

ООО «Доктор Веб»

Dr.Web Security Space
Руководство по быстрой установке
и развертыванию

Версия 12.0

Методическое пособие для практических
занятий по курсу

DWCERT-001-12

«Защита компьютерных систем на базе антивирусного решения Dr.Web Security Space»

Версия программного обеспечения	12.00
Версия документа	1.1
Статус документа	Утвержден
Дата последнего изменения	11 марта 2019 года

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Внимание! Материалы, представленные в настоящем документе, являются собственностью ООО «Доктор Веб». Защита авторских прав на данный документ осуществляется в соответствии с действующим законодательством РФ. Ни одна из частей данного документа не может быть сфотографирована, размножена или распространена другим способом без согласия ООО «Доктор Веб». Если вы собираетесь использовать, копировать или распространять материалы настоящего курса, свяжитесь, пожалуйста, с представителями ООО «Доктор Веб» через специальную форму, расположенную на официальном сайте:

<http://support.drweb.ru/new/feedback>.

Dr.Web®, SpIDer Guard®, SpIDer Mail®, Dr.Web CureIt! и логотип Dr.WEB — зарегистрированные товарные знаки ООО «Доктор Веб» в России и/или других странах.

Другие названия продуктов, упоминаемые в тексте курса, являются товарными знаками или зарегистрированными товарными знаками соответствующих фирм.

Ограничение ответственности

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

Возможности изучаемого продукта не ограничиваются функционалом, описанным в данном документе. Для ознакомления с возможностями решения используйте документацию к продуктам.

Внимание! В программные продукты, выпускаемые ООО «Доктор Веб», могут вноситься изменения, не отраженные в данном документе. Со всеми изменениями, вносимыми в программные продукты ООО «Доктор Веб», можно ознакомиться на сайте <http://www.drweb.ru>.

© ООО «Доктор Веб», 2003–2019

<http://www.drweb.ru>

Содержание

1.	Введение	5
2.	Требования к специалисту, изучающему курс	5
3.	Назначение продукта	5
4.	Получение демонстрационного ключевого файла	9
4.1.	Получение демонстрационного ключевого файла после установки продукта.....	9
5.	Установка Dr.Web Security Space	11
5.1.	Установка из командной строки	11
5.2.	Установка с помощью мастера установки.....	12
6.	Удаление	19
7.	Продление лицензии. Замена ключевого файла	23
7.1.	Замена ключевого файла	26
7.2.	Продление действия приобретенной лицензии на 150 дополнительных дней.....	30
8.	Настройка антивирусной защиты	35
8.1.	Начало работы.....	35
8.2.	Настройка языка интерфейса.....	38
8.3.	Изменение уровня подробности протокола событий.....	39
8.4.	Запуск и останов компонентов защиты	40
8.5.	Антивирусная проверка станции. Выбор приоритета сканирования	42
8.5.1.	Антивирусная проверка Сканером.....	44
8.5.2.	Проверка с правами другого пользователя.....	51
8.5.3.	Запуск антивирусной проверки из командной строки	52
8.6.	Настройка действий Dr.Web Security Space с вредоносными файлами	53
8.6.1.	Настройка файлового сторожа	54
8.6.1.1.	Обнаружение вредоносных скриптов.....	59
8.6.1.2.	Настройка исключений	61
8.6.2.	Настройка параметров работы антивирусного сканера.....	63
8.6.3.	Настройка проверки почтового трафика	63
8.6.3.1.	Настройка исключений проверяемых адресов	69
8.6.4.	Настройка правил фильтрации в Microsoft Outlook	70
8.6.5.	Настройка проверки интернет-трафика.....	73
8.6.5.1.	Настройка проверки зашифрованного трафика.....	76
8.6.5.2.	Настройка исключений доступа к сетевым ресурсам	77
8.6.6.	Настройка исключений для работающих приложений.....	77
8.7.	Настройка системы обновлений Dr.Web Security Space	79
8.7.1.	Поисковый модуль Dr.Web	90
8.8.	Настройка компонента Dr.Web Cloud	93
8.9.	Настройка параметров Dr.Web Security Space, обеспечивающих обнаружение ранее неизвестных вредоносных файлов	94
8.10.	Ограничения возможности проникновения программ-шифровальщиков на компьютер.....	105
8.10.1.	Ограничения времени доступа к сетевым ресурсам	106
8.10.2.	Ограничения времени доступа к Интернету и учетной записи	110
8.10.3.	Контроль доступа к локальным ресурсам	111
8.11.	Функционал «Защита от потери данных».....	121
8.12.	Проверка работоспособности продукта	122
8.13.	Настройка Брандмауэра Dr.Web	136
8.13.1.	Ограничение прав сетевых приложений	141
8.13.2.	Настройка параметров работы известных сетей	146
8.13.3.	Игровой режим.....	152
8.14.	Управление антивирусной защитой удаленного компьютера	154

8.15.	Просмотр статистики работы	157
8.16.	Карантин	158
8.17.	Включение и отключение самозащиты	161
8.18.	Установка пароля доступа к настройкам антивирусной защиты	162
8.19.	Получение услуг службы технической поддержки	163
8.19.1.	Сбор информации для службы технической поддержки	169
8.20.	Отсылка образцов на анализ	172
9.	Получение документации по продуктам Dr.Web	172
10.	Работа со справкой о программе	172
11.	Дополнительная информация	174

1. Введение

Данный документ содержит сведения, описывающие:

- детали реализации комплексной антивирусной защиты рабочих станций компаний и организаций, а также личных компьютеров их сотрудников с помощью **Dr.Web Security Space**.

Внимание! Данный документ *не содержит* сведений о следующем:

- общие принципы организации антивирусной защиты,
- основные угрозы в области информационной безопасности,
- принципы выбора мер и средств защиты на основе анализа актуальности угроз безопасности.

В данном пособии описаны основные возможности решения **Dr.Web Security Space**, входящие в него компоненты, а также последовательности шагов по выполнению наиболее распространенных действий по настройке продукта, контролю его состояния и поддержанию безопасного состояния защищаемого им компьютера.

Все разделы снабжены иллюстрациями, с помощью которых администратор антивирусной защиты может легко освоить продукт и выполнять все необходимые ему задачи. Информации, приведенной в пособии, достаточно, чтобы разобраться в настройках продукта с нуля.

Внимание! В настоящем пособии описаны только самые важные возможности и настройки **Dr.Web Security Space**, наиболее часто использующиеся процедуры выполнения действий. Полная информация о возможностях продукта приведена в документации на него.

Внимание! Перед прочтением документа убедитесь, что это последняя версия. Актуальную версию можно найти на официальном веб-сайте компании «Доктор Веб» <https://training.drweb.ru/external/courses/?lng=ru>.

Данный документ адресован *администратору антивирусной сети* — сотруднику организации, которому поручено руководство антивирусной защитой компьютеров (рабочих станций и серверов) этой сети.

2. Требования к специалисту, изучающему курс

Предполагается, что обучающийся обладает следующими знаниями и навыками:

- базовые знания по установке, подключению и использованию компьютерной техники;
- знания и практические навыки администрирования локальных сетей на базе ОС Windows версий XP и выше;
- знакомство с документацией по продукту **Dr.Web Security Space** версии 12.0.

3. Назначение продукта

Dr.Web Security Space обеспечивает многоуровневую защиту всех компонентов защищаемых компьютеров: системной памяти, жестких дисков и сменных носителей от проникновений вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и различных вредоносных объектов из любых внешних источников.

Важной особенностью **Dr.Web Security Space** является модульная архитектура. **Dr.Web Security Space** использует программное ядро и вирусные базы, общие для всех программных продуктов компании «Доктор Веб», на какой бы платформе они ни работали. Во многом именно благодаря этому продукты Dr.Web позволяют организовать эффективную антивирусную защиту в различных операционных системах, на базе различных платформ —

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

эффективную не только по качеству защиты, но и с точки зрения минимизации системных требований и затрат на сопровождение.

Dr.Web Security Space предлагает пользователю комплекс настроек компонентов, с помощью которых можно защитить файловую систему:

- **Сканер Dr.Web** — антивирусный сканер с графическим интерфейсом, который запускается по запросу пользователя или по расписанию и производит антивирусную проверку компьютера.
- **Консольный сканер Dr.Web** — версия **Сканера Dr.Web** с интерфейсом командной строки.
- **SpIDer Guard** — антивирусный сторож, который постоянно находится в оперативной памяти, осуществляя проверку файлов и памяти «на лету», а также обнаруживая проявления вирусной активности.
- **SpIDer Mail** — почтовый антивирусный сторож, который перехватывает обращения любых почтовых клиентов, работающих на компьютере, к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP (под IMAP4 имеется в виду IMAPv4rev1), обнаруживает и обезвреживает угрозы до получения писем почтовым клиентом с сервера или до отправки письма на почтовый сервер.
- **Dr.Web для Outlook** — подключаемый модуль, который проверяет почтовые ящики Microsoft Outlook на угрозы.
- **Брандмауэр Dr.Web** — персональный межсетевой экран, предназначенный для защиты вашего компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети.
- **Родительский контроль** — компонент, который ограничивает доступ к сайтам, файлам и папкам, а также позволяет ограничить время работы в сети Интернет и за компьютером для каждой учетной записи Windows.
- **Поведенческий анализ** — компонент, контролирующий доступ приложений к критически важным объектам системы и обеспечивающий целостность запущенных приложений.
- **Защита от эксплойтов** — компонент, блокирующий вредоносные объекты, которые используют уязвимости в приложениях.
- **Защита от вымогателей** — компонент, обеспечивающий защиту от вирусов-шифровальщиков.
- **Модуль обновления Dr.Web** — компонент, который позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов **Dr.Web**, а также производит их автоматическую установку.
- **SpIDer Agent** — модуль управления, с помощью которого осуществляются запуск и настройка компонентов программы **Dr.Web**.

Dr.Web Security Space использует удобные и эффективные механизмы обновления вирусных баз и используемых компонентов программного обеспечения, что делает незаметной всю процедуру обновления и снижает до нуля необходимость вмешательства в нее конечного пользователя, избавляя его от «головной боли» необходимости контроля за антивирусом.

Для обнаружения вредоносных объектов в **Dr.Web Security Space** используются уникальные технологии, многие из которых не имеют аналогов.

- **Сигнатурный анализ.** Выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов — соответствия признакам,
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

позволяющим идентифицировать тот или иной вирус. Вирусные базы Dr.Web составлены так, что, имея одну запись, можно обнаруживать целые классы угроз.

Заблуждение

Антивирусы ловят вирусы по сигнатурам (записям в вирусных базах) — если бы это было так, антивирус был бы беспомощен перед лицом **неизвестных** угроз.

Однако антивирус не перестал быть лучшим и **единственным** эффективным средством защиты от всех типов вредоносных угроз — и что особенно важно — как **известных**, так и **неизвестных** вирусной базе антивируса — в продуктах Dr.Web для обнаружения и обезвреживания неизвестного вредоносного ПО применяется множество эффективных несигнатурных технологий, сочетание которых позволяет обнаруживать новейшие (неизвестные) угрозы до внесения записи в вирусную базу.

- **Традиционный эвристический анализатор** — содержит механизмы обнаружения неизвестных вредоносных программ. Работа эвристического анализатора опирается на знания (эвристики) об определенных особенностях (признаках) вирусов — как характерных именно для вирусного кода, так и, наоборот, крайне редко встречающихся в вирусах. Каждый из таких признаков характеризуется своим «весом» — числом, модуль которого определяет важность, серьезность данного признака, а знак, соответственно, указывает на то, подтверждает он или опровергает гипотезу о возможном наличии неизвестного вируса в анализируемом коде.
- **Модуль эмуляции исполнения** — технология эмуляции исполнения программного кода необходима для обнаружения полиморфных и сложношифрованных вирусов, когда непосредственное применение поиска по контрольным суммам невозможно либо крайне затруднено (из-за невозможности построения надежных сигнатур). Метод состоит в имитации исполнения анализируемого кода эмулятором — программной моделью процессора (и отчасти компьютера и ОС).
- **Технология FLY-CODE** — обеспечивает качественную проверку упакованных исполняемых объектов, распаковывает любые (даже нестандартные) упаковщики методом виртуализации исполнения файла, что позволяет обнаружить вирусы, упакованные даже неизвестными антивирусному ПО Dr.Web упаковщиками.
- **Технология анализа структурной энтропии** — обнаруживает неизвестные угрозы по особенностям расположения участков кода в защищенных криптоупаковщиками проверяемых объектах.
- **Технология ScriptHeuristic** — предотвращает исполнение любых вредоносных скриптов в браузере и PDF-документах, не нарушая при этом функциональности легитимных скриптов. Защищает от заражения неизвестными вирусами через веб-браузер. Работает независимо от состояния вирусной базы Dr.Web совместно с любыми веб-браузерами.
- **Origins Tracing.** Технология позволяет определить новые вирусы или модификации имеющихся, которые используют известные механизмы заражения. Origins Tracing позволяет значительно снизить количество ложных срабатываний эвристического анализатора. При сканировании исполняемого файла он рассматривается как некий образец, построенный характерным образом, после чего производится сравнение полученного образа с базой известных вредоносных программ.
- **Dr.Web Process Heuristic.** Технология поведенческого анализа Dr.Web Process Heuristic защищает от новейших, наиболее опасных вредоносных программ, способных избежать обнаружения традиционными сигнатурными и эвристическими механизмами.

Dr.Web Process Heuristic контролирует любые попытки изменения системы, а также анализирует поведение каждой запущенной программы, сверяясь с постоянно обновляемыми 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.

- **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.
- **Dr.Web ShellGuard.** Технология Dr.Web ShellGuard защищает распространенные приложения, устанавливаемые на компьютеры под управлением Windows, от эксплойтов — вредоносных объектов, пытающихся использовать уязвимости с целью получения контроля над атакуемыми приложениями или операционной системой в целом.

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;
 - алгоритмы защиты тех или иных приложений.
- **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

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

классифицируются на категории: чистые, подозрительные, вредоносные и т. д.

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

Именно постоянная работа над повышением качества обнаружения и лечения (антивирус должен лечить!) вредоносных объектов любого типа выделяет решения компании «Доктор Веб».

Dr.Web Security Space очень прост в управлении, и для его освоения не понадобятся какие-либо дополнительные навыки. При богатстве возможностей продукта все его настройки интуитивно понятны и расположены так, что путь к ним не занимает времени. Однако в настоящее время мало простого наличия возможностей у продукта — в мире постоянно возникающих новых угроз надо уметь пользоваться продуктом максимально эффективно. О том, как это сделать, и пойдет речь в данном пособии.

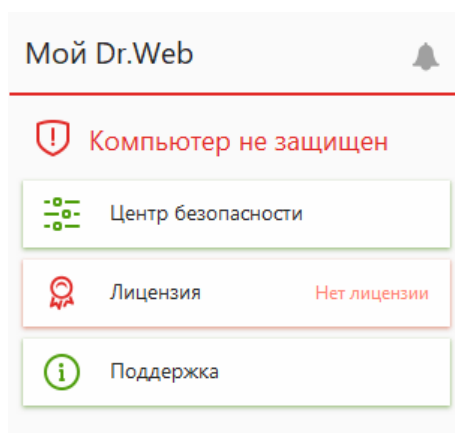
4. Получение демонстрационного ключевого файла

Если вы хотите получить демонстрационный ключевой файл (срок его действия — 30 дней, и его нельзя запрашивать повторно раньше чем через 4 месяца после первого запроса), выберите соответствующий пункт в процессе установки либо после ее завершения с помощью **Менеджера лицензий**, выбрав пункт **Получить пробную версию**. Затем укажите свою регистрационную информацию (только реальные данные, каждый запрос рассматривается индивидуально). Менеджер лицензий автоматически заменит имеющийся ключевой файл на актуальный.

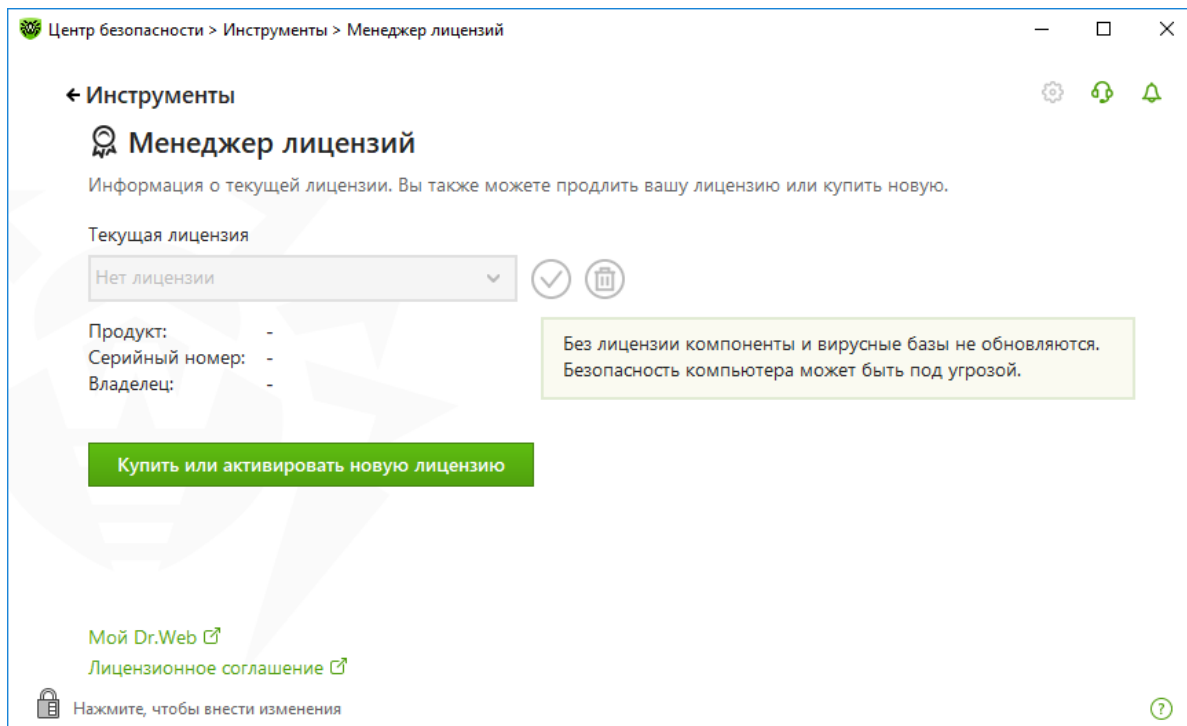
Демонстрационный ключевой файл также можно получить напрямую на сайте компании «Доктор Веб»: <https://download.drweb.ru/demoreq/biz/v2>. С помощью мастера вы можете выбрать продукт и заполнить регистрационную форму. Демоключ в архиве будет выслан на указанный почтовый адрес в кратчайшие сроки. После получения не забудьте сохранить его на диске и распаковать из архива.

4.1. Получение демонстрационного ключевого файла после установки продукта

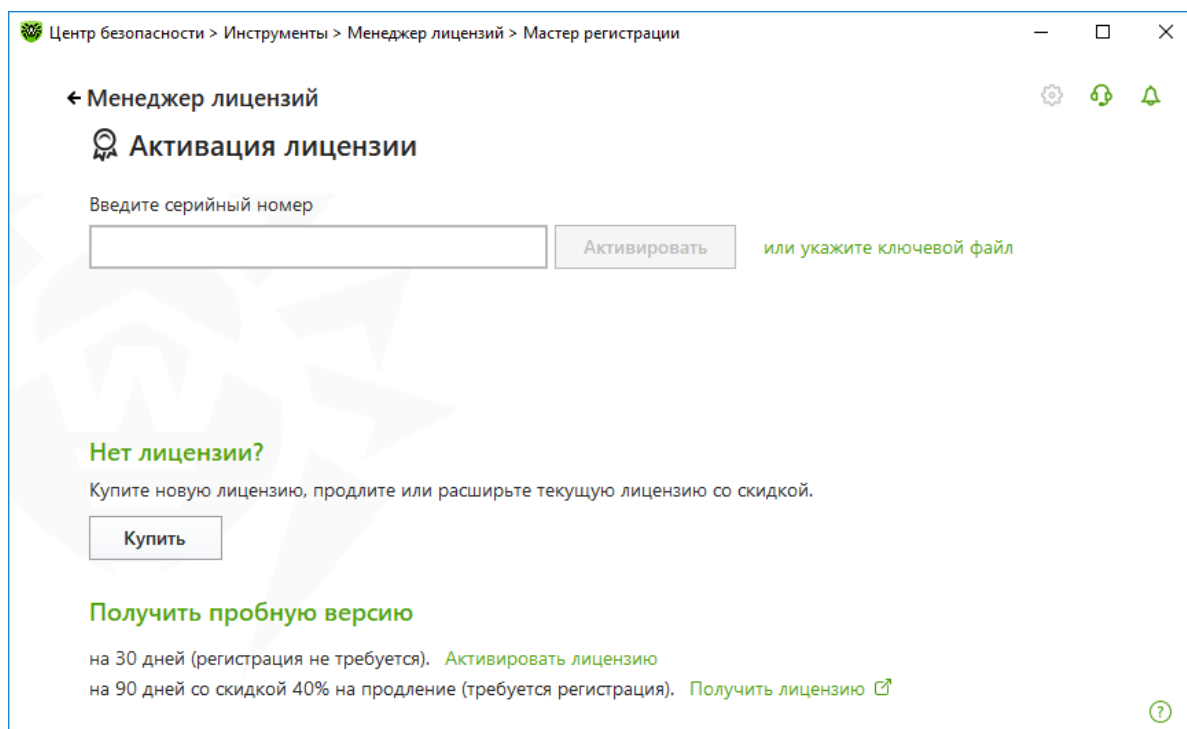
Щелкните по значку антивируса (паучку) в области уведомлений.



Выберите пункт **Лицензия**.



В открывшемся окне нажмите на кнопку **Купить или активировать новую лицензию**. На следующем шаге кликните на ссылку **Получить лицензию**.



На открывшейся странице сайта «Доктор Веб» заполните анкету. На указанный в анкете e-mail-адрес будет отправлено письмо со ссылкой. Перейдите по ссылке, чтобы подтвердить e-mail и завершить регистрацию. На этот же адрес будут высланы серийный номер Dr.Web и инструкция по его активации в программе.

В окне **Менеджера лицензий** укажите серийный номер. Ключ будет скачан и установлен автоматически.

В случае необходимости замены ключа в каталоге установки вручную, отключите самозащиту.

Dr.Web® Security Space. Руководство по быстрой установке и разворачиванию

5. Установка Dr.Web Security Space

Внимание! На компьютере, подключенном к сети Интернет, должны быть установлены все исправления безопасности, причем не только для операционной системы, но и для всех используемых программ — современной тенденцией является использование для проникновения на локальный компьютер уязвимостей именно в программах, а не в операционной системе. Использование всех обновлений безопасности является необходимым условием обеспечения безопасности, так как данные обновления закрывают для вирусописателей доступ в систему через известные уязвимости. Рекомендуется установить эти обновления до начала установки Dr.Web Security Space.

До момента установки рекомендуется проверить при помощи системных средств файловую систему и устранить обнаруженные дефекты.

Внимание! На время установки антивирусной защиты компьютер не является защищенным. Не рекомендуется в это время заниматься веб-серфингом, скачивать файлы, проверять личную почту. Как правило, фактическим окончанием установки служит только перезагрузка компьютера, которую требует установка системных компонентов. Начиная с этого момента безопасность компьютера будет гарантироваться.

Внимание! Рекомендуется до начала установки удалить ранее используемые антивирусные или антишпионские программы. Dr.Web Security Space способен самостоятельно находить и удалять антивирусные программы, но лучше проделать эту операцию с помощью штатного инсталлятора — в том числе и потому, что деинсталляция может быть защищена паролем, который знаете только вы. Если планируется установка компонента **Брандмауэр Dr.Web**, удалите с компьютера ранее установленные межсетевые экраны. Отключение встроенного брандмауэра операционной системы производится автоматически.

Внимание! Если вы не используете русифицированную версию операционной системы, но планируете использовать антивирус с русской локализацией, убедитесь в том, что на ней установлены все необходимые для отображения кириллических символов компоненты.

Внимание! Для установки антивирусной защиты требуются права администратора данного компьютера — только в этом режиме антивирус может противостоять вирусным угрозам.

Установка может производиться:

- в обычном (рекомендуемом) режиме (с помощью мастера);
- в фоновом режиме (из командной строки).

5.1. Установка из командной строки

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

Рассмотрим вариант команды, при запуске которой будет проведена установка Dr.Web Security Space и проведена перезагрузка после установки (в данном примере дистрибутив продукта расположен в C:\Documents and Settings):

```
C:\Documents and Settings\drweb-12.0-ss-win.exe /installFirewall /silent yes /reboot yes
```

Если необходимо установить Dr.Web Security Space на определенном языке, задайте дополнительно следующий параметр:

```
/lang <код _ языка>
```

Значение параметра — код языка в формате ISO 639-1. Для русского языка значение кода — ru.

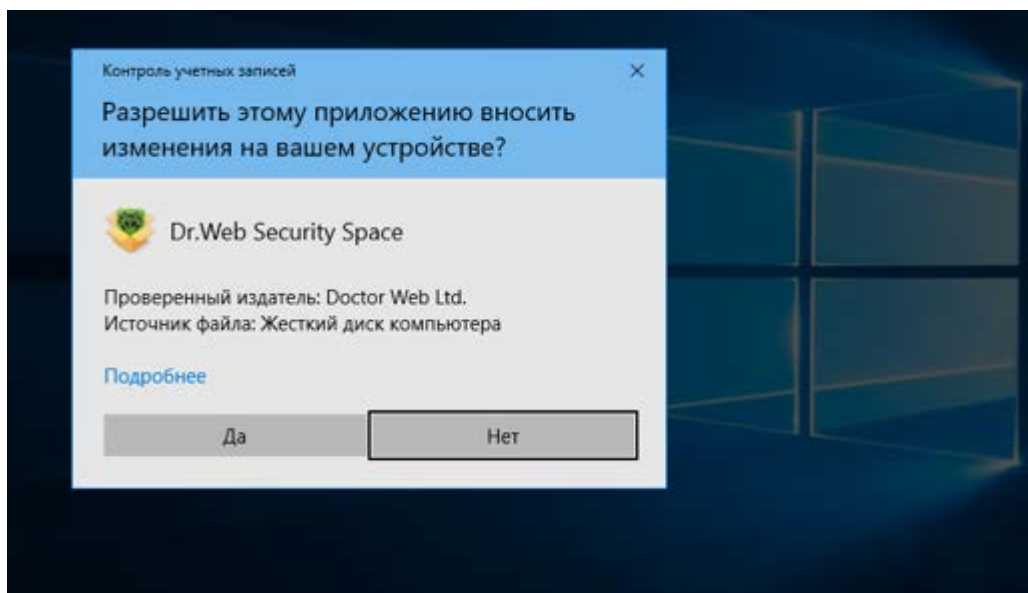
Ознакомиться с параметрами командной строки можно в документации по продукту.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

5.2. Установка с помощью мастера установки

Запустите полученный файл установки и следуйте инструкциям мастера установки. В случае поставки установочного комплекта на фирменном диске вставьте диск в привод. Если для привода включен режим автозапуска диска, процедура установки запустится автоматически. Если режим автозапуска отключен, запустите на выполнение файл autorun.exe, расположенный на диске.

Если установка производится на операционных системах Windows Vista и выше, то в зависимости от настроек операционной системы может появиться запрос системы контроля учетных записей (UAC).



В случае появления такого запроса нажмите **Да**.

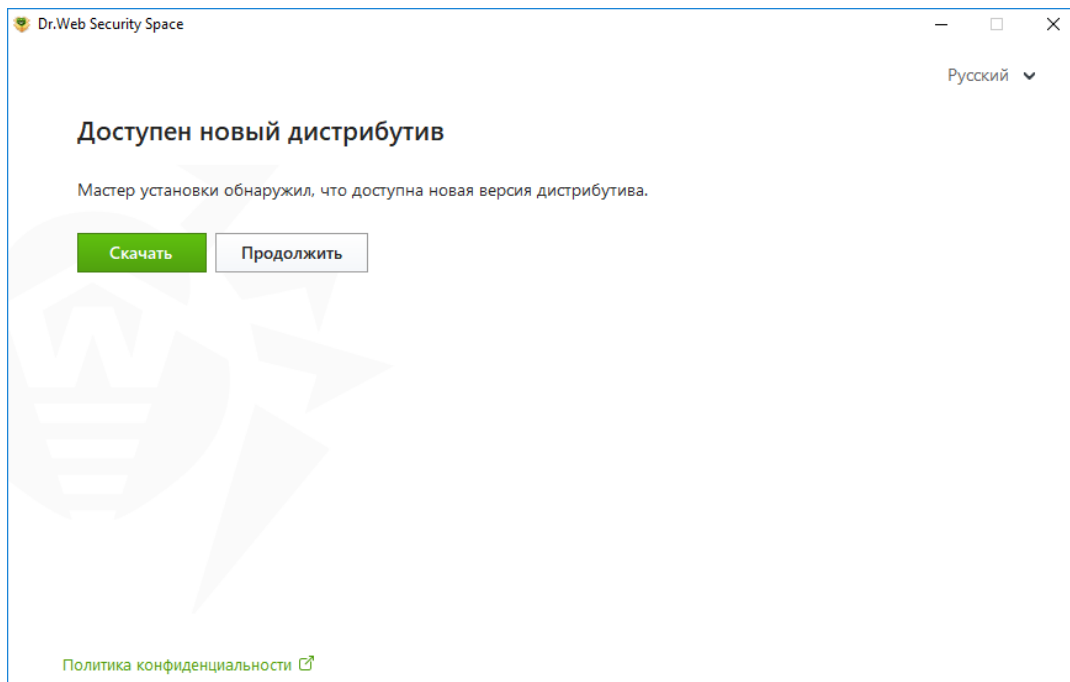
Если антивирусные программы уже установлены на компьютере, то мастер установки предпримет попытку их удалить. Если попытка окажется неудачной, удалите используемое антивирусное ПО самостоятельно (в том числе ПО других версий антивирусных программ Dr.Web).

