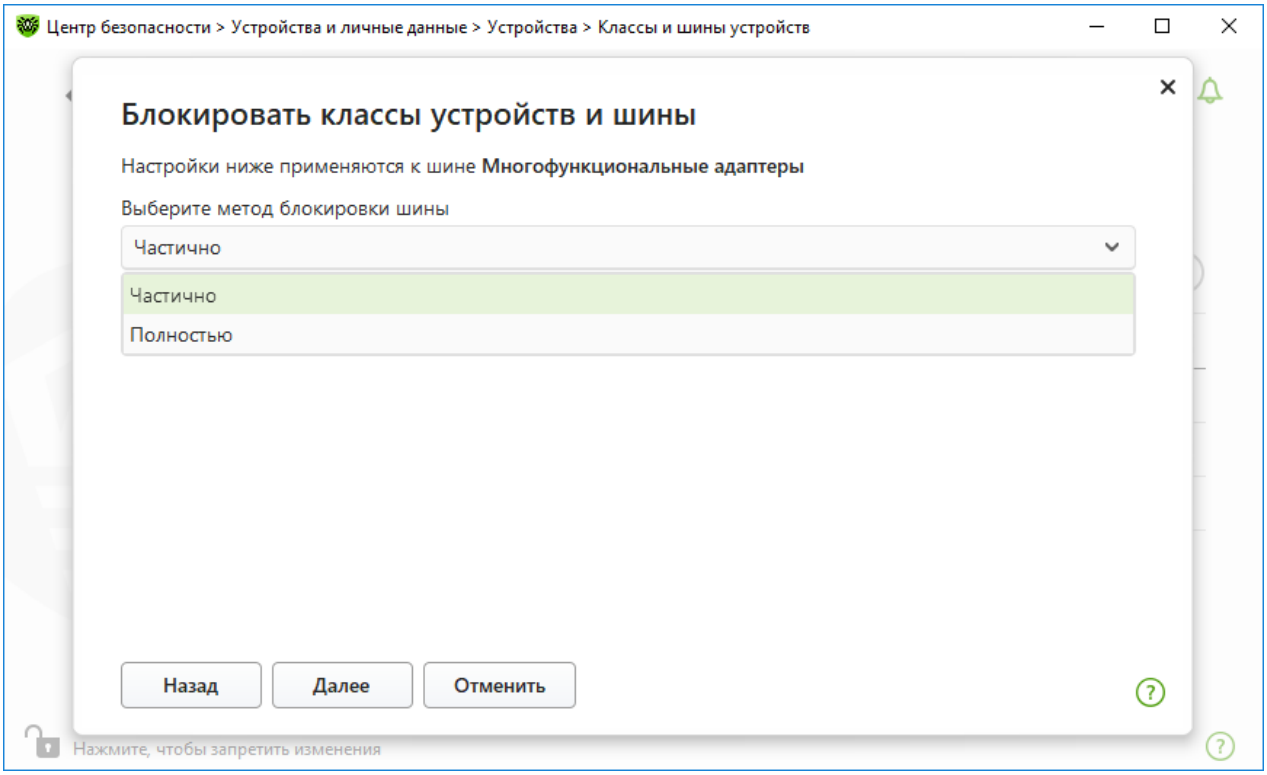

Рисунок 72. Выбор метода блокировки шины

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

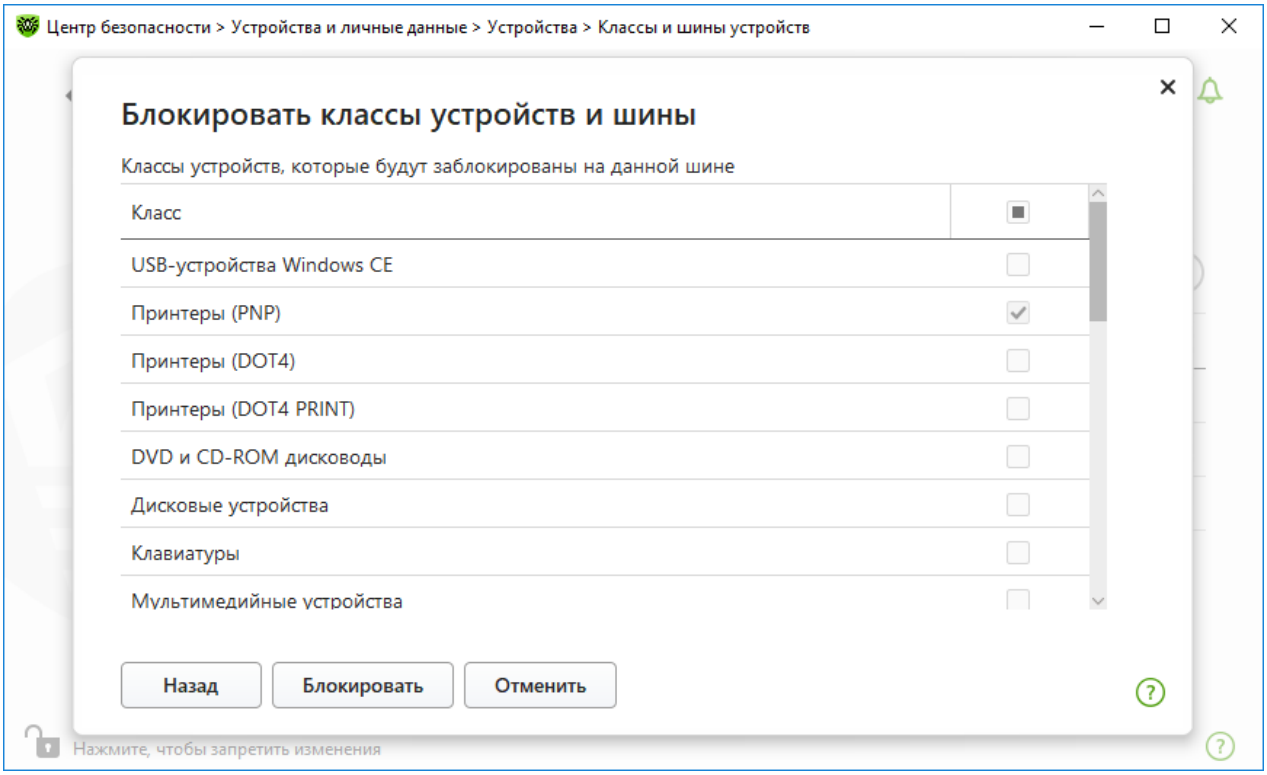

Рисунок 73. Выбор классов устройств на шине

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**.