Если ранее на компьютере использовалась предыдущая версия Dr.Web Security Space или Антивируса Dr.Web, а в ходе удаления предыдущей версии возникают ошибки и удалить антивирус не удается, воспользуйтесь утилитой для аварийного удаления «остатков» от некорректных/поврежденных инсталляций Dr.Web, скачав ее по ссылке: http://download.geo.drweb.com/pub/drweb/tools/drw_remover.exe. Либо обратитесь в службу технической поддержки по адресу <https://support.drweb.ru>.

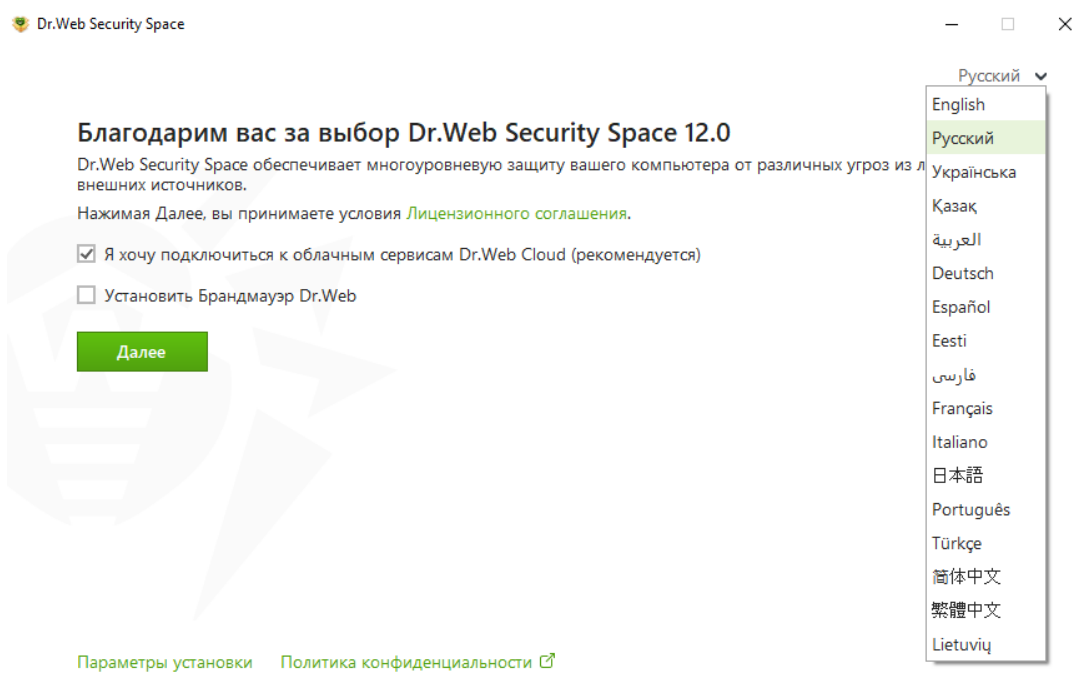


Перед началом установки проверяется актуальность установочного файла. В случае если существует более новый установочный файл, программа предложит его скачать.

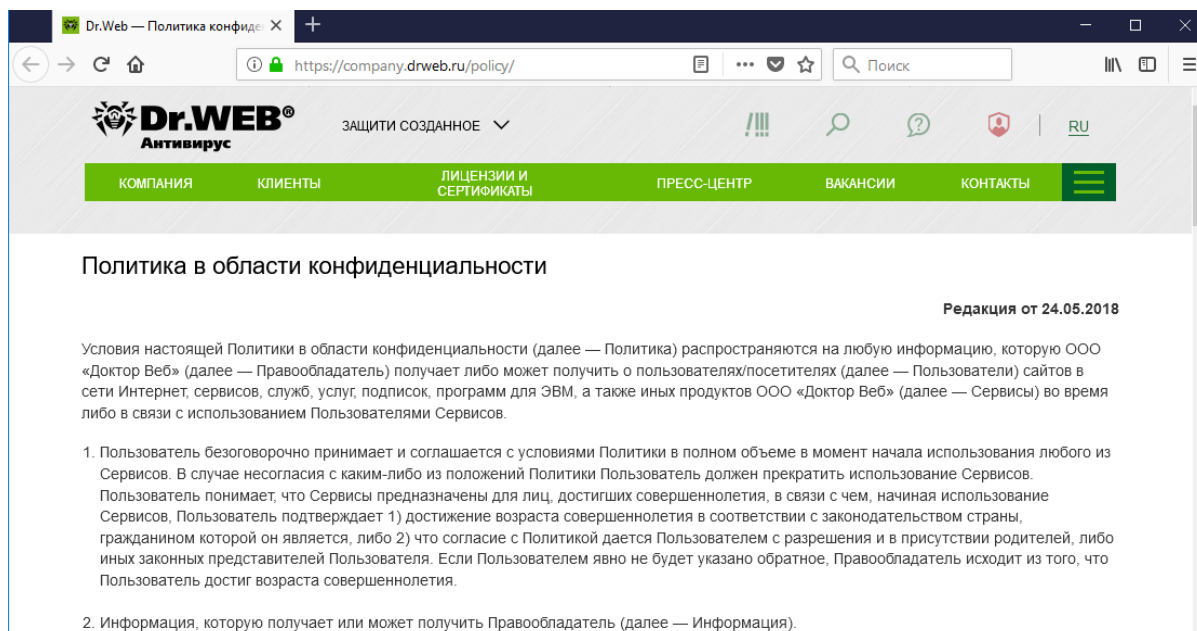
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию



В начале установки новой версии откроется окно мастера установки.



В открывшемся окне ознакомьтесь с политикой конфиденциальности, перейдя по соответствующей ссылке (<https://company.drweb.ru/policy>).



В начале установки предлагается подключиться к облачным сервисам **Dr.Web Cloud**, чтобы получать свежую информацию об угрозах, обновляемую на серверах компании «Доктор Веб» в режиме реального времени. Использование облачных сервисов дает возможность «на лету» проверять любые ссылки в Интернете по самым свежим базам Dr.Web. Выберите нужную опцию и нажмите **Далее**.

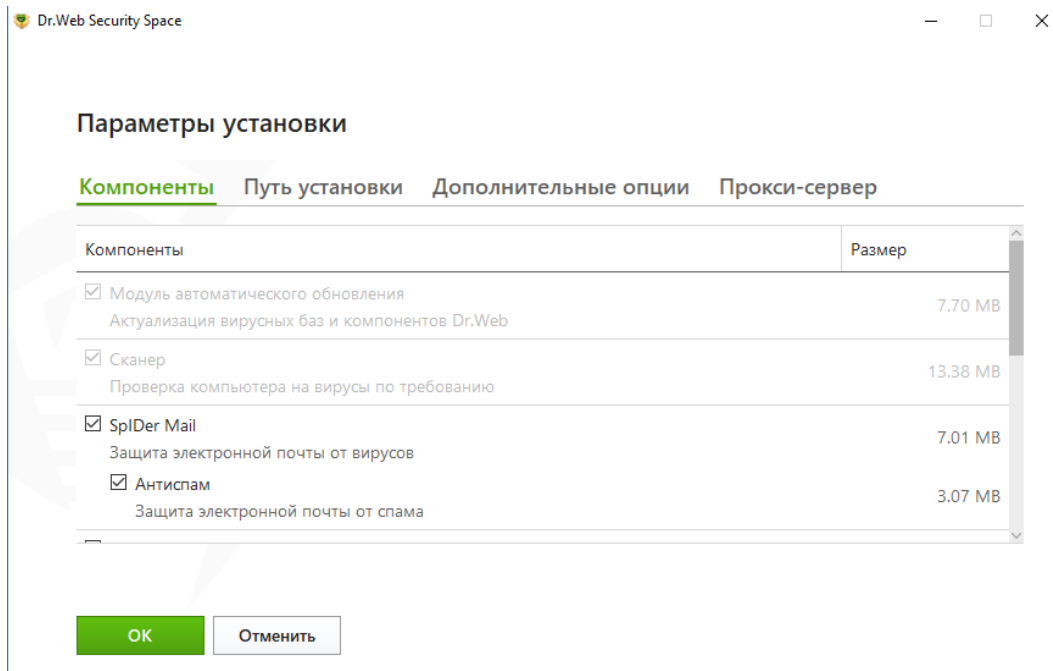
На этом же этапе предлагается установить **Брандмауэр Dr.Web** для защиты компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети. Если необходимо установить **Брандмауэр Dr.Web**, установите соответствующий флаг. Для возможности самостоятельного выбора компонентов антивирусной защиты кликните на ссылку **Параметры установки**.

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

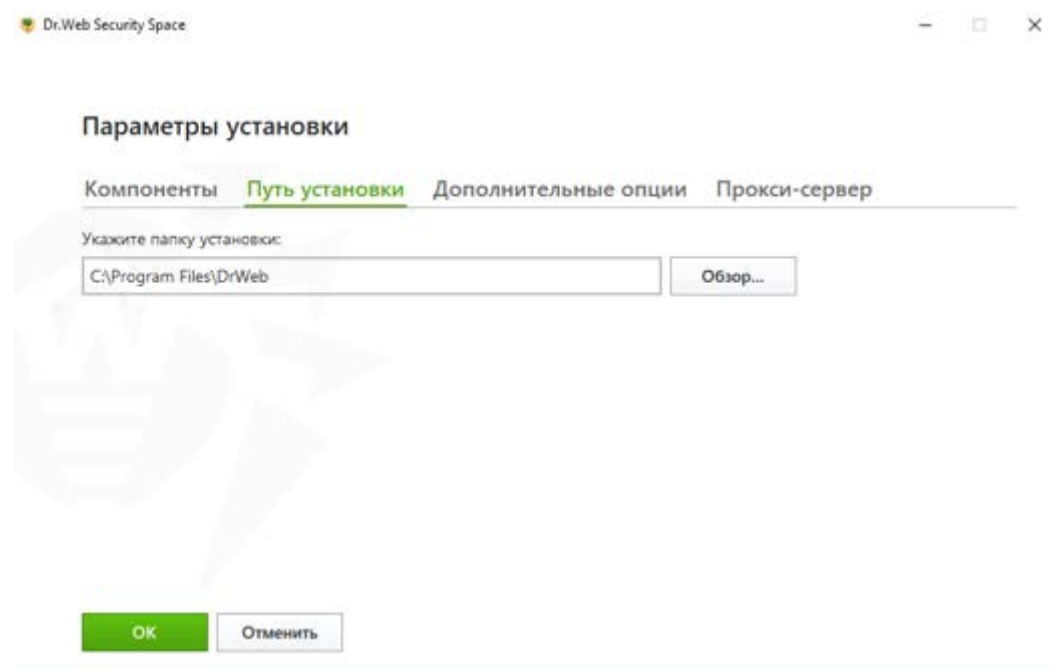
Внимание! Данная опция предназначена для опытных пользователей; для получения подробной информации обратитесь к документации **Руководство пользователя**.

На вкладке **Компоненты** будет предоставлен выбор устанавливаемых компонентов антивирусного пакета. Отметьте компоненты, которые необходимо установить на компьютер.

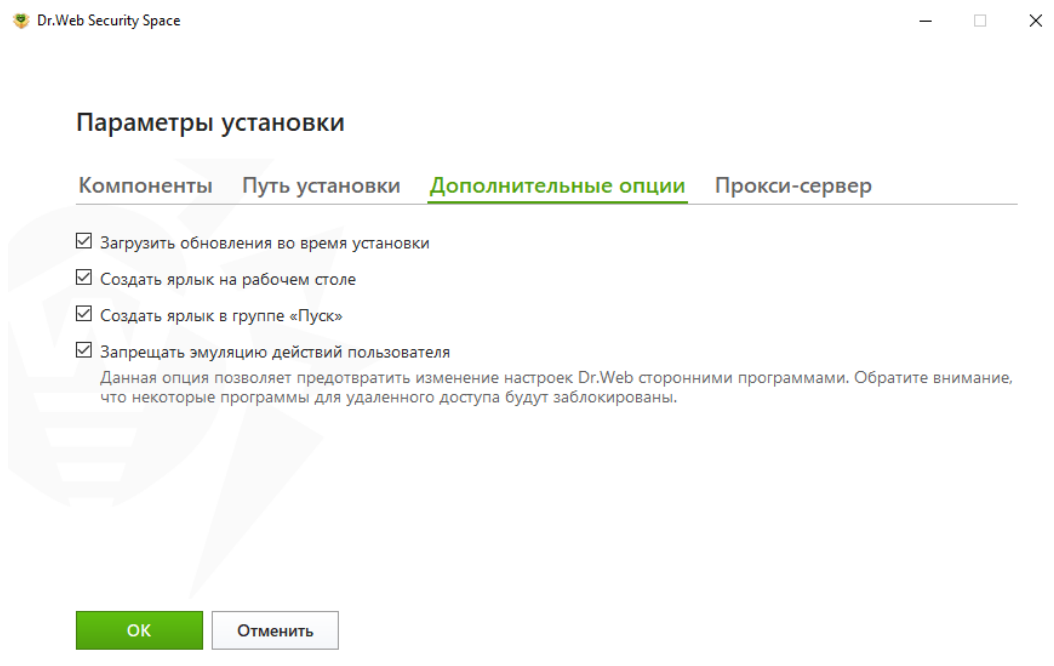
Внимание! Некоторые компоненты могут быть недоступны.



На вкладке **Путь установки** задайте каталог, в который будет установлено антивирусное ПО. По умолчанию выбран каталог *Dr.Web*, расположенный в каталоге *Program files* на системном диске.

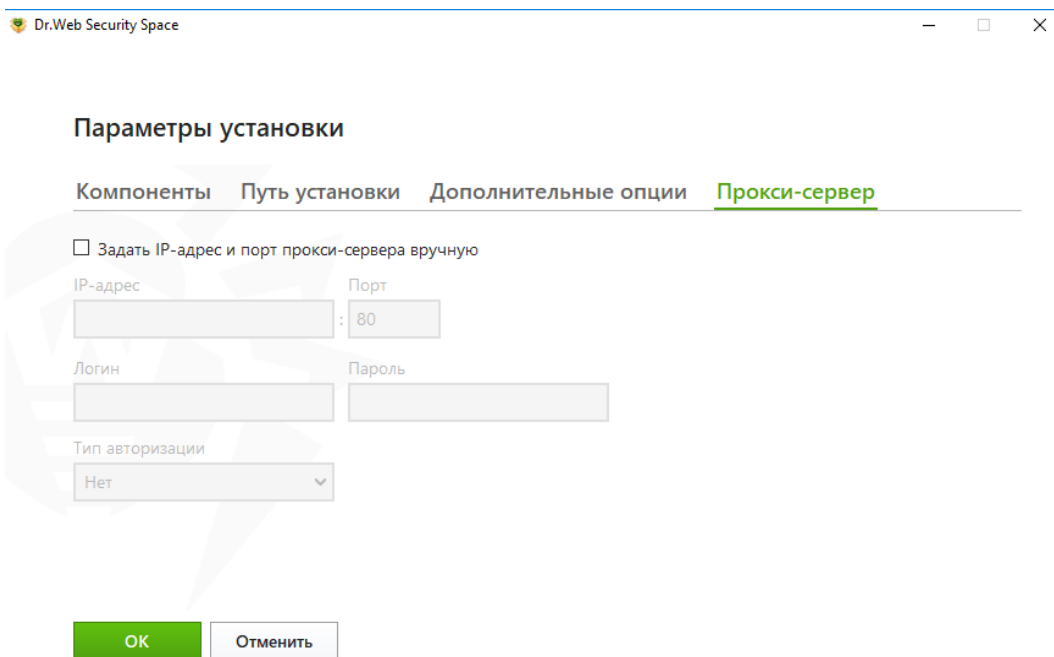


В случае если установка производится на компьютере без доступа в сеть Интернет — перейдите на закладку **Дополнительные опции** и снимите отметку с пункта **Загрузить обновления во время установки**.



Также на вкладке **Дополнительные опции** можно настроить параметры создания ярлыков для запуска **Антивируса Dr.Web**.

При необходимости укажите параметры прокси-сервера.



Рекомендуется использовать установку по умолчанию — все продукты компании «Доктор Веб» поставляются с оптимизированными для комфортной работы настройками. Опытные пользователи могут выбрать пользовательскую установку и самостоятельно решить, какие компоненты будут установлены.

Для сохранения внесенных изменений нажмите **ОК** и вернитесь к предыдущему окну.

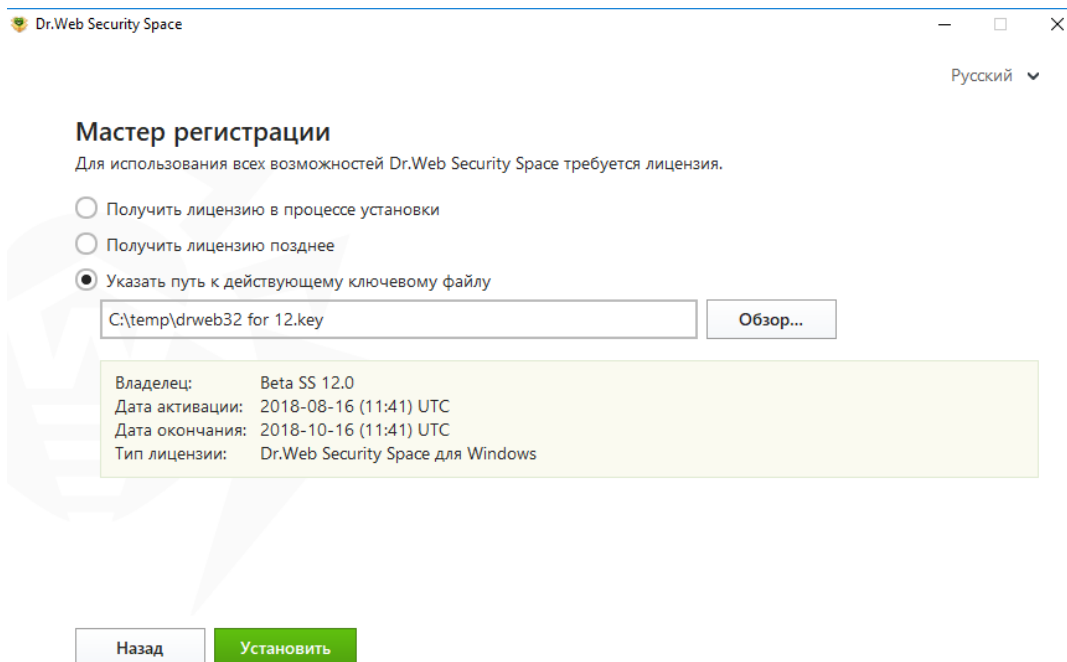
Нажмите **Далее**, чтобы продолжить установку. Обратите внимание, что тем самым вы принимаете условия лицензионного соглашения.

В следующем окне укажите серийный номер или ключевой файл (при наличии). В случае если необходимо оценить возможности продукта в отсутствие серийного номера или

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

ключевого файла, нажмите **Получить лицензию позднее** — после завершения установки продукта, в этом случае можно начать работу с временным ключевым файлом.

Внимание! Будьте внимательны — хотя сама процедура получения демонстрационного ключа полностью автоматизирована, для нее необходим доступ в Интернет.



Внимание! Обновления не будут загружаться до тех пор, пока вы не укажете или не получите ключевой файл.

Мастер регистрации, запускающийся при выборе пункта **Получить файл в процессе установки**, предлагает зарегистрировать имеющуюся лицензию или получить демонстрационный ключевой файл.

Активировать лицензию вы можете с помощью мастера регистрации в процессе установки или в любой другой момент, получив ключевой файл во время регистрации лицензии на официальном сайте «**Доктор Веб**» или указав путь к имеющемуся у вас действительному ключевому файлу в процессе установки либо в мастере регистрации.

В случае необходимости в своем личном кабинете или на странице <https://products.drweb.ru/register/certificate> сгенерируйте для уже зарегистрированного серийного номера лицензионный сертификат в формате PDF, распечатайте его на принтере или сохраните в электронном виде.

Внимание! В случае утраты ключевого файла может потребоваться повторная активация лицензии. В случае повторной активации лицензии выдается тот же ключевой файл, который был выдан ранее, при условии что срок его действия не истек. При переустановке продукта или в случае, когда лицензия предоставляет право установки продукта на несколько компьютеров, повторная активация серийного номера не требуется. Вы можете использовать ключевой файл, полученный при первой регистрации.

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

При наличии двух и более действующих ключевых файлов с помощью мастера регистрации можно получить 150 бонусных дней.

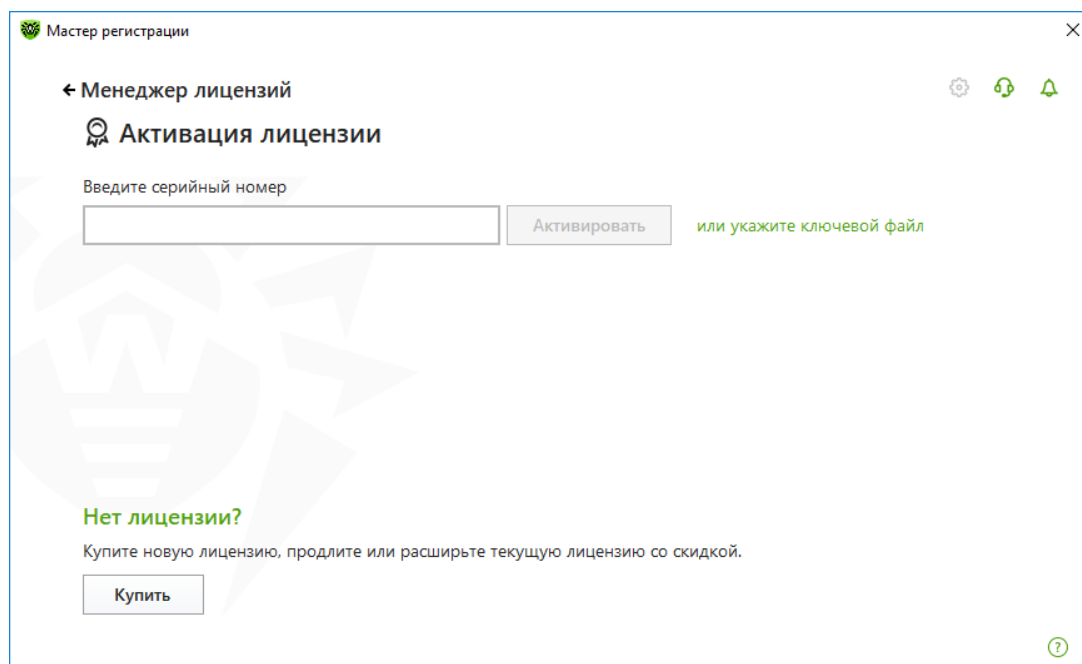
Если на ПК ранее уже был установлен антивирус Dr.Web, то при переходе на версию 12 с более ранних версий антивирус при установке автоматически находит ключевой файл. Если файл не найден, нажмите **Обзор** и укажите путь к имеющемуся ключевому файлу (который использовался старой версией).

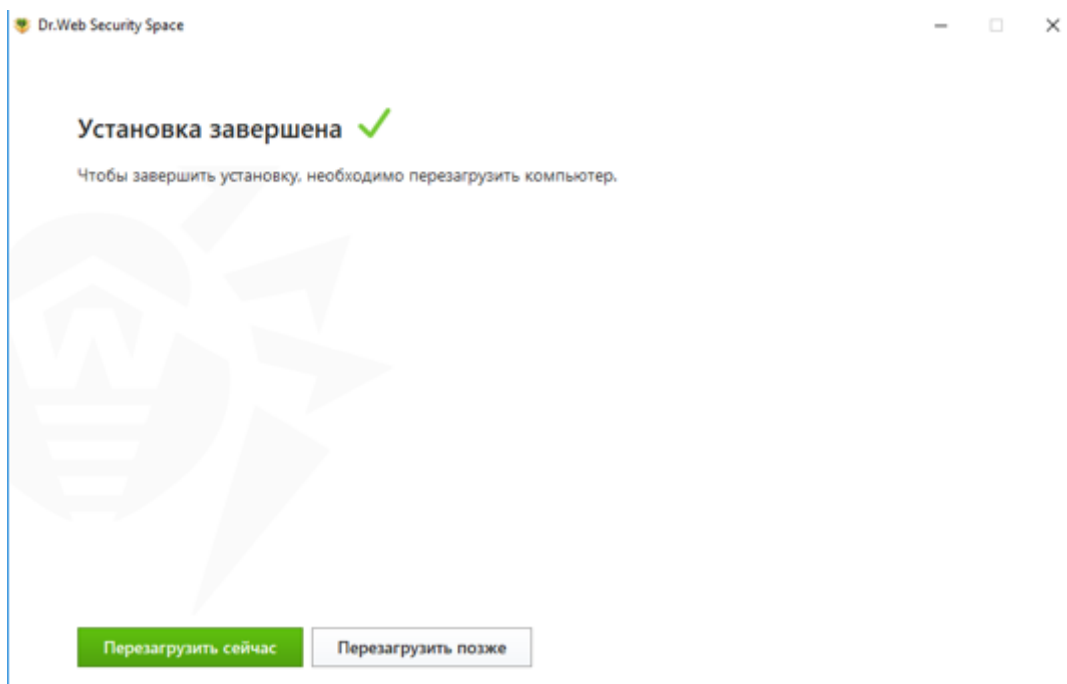
Для завершения установки антивируса нажмите **Установить**.

Ход установки также отображается в мастере.



Если вы ранее выбрали **Получить лицензию в процессе установки**, укажите ключевой файл или серийный номер в следующем окне.

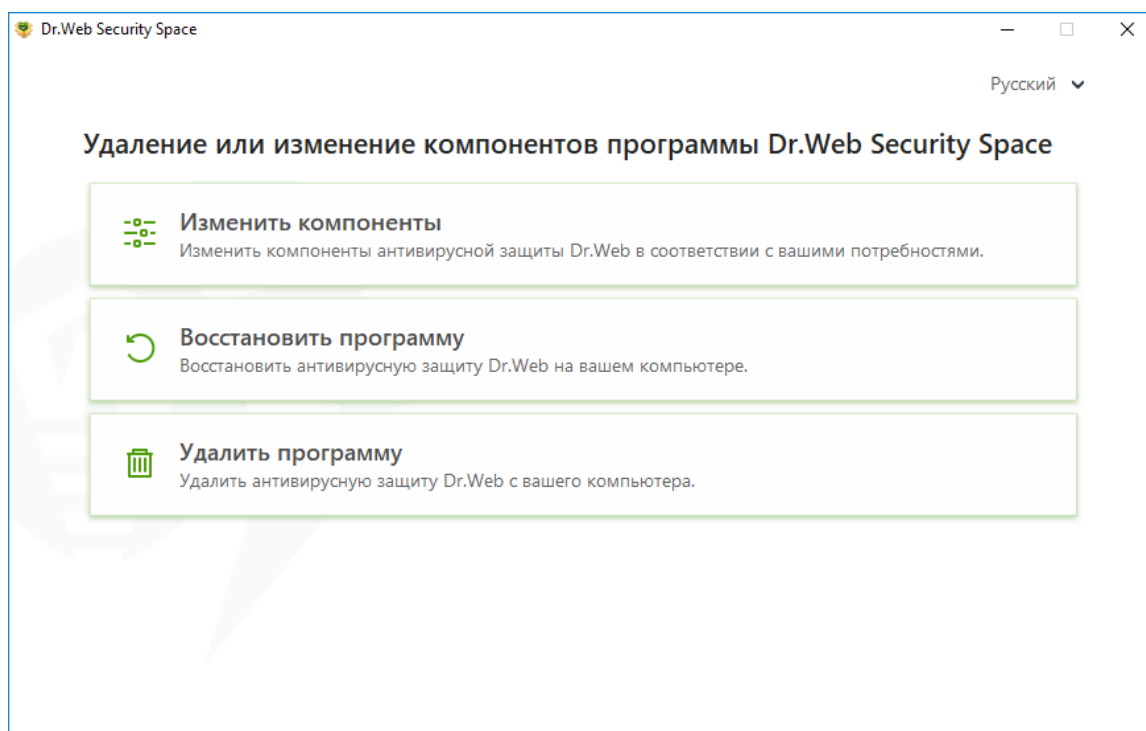




После выполнения всех необходимых действий мастер установки запросит разрешение на перезагрузку. Перезагрузка необходима, в частности, для того, чтобы можно было гарантировать, что ни один вирус не был загружен до антивируса — что крайне важно для борьбы с руткитами. Сохраните все необходимые данные, нажмите кнопку **Перезагрузить сейчас** и дождитесь перезагрузки компьютера.