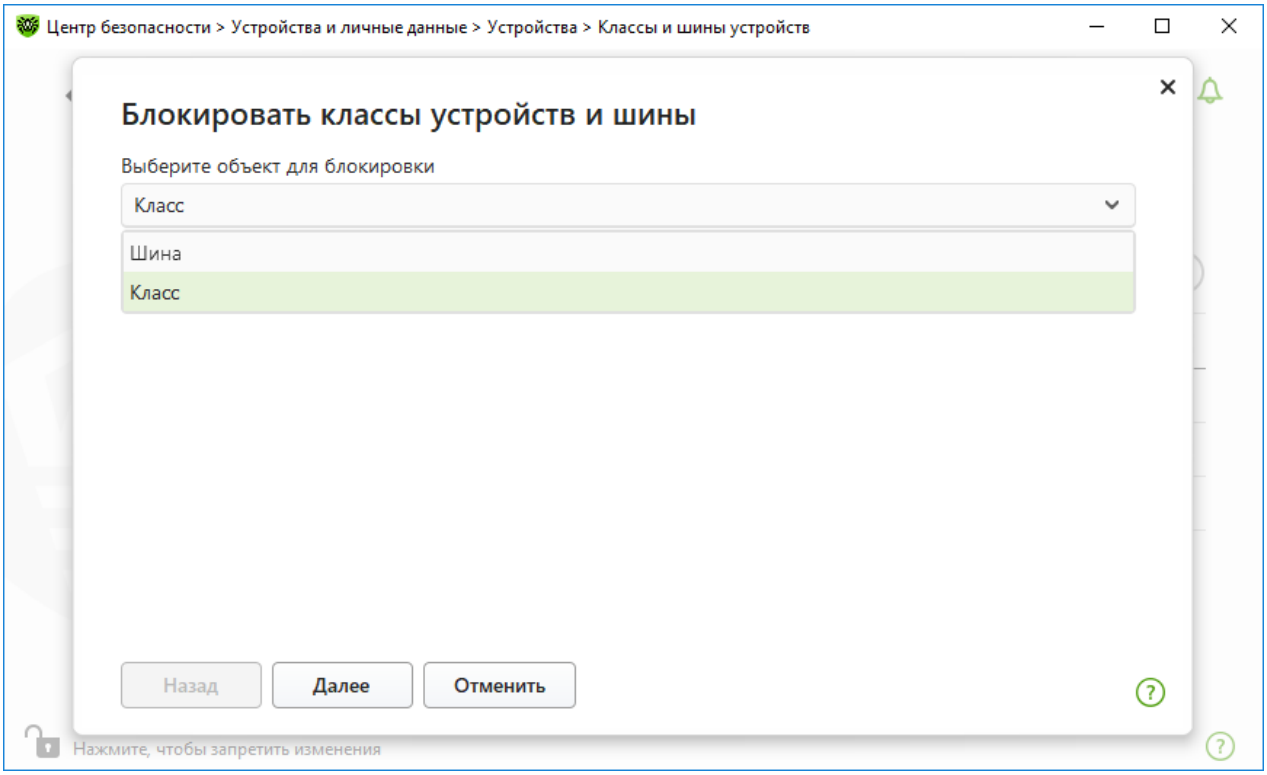

Рисунок 74. Выбор объекта для блокировки

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

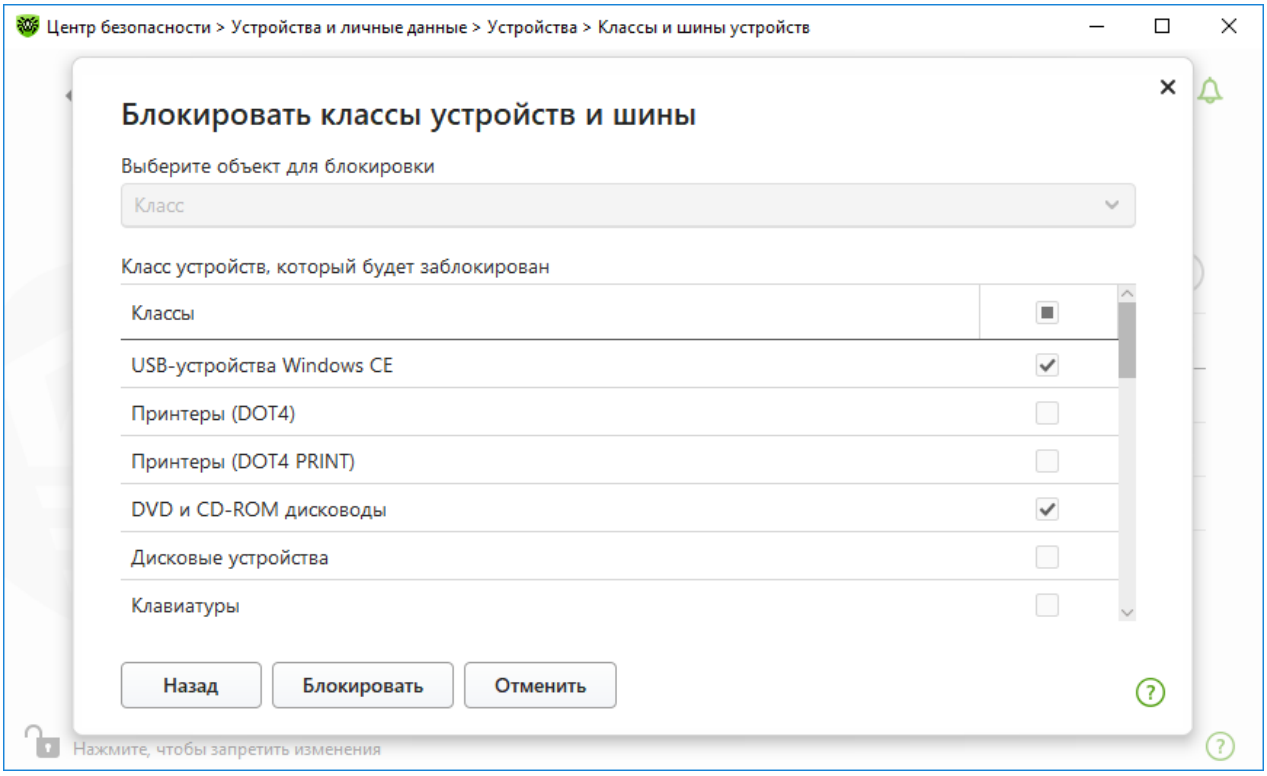

Рисунок 75. Выбор классов устройств

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 и отправку этих уведомлений на электронную почту.

13.2.2. 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 и личные данные**.
3. В открывшемся окне нажмите плитку **Устройства**.
4. 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:

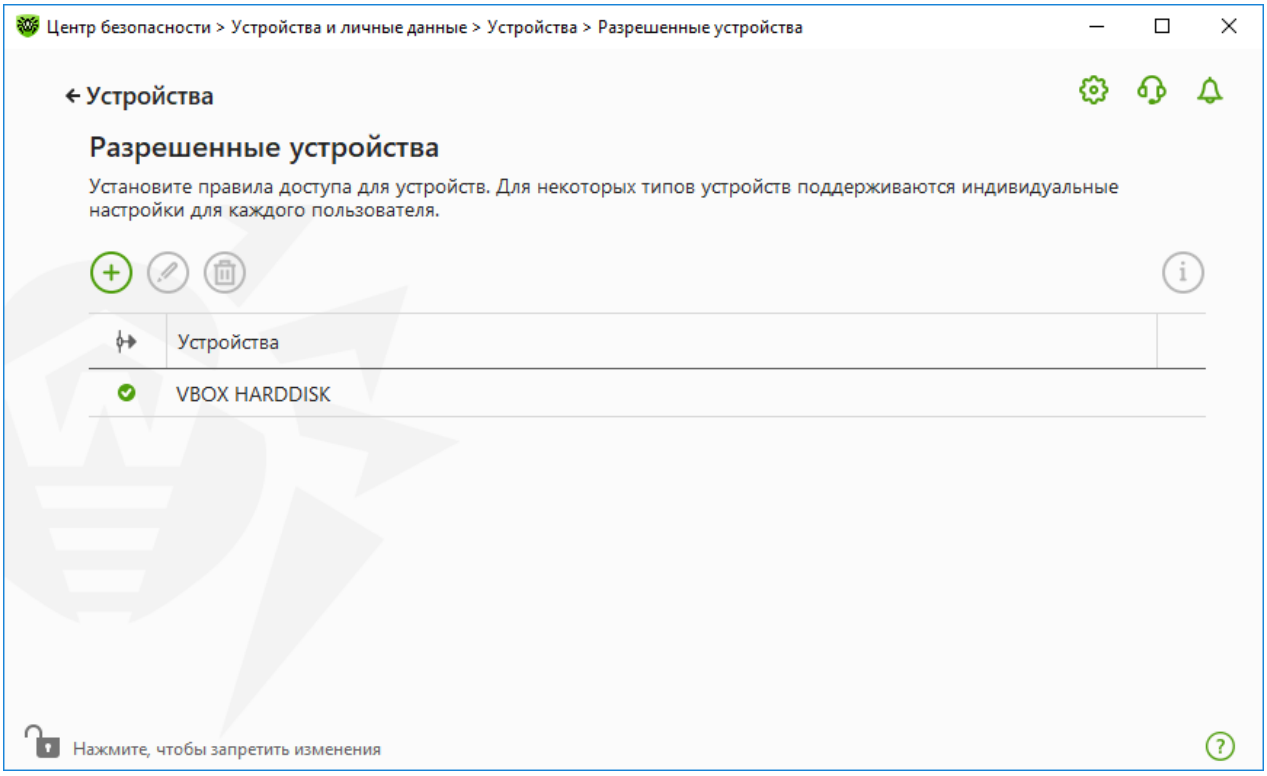

Рисунок 76. Разрешенные устройства

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**.

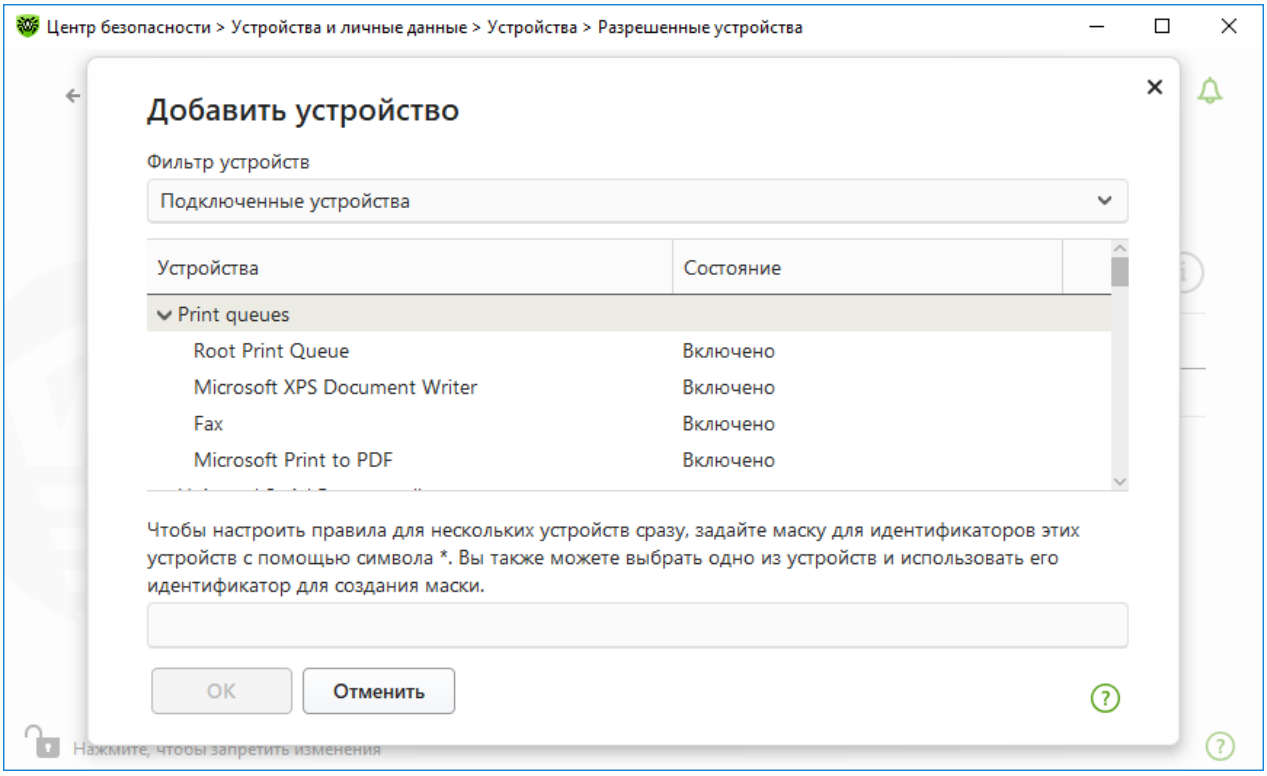

Рисунок 77. Добавление устройства в список разрешенных

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 🗑.