6. Удаление

При наличии дистрибутива для удаления данной версии продукта запустите установочный файл и следуйте инструкциям мастера.



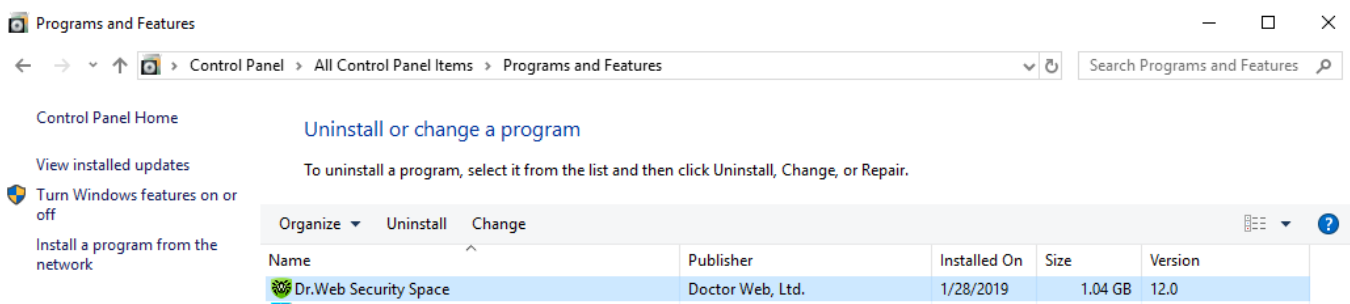
В случае отсутствия дистрибутива в зависимости от используемой операционной системы:

- для Windows Vista (в зависимости от вида меню «Пуск»):

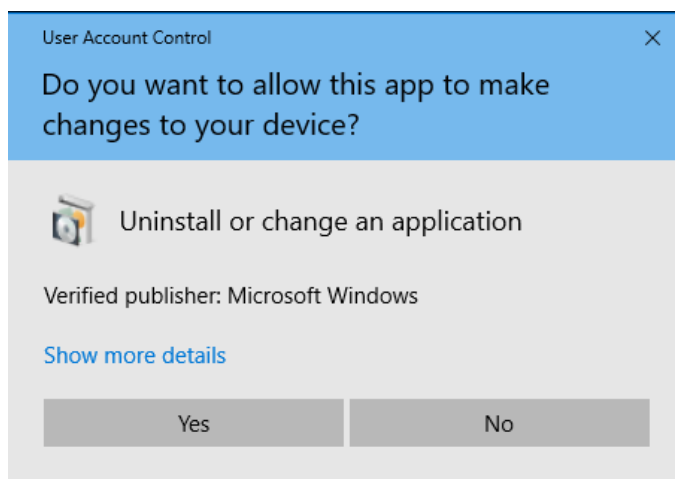
Dr.Web® Security Space. Руководство по быстрой установке и разворачиванию

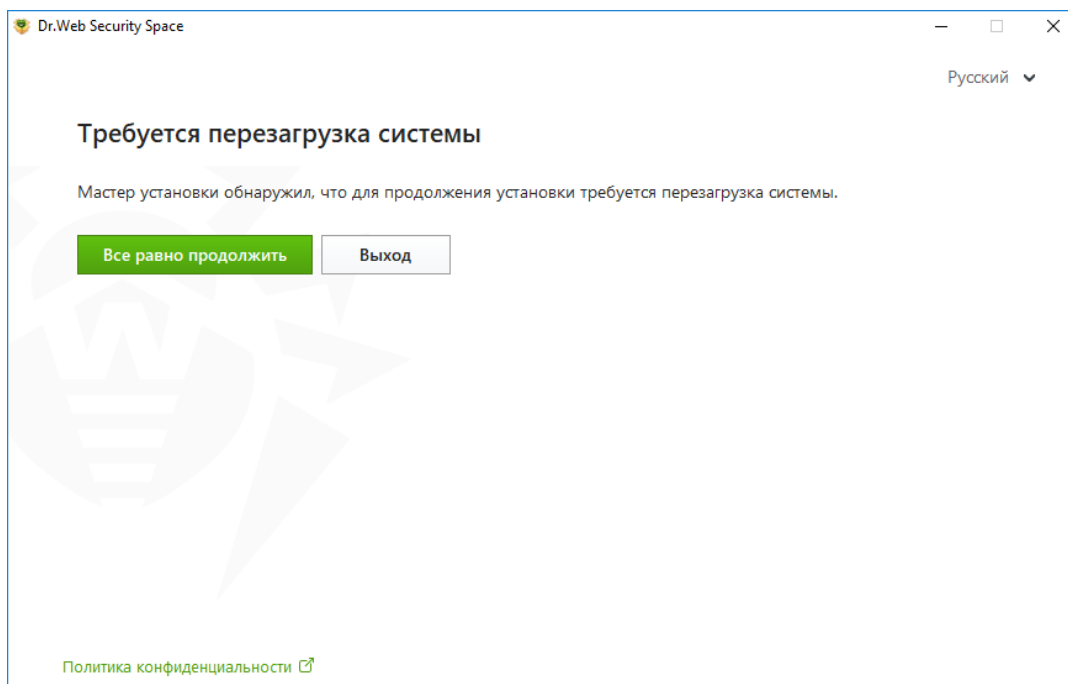
- Меню «Пуск»: **Пуск** → **Панель управления**, далее в зависимости от вида Панели управления:
 - Классический вид: **Программы и компоненты**.
 - Домашняя страница: **Программы** → **Программы и компоненты**.
- Классическое меню «Пуск»: **Пуск** → **Настройка** → **Панель управления** → **Программы и компоненты**.
- для Windows 7 выберите **Пуск** → **Панель управления**, далее в зависимости от вида Панели управления:
 - Мелкие/крупные значки: **Программы и компоненты**.
 - Категория: **Программы** → **Удаление программ**.
- для Windows 8/8.1/10 откройте **Панель управления** любым удобным способом, например через пункт **Панель управления** в контекстном меню, вызываемом правым щелчком мыши по левому нижнему углу экрана. Далее в зависимости от типа настройки **Просмотр** для Панели управления:
 - Мелкие/крупные значки: **Программы и компоненты**.
 - Категория: **Программы** → **Удаление программ**.

В открывшемся списке выберите строку Dr.Web Security Space и нажмите **Удалить**.



И подтвердите разрешение на запуск программы деинсталляции.

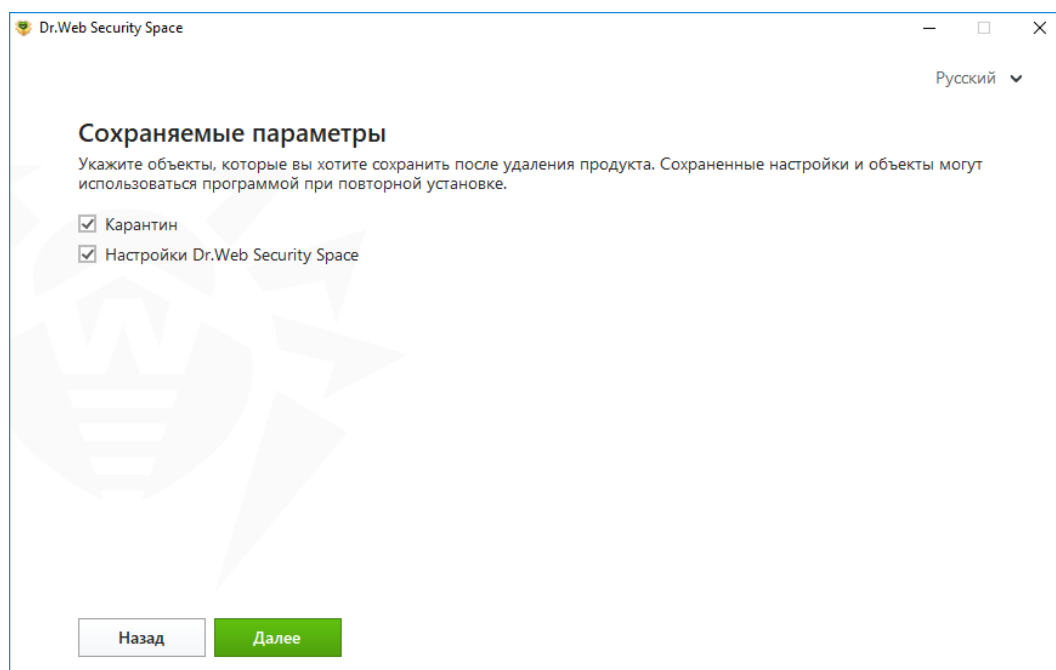




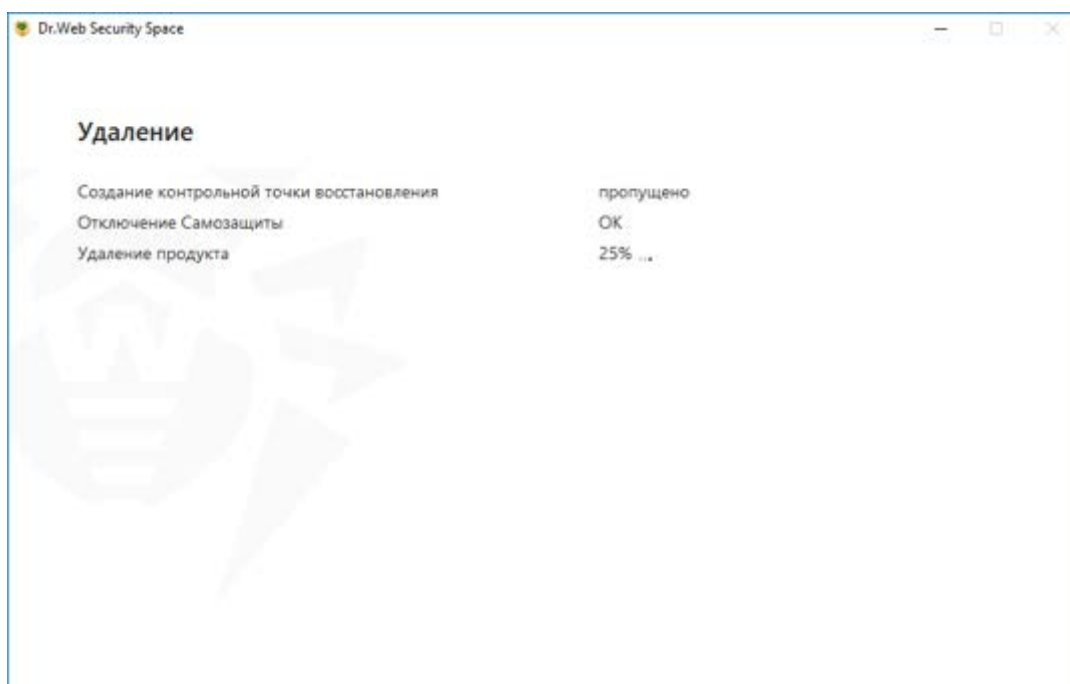
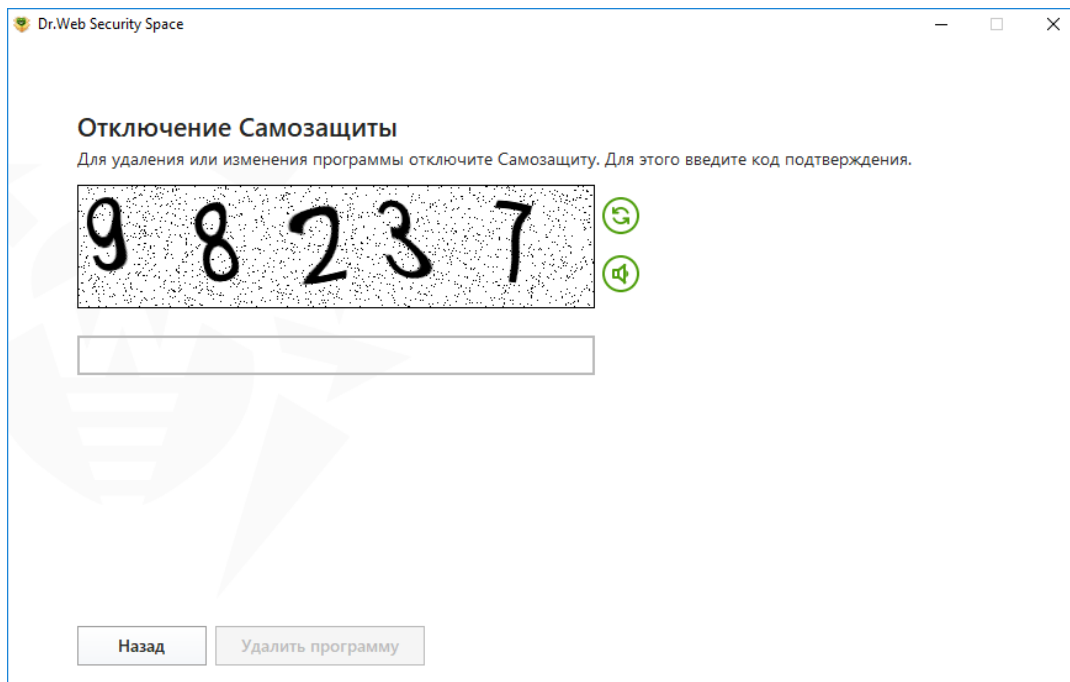
Подтвердите согласие на перезагрузку.


На следующем шаге определите необходимость удаления настроек и карантина ранее установленного продукта.

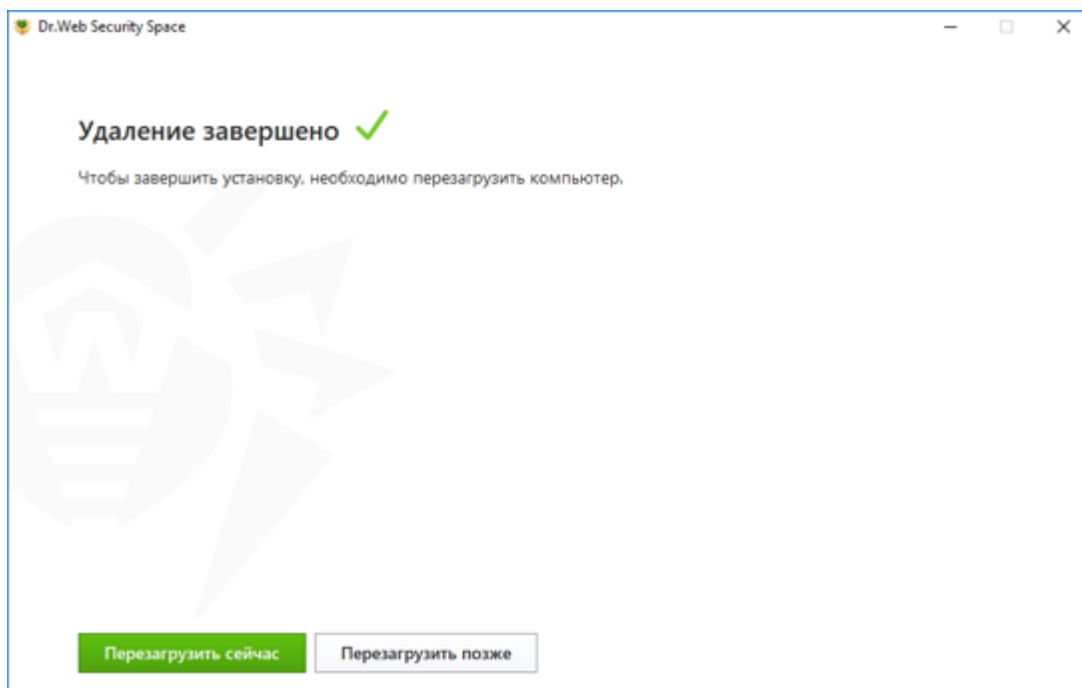
Если вы предполагаете в дальнейшем установить Dr.Web Security Space, то в окне **Сохраняемые параметры** установите флажки для объектов, которые следует сохранить после удаления программы. Сохраненные объекты и настройки будут использоваться программой при повторной установке. По умолчанию выбраны все опции — **Карантин, Настройки**. Нажмите кнопку **Далее**.



Для удаления каких-либо компонентов **Dr.Web** необходимо отключение самозащиты продукта. В связи с этим в окне **Отключение самозащиты** введите изображенный код и нажмите кнопку **Удалить программу**.



В процессе удаления иконка Dr.Web Security Space в системном трее изменит свой вид на . По завершении процедуры удаления программы перезагрузите компьютер для завершения процедуры удаления или изменения состава компонентов **Dr.Web**.



7. Продление лицензии. Замена ключевого файла

Внимание! Ключевой файл поставляется в виде файла с расширением .key или в виде ZIP-архива, содержащего этот файл. В данном файле содержится информация об используемом продукте, он необходим для нормальной работы антивируса.

Чтобы приобрести лицензию в онлайн-магазине компании «Доктор Веб», в **Менеджере лицензий** нажмите кнопку **Купить** и выполните требуемые действия.

https://estore.drweb.ru/home/ 60%


Dr.WEB® ЗАЩИТИ СОЗДАННОЕ

ПК/МАС ПОДПИСКА ИГОЛЬНЫЕ БИЗНЕСУ ПРОДЛИТЬ / РАСШИРИТЬ САМОПОДДЕРЖКА

СПОСОБЫ ОПЛАТЫ

СВЯЖИТЕСЬ С НАМИ

DR.WEB SECURITY SPACE РЕКОМЕНДУЕМ!
Максимальная свобода жизни в Сети без ограничений в безопасности



ВЫБЕРИТЕ

Срок лицензии 1 год

Количество ПК/Мас (1 серийный номер) 1 ПК/Мас

Вы сможете защитить бесплатно такое же количество моб. устройств.

ЭКОНОМИЯ (2): 0.00 РУБ.

СТОИМОСТЬ ЗАКАЗА: 1290.00 РУБ.

Купить >

- Лучшая защита Dr.Web для Windows, macOS, Linux
- Защита для Android БЕСПЛАТНО! Используйте для активации Dr.Web для Android серийный номер/ключевой файл, полученный при покупке лицензии на Dr.Web.

Получайте до 7% бонусами СПАСИБО и обменивайте бонусы на скидки до 99%

спасибо ОТ СОСРАНИКА

ОПИСАНИЕ

СПОСОБЫ ОПЛАТЫ. ДОКУМЕНТЫ

ДОСТАВКА

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

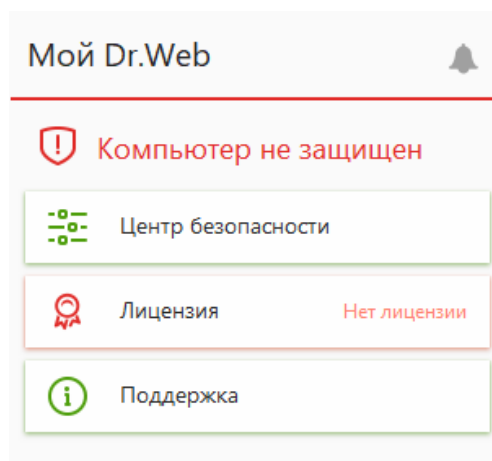
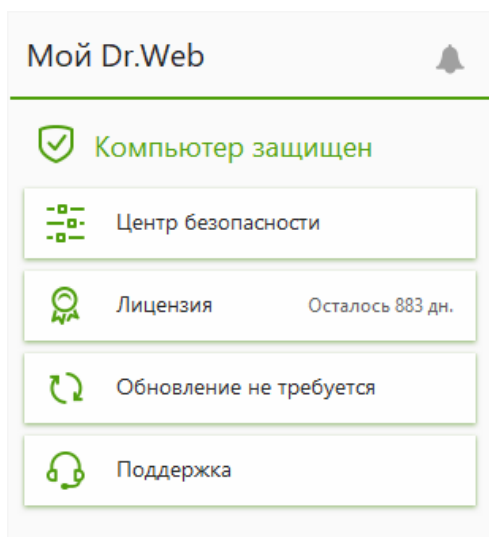
УСЛОВИЯ ПРОДЛЕНИЯ

ПРОГРАММА ЛОЯЛЬНОСТИ

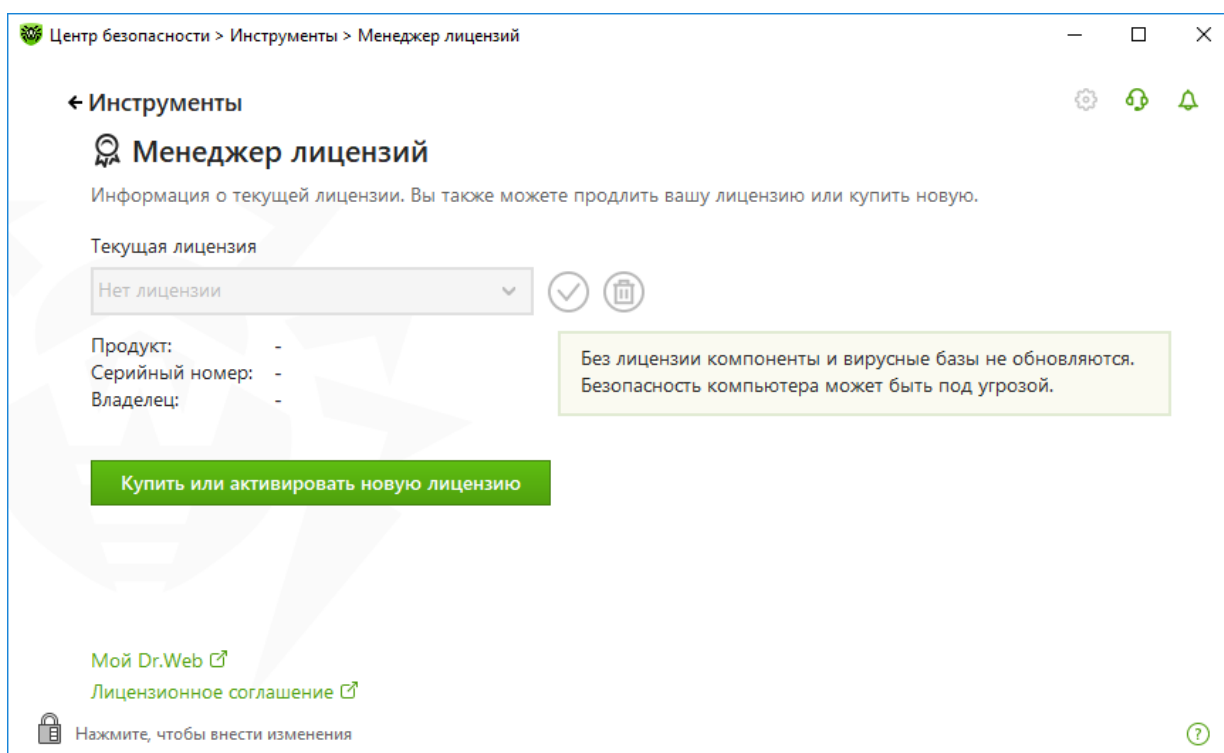
В некоторых случаях ключевой файл необходимо заменить. Это может понадобиться, например, при истечении срока действия имеющейся лицензии или приобретении лицензионного ключевого файла после использования демонстрационного. Узнать параметры вашей лицензии или продлить срок ее действия можно с помощью **Менеджера лицензий**. Для того чтобы попасть в менеджер лицензий, выберите пункт **Лицензия** в основном меню **SpIDer Agent'a**.

Меню с еще действующей лицензией

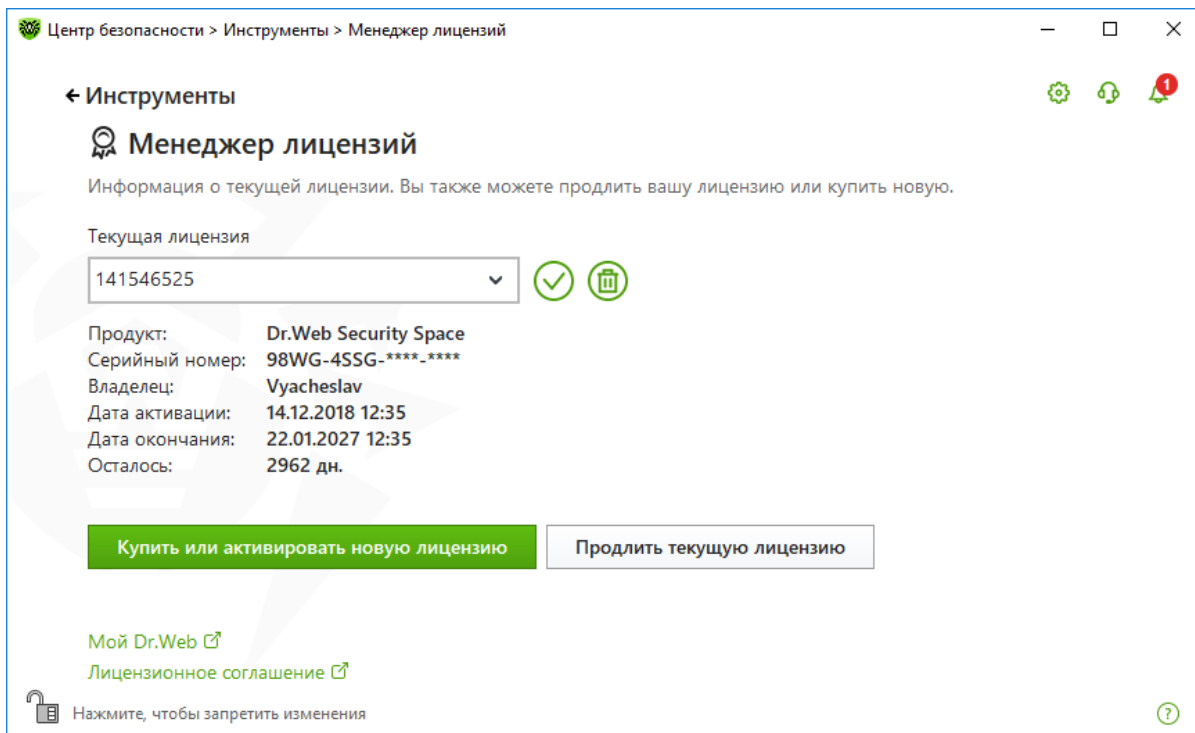
Меню с истекшей лицензией



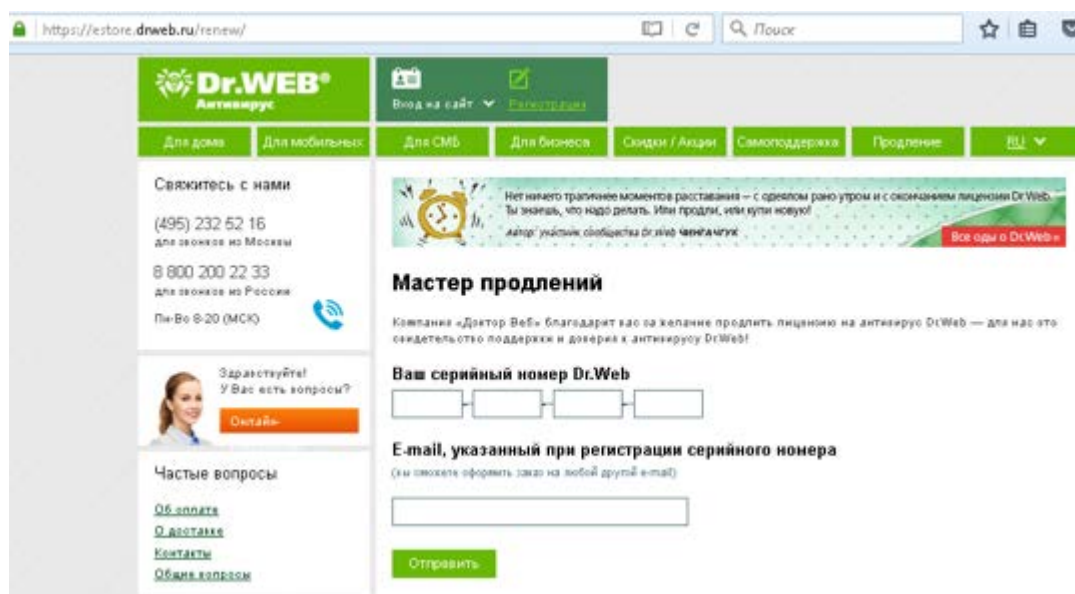
Если на компьютере не использовалась ранее ни одна лицензия, окно **Менеджера лицензий** будет выглядеть следующим образом:



Если у вас есть предыдущая лицензия и она еще действует, то в **Менеджере лицензий** будет показан ее номер.