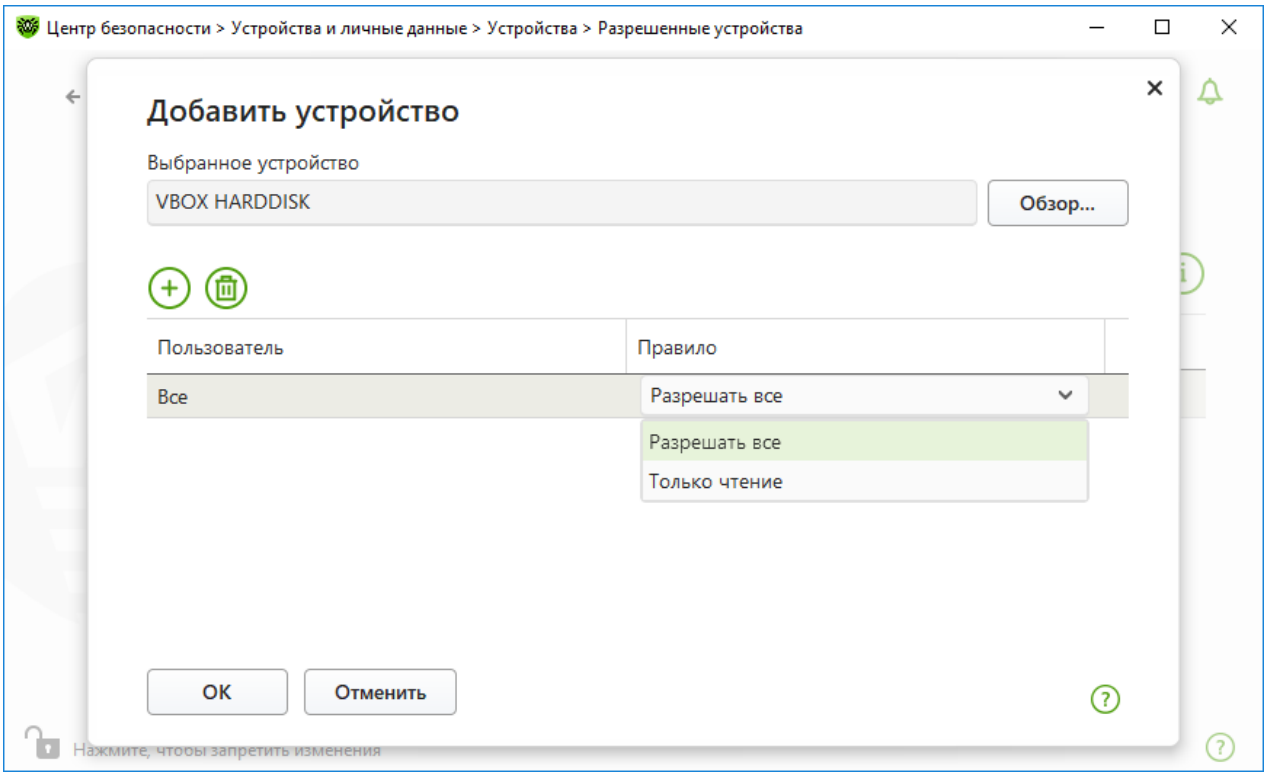

Рисунок 78. Выбор правила для конкретного пользователя

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

14. Инструменты

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

Чтобы перейти в группу настроек Инструменты

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

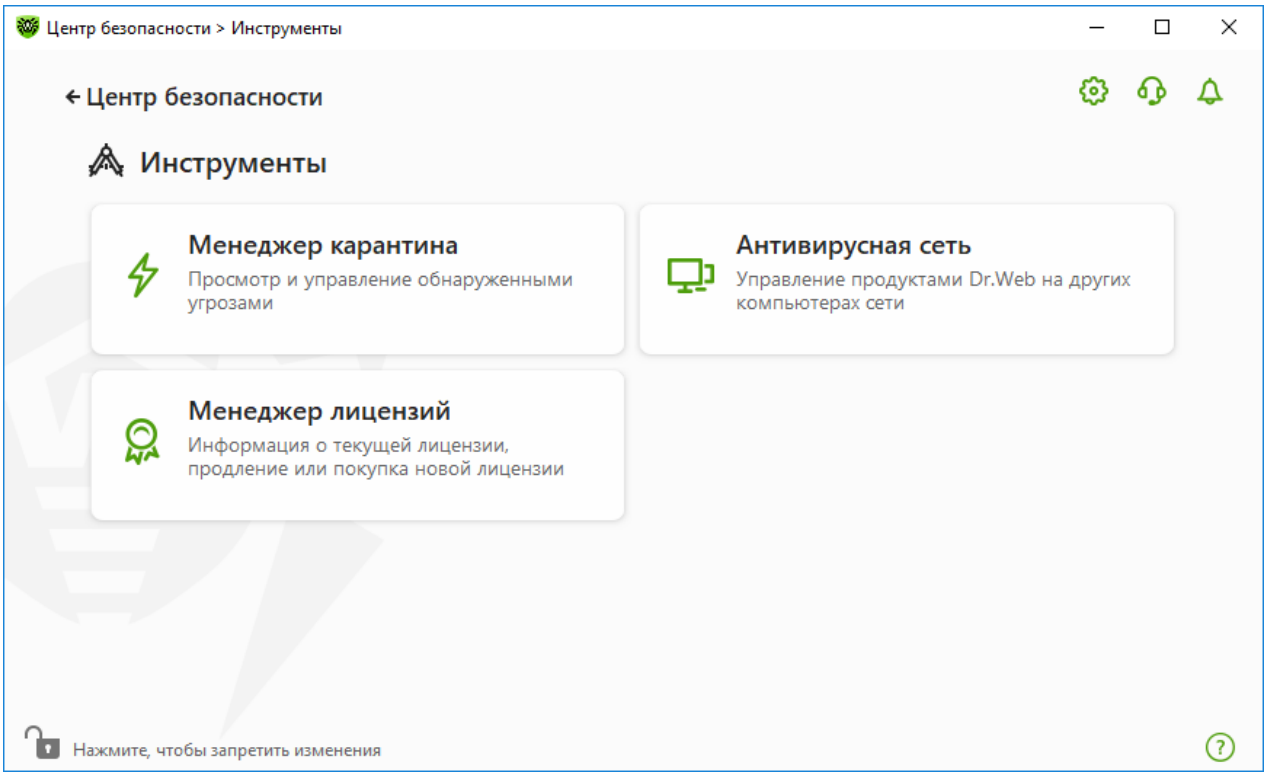

Рисунок 79. Окно Инструменты

Для перехода к необходимому инструменту нажмите соответствующую плитку.

В этом разделе:

- Менеджер карантина — список изолированных файлов и возможность их восстановления.
- Антивирусная сеть — удаленный доступ к продуктам Dr.Web, установленных на других компьютерах внутри вашей сети.
- Менеджер лицензий — информация о лицензии, получение новой лицензии.

14.1. Менеджер карантина

Менеджер карантина — инструмент, позволяющий управлять изолированными файлами. В карантине содержатся файлы, в которых были обнаружены вредоносные объекты. Также в карантин помещаются резервные копии файлов, обработанных Dr.Web. Менеджер карантина предоставляет возможность удаления, перепроверки и восстановления изолированных файлов.

Чтобы перейти в окно Менеджер карантина

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

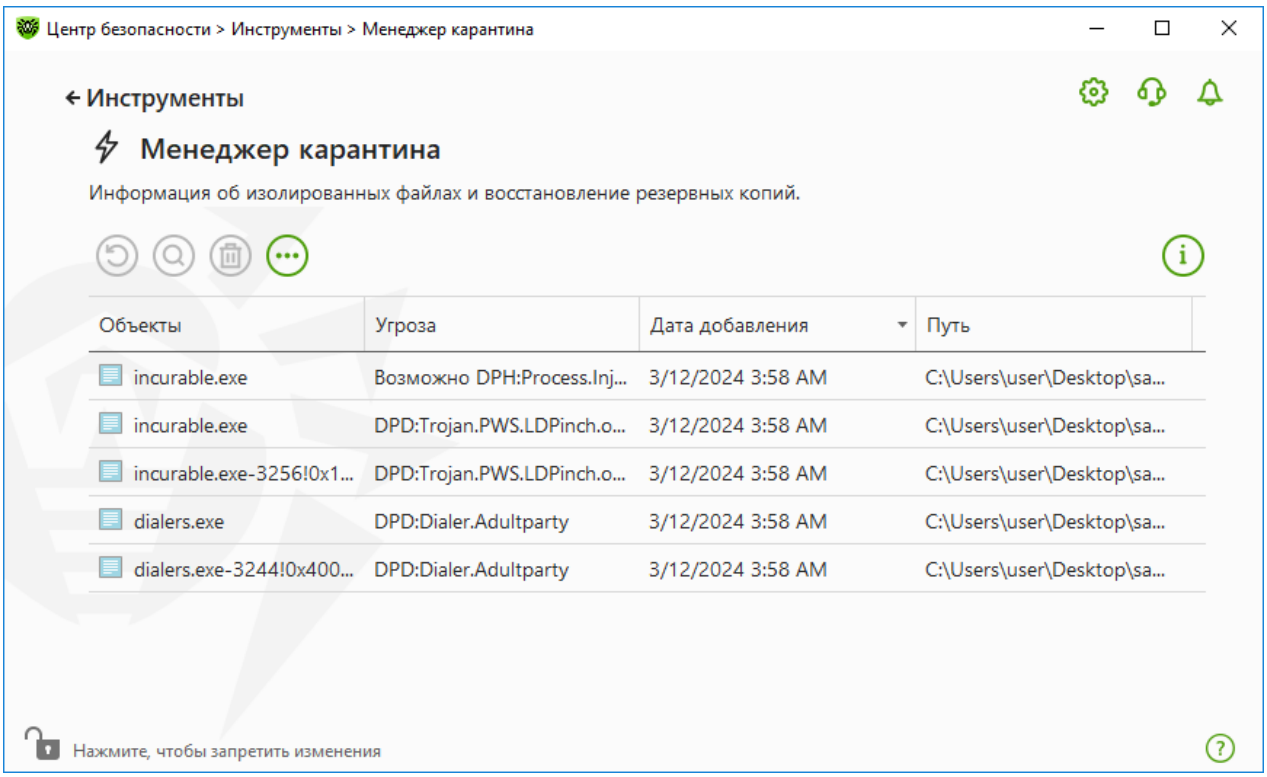

Рисунок 80. Объекты в карантине

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.