При нажатии на кнопку **Купить или активировать новую лицензию** программа откроет окно мастера регистрации, который подскажет вам дальнейшие действия. При нажатии на кнопку **Продлить текущую лицензию** программа откроет страницу на сайте компании «Доктор Веб», на которую будут переданы параметры используемой лицензии.



Если вам необходимо продлить лицензию, на первом шаге укажите серийный номер вашего продукта (серийный номер индивидуален для каждого вашего продукта, вы можете найти его в комплекте поставки или в присланном вам письме с ключевым файлом). Затем укажите свою регистрационную информацию (только реальные данные, каждый запрос рассматривается индивидуально). Менеджер лицензий автоматически заменит имеющийся ключевой файл на актуальный.

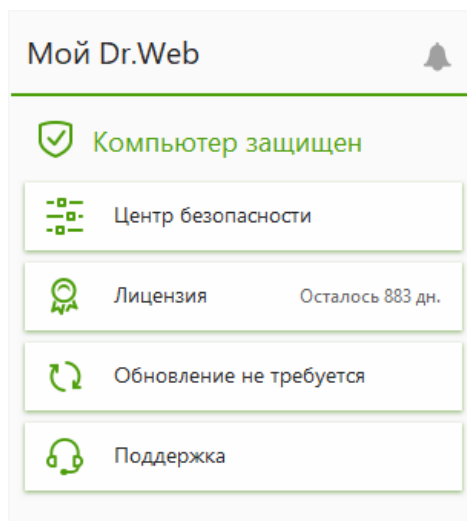
7.1. Замена ключевого файла

Вы можете получить ключевой лицензионный файл одним из следующих способов:

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

- при помощи регистрации продукта вручную на официальном сайте «Доктор Веб»;
- вместе с дистрибутивом продукта, если лицензионный файл был включен в комплект поставки. Для этого в ходе установки выберите пункт **Получить лицензию в процессе установки**, что запустит процедуру активации имеющейся у вас лицензии;
- на отдельном носителе.

Рассмотрим случай, когда ключевой файл необходимо заменить. Это может понадобиться, например, при истечении срока действия имеющейся лицензии (чтобы проверить, сколько осталось дней до истечения ее срока действия, откройте меню агента или зайдите в раздел **Менеджер лицензий**).



Для приобретения новой лицензии или продления текущей лицензии вы также можете воспользоваться вашей персональной страничкой на официальном сайте компании «Доктор Веб», которая открывается в окне интернет-браузера по умолчанию при выборе пункта **Мой Dr.Web** как в **Менеджере лицензий**, так и в меню **SpIDer Agent'a**.

← Инструменты

Менеджер лицензий

Информация о текущей лицензии. Вы также можете продлить вашу лицензию или

Текущая лицензия

✓ 141546525

Мой Dr.Web

Продукт: Dr.Web Security
Серийный номер: 98WG-4SSG-***
Владелец: Vyacheslav
Дата активации: 12/14/2018 12:30
Дата окончания: 1/22/2027 12:30
Осталось: 2901 дн.

Компьютер защищен

Центр безопасности

Лицензия Осталось 2901 дн.

Загрузка файлов 0%

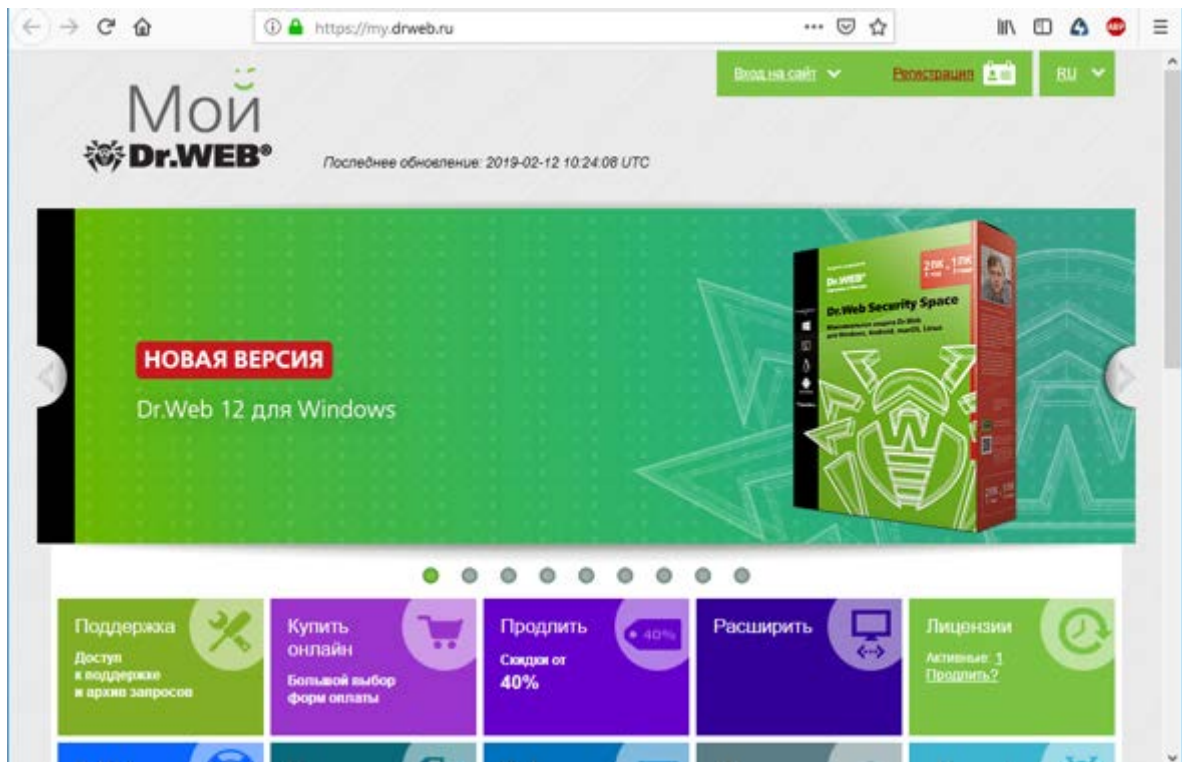
Поддержка

Купите или активировать новую лицензию

[Мой Dr.Web](#)

[Лицензионное соглашение](#)

Нажмите, чтобы запретить изменения



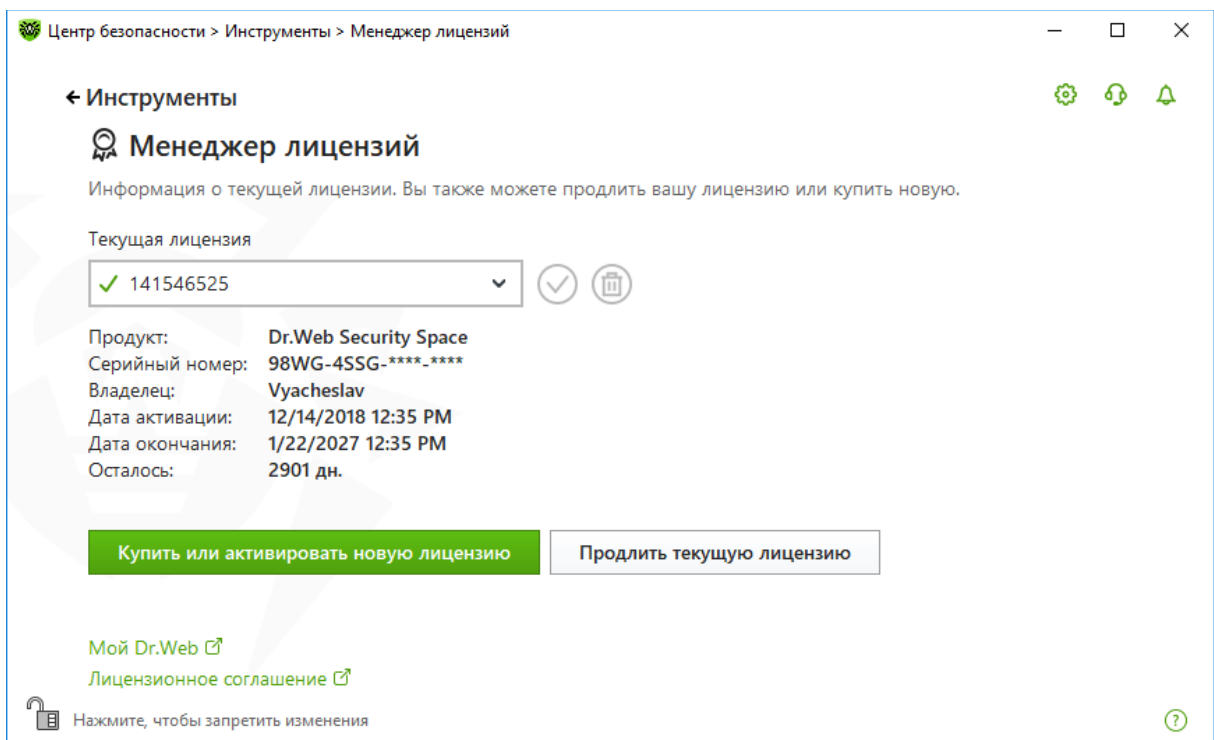
Лицензии	Всего: 6	Активные: 1	Продлены: 5	Истекли, не продлены: 0
	Блокированы: 0	На главную		

Лицензии

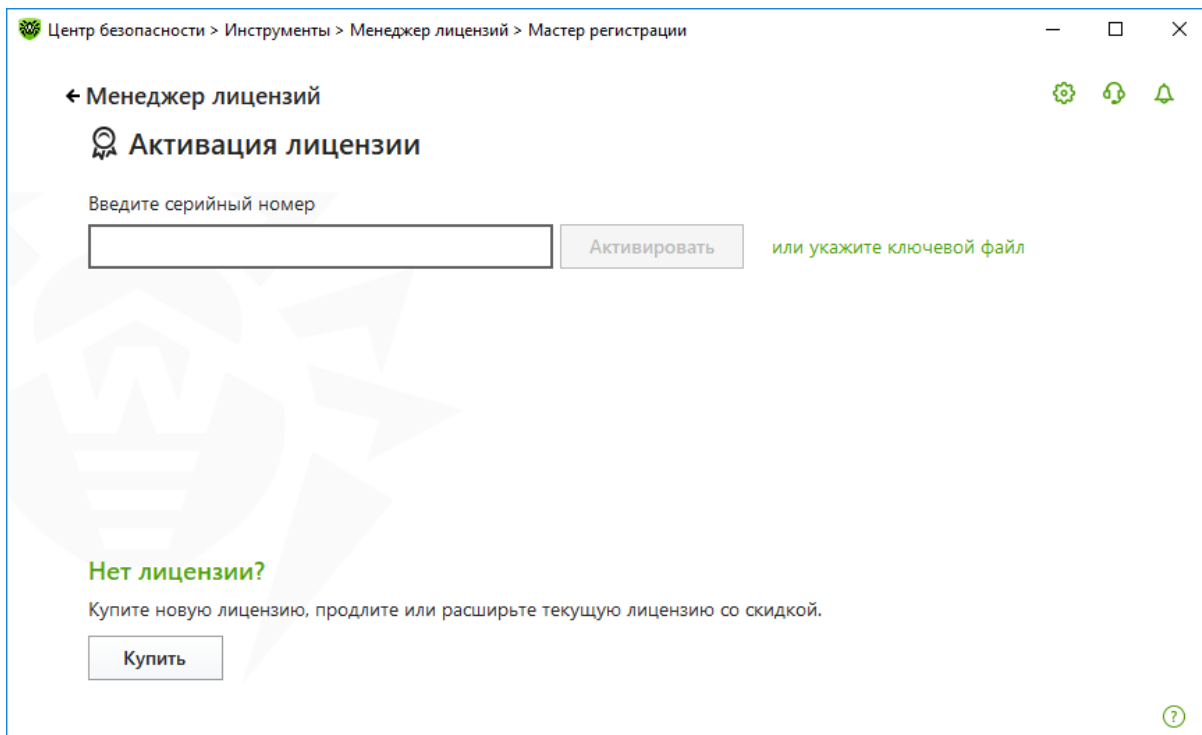
Лицензия	Поставщик
Серийный номер: 98WG-4SSG-FCK4-****	
Дата начала действия (активации): 2018-12-14	DWMoscow
Дата окончания действия: 2027-01-22	125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А
Статус: Лицензия активна	www.drweb.com
Владелец лицензии: Vyacheslav	devnull@drweb.com
Продукт: Продукты для Дома (Dr.Web Security Space)	+7 (495) 789-45-86
Лицензия: Рабочие станции: 1 / 12m	
Получить лицензионный сертификат	

Внимание! Если текущий ключевой файл недействителен, но в вашем **Менеджере лицензий** зарегистрировано несколько ключевых файлов, Dr.Web переключится на использование нового ключевого файла.

Чтобы продлить лицензию, используйте **Менеджер лицензий**. Нажмите кнопку **Купить или активировать новую лицензию**.

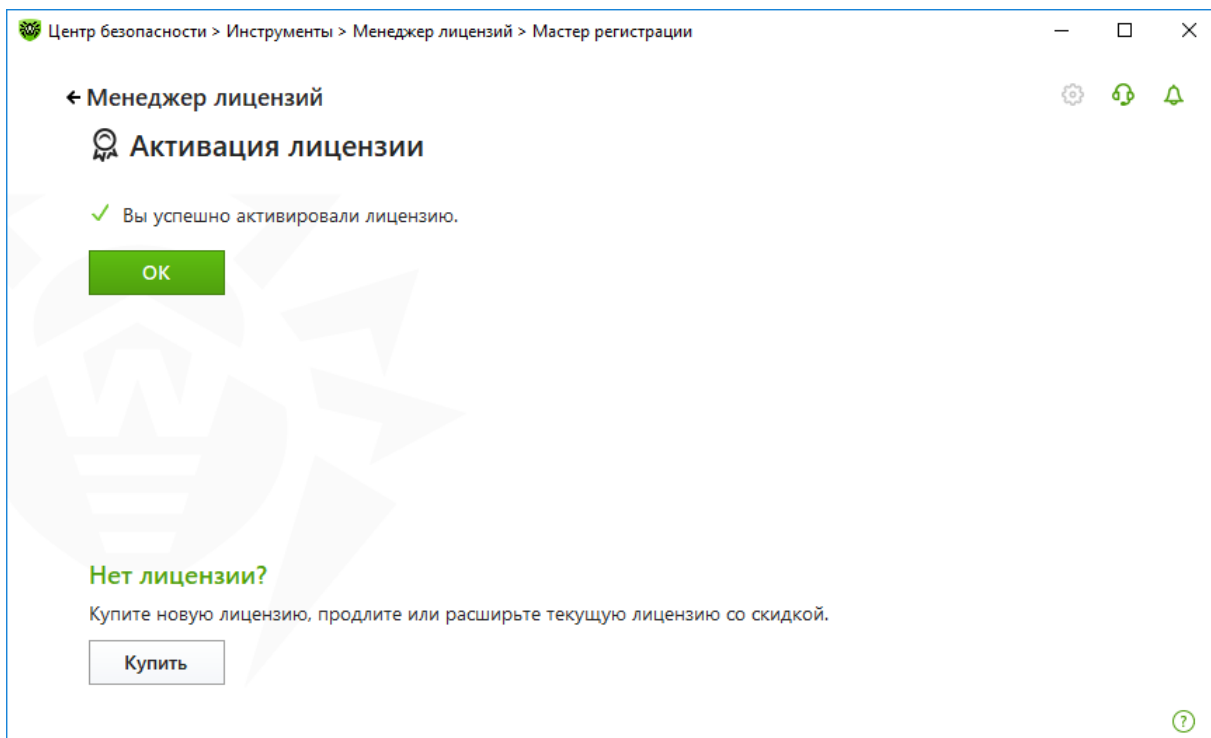


Откроется окно **Мастера регистрации**.



Для активации лицензии вам потребуется серийный номер, выданный вам при приобретении продукта — укажите его в поле ввода и нажмите кнопку **Активировать** — или укажите действительный ключевой файл, если вы уже активировали лицензию.

При вводе серийного номера для активации лицензии откроется окно ввода регистрационных данных.



7.2. Продление действия приобретенной лицензии на 150 дополнительных дней

Если вы уже являлись пользователем **Dr.Web**, то вы сможете продлить действие приобретенной лицензии на 150 дополнительных дней.

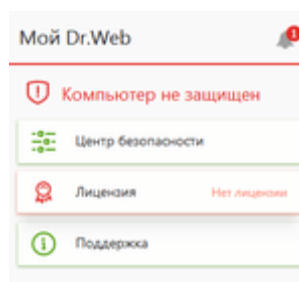
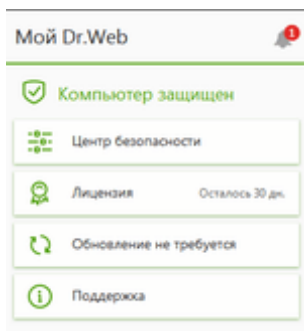
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Чтобы получить бонус в 150 дополнительных дней к сроку действия лицензии, необходимо выполнение следующих условий:

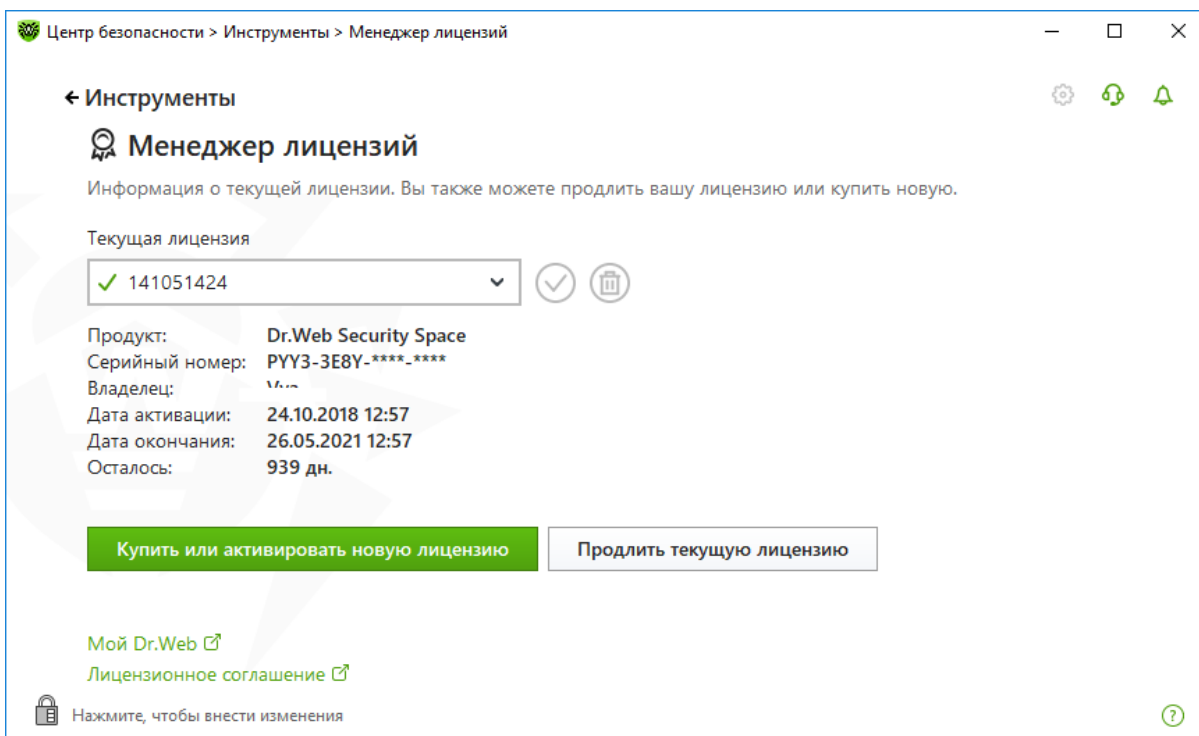
- срок действия лицензии, которая была зарегистрирована ранее, должен быть 3 месяца и более;
- срок действия лицензии, которая регистрируется, должен быть от 12 месяцев. Лицензия может быть зарегистрирована как в период действия предыдущей (далее — первой) лицензии, так и после его окончания. Истекшая лицензия не должна была продлеваться ранее.

С помощью левой или правой клавиши мыши щелкните по пиктограмме Dr.Web (пауку) в правом нижнем углу экрана. В появившемся меню выберите пункт **Лицензия**.

Меню с еще действующей лицензией Меню с истекшей лицензией

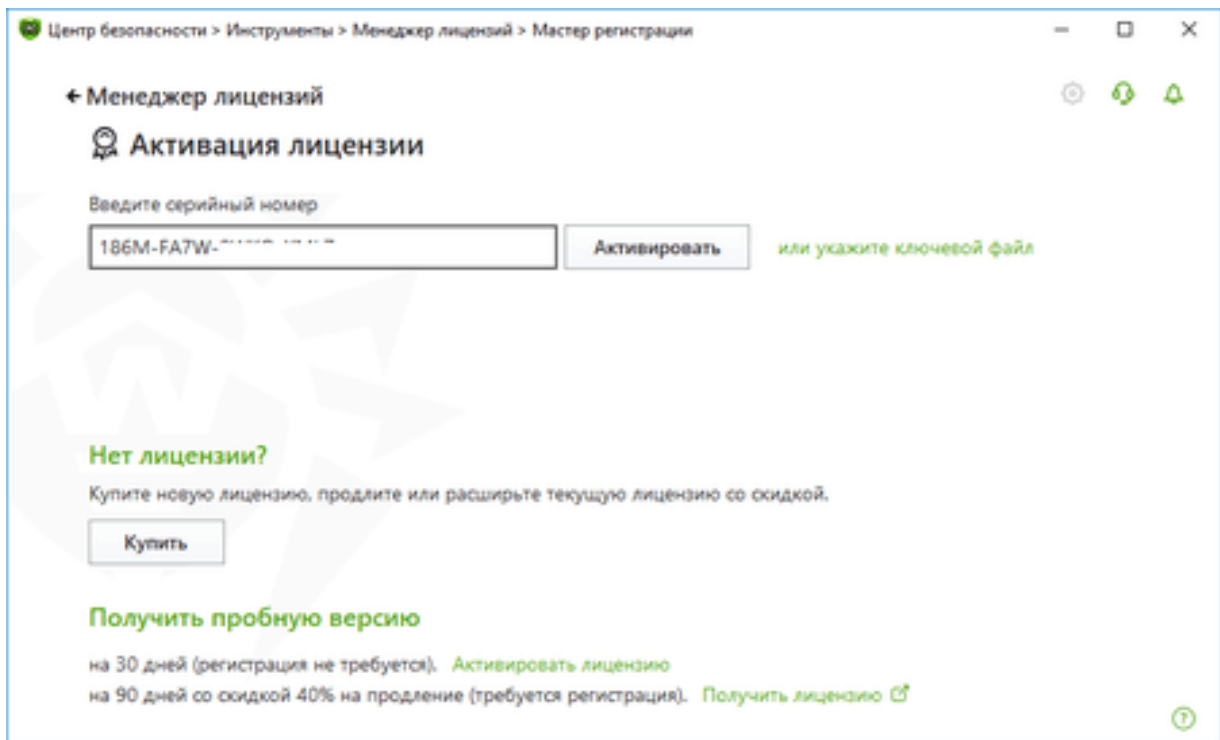


Для получения бонуса у вас должна быть действующая или истекшая лицензия, удовлетворяющая вышеописанным условиям. Если у вас есть предыдущая лицензия и она еще действует, то в **Менеджере лицензий** будет показан ее номер.

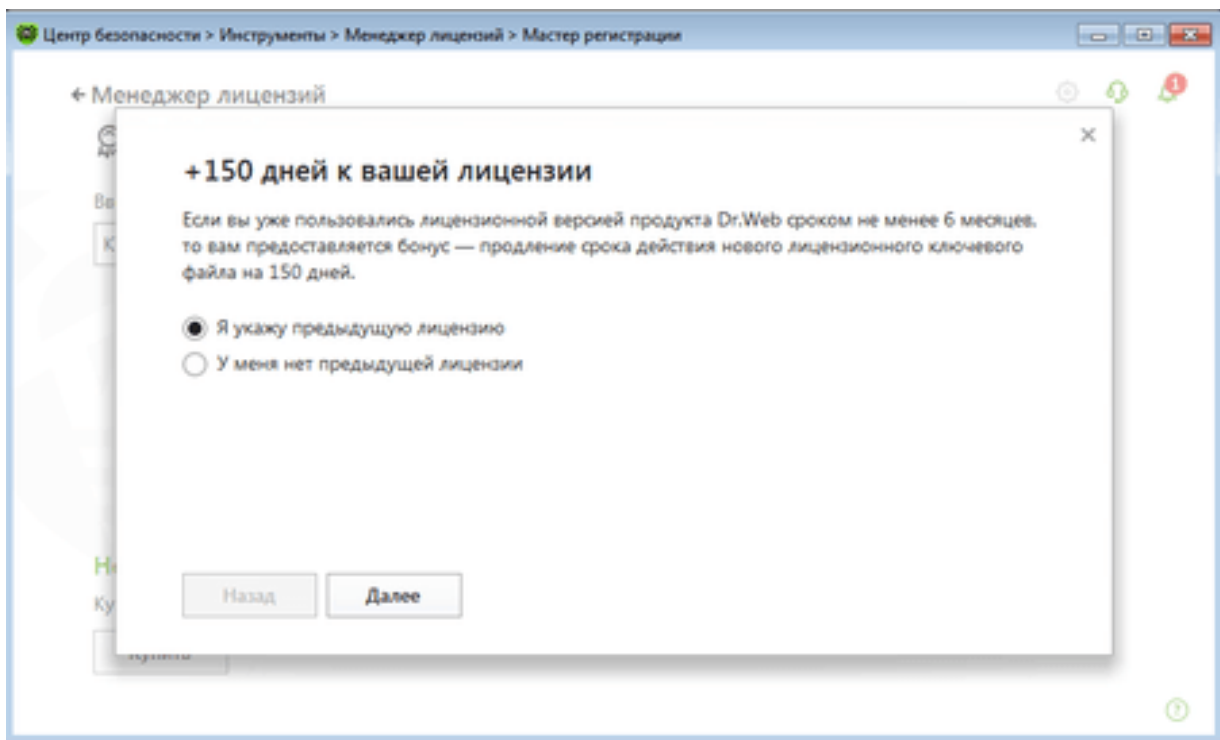


В открывшемся окне **Менеджера лицензий** нажмите на кнопку **Купить или активировать новую лицензию**.

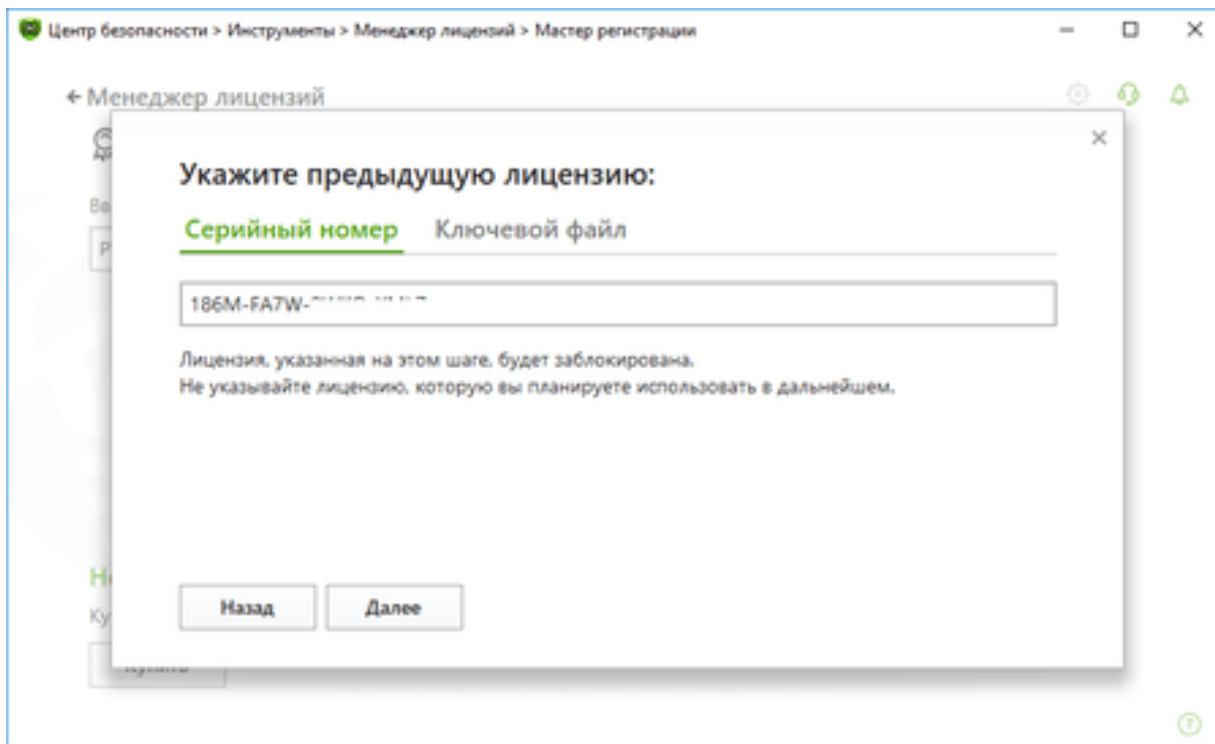
Откроется окно **Мастера регистрации**. Введите новый серийный номер.