14.2. Антивирусная сеть

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

Чтобы перейти в окно Антивирусная сеть

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

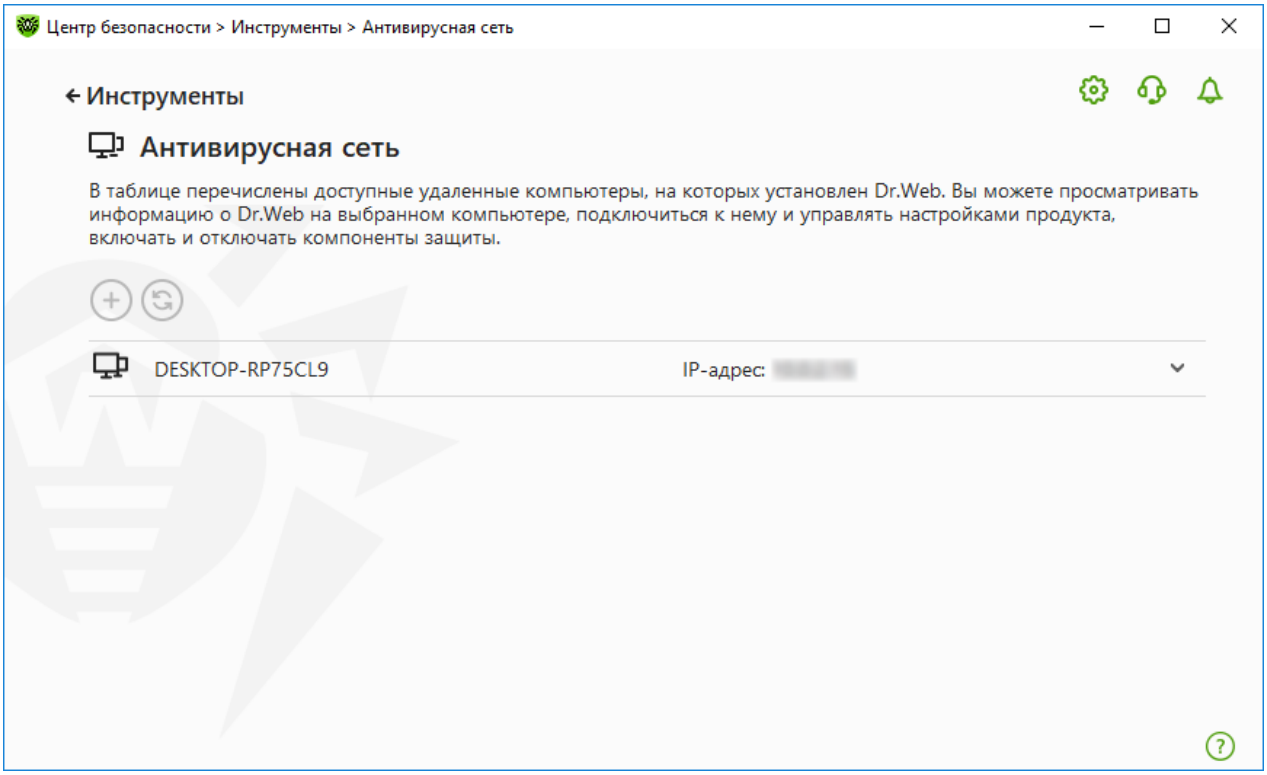

Рисунок 81. Компьютеры антивирусной сети

Компьютеры в локальной сети отображаются в списке только в том случае, если в установленном на них продукте Dr.Web разрешено удаленное управление. Вы можете разрешить подключение к Dr.Web на вашем компьютере в окне настроек Антивирусной сети.

Если необходимый компьютер не отображается в сети, попробуйте добавить его вручную. Для этого нажмите кнопку ⊕ и введите IP-адрес в формате IPv4 или IPv6.

Если на станции отключен какой-либо из компонентов, появляется индикация в виде восклицательного знака.

Параметры работы Антивирусной сети

В ходе работы антивирусной сети используются multicast и UDP-запросы со следующими параметрами:

Параметры для multicast:

- IP-адрес: 239.194.75.48 или ff08::28 для IPv4 и IPv6 соответственно
- Порт: 55566
- Интервал опроса: 2000 мс

Параметры для UDP-запроса:

- Порт: 55566
- Интервал опроса: 2000 мс

Чтобы подключиться к удаленному антивирусу

1. Выберите нужный компьютер из списка. В раскрывшейся строке отобразится подробная информация о статусе компонентов на станции и о последнем обновлении.
2. Нажмите кнопку **Подключиться**.
3. Введите код, заданный в настройках удаленного антивируса. В области уведомлений Windows вашего компьютера появится значок удаленного антивируса  , а также будет показано уведомление об успешном подключении.

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

Вы можете просматривать статистику, включать и отключать модули, а также изменять их параметры. Антивирусная сеть, Карантин, Сканер и Защита от потери данных недоступны.

Также вам доступен пункт **Отсоединиться**, при выборе которого завершается установленное соединение с удаленным антивирусом.

14.3. Менеджер лицензий

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

Чтобы перейти в окно Менеджер лицензий из Центра безопасности

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

Чтобы перейти в окно Менеджер лицензий из Меню программы

1. Откройте меню Dr.Web.
2. Выберите пункт **Лицензия**.

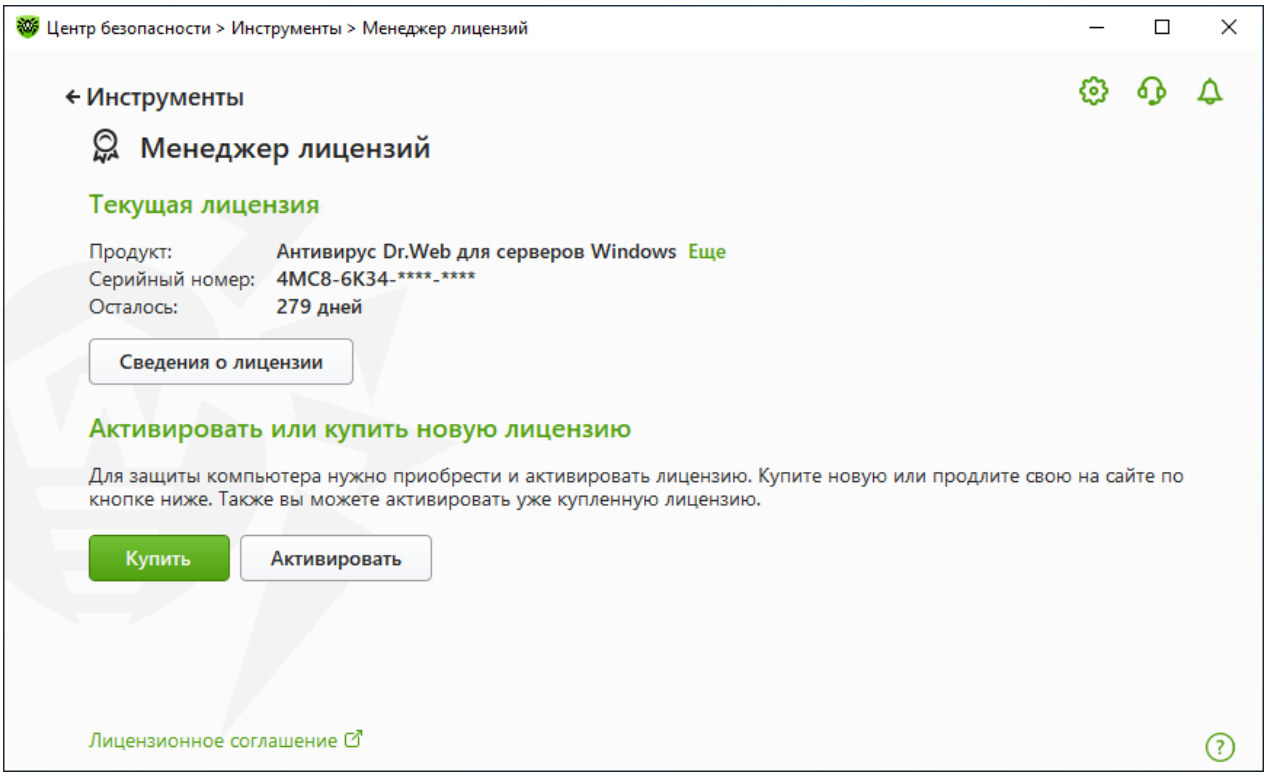

Рисунок 82. Менеджер лицензий

Чтобы посмотреть подробную информацию о текущей лицензии, нажмите кнопку **Сведения о лицензии**.

Чтобы просмотреть информацию о лицензии, которая на данный момент не является текущей

1. Нажмите кнопку **Сведения о лицензии**. Откроется окно Сведений о лицензии.
2. В выпадающем списке выберите подходящую лицензию.

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

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

Чтобы удалить лицензию

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

Чтобы назначить текущую лицензию

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

При нажатии кнопки **Купить** программа откроет страницу на сайте компании «Доктор Веб», где вы можете купить или продлить лицензию.

- Если у вас нет активированной лицензии, программа откроет страницу покупки лицензии. Следуйте инструкциям на сайте, чтобы приобрести новую лицензию и активировать ее.
- Если у вас уже есть активированная лицензия, программа откроет страницу продления лицензии, на которую будут переданы параметры используемой лицензии. Следуйте инструкциям на сайте, чтобы приобрести и активировать продление действия лицензии. Подробнее о продлении см. в разделе Продление лицензии.

При нажатии кнопки **Активировать** откроется окно, в котором вы можете активировать новую лицензию.