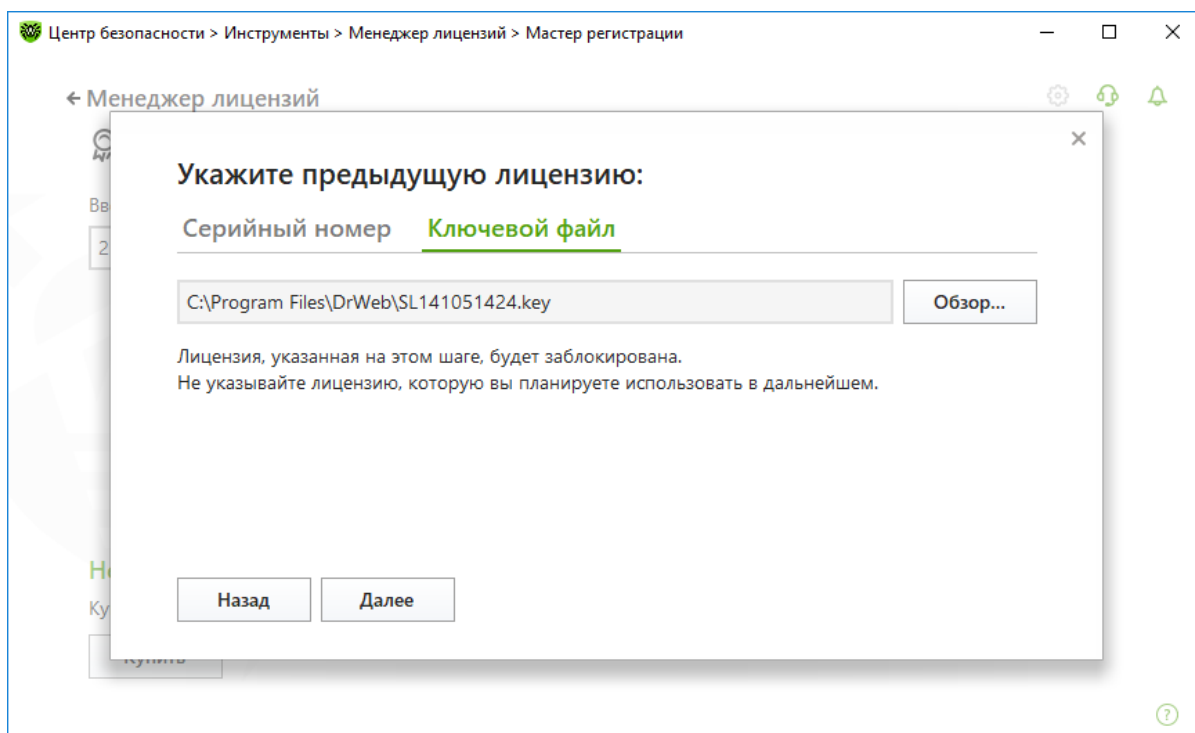
В открывшемся окне отметьте пункт **Я укажу предыдущую лицензию**.



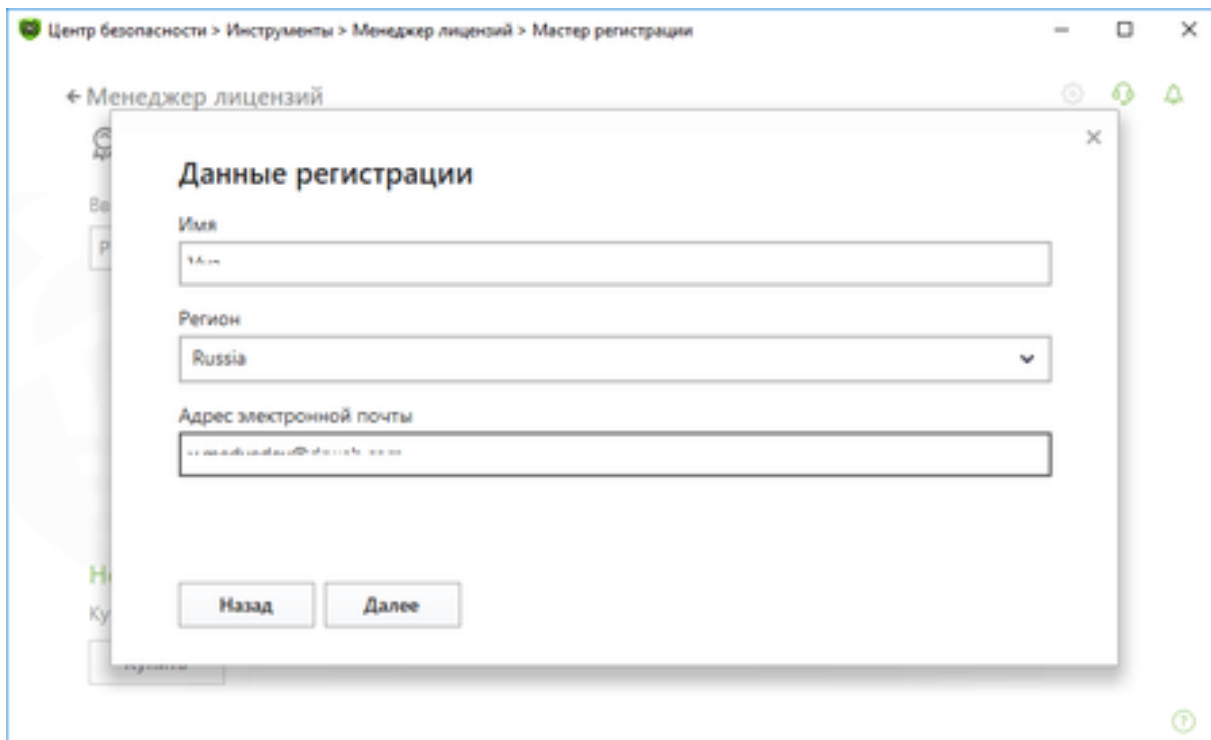
В открывшемся окне укажите серийный номер или ключевой файл предыдущей лицензии.



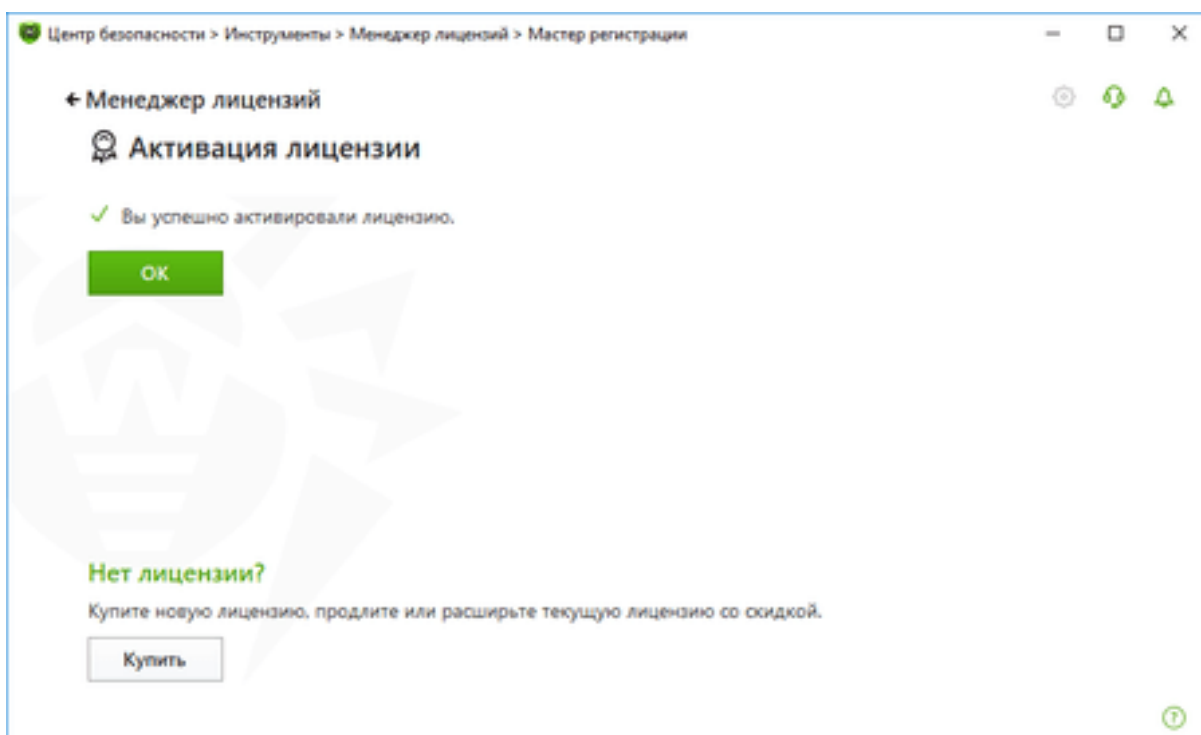
По умолчанию предлагается ввести серийный номер, но вы также можете указать ключевой файл.



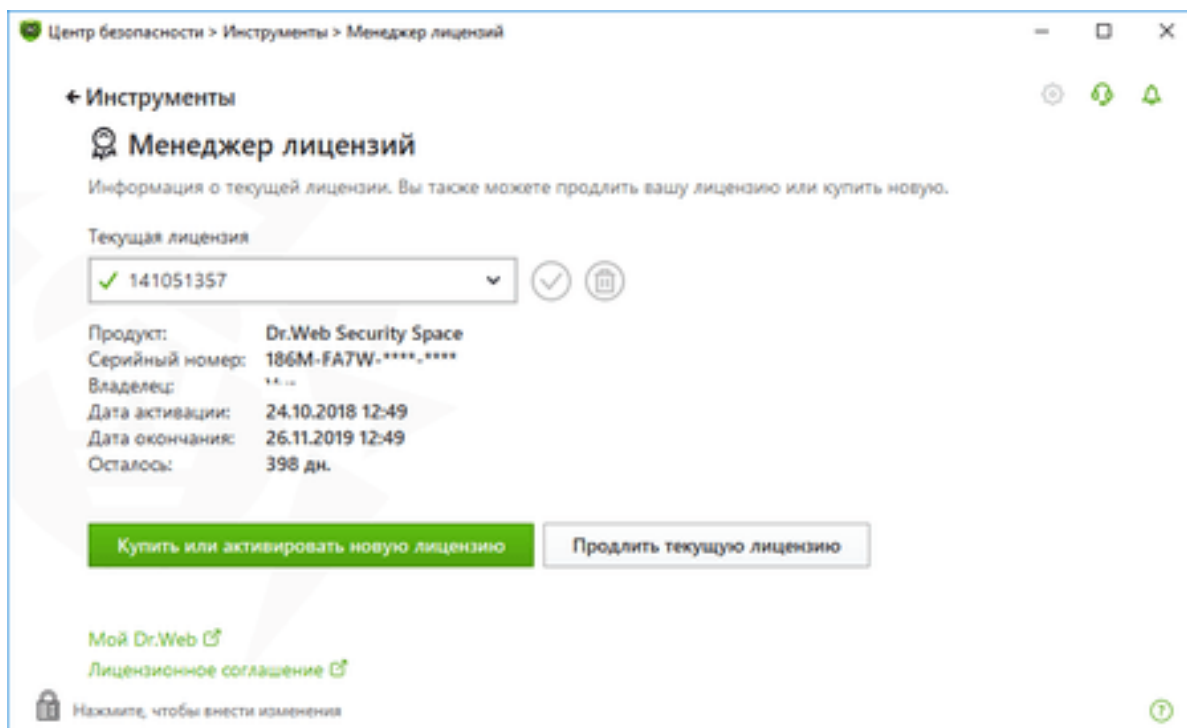
Заполните регистрационную форму и нажмите на кнопку **Далее**.



Нажмите на кнопку **ОК**.



Откроется окно **Менеджера лицензий**.




В результате регистрации нового серийного номера:

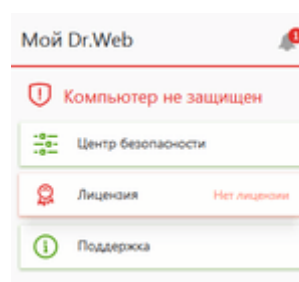
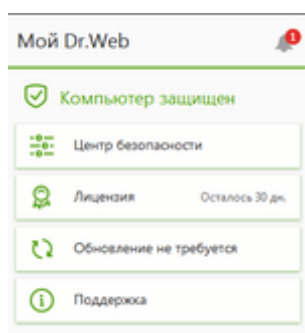
- текущая лицензия будет заблокирована;
- к сроку действия лицензии, использованной для продления, будет добавлено 150 дней. А если вы продлевали еще не истекшую лицензию, этот срок будет увеличен на количество неиспользованных дней в предыдущей лицензии.

8. Настройка антивирусной защиты

8.1. Начало работы



Сразу после установки агента защиты в трее (правом нижнем углу экрана) появляется значок Агента , с помощью которого можно осуществлять управление всеми настройками антивируса.

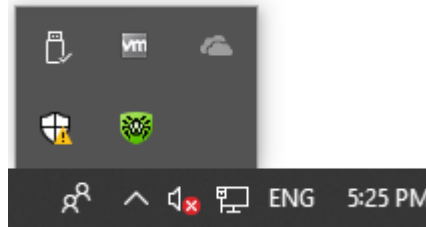
Меню с еще действующей лицензией **Меню с истекшей лицензией**



Если **SpIDer Agent** не запущен и значок Агента отсутствует, в меню **Пуск** раскройте группу **Dr.Web** и нажмите на пункт **SpIDer Agent**.





Внимание! При использовании Windows 7 и выше для получения доступа к данному значку

нажмите на кнопку . Рекомендуется включить отображение иконки (для разных версий ОС Windows порядок настройки отличается. Например, щелкните на значок  на тулбаре, выберите пункт **Customize** и настройте желательный вид отображения иконки), так как по изменению ее вида можно контролировать состояние антивирусной защиты.



Значок **SpIDer Agent'a** не будет отображаться в области уведомлений при использовании централизованной защиты в случае установки соответствующей настройки в Центре управления.

Значок **SpIDer Agent'a** отражает текущее состояние Агента Dr.Web:

-  все компоненты, необходимые для защиты компьютера, запущены и работают правильно, соединение с сервером централизованной защиты установлено;
-  Самозащита, Агент Dr.Web или важный компонент (сторож **SpIDer Guard**, **Брандмауэр**) отключены, что ослабляет защиту антивируса и компьютера; либо ожидается соединение с сервером, но оно еще не установлено. Включите Самозащиту или отключенный компонент, дождитесь соединения с сервером;
-  Ожидается запуск компонентов после старта операционной системы, дождитесь запуска компонентов программы, или в процессе запуска одного из ключевых компонентов Агент Dr.Web возникла ошибка. Компьютер находится под угрозой заражения. Проверьте наличие действительного ключевого файла и при необходимости установите его или обратитесь к администратору антивирусной сети.
-  В данный момент Сканер проводит проверку.

Если настройки уведомлений не были изменены, над значком могут появляться сообщения-подсказки.


Запуск и настройка компонентов антивирусного агента осуществляются с помощью контекстного меню значка модуля управления, появляющегося при нажатии на левую или правую кнопку мыши. Для доступа к настройкам компонентов и для перехода к онлайн-сервису **Мой Dr.Web** введите пароль, если в разделе **Настройки** вы включили опцию **Защищать паролем настройки Dr.Web**. Если вы забыли пароль к настройкам продукта, обратитесь в службу технической поддержки.

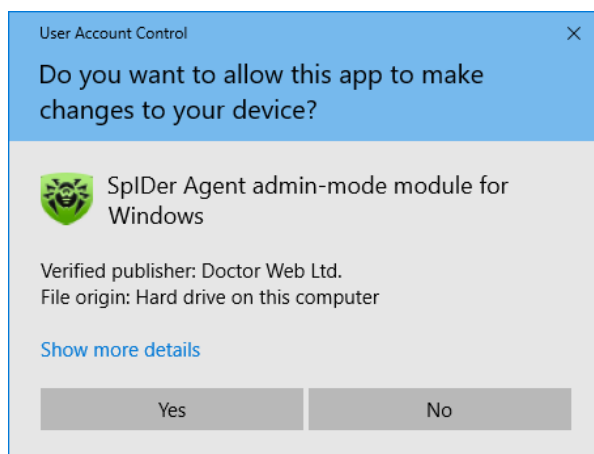
Внимание! Доступ к настройкам и компонентам защиты, а также отключение компонентов возможны только при работе с правами администратора.

Назначение пунктов главного меню Агента:

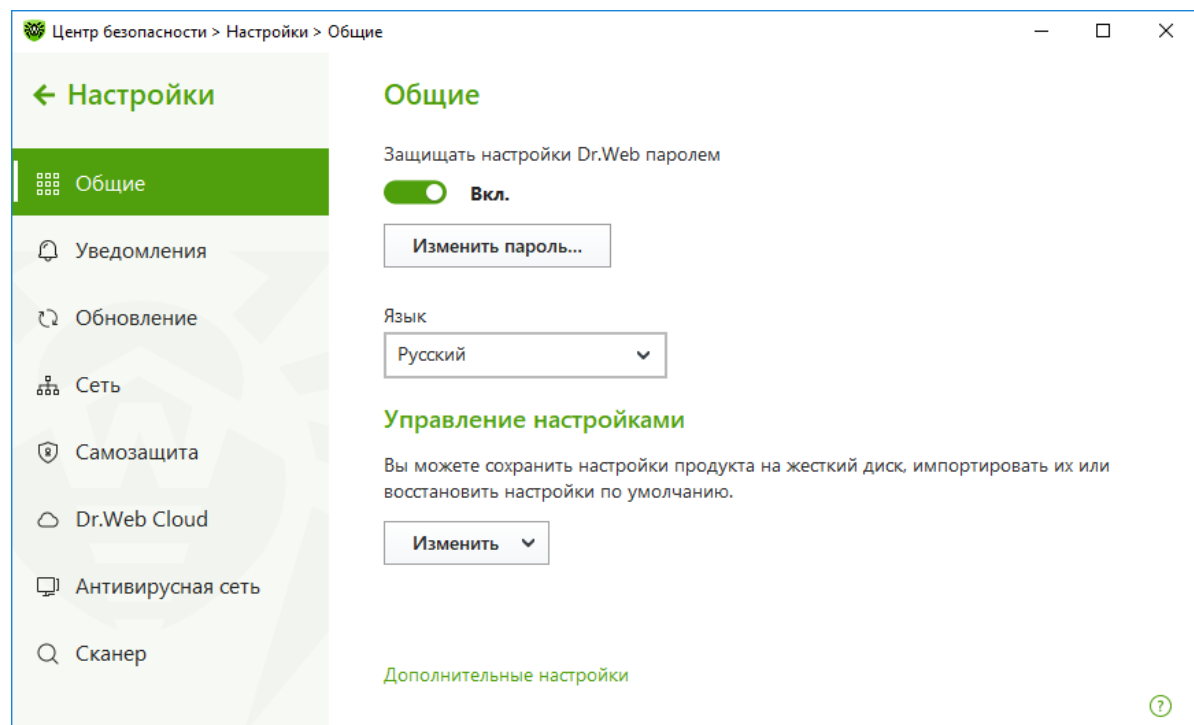
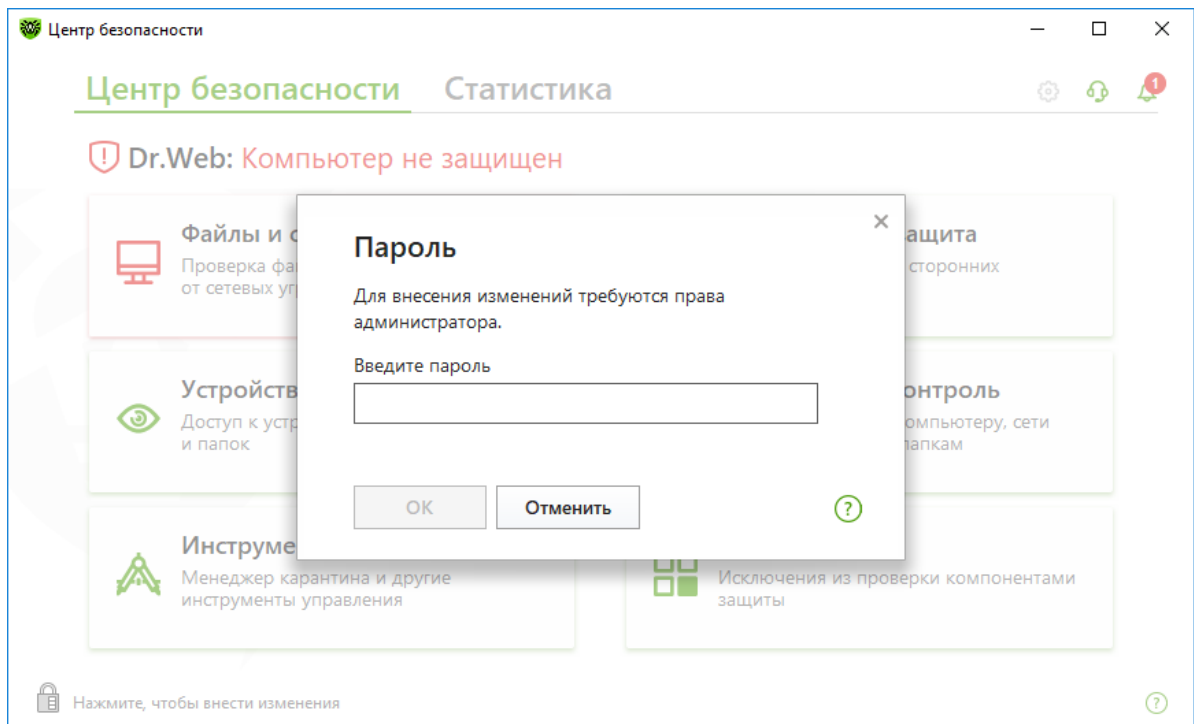
- **Мой Dr.Web.** Открывает персональную страницу пользователя на сайте компании «Доктор Веб». На данной странице вы сможете получить информацию о вашей лицензии (срок действия, серийный номер), продлить срок ее действия, задать вопрос службе поддержки и многое другое.

- 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.
- **Лицензия**. Открывает **Менеджер лицензий**.
- **Обновление**. Информация об актуальности вирусных баз и времени последнего обновления. Запускает обновление компонентов программы и вирусных баз.
- **Поддержка**. Открывает окно поддержки.
- **Ограничение времени** (появляется при включенной опции ограничения времени работы за компьютером и в сети Интернет компонента Родительский контроль). Краткая информация об ограничениях работы за компьютером и в сети Интернет, а также о длительности перерыва при интервальном ограничении.
- **Самозащита** (появляется при отключении Самозащиты). С помощью переключателя вы можете снова включить Самозащиту Dr.Web.





По умолчанию Dr.Web запускается в ограниченном режиме — режиме пользователя, в котором недоступна возможность настройки компонентов защиты. Для переключения в другой режим нажмите на  в левом нижнем углу окна **Центр безопасности**. При включенном UAC операционная система выдаст запрос на повышение прав.

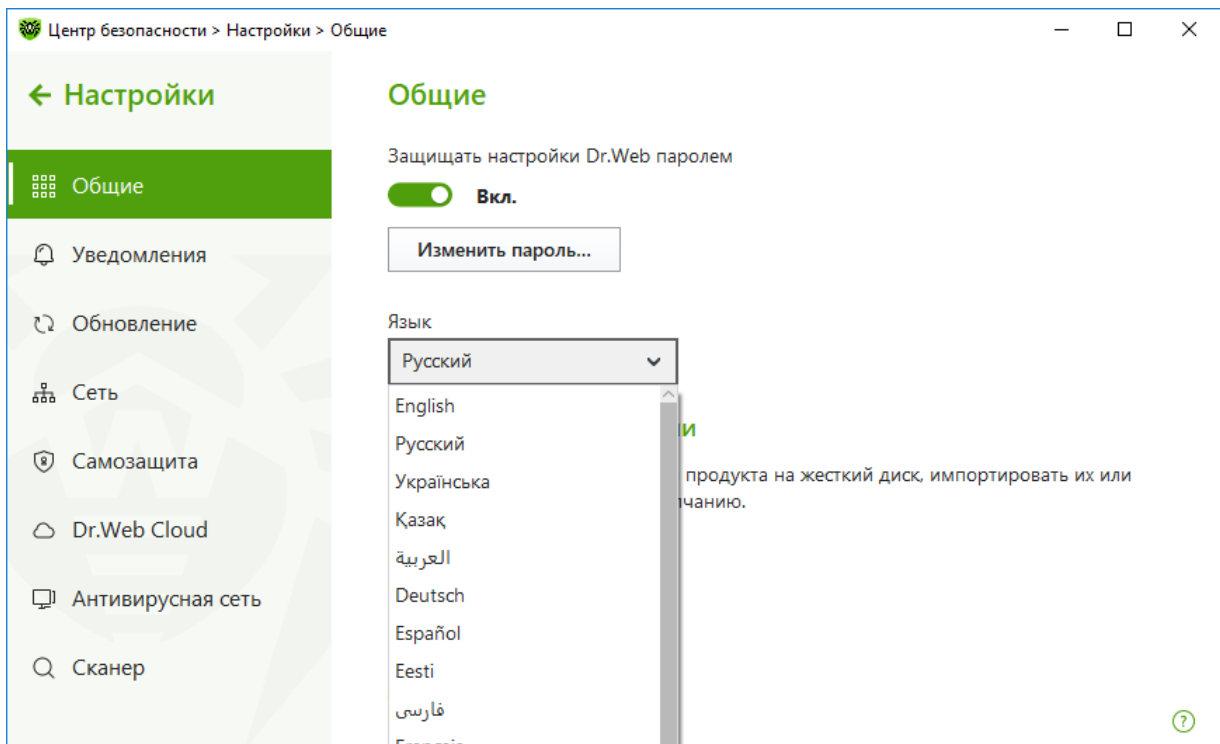


Для изменения режима работы введите пароль, если в разделе **Настройки** → **Общие** была включена опция **Защищать настройки Dr.Web паролем**.







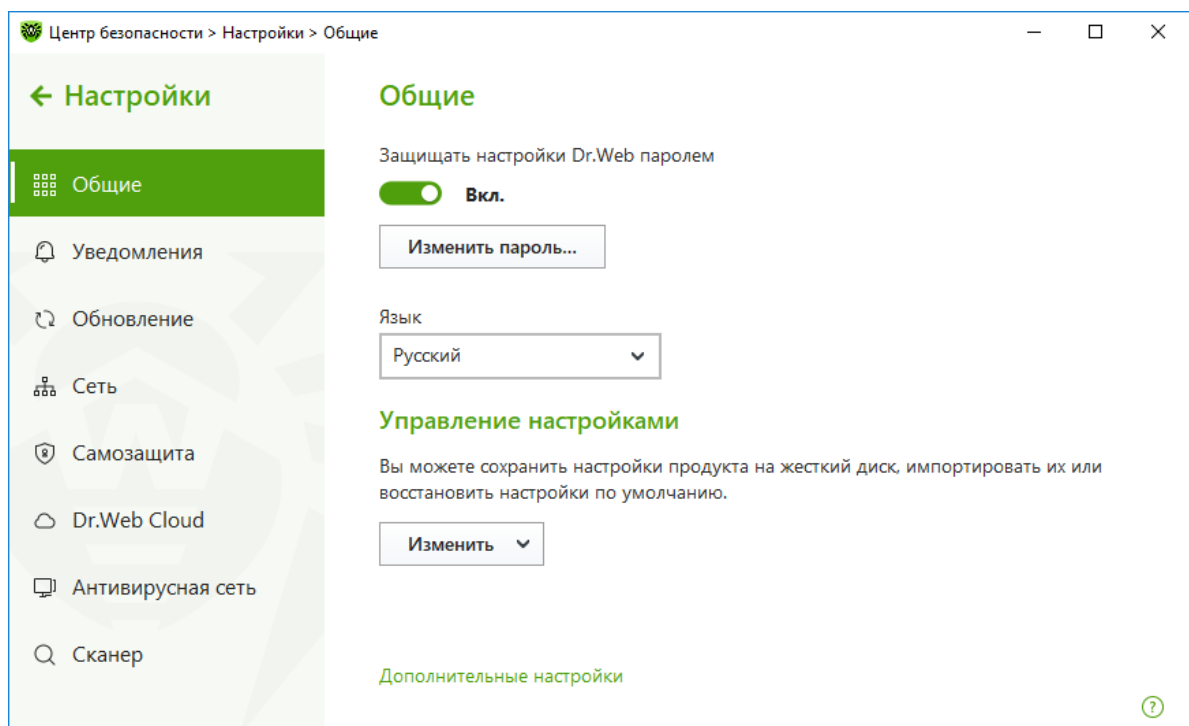
8.2. Настройка языка интерфейса

Для смены языка кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . Нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Общие**. В выпадающем списке **Язык** укажите необходимый язык интерфейса.