Дополнительно

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

15. Исключения

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

Чтобы перейти в группу настроек Исключения

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

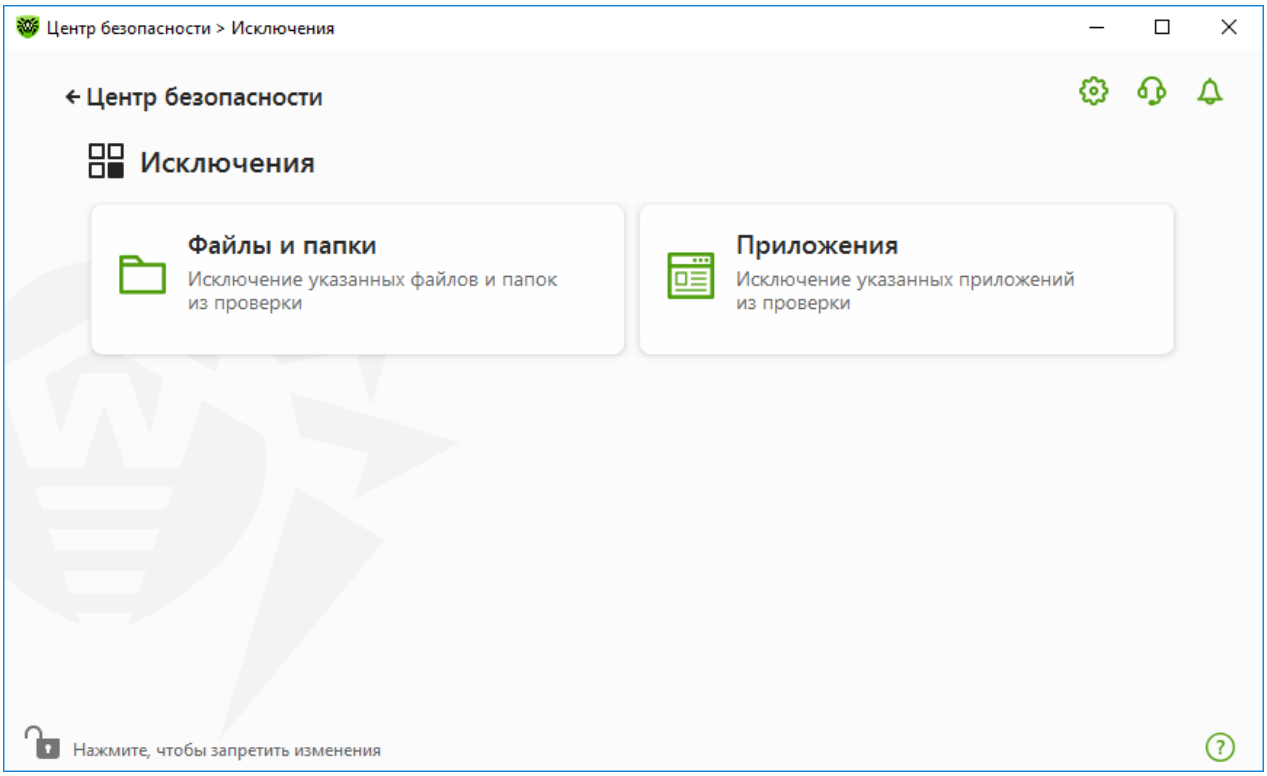

Рисунок 83. Окно Исключения

Чтобы перейти к параметрам исключений

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

В этом разделе:

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

15.1. Файлы и папки

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

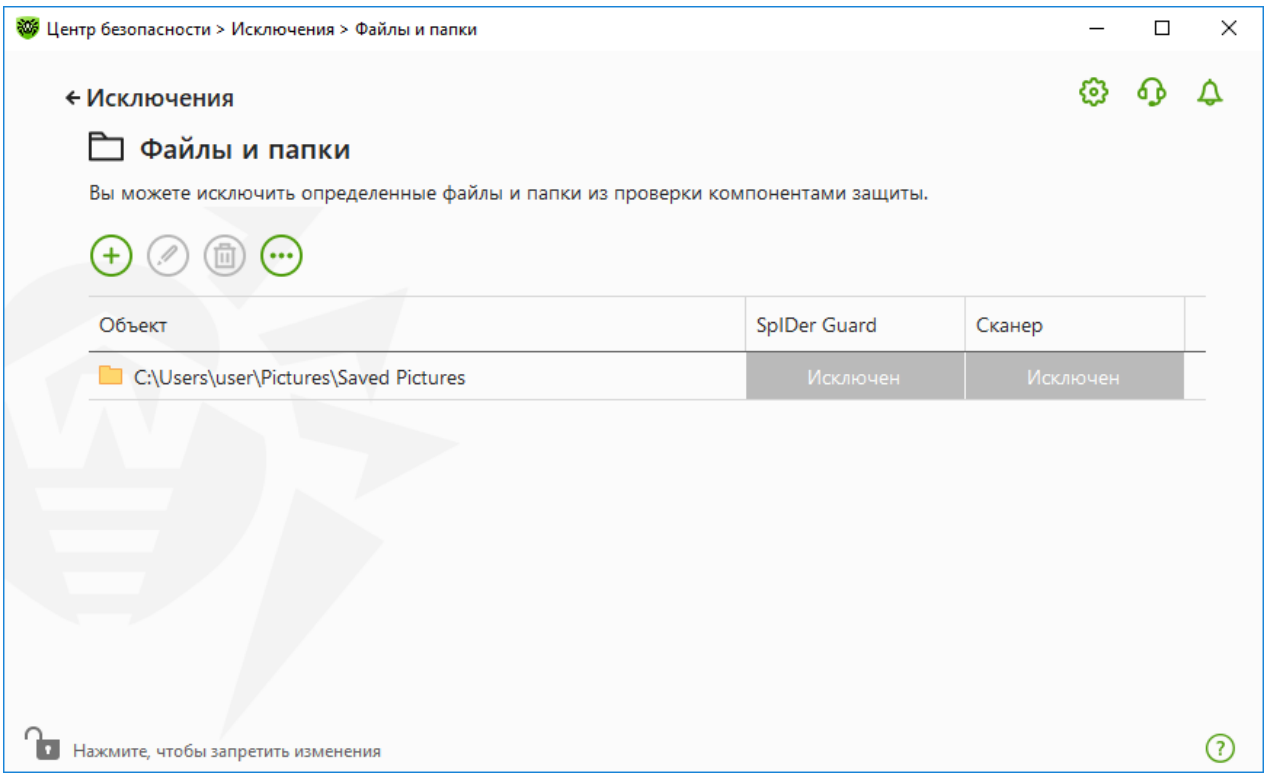

Рисунок 84. Список исключаемых файлов и папок

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.

15.2. Приложения

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

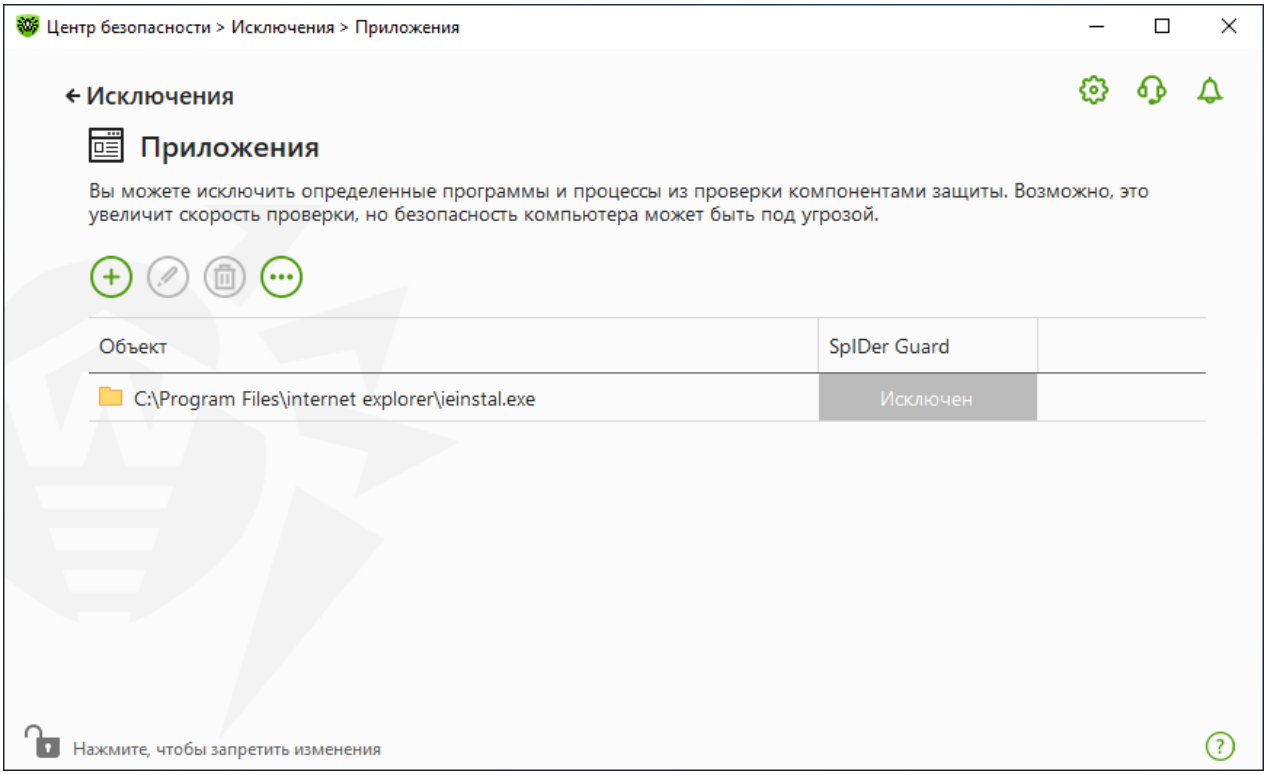

Рисунок 85. Список исключаемых приложений

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 Server 2008 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, что SpIDer Guard не должен проводить проверку выбранного приложения.

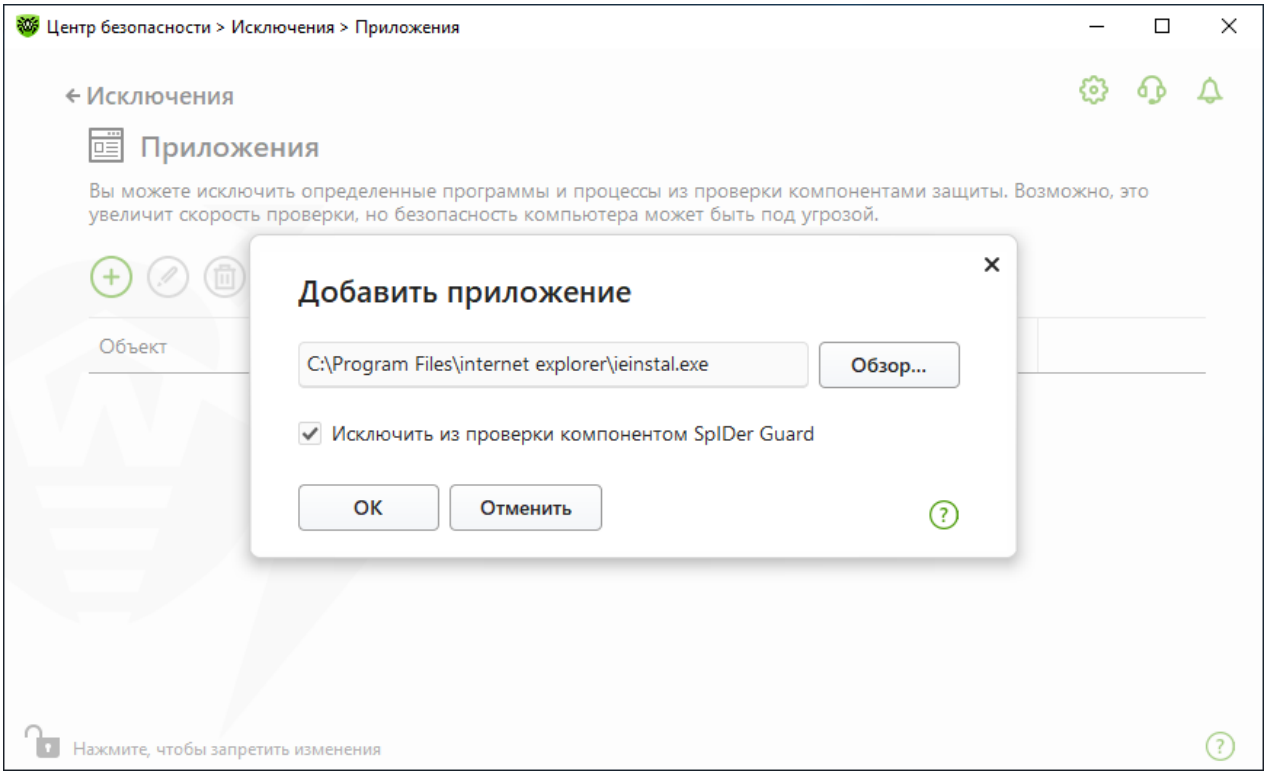

Рисунок 86. Добавление приложений в исключения

3. Нажмите кнопку **OK**. Выбранное приложение появится в списке.
4. 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.

16. Статистика работы компонентов

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

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

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

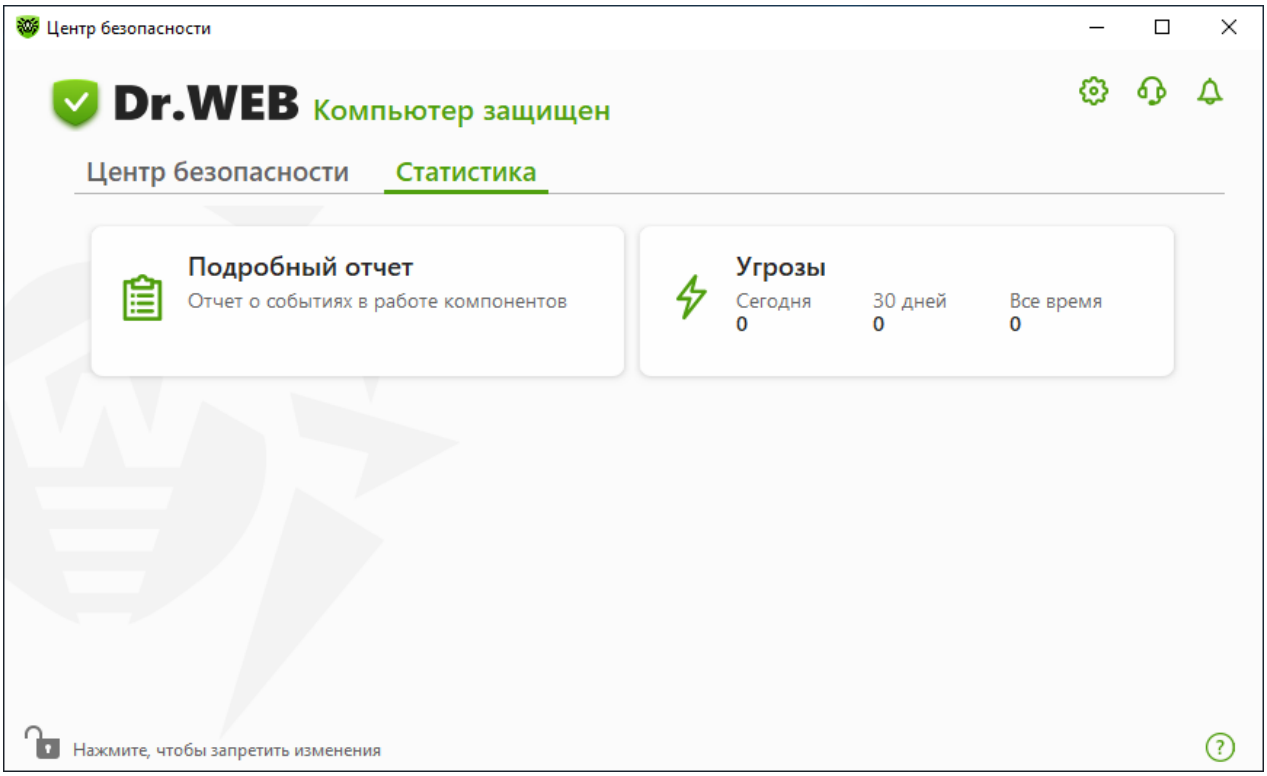

Рисунок 87. Статистика работы компонентов

4. Выберите группу для просмотра отчетов.

Подробный отчет

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

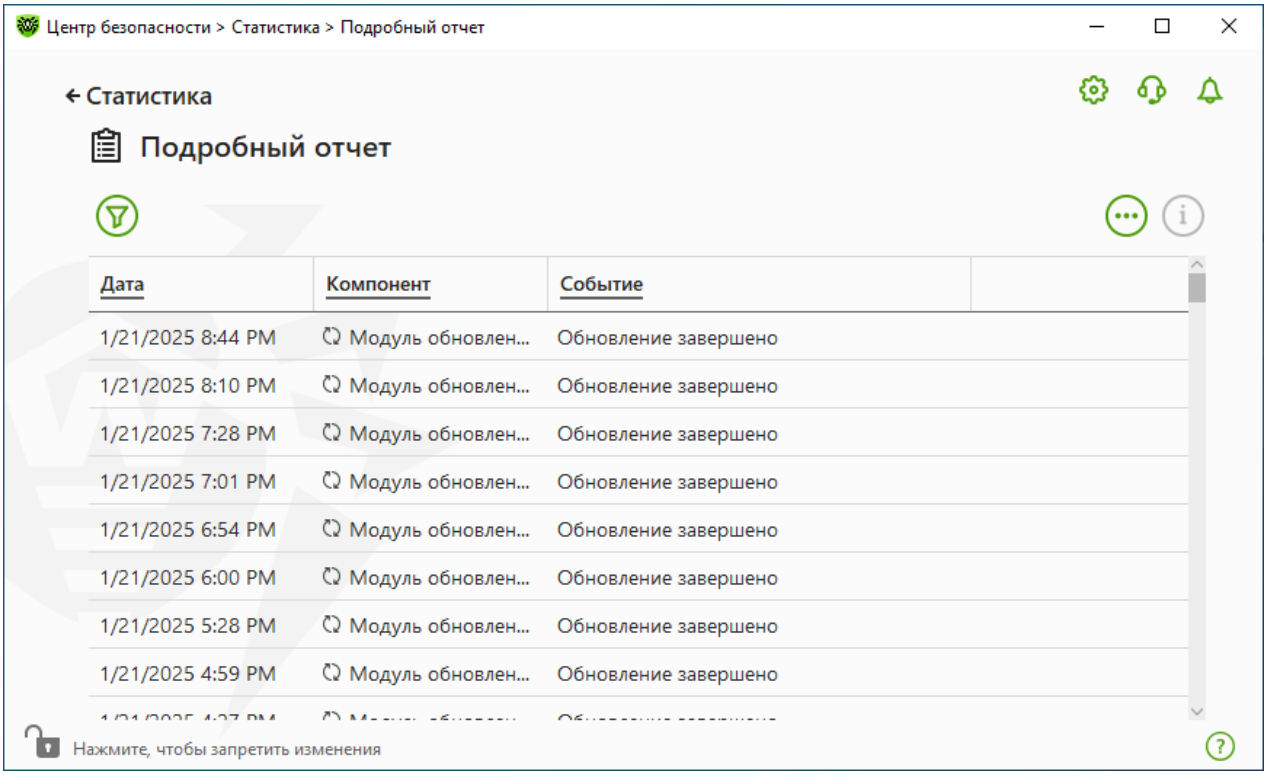

Рисунок 88. Окно подробного отчета

В отчете фиксируются следующие сведения:

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

По умолчанию отображаются все события за все время.

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

Для отбора событий можно воспользоваться дополнительными фильтрами.

Угрозы

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

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

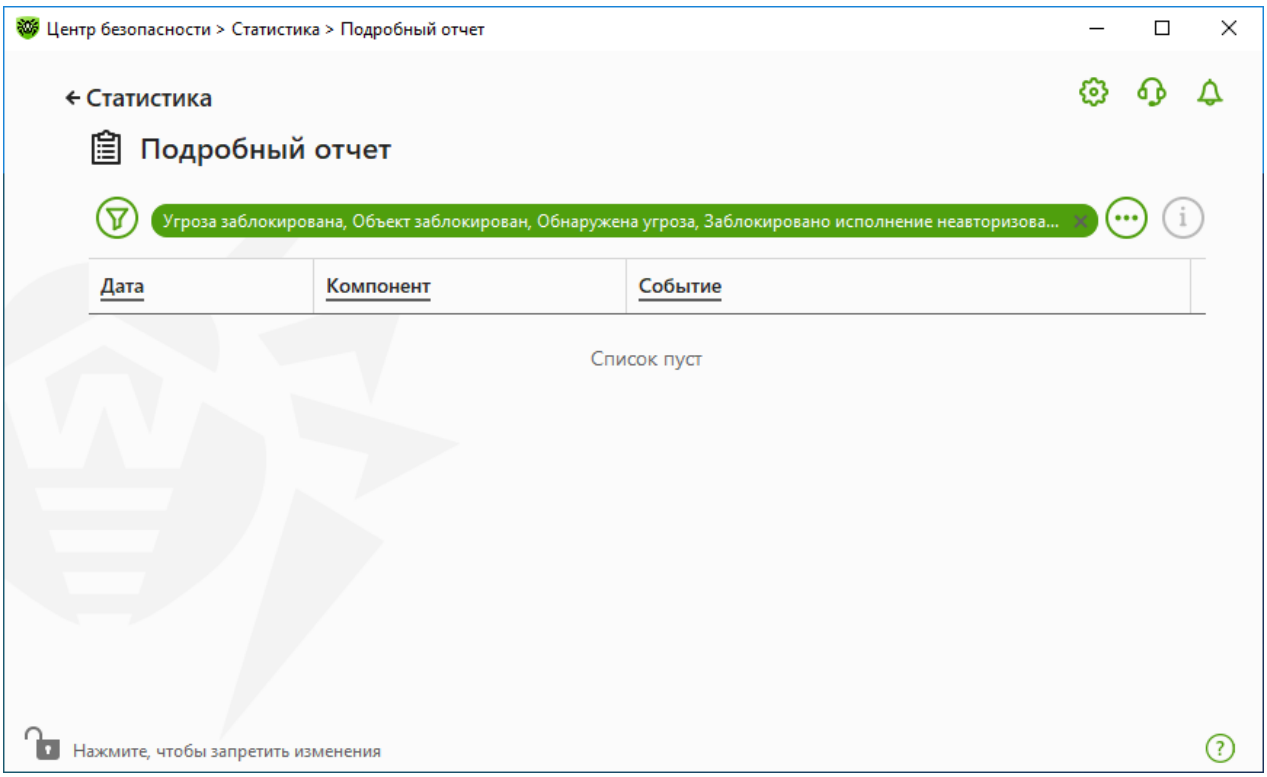

Рисунок 89. Окно статистики по угрозам

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.