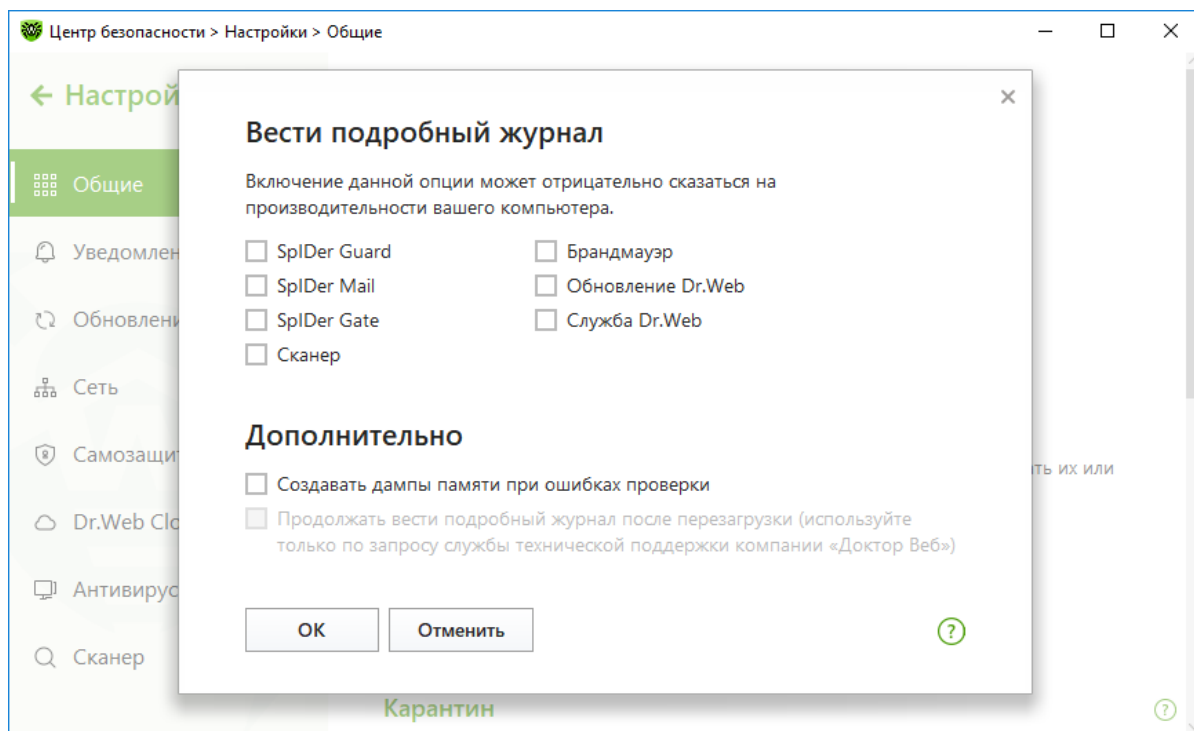
8.3. Изменение уровня подробности протокола событий

Для изменения уровня подробности протокола работы компонентов кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . Нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Общие**.



Кликните на **Дополнительные настройки**. В группе настроек **Журнал** нажмите на **Изменить**.

Отметьте компоненты, для которых уровень подробности журнала требуется изменить.



Сохраните изменения.




При ведении подробного журнала фиксируется максимальное количество информации о работе компонентов Dr.Web. Это приведет к отключению ограничения на размер файлов журнала (по умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ (для компонента SpIDer Guard — 100 МБ)) и снизит производительность работы Dr.Web и операционной системы. Используйте этот режим только при возникновении проблем в работе компонентов или по просьбе технической поддержки компании «Доктор Веб».

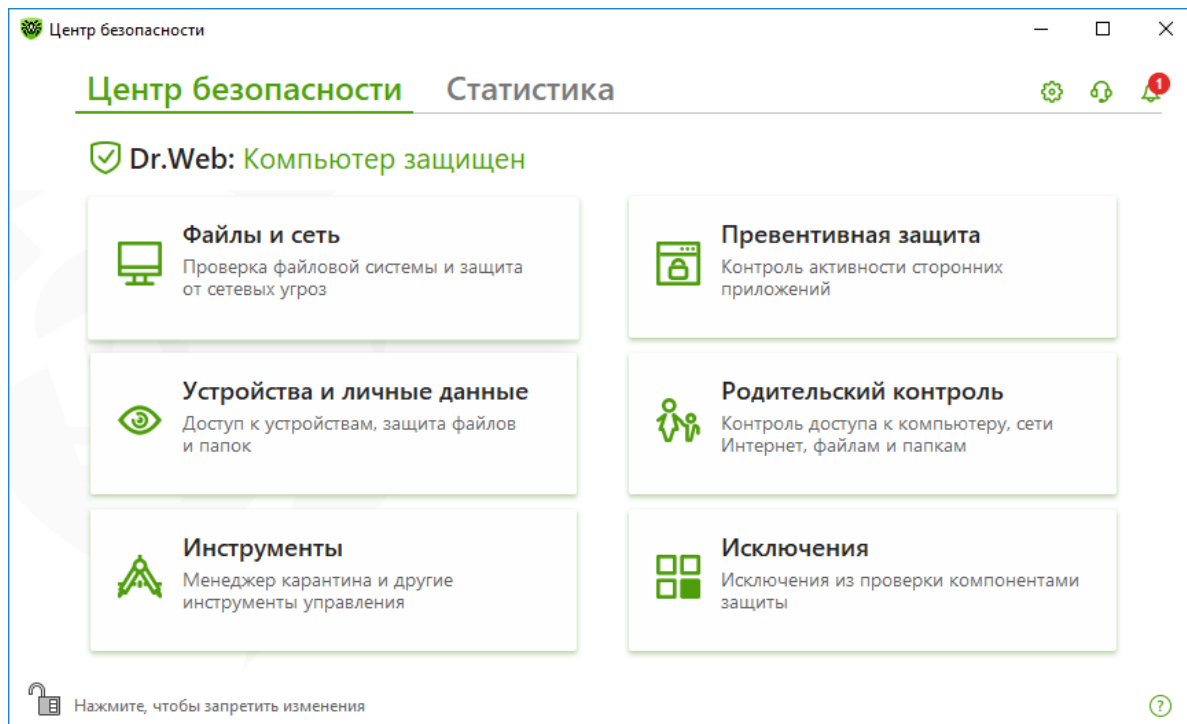
По умолчанию подробный журнал ведется до первой перезагрузки операционной системы. Если необходимо зафиксировать поведение компонента в период до и после перезагрузки, установите флажок **Продолжать вести подробный журнал после перезагрузки**.

При превышении максимального размера файл журнала урезается до:

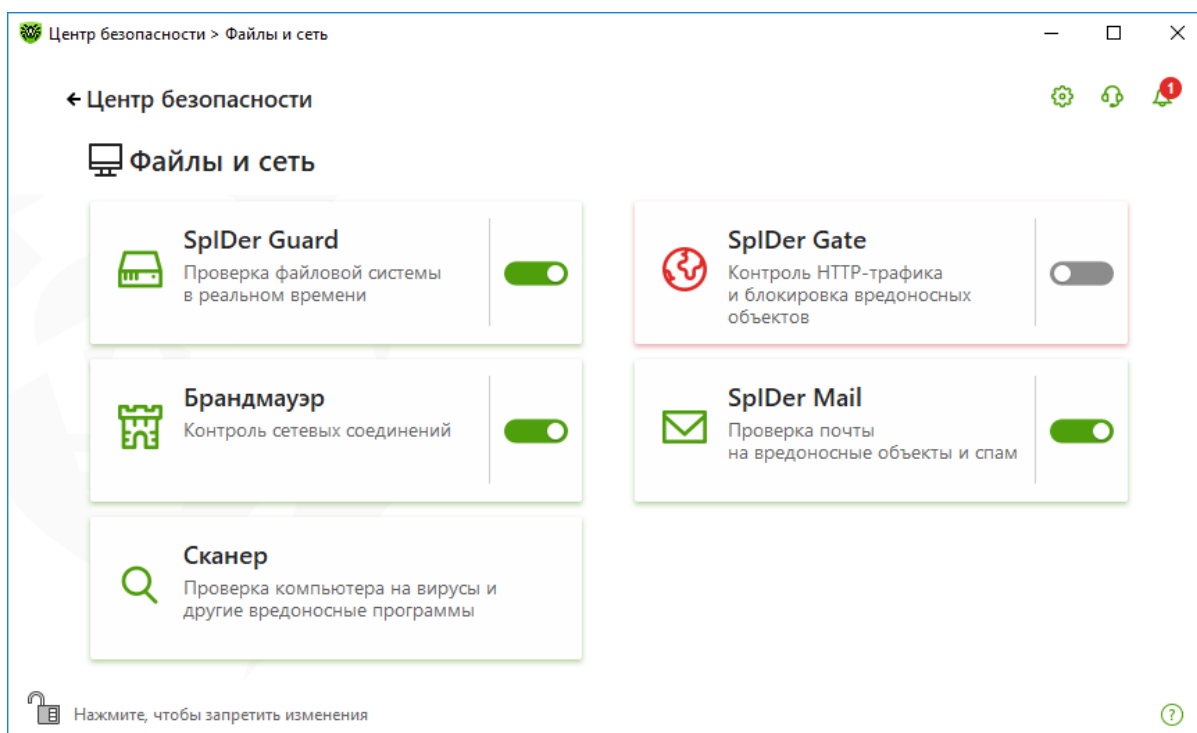
- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер.

8.4. Запуск и останов компонентов защиты

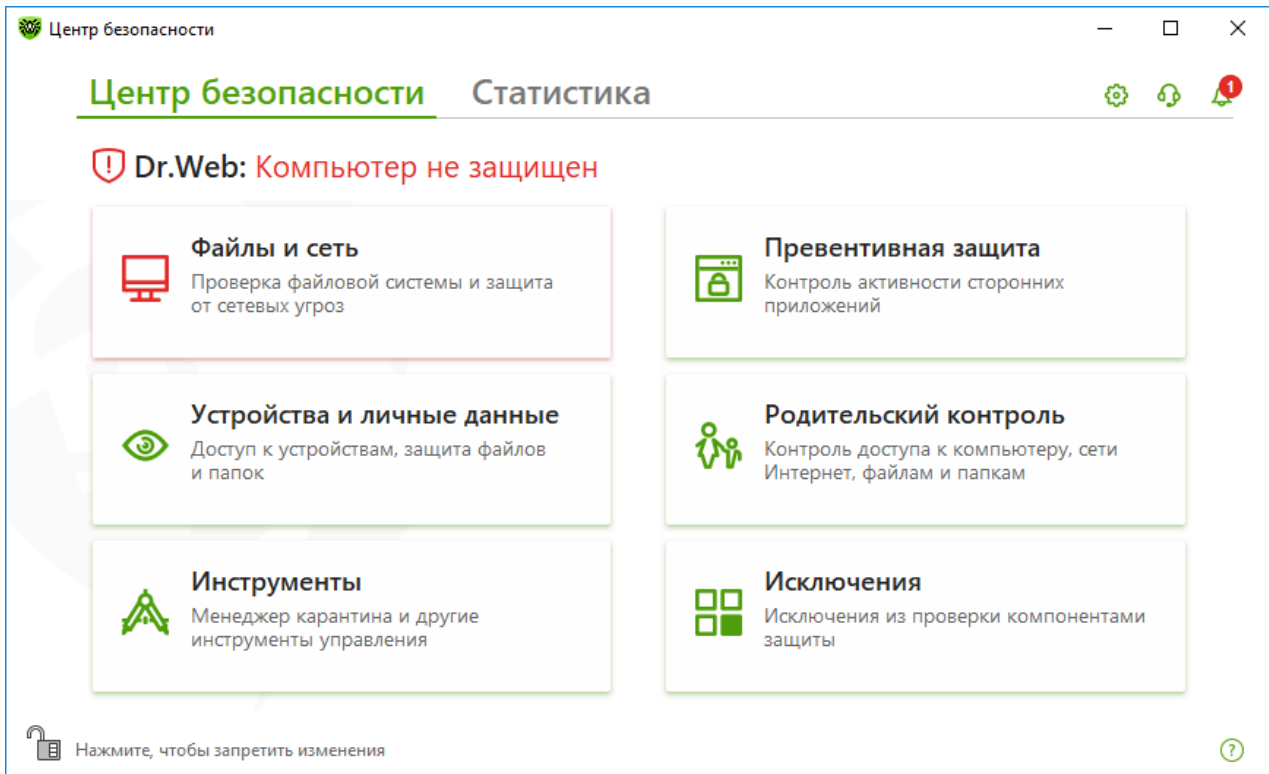
В случае наличия прав пользователь может остановить или запустить действующие у него на компьютере компоненты защиты. Для выполнения этих действий кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на .



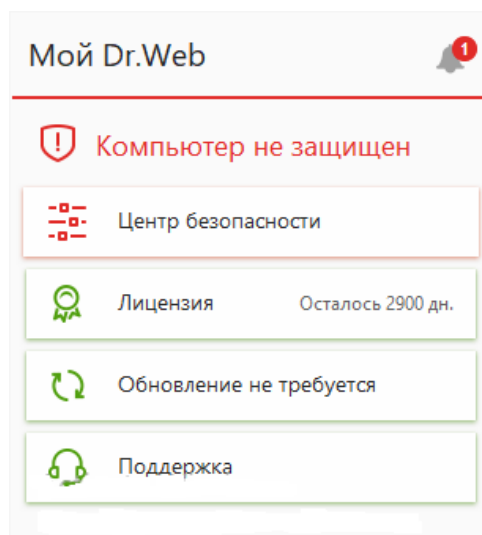
Выберите нужную группу компонентов. Например, **Файлы и сеть**.



Нажмите левую или правую сторону переключателя справа от названия компонента. Кнопка с названием компонента будет помещена в красную рамку, как и группа настроек, в которую входит компонент.



Статус защиты в окне **Центр безопасности** и меню агента изменится на **Компьютер не защищен**.






Значок в трее изменит вид на .

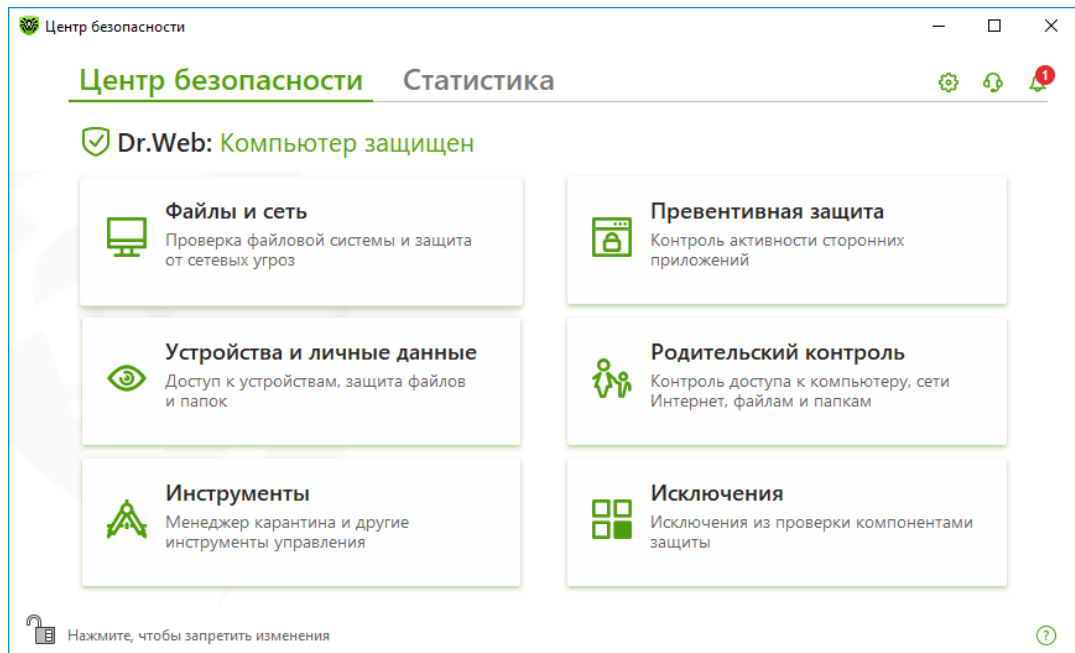
8.5. Антивирусная проверка станции. Выбор приоритета сканирования

Рекомендуется сразу после инсталляции провести полную проверку системы, а также проводить ее регулярно. В частности, это необходимо в связи с тем, что проверенные файловым монитором и записанные на диск файлы (в том числе сохраненные в архивы) могут содержать вирусы, неизвестные на момент их записи на диск, а значит, при передаче их на незащищенные компьютеры (при отсутствии проверки исходящего трафика) возникает риск их заражения.

Рекомендуется запускать Сканер от имени пользователя, обладающего правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут подвергнуты проверке.

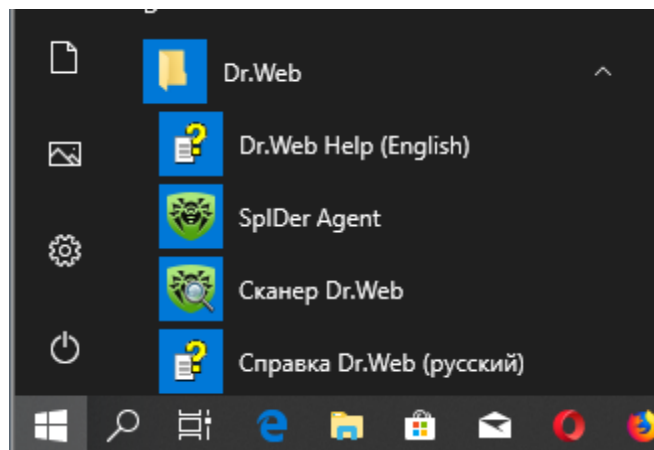
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Для проведения проверки щелкните кнопкой мыши по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на .



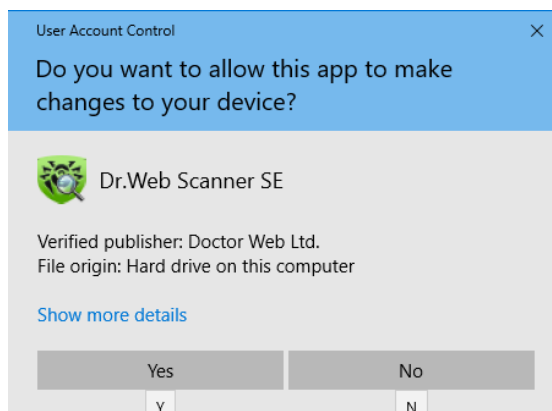
Выберите **Файлы и сеть** и далее **Сканер**.

Или выберите пункт меню **Сканер Dr.Web** в папке **Dr.Web** Главного меню Windows (открывается по кнопке **Пуск**) либо используйте команду операционной системы Windows для запуска Сканера из командной строки.



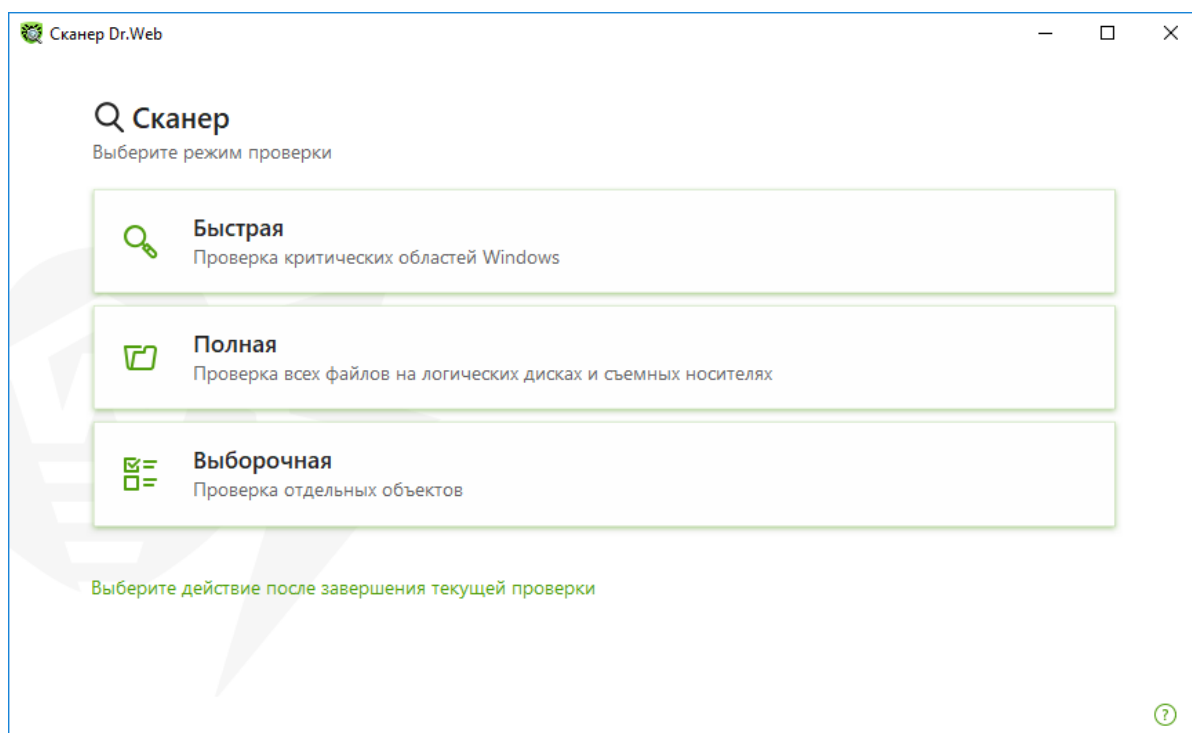
Чтобы запустить Сканер с настройками по умолчанию для проверки конкретного файла или каталога, выберите в контекстном меню значка файла или каталога (на Рабочем столе или в Проводнике операционной системы Windows) пункт **Проверить Dr.Web**.

Внимание! При использовании ОС Windows Vista и старше (включая Windows 7/8) с включенной функцией контроля учетных записей Windows (UAC) подтвердите запуск программы, нажав на **Yes**.







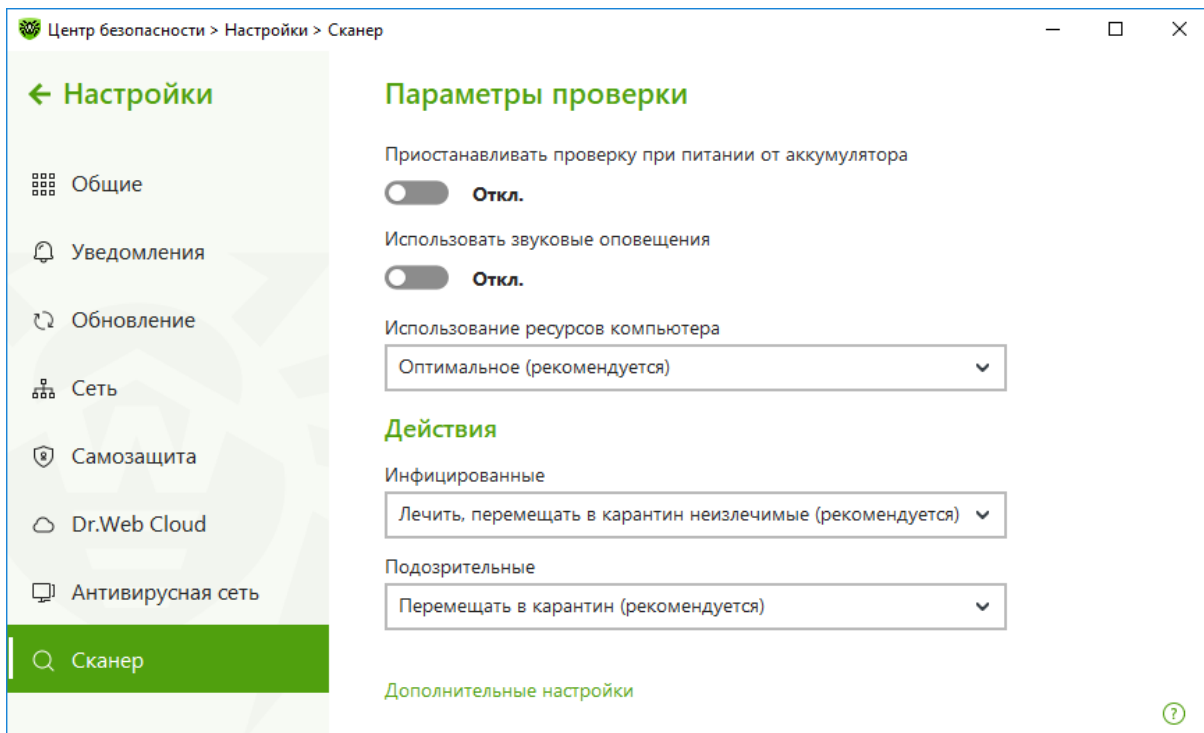
8.5.1. Антивирусная проверка Сканером

После завершения загрузки сканера в главном окне выберите нужный тип проверки — быстрый, полный или выборочный.



При старте компьютера или перед выполнением критических операций рекомендуется запускать быструю проверку.

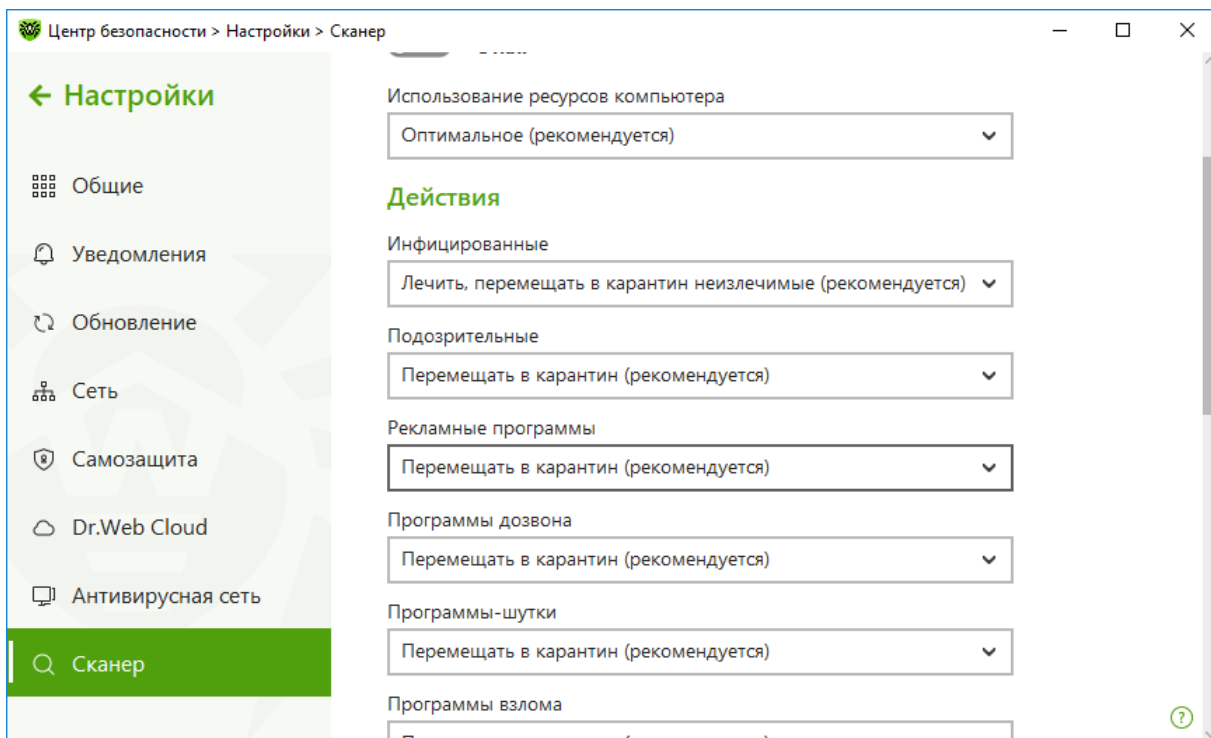
Пользователь может как запустить проверку с настройками по умолчанию, так и изменить предложенные настройки. Для изменения параметров проверки кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . Нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Сканер**.



Нажав пункт **Дополнительные настройки**, пользователь может определить действия, применяемые к вредоносным объектам различного типа. По умолчанию для всех объектов (кроме инфицированных) стоит действие **Перемещать в карантин**.

Необходимо отметить, что для различных объектов список возможных действий является различным. Так, для неизлечимых пункт **Лечить** недоступен — в отличие от инфицированных.