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.

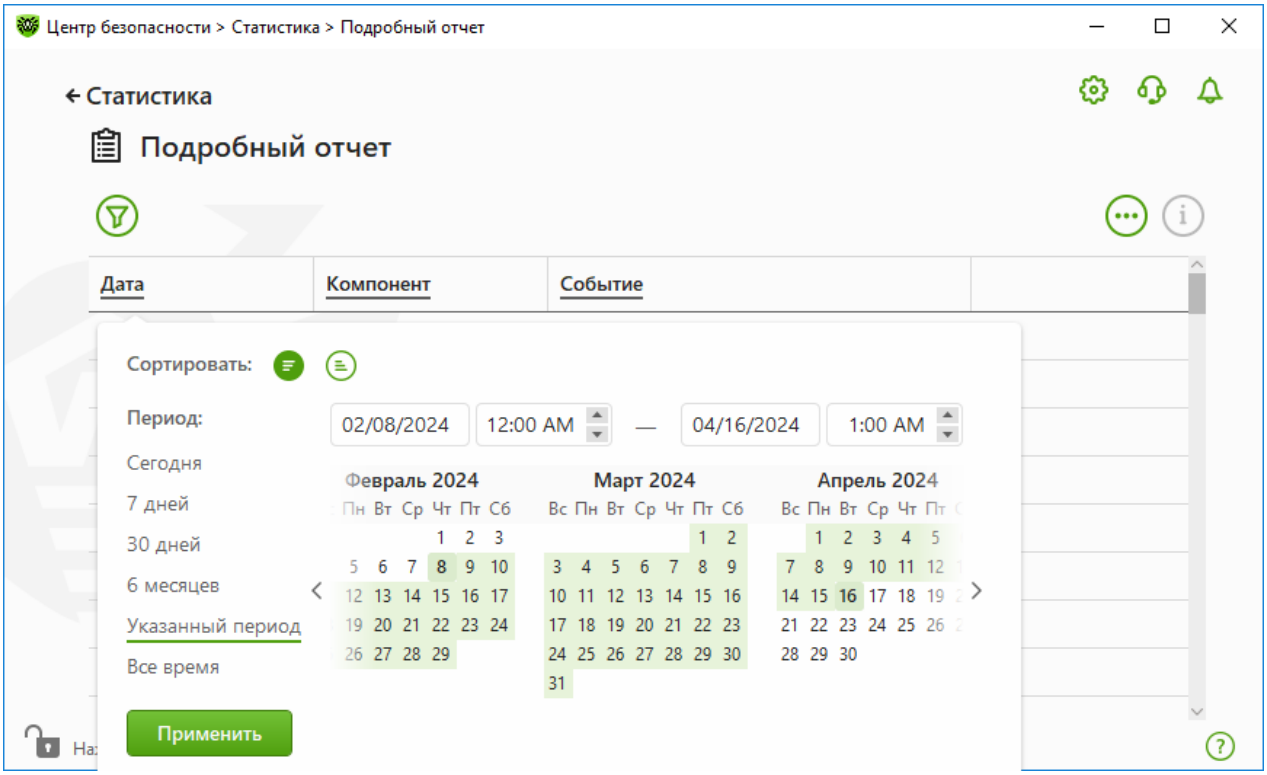

Рисунок 90. Сортировка по дате

- Сортировка по компоненту. Вы можете отметить те компоненты, информация от которых будет отображаться в отчете, либо отсортировать записи по возрастанию или убыванию.
- Сортировка по событию. Вы можете отметить события для отображения в отчете либо отсортировать записи по возрастанию или убыванию.

2. После выбора параметров фильтрации нажмите **Применить**. Выбранные элементы будут отображаться над таблицей.
3. Чтобы сохранить фильтр, нажмите ⓕ и выберите **Сохранить фильтр**.
4. В открывшемся окне укажите название нового фильтра. Нажмите **Сохранить**.

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

Чтобы создать отчет при помощи Мастера отчетов

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

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

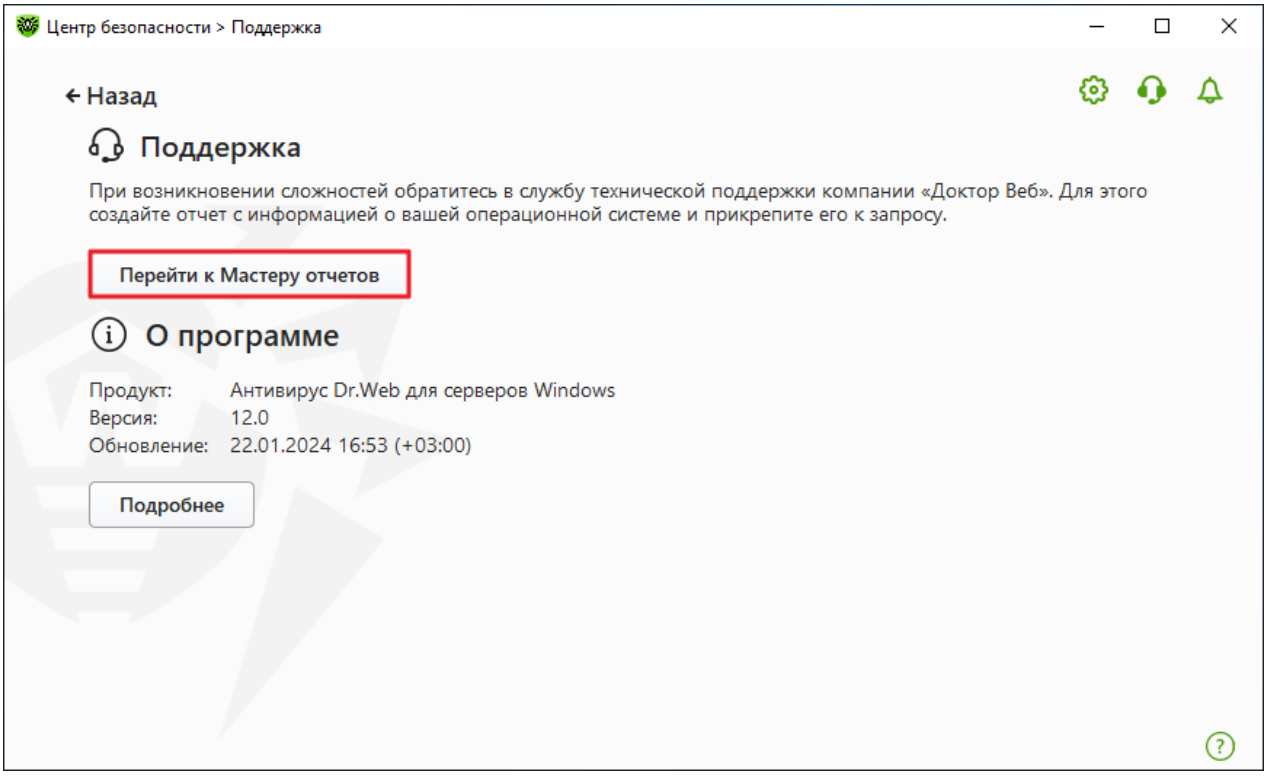

Рисунок 91. Поддержка

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

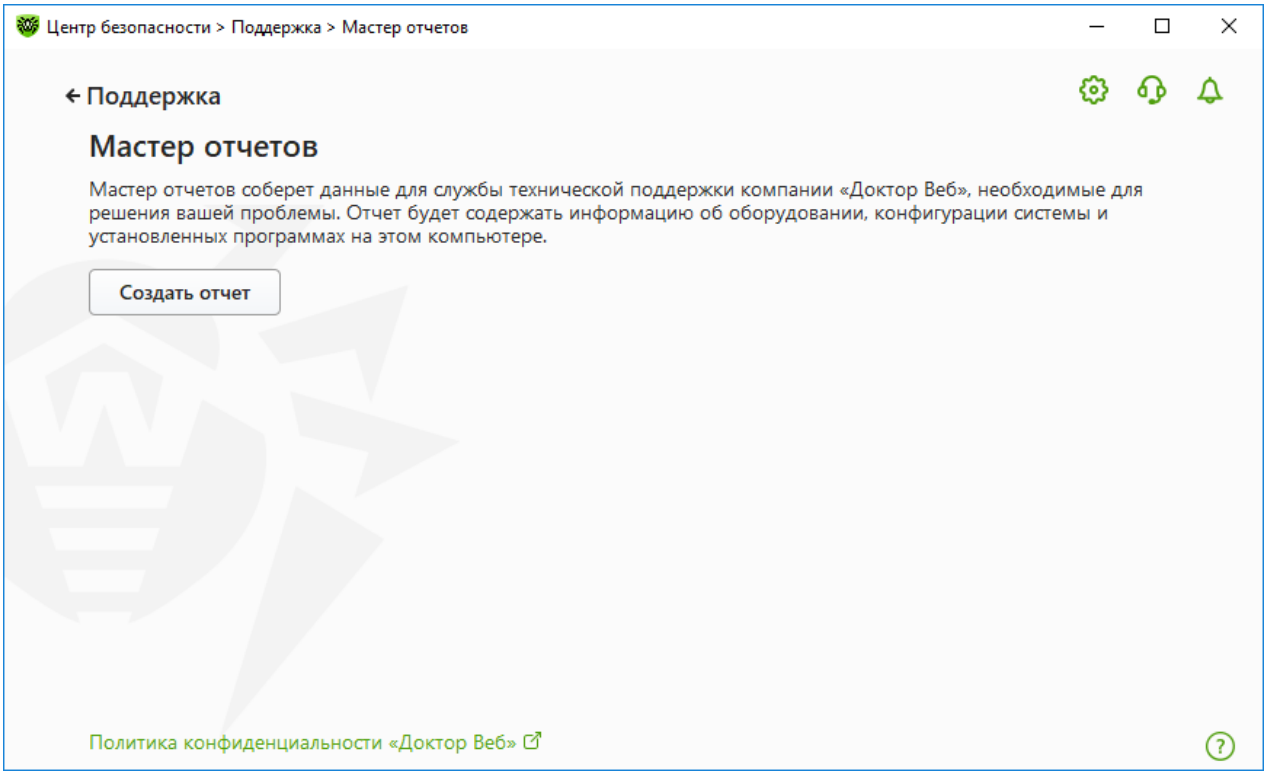

Рисунок 92. Создание отчета для технической поддержки

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.