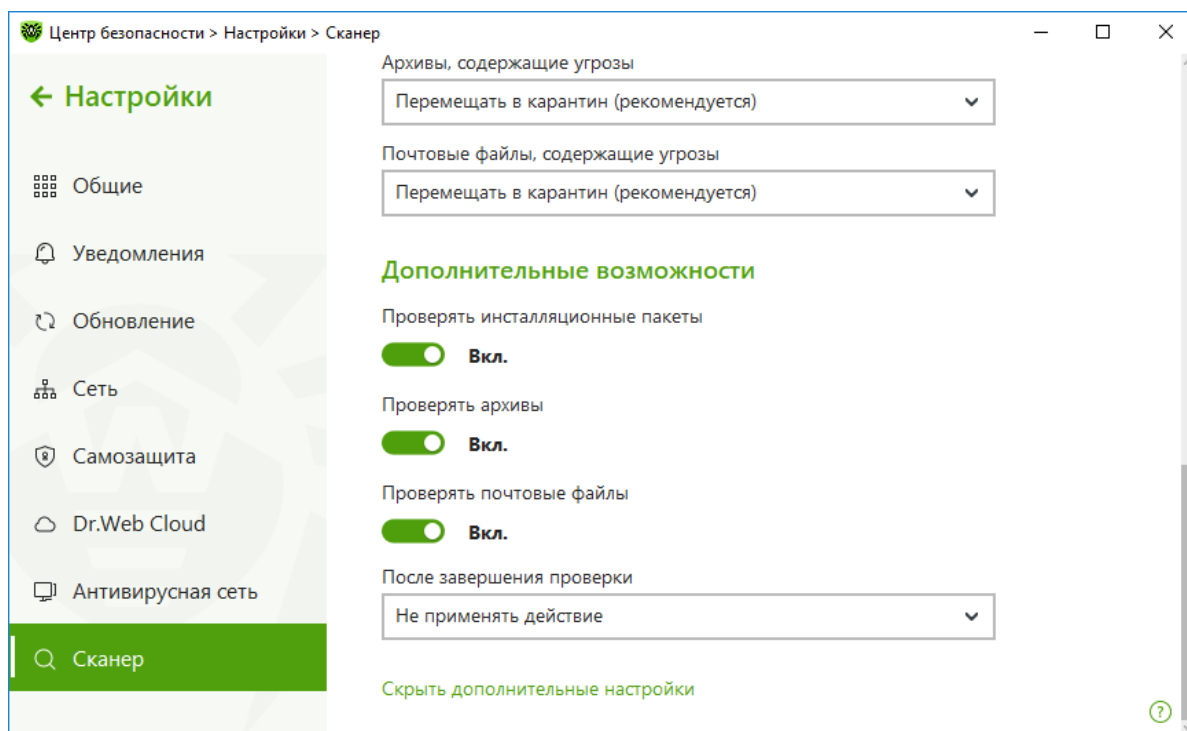
Внимание! Сканер не поддерживает действие **Переименовать** в связи с отсутствием гарантий последующей безопасности системы при применении этого действия — возможностью отмены этого действия вручную.



По умолчанию файловый монитор не проверяет архивы и почтовые файлы, так как их
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

проверка занимает много времени, а вредоносные файлы из них могут быть запущены только после обработки архиваторами или почтовыми программами, в ходе чего они будут обнаружены специализированными компонентами. Если пользователь желает проверять эти форматы в ходе сканирования, он может отметить их, выбрав соответствующие пункты.

Проверять архивы, Проверять почтовые файлы и Проверять инсталляционные пакеты.



Внимание! Рекомендуется всегда проверять архивы перед их отправкой кому-либо.

Антивирусное ядро Dr.Web позволяет производить проверку большого числа типов архивов, упаковщиков и баз данных различного назначения. В том числе антивирусное ядро позволяет производить:

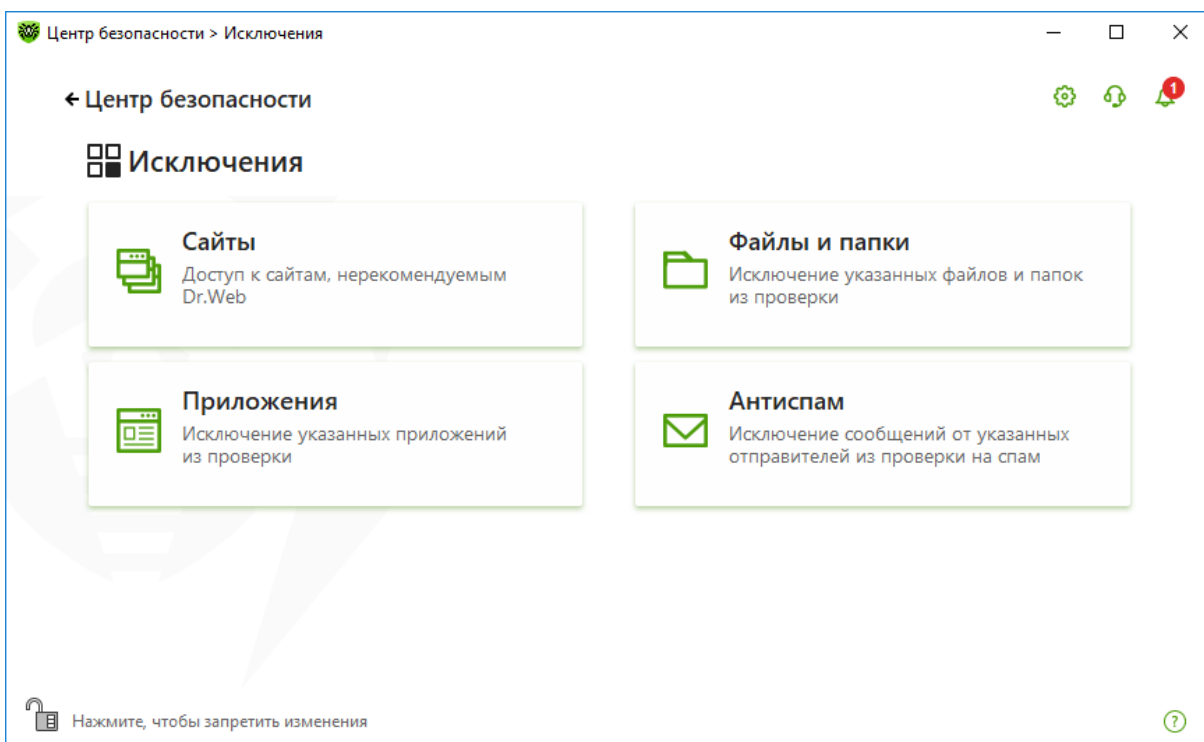
- удаление вредоносных файлов как из файлов, упакованных такими программами, как PKLITE, LZEXE, DIET, COM2EXE и т. п., так и из файлов, скрытых под неизвестными упаковщиками;
- проверку исполняемых файлов, упакованных такими упаковщиками, как PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT;
- обнаружение вредоносных файлов внутри контейнеров и архивных файлов формата ACE, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO, ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т. д. без ограничений на уровень вложенности проверяемых объектов;
- обнаружение вредоносных файлов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т. д.);
- обнаружение вредоносных файлов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
- обнаружение вредоносных файлов в файлах и объектах, имеющих формат Smart Install Maker, DMG, HFS, XAR, Universal Binary, SIS, INNO SETUP, SETUP FACTORY,

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

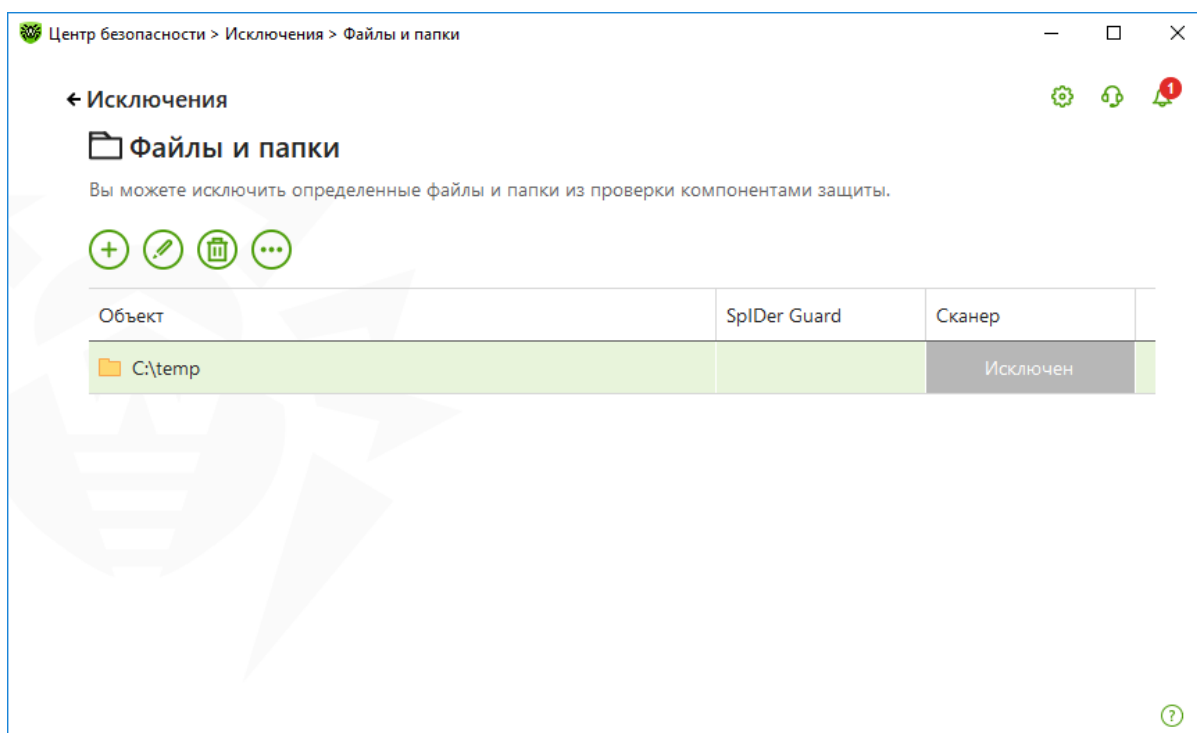
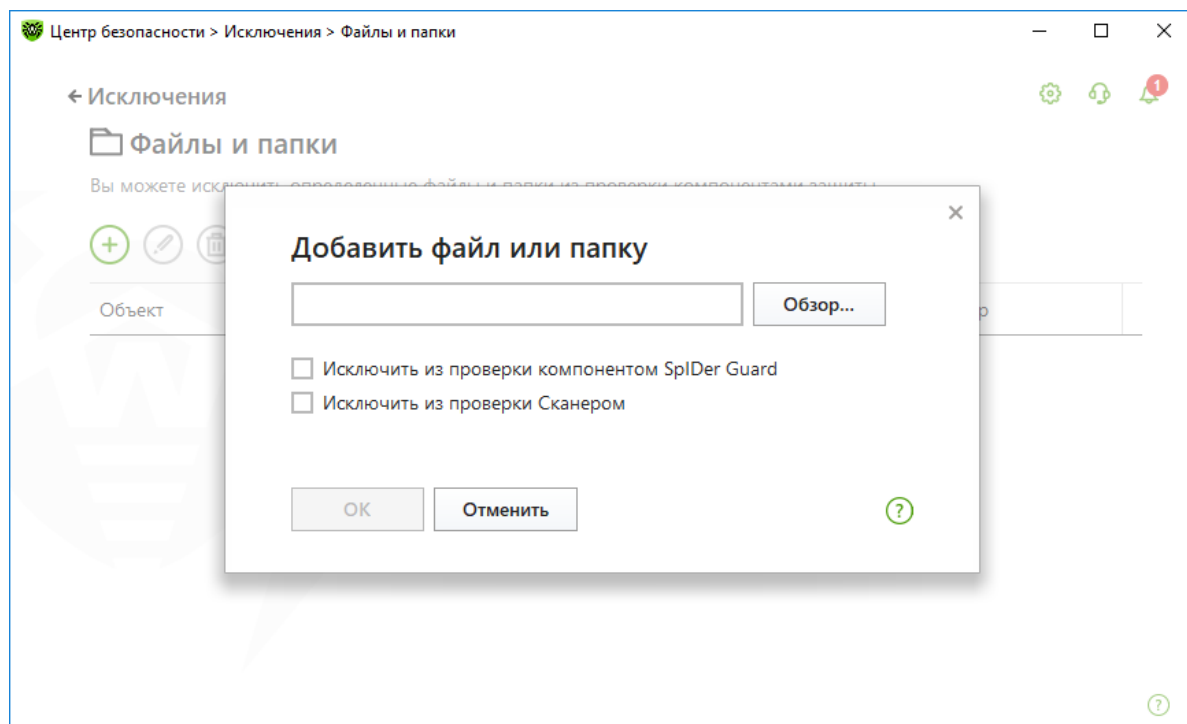
XENOCODE, TARMA INSTALL, XZ (UNIX), COMPRESS, SQUAHFS, CHILKAT ZIP, пакетов LHA (AWARD BIOS);

- обнаружение вредоносных файлов в таких самораспаковывающихся архивах, как AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFEX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
- проверку как почтовых файлов Mozilla Thunderbird, так и неформатированных почтовых баз, обработку писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW).

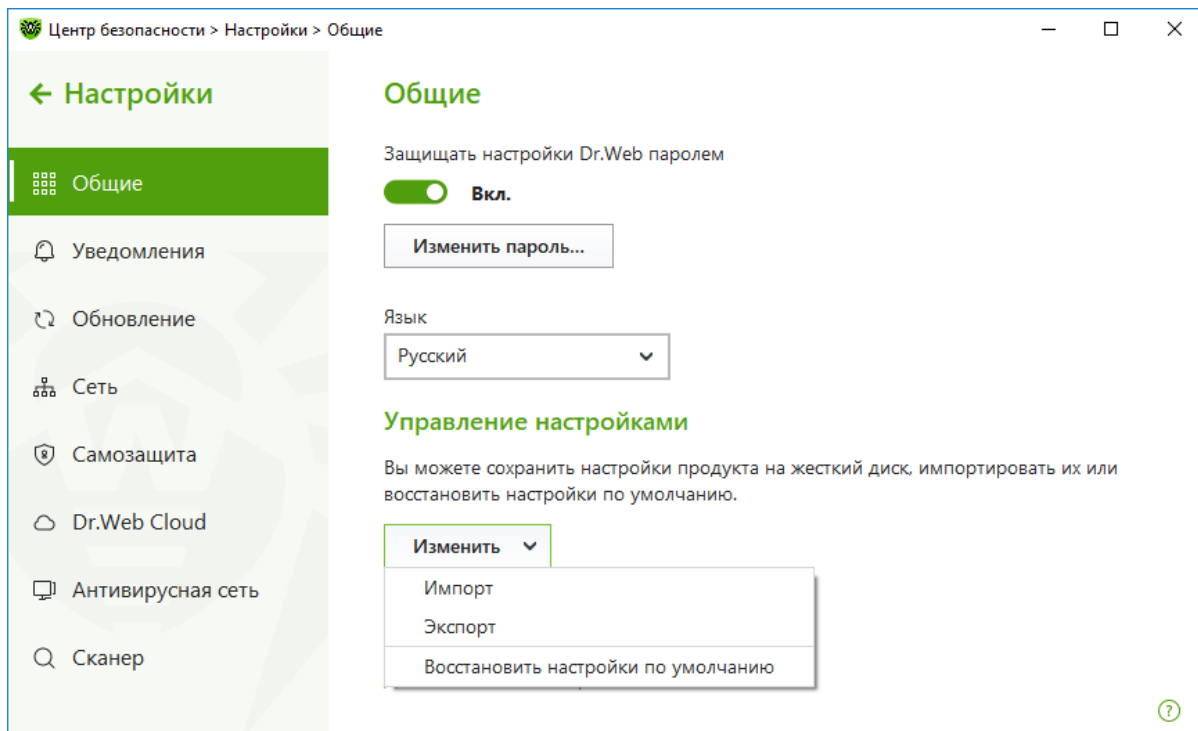
Для того чтобы составить список исключаемых из проверки (в том числе сканером) файлов и папок, в окне **Центр безопасности** выберите **Исключения** и далее **Файлы и папки**.



Для добавления папки нажмите на иконку , выберите файл или папку и отметьте, для какого компонента будет добавлено исключение.



Пользователь всегда может вернуться к настройкам по умолчанию, перейдя в окне **Настройки** → **Общие** и в выпадающем меню **Изменить** группы настроек **Управление настройками**, выбрав **Восстановить настройки по умолчанию**.

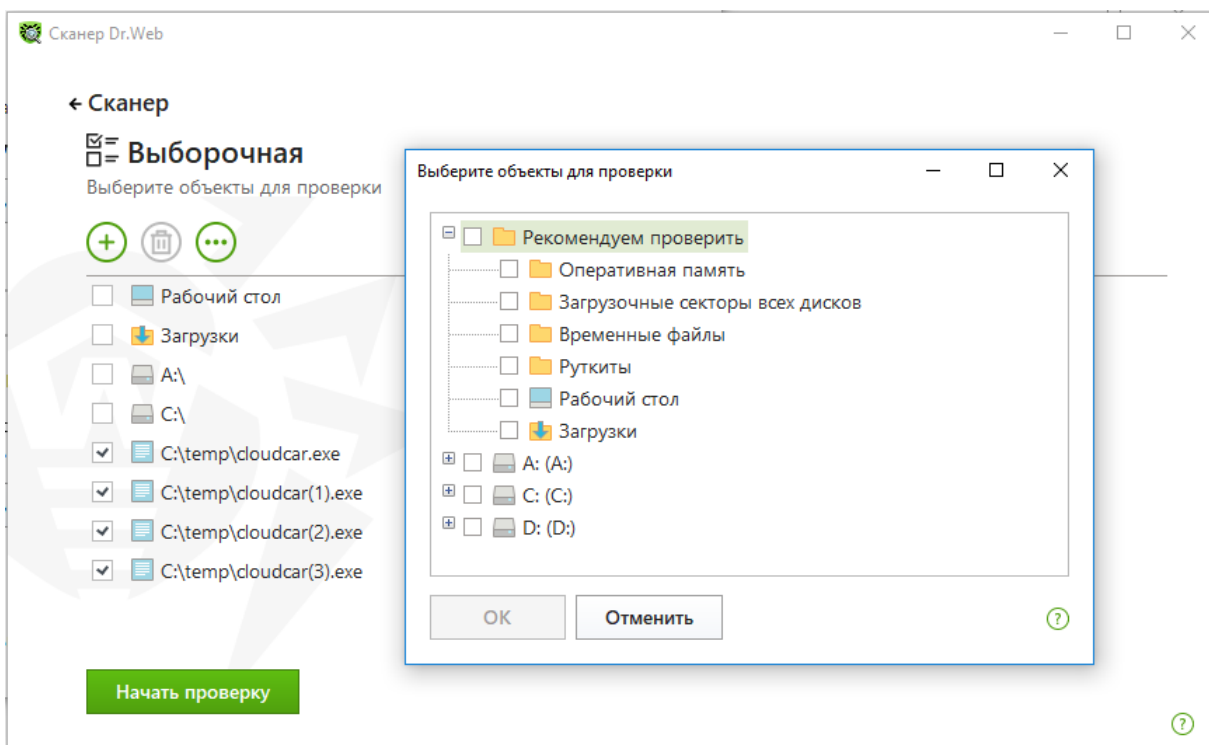


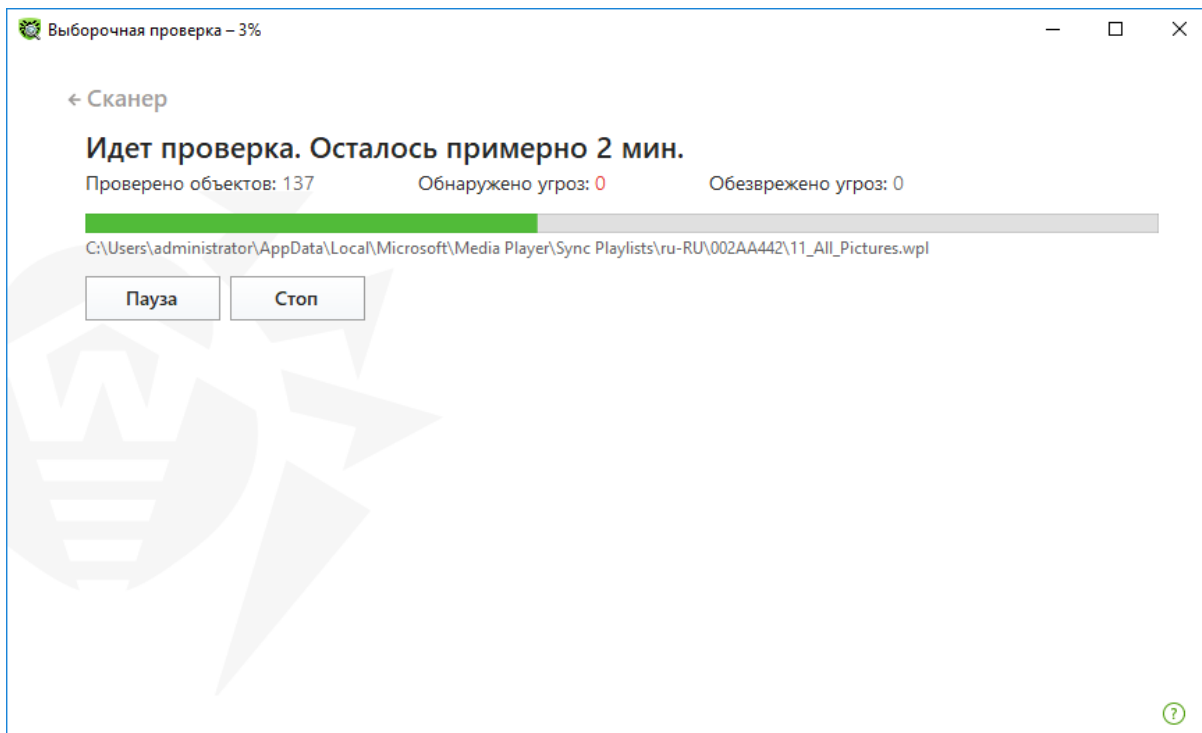
Порядок изменения уровня детализации отчета описан в главе **Изменение уровня подробности протокола событий**.

Не рекомендуется отказываться от ведения отчета о проверке, хотя это и несколько ускоряет ее ход.

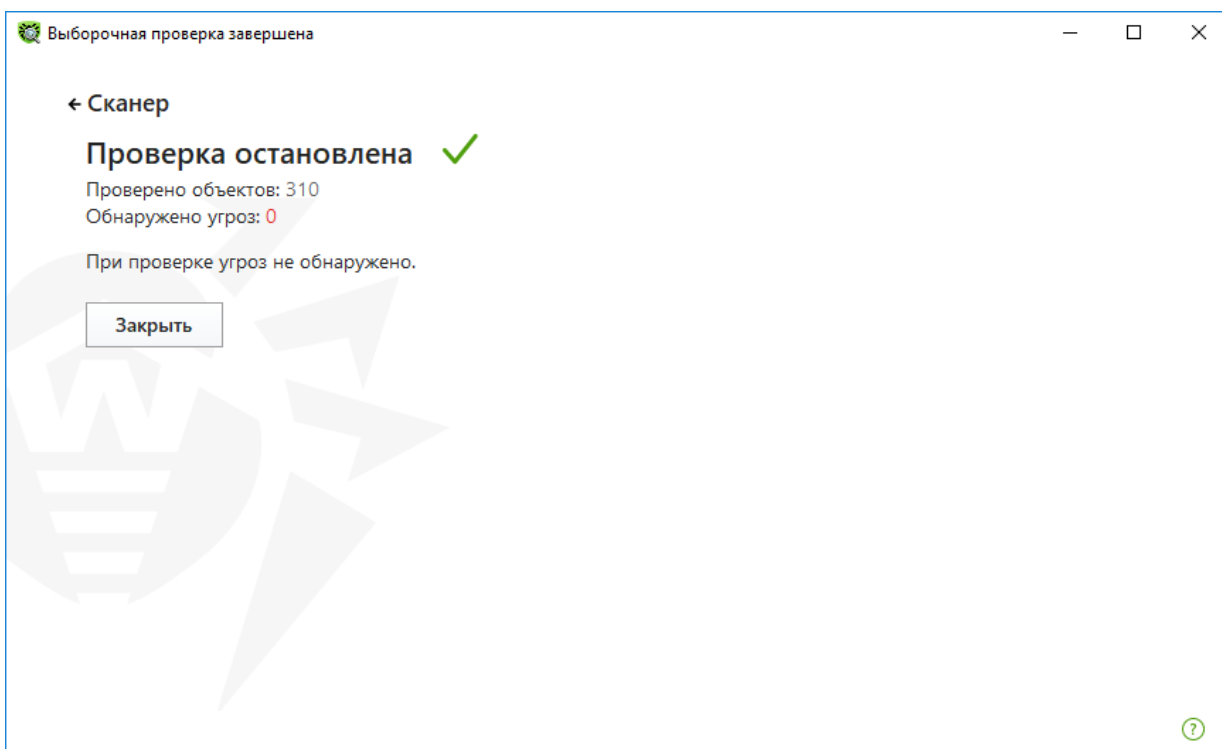
Для запуска быстрой или полной проверки в главном окне сканера нажмите на пункты **Быстрая** и **Полная** соответственно. Выборочная проверка запускается из окна настроек **Выборочная**.

В случае выборочного типа проверки пользователь может указать интересующие объекты проверки.





Остановить проверку компьютера можно, нажав **Стоп**.



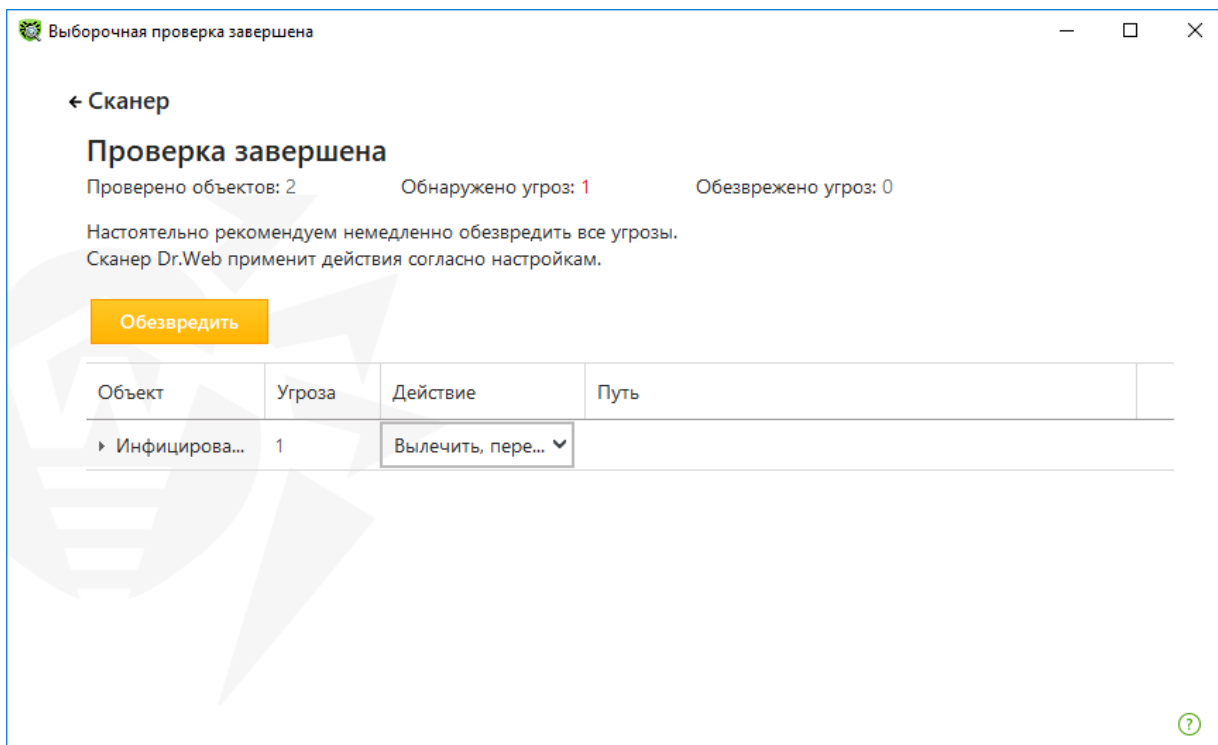
Кнопка **Пауза** недоступна во время проверки оперативной памяти и процессов.

Внимание! Быстрая проверка сканером системы не гарантирует полной очистки компьютера от всех известных вирусов. В частности, потому, что работающие вирусы могут заражать уже проверенные («чистые») файлы. В случае обнаружения вирусов мы рекомендуем проверить компьютер до начала установки с помощью бесплатной утилиты Dr.Web CureIt!, которую можно получить на сайте компании «Доктор Веб» в разделе бесплатных программ.

Если в настройках Сканера Dr.Web был установлен флажок **Обезвредить обнаруженные угрозы**, то обезвреживание угроз будет произведено автоматически, в противном случае по

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

окончании проверки Сканер Dr.Web лишь информирует об обнаруженных угрозах и предлагает применить к ним наиболее оптимальные действия по обезвреживанию.



По умолчанию после окончания проверки для обезвреживания выбраны все объекты. Вы можете обезвредить все обнаруженные угрозы одновременно. Для этого после завершения проверки нажмите кнопку **Обезвредить**. По нажатию кнопки **Обезвредить** к выбранным объектам в таблице применяются predetermined actions. Чтобы изменить действие для части объектов, в поле **Действие** в выпадающем списке выберите необходимое действие для каждого объекта.