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**.

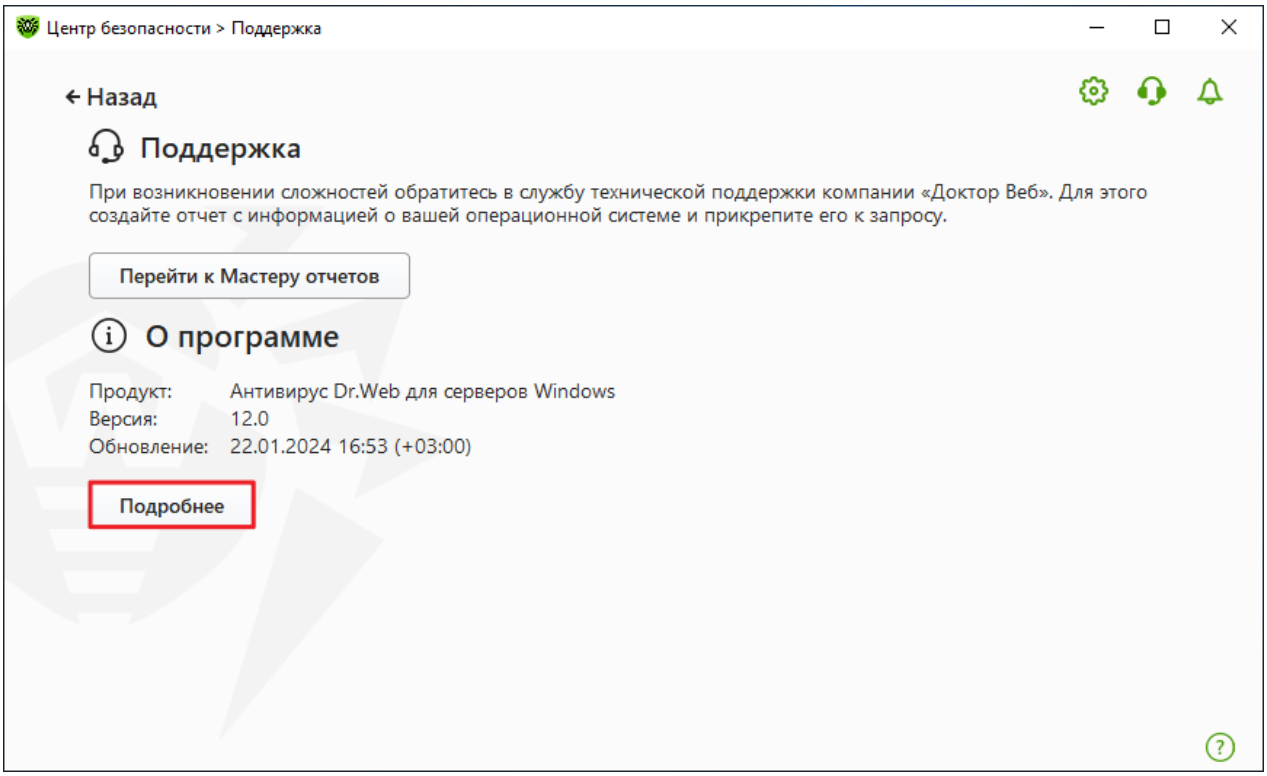

Рисунок 93. Доступ к окну О программе Dr.Web

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 Модулю автоматического обновления.

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.
/CUSTOM	Запустить Сканер на странице выборочной проверки. Если при этом заданы дополнительные параметры (например, объекты

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

Ключ	Описание
/H или /?	Вывести на экран краткую справку о работе с программой. (Только для Консольного сканера).
/HA	Производить эвристический анализ файлов и поиск в них неизвестных угроз. По умолчанию опция включена.
/KEY:<*ключевой_файл*>	Указать путь к ключевому файлу. Параметр необходим в том случае, если ключевой файл находится не в той же папке, что и сканер. По умолчанию используется drweb32.key или другой подходящий из папки C:\Program Files\DrWeb\.
/LITE	Произвести стартовую проверку системы, при которой проверяются оперативная память и загрузочные секторы всех дисков, а также провести проверку на наличие руткитов. (Только для Сканера).
/LN	Проверять файлы, на которые указывают ярлыки. По умолчанию опция отключена.
/LS	Проверять под учетной записью LocalSystem. По умолчанию опция отключена.
/MA	Проверять почтовые файлы. По умолчанию опция включена.
/MC:<*число_попыток*>	Установить максимальное число попыток вылечить файл. По умолчанию — без ограничений.
/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.

Ключ	Описание
/PAL:<*уровень_вложенности*>	Максимальный уровень вложенности упаковщиков исполняемого файла. Если уровень вложенности превышает указанный, проверка будет производиться только до указанного уровня вложенности. По умолчанию — 1000.
/QL	Вывести список всех файлов, помещенных в карантин на всех дисках. (Только для Консольного сканера).
/QL:<*имя_логического_диска*>	Вывести список всех файлов, помещенных в карантин на указанном логическом диске. (Только для Консольного сканера).
/QNA	Выводить пути в двойных кавычках.
/QR[:[d][:p]]	Удалить файлы с указанного диска <d> (имя_логического_диска), находящие в карантине дольше <p> (количество) дней. Если <d> и <p> не указаны, то будут удалены все файлы, находящиеся в карантине, со всех логических дисков. (Только для Консольного сканера).
/QUIT	Закрыть Сканер после проверки (вне зависимости от того, были ли применены действия к обнаруженным угрозам). (Только для Сканера).
/RA:<*имя файла*>	Дописать отчет о работе программы в указанный файл. По умолчанию запись в файл журнала не производится (при запуске Сканера из командной строки).
/REP	Проверять по символьным ссылкам. По умолчанию опция отключена.
/RK	Проверка на наличие руткитов. По умолчанию опция отключена.
/RP:<*имя файла*>	Записать отчет о работе программы в указанный файл. По умолчанию запись в файл журнала не производится (при запуске Сканера из командной строки).
/RPC:<*сек*>	Тайм-аут соединения со сканирующим ядром Scanning Engine, в секундах. По умолчанию — 30 секунд. (Только для Консольного сканера).
/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).

Ключ	Описание
/SPN	Выводить название упаковщика. По умолчанию опция отключена.
/SPS	Отображать процесс проведения проверки. По умолчанию опция включена. (Только для Консольного сканера).
/SST	Выводить время проверки объекта. По умолчанию опция отключена.
/ST	Запуск Сканера в фоновом режиме. Если не задан параметр /GO, то графический режим отображается только при обнаружении угроз. В этом режиме при переходе на работу от батареи проверка прекращается.
/TB	Выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.
/TM	Выполнять поиск угроз в оперативной памяти (включая системную область Windows).
/TR	Проверять системные точки восстановления.
/W:<*сек*>	Максимальное время проверки, в секундах. По умолчанию — без ограничений.
/WCL	Вывод, совместимый с drwebwcl. (Только для Консольного сканера).
/X:S[:R]	По окончании проверки перевести машину в указанный режим: выключение/перезагрузка/ждущий режим/спящий режим.

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

Действие	Описание
/AAD:<*действие*>	действия для рекламных программ (возможные действия: DQIR)
/AAR:<*действие*>	действия с инфицированными архивами (возможные действия: DQIR)
/ACN:<*действие*>	действия с инфицированными контейнерами (возможные действия: DQIR)
/ADL:<*действие*>	действия с программами дозвона (возможные действия: DQIR)

Действие	Описание
/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)
/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. 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 Модуля обновления

Общие параметры:

Параметр	Описание
-h [--help]	Вывести на экран краткую справку о работе с программой.
-v [--verbosity] arg	Уровень детализации журнала: `error` (только ошибки), `info` (стандартный), `debug` (отладочный).
--rotate arg	Ротация журнала в формате <*количество файлов*>, <*размер*> <*единица измерения*> (`k` — килобайт, `m` — мегайбайт, `g` — гигабайт).
-d [--data-dir] arg	Папка, в которой размещены репозиторий и настройки.
--log-dir arg	Папка, в которой будет сохранен журнал.
-r [--repo-dir] arg	Папка репозитория (по умолчанию <*data_dir*>`/repo`).
-t [--trace]	Включить трассировку.
-c [--command] arg (=update)	Выполняемая команда: `update` — обновить, `uninstall` — удалить, `exec` — выполнить, `keyupdate` — обновить ключ, `download` — скачать, `mirror` — создать зеркало обновлений.
-z [--zone] arg	Список зон, который будет использоваться вместо заданных в конфигурационном файле.

Параметры команды обновления (update):

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

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

Параметры команды удаления (uninstall):

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

Параметры команды автоматического обновления ключа (keyupdate):

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

Параметры команды скачивания (download):

Параметр	Описание
--zones arg	Файл, содержащий список зон.
--key-dir arg	Папка, в которой находится ключевой файл.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.
-g [--proxy] arg	Прокси-сервер для обновления в формате <*адрес*>: <*порт*>.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-s [--version] arg	Имя версии.
-p [--product] arg	Название продукта, который необходимо скачать.

Параметры команды создания зеркала обновлений (mirror):

Параметр	Описание
--zones arg	Файл, содержащий список зон.
--key-dir arg	Папка, в которой находится ключевой файл.

Параметр	Описание
-g [--proxy] arg	Прокси-сервер для обновления в формате *<адрес>: <порт>*.
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-s [--version] arg	Имя версии.

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.
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.

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.

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.