Существуют следующие ограничения:

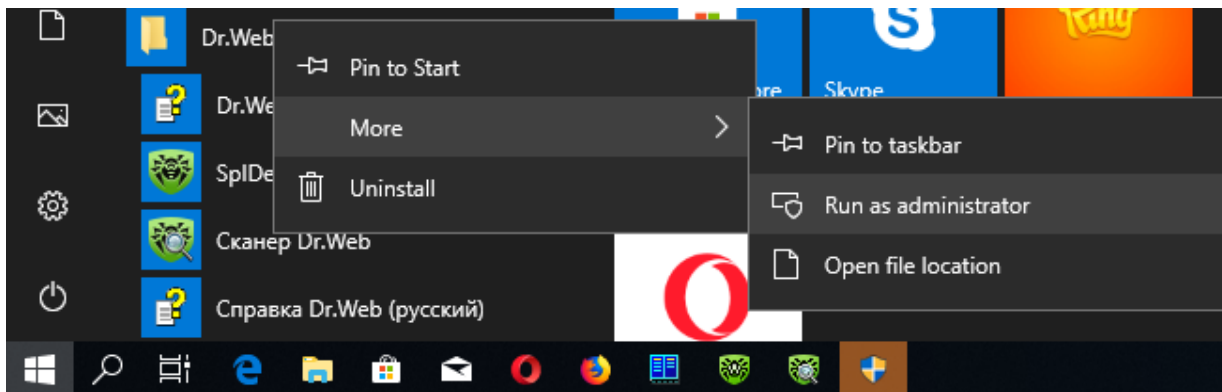
- лечение подозрительных объектов невозможно;
- перемещение или удаление объектов, не являющихся файлами (например, загрузочных секторов), невозможно;
- невозможны любые действия для отдельных файлов внутри архивов, установочных пакетов или в составе писем — действие в таких случаях применяется только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

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

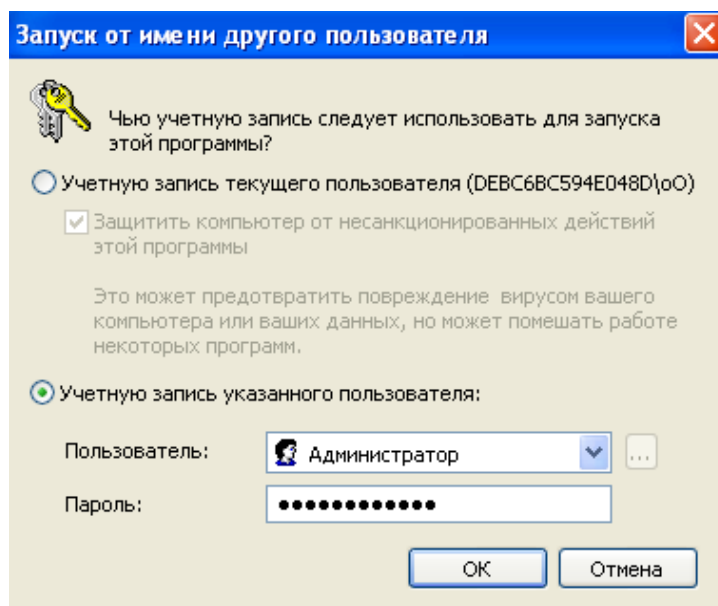
8.5.2. Проверка с правами другого пользователя

В некоторых случаях сканирование каталогов или файлов возможно только при наличии прав администратора. В частности, это относится к некоторым системным разделам, доступ к которым для обычного пользователя запрещен. Чтобы иметь возможность сканировать тот или иной каталог, выполните одно из двух действий:

- Запустите **Сканер** от имени другого пользователя. Для этого нажмите правой кнопкой на значок **Сканера**, в контекстном меню выберите пункт **Запуск от имени (Run as)...**



Затем в появившемся окне выберите пользователя с правами администратора, если необходимо.



8.5.3. Запуск антивирусной проверки из командной строки

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

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

где:

<объекты> — список объектов для проверки;

<ключи> — параметры командной строки, которые задают настройки работы Сканера. При их отсутствии проверка выполняется с ранее сохраненными настройками (или настройками по умолчанию, если они не были изменены).

По умолчанию <путь_к_программе> — C:\Program Files\DrWeb

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

/FAST — произвести быструю проверку системы;

/FULL — произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы);

/LITE — произвести стартовую проверку системы, при которой проверяются оперативная память, загрузочные секторы всех дисков, а также провести проверку на наличие руткитов.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

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

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

Чтобы запустить **Консольный сканер**, воспользуйтесь следующей командой:

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

где:

<объекты> — список объектов для проверки;

<ключи> — список параметров командной строки, которые задают настройки работы **Консольного сканера**. Ключ начинается с символа «/», несколько ключей разделяются пробелами.

Список объектов проверки может быть пуст или содержать несколько элементов, разделенных пробелами.

Список ключей **Консольного сканера** содержится в Приложении А документации.

После выполнения проверки **Консольный сканер** возвращает один из следующих кодов:

0 — проверка успешно завершена, инфицированные объекты не найдены;

1 — проверка успешно завершена, найдены инфицированные объекты;

10 — указаны некорректные ключи;

11 — ключевой файл не найден либо не поддерживает **Консольный сканер**;



12 — не запущен Scanning Engine;

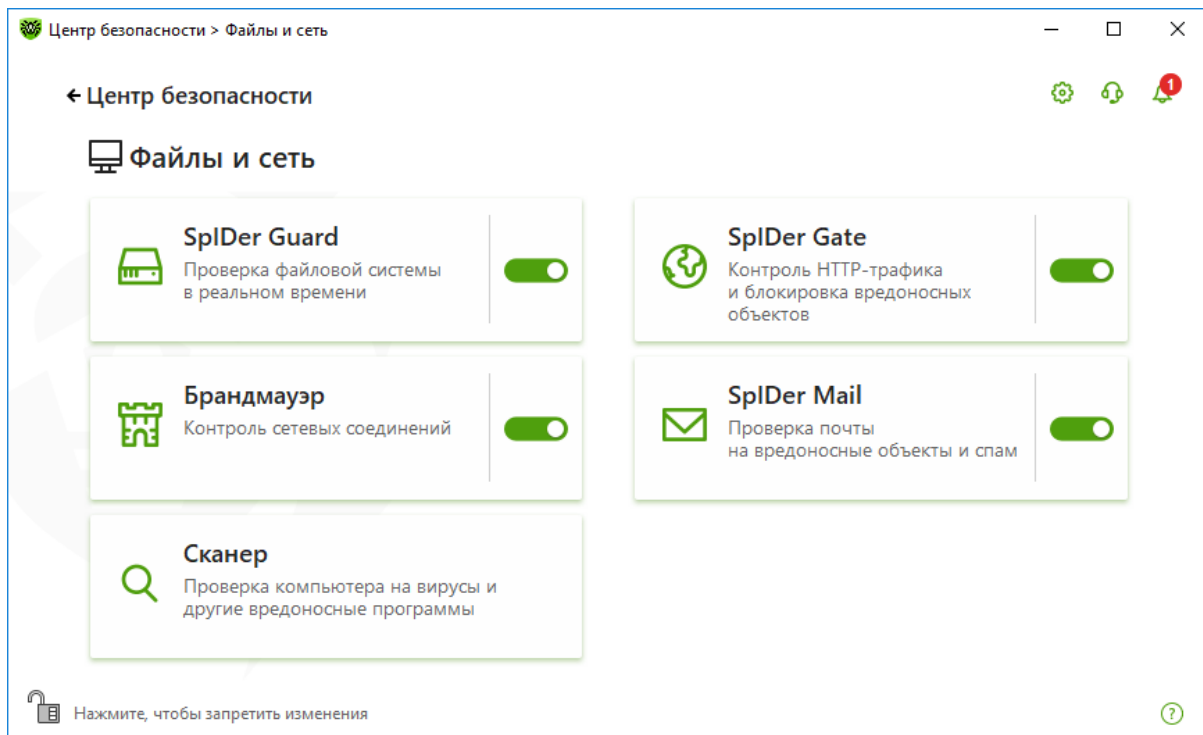
255 — проверка прервана пользователем.

8.6. Настройка действий Dr.Web Security Space с вредоносными файлами

По умолчанию для большинства вредоносных объектов стоит действие **Перемещать в карантин**. По этому действию пользователь сам должен принимать решение о том, что делать с обнаруженными вредоносными объектами.

Внимание! Вредоносные файлы семейства Trojan.Encoder относятся к неизлечимым объектам. Для восстановления данных из зашифрованных файлов желательно иметь сам вредоносный файл, который произвел данное действие. В связи с этим в качестве действия по умолчанию должно быть выбрано перемещение в карантин.

Кликните по значку значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).



Внимание! Не удаляйте объекты из карантина сразу после того, как они были помещены туда системой защиты, так как в некоторых случаях вредоносные файлы могут содержать ключи, которые могут помочь при расшифровке.

8.6.1. Настройка файлового сторожа

В окне **Центр безопасности** выберите **Файлы и сеть** и далее **SpIDer Guard**.

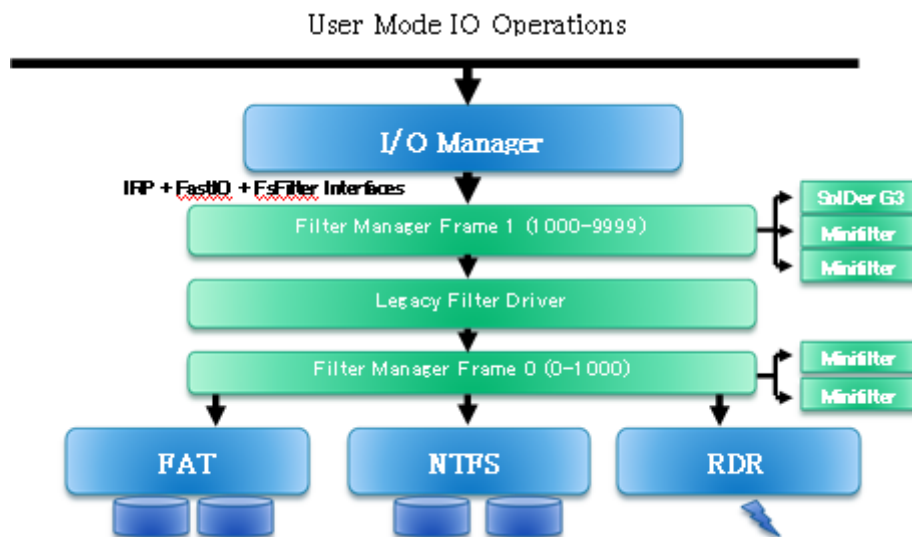
Изменение основных настроек возможно при наличии соответствующих прав, настраиваемых в Центре управления для группы или отдельной станции.

Для доступа к настройкам запрашивается пароль, если в разделе **Настройки** была включена опция **Защищать настройки Dr.Web паролем**.

Антивирусный сторож **SpIDer Guard** постоянно находится в оперативной памяти компьютера, осуществляя проверку файлов «на лету», а также обнаруживая проявления вирусной активности.

Файловый монитор — наиболее гибкий из компонентов антивирусной системы в смысле количества настроек, которые можно задать в реестре. Большинство настроек, которые можно произвести через интерфейс **SpIDer Guard**, применяются сторожем без перезагрузки.

В **SpIDer Guard G3** используется архитектура, базирующаяся на технологии мини-фильтров (Minifilter). Суть построения фильтра: имеется фильтр-менеджер и два фрейма. Только фильтр-менеджер обрабатывает все запросы, что в разы ускоряет работу системы. Всё остальное, в том числе **SpIDer Guard**, — это мини-фильтры. Всеми поступающими запросами управляет фильтр-менеджер, распределяя их по соответствующим мини-фильтрам. Плюсы архитектуры: нет конфликтов между фильтрами, все основные операции по обработке запросов на себя берет фильтр-менеджер, а все остальные (в том числе **SpIDer Guard**) используют ресурсы самой ОС.



Архитектура SpIDer Guard G3

SpIDer Guard запускается автоматически при каждой загрузке операционной системы, при этом запущенный сторож не может быть выгружен в течение текущего сеанса работы операционной системы. При необходимости (например, в случае выполнения критически чувствительного к загрузке процессора задания в реальном масштабе времени) вы можете временно отключить сканирование файлов «на лету».

Начиная с 11 версии Dr.Web Security Space для перехвата обращений к файлам используется компонент Dr.Web HyperVisor. Компонент Dr.Web позволил усовершенствовать систему обнаружения и лечения угроз, а также усилить самозащиту Dr.Web путем использования возможностей современных процессоров. Компонент запускается и работает на уровне драйверов, что гарантирует контроль всех программ и процессов операционной системы, обращений к ее ресурсам, невозможность перехвата вредоносными программами контроля над защищаемой Dr.Web системой. Внедрение компонента Dr.Web HyperVisor позволило преодолеть ограничения, накладываемые на антивирусы особенностями 64-битных операционных систем, вынуждавших антивирус функционировать на том же уровне, что и вредоносные программы.

При настройках по умолчанию сторож **SpIDer Guard** «на лету» проверяет все создаваемые или изменяемые файлы и загрузочные сектора, а на сменных носителях — также все открываемые файлы. Сканирование проводится аналогично тому, как работает Сканер Dr.Web, однако с более «мягкими» условиями проверки. Кроме того, сторож **SpIDer Guard** постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при обнаружении угроз безопасности блокирует соответствующие процессы.

По умолчанию файлы внутри архивов и почтовые ящики не проверяются. Если какой-либо файл в архиве или почтовом вложении инфицирован, то вредоносный объект будет обнаружен сторожем при извлечении файла до появления возможности заражения компьютера. Включение проверки архивов или почтовых файлов значительно увеличивает нагрузку на компьютер. Для предотвращения проникновения на ваш компьютер вредоносных объектов, распространяемых посредством электронной почты, используйте почтовый сторож **SpIDer Mail**.

При обнаружении зараженных объектов сторож **SpIDer Guard** применяет к ним действия согласно установленным настройкам. Соответствующим изменением настроек вы можете изменить автоматическую реакцию сторожа на вирусные события. Результаты работы сторожа отражаются в окне статистики и файле отчета.

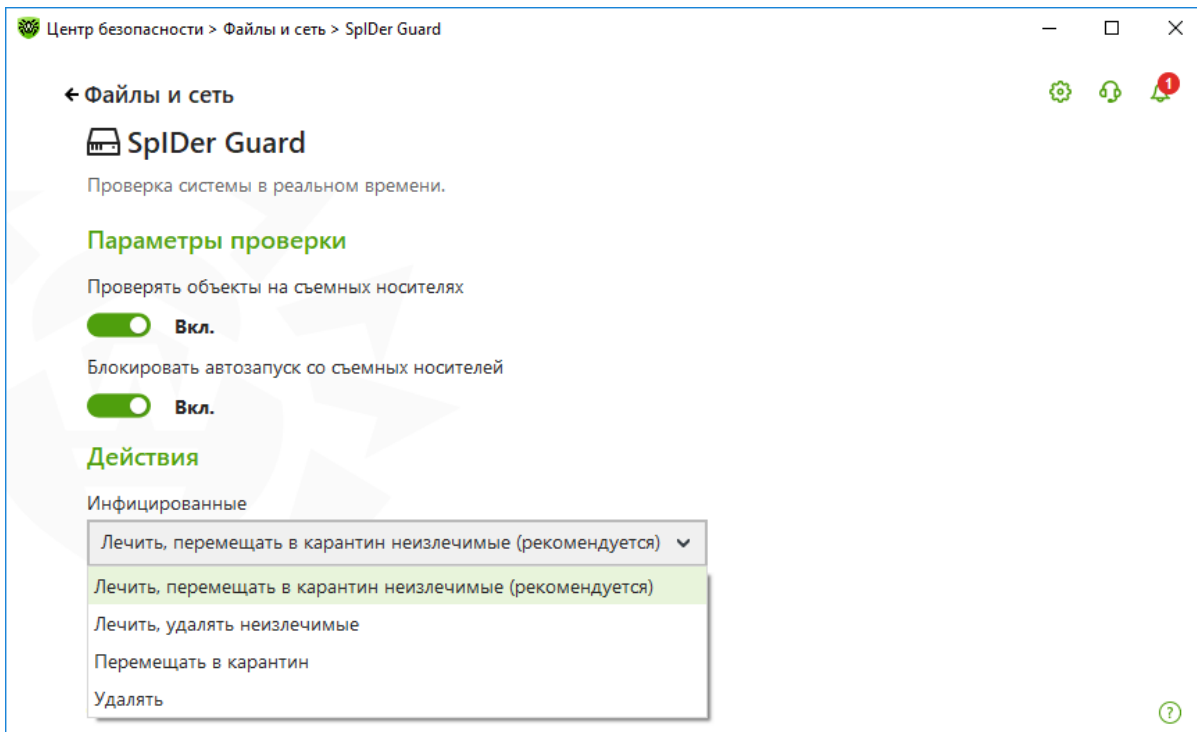
Следует помнить, что настройки программы по умолчанию являются оптимальными для

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

большинства применений, их не следует изменять без необходимости.

Вы можете временно отключать фоновую антивирусную проверку. Для этого в окне **Центр безопасности** выберите **Файлы и сеть**, далее **SpIDer Guard** и передвиньте переключатель компонента влево.

Будьте осторожны: в период отключения функций сторожа не следует подключаться к сети Интернет, а также считывать файлы с носителей, не проверенных Сканером Dr.Web.



Опция **Проверять объекты на съемных носителях** включает/отключает проверку на чтение и запись файлов на сменных носителях **SpIDer Guard**. Отключать не рекомендуется. Запускаемые процессы и модули на сменных носителях проверяются независимо от состояния опции.

Также вы можете запретить автоматический запуск активного содержимого внешних носителей данных (CD/DVD-дисков, флеш-памяти и т. д.), установив флажок **Блокировать автозапуск со сменных носителей**. Опция блокирует обращение к файлам autorun.inf на всех дисках в корневых каталогах, в том числе на сменных носителях. Включение опции позволяет избежать заражения сменного носителя, если поражена ОС, и системы, если инфицирован носитель. Использование этой настройки помогает предотвратить заражение вашего компьютера через внешние носители.

Вы можете задать проверку:

- файлов запускаемых процессов вне зависимости от их расположения,
- установочных файлов,
- файлов на сетевых дисках,
- файлов и загрузочных секторов на съемных носителях.

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

По умолчанию сторож **SpIDer Guard** пытается вылечить файлы, зараженные известными и потенциально излечимыми вирусами, остальные наиболее опасные объекты перемещает в **Карантин**. Программы-шутки, программы взлома и неблагонадежные объекты по *Dr.Web® Security Space. Руководство по быстрой установке и развертыванию*

умолчанию игнорируются. Реакции сторожа **SpIDer Guard** аналогичны соответствующим реакциям **Сканера Dr.Web**.

Существуют следующие действия, применяемые к обнаруженным объектам:

- **Лечить, перемещать в карантин неизлечимые** — восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов.
- **Лечить, удалять неизлечимые** — восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов.
- **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 следующих вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

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

- Инфицированные файлы, зараженные известным и (предположительно) излечимым вирусом
- Неизлечимые объекты, зараженные неизлечимым вирусом
- Подозрительные файлы, предположительно зараженные вирусом или содержащие вредоносный объект
- Различные потенциально опасные объекты

При этом:

- **SpIDer Guard** не проверяет составные объекты, поэтому никакие действия над ними или входящими в их состав файлами не производятся. После выполнения предписанного действия сторож **SpIDer Guard** по умолчанию выводит соответствующее оповещение в область уведомлений Windows.
- Резервные копии обработанных объектов сохраняются в **Карантине**.

Предлагаемый для компонента список действий различается для вредоносных программ различного типа. Так, для инфицированных программ на выбор предлагаются действия **Лечить**, **Перемещать в карантин** и **Удалить**. Необходимо понимать, что для троянских программ действие **Лечить** невозможно — программы такого типа не имеют механизма размножения, и их лечение невозможно.

Важно! Как правило, шифровальщики относятся к таким типам вредоносных файлов, как вирусы и троянцы. Однако функция шифрования файлов также может использоваться вирусописателями и в других типах вредоносных программ. Например, в майнерах. В связи с этим не рекомендуется выставлять действие перемещения в карантин только для пунктов **Инфицированные** и **Подозрительные**. Как минимум данное действие рекомендуется

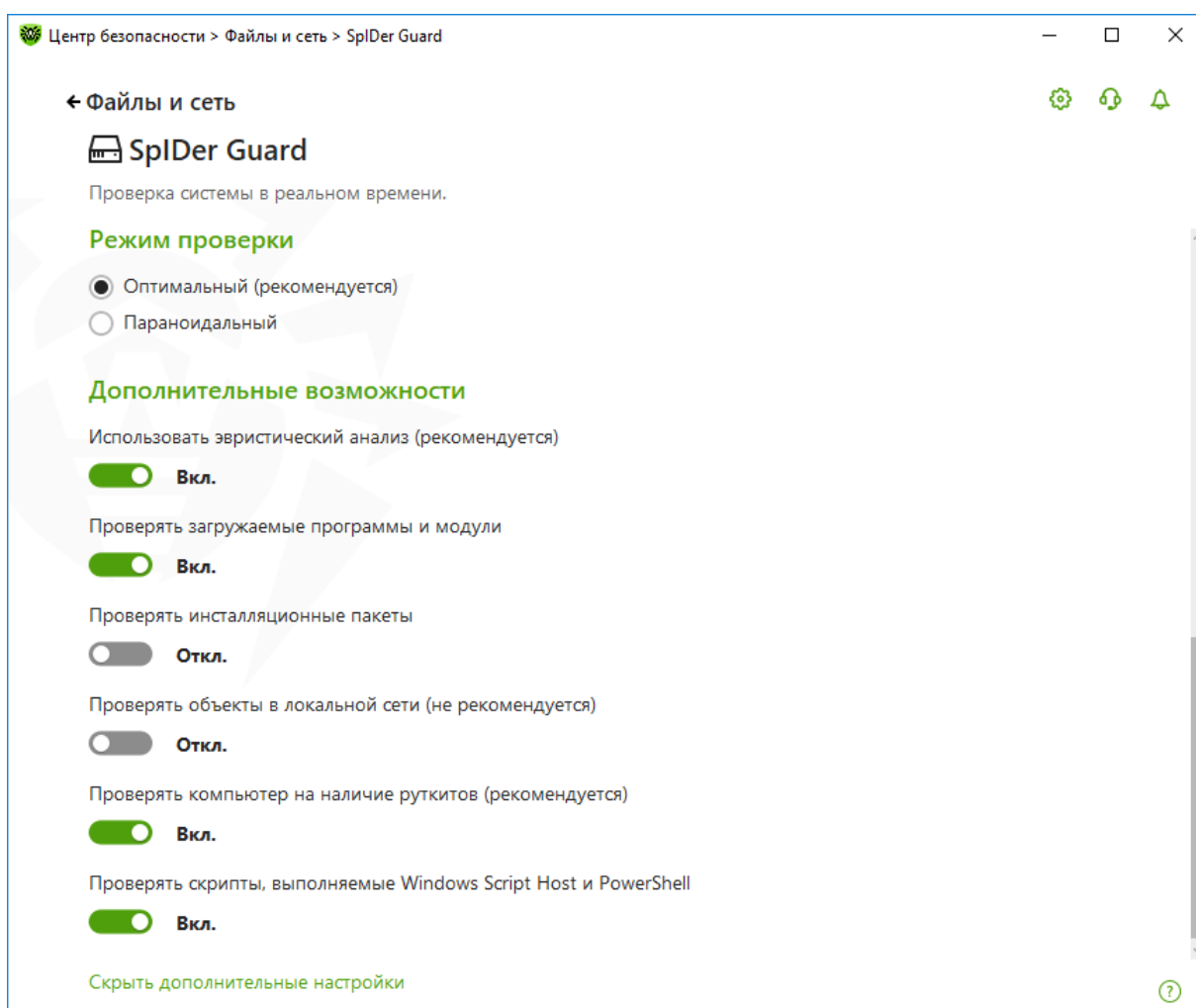
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

выставить для пункта **Потенциально опасные**. Для доступа к данному пункту в окне **SpIDer Guard** нажмите на **Дополнительные настройки**.

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

По умолчанию установлен режим проверки **Оптимальный**: сканирование на жестких дисках — только запускаемых, создаваемых или изменяемых файлов, на сменных носителях и сетевых дисках — всех открываемых файлов.

В режиме **Параноидальный** производится проверка всех открываемых, создаваемых или изменяемых файлов на жестких дисках, сменных носителях и сетевых дисках. При включенной опции любое обращение к файлу будет заблокировано и проверено **SpIDer Guard**. Включать не рекомендуется, поскольку очень резко возрастает нагрузка на систему.



Опция **Проверять объекты в локальной сети** включает/отключает проверку на чтение файлов с сетевых дисков и ресурсов **SpIDer Guard**. Запускаемые процессы и модули на сетевых дисках и ресурсах проверяются независимо от состояния опции.

При необходимости задайте здесь же режим проверки на заражение руткитами.

Антивруткит **Dr.Web Shield** — это специальный драйвер, который помогает компонентам антивируса **Dr.Web** для Windows обнаруживать вирусы, скрывающие свое присутствие в системе с помощью перехвата функций операционной системы (Windows API). Для его работы требуются права администратора.



Драйвер Антируткита позволяет антивирусу Dr.Web получать полный доступ к файлам, к которым обычно доступ запрещен системой, не только в безопасном режиме Windows, но и в обычном. Использование Антируткита позволяет гораздо эффективнее, чем прежде, противодействовать активным вредоносным программам, находящимся в системе. Так, **Антируткит Dr.Web**, например, позволяет антивирусу Dr.Web противодействовать так называемым буткитам — вредоносным программам, которые прописывают себя в загрузочный сектор жесткого диска и обеспечивают скрытую установку своего драйвера в памяти. Подобные руткит-драйверы записываются в последние сектора физического диска и, таким образом, не существуют в виде файла.

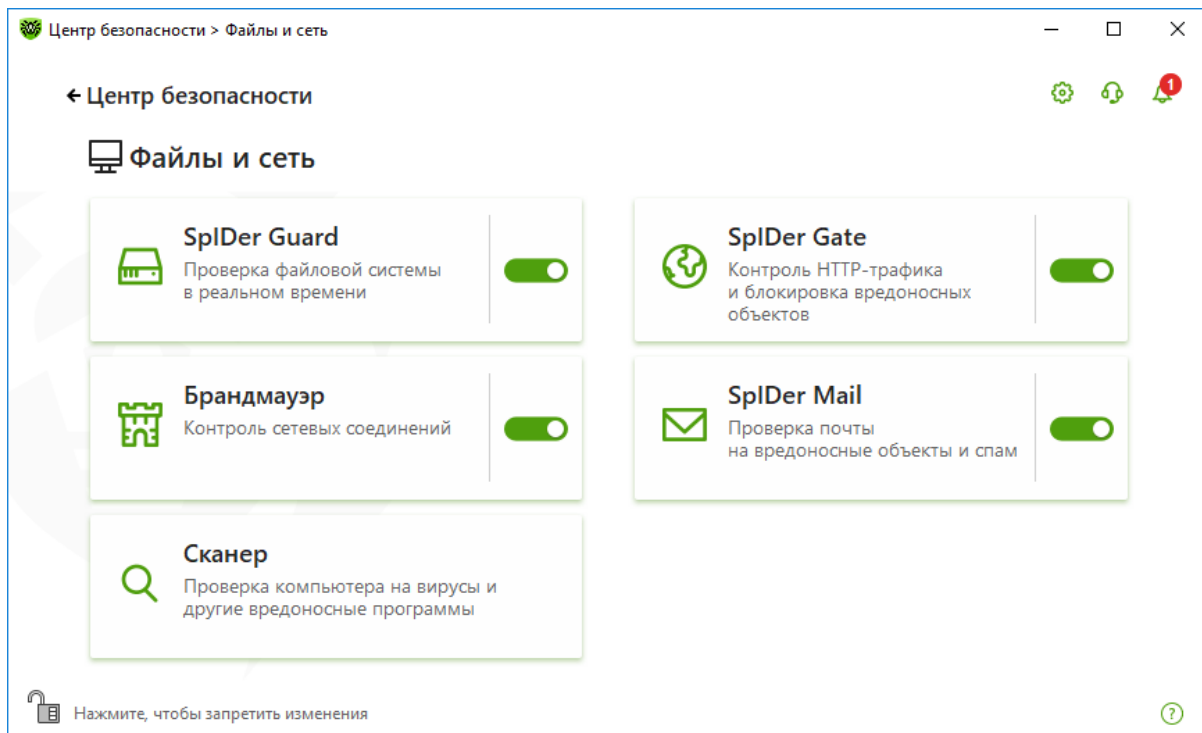
Драйвер **Антируткита Dr.Web** используется в **Сканере Dr.Web — Антируткит Dr.Web** внедрен в исполняемый файл GUI-сканера. Драйвер автоматически устанавливается в систему при запуске GUI-сканера и автоматически же из нее удаляется, когда в нем отпадает необходимость.

Отчет сторожа **SpIDer Guard** хранится в файле spiderg3.log, расположенном в каталоге %allusersprofile%\Application Data\Doctor Web\Logs\ (в Windows 7, %allusersprofile%\Doctor Web\Logs).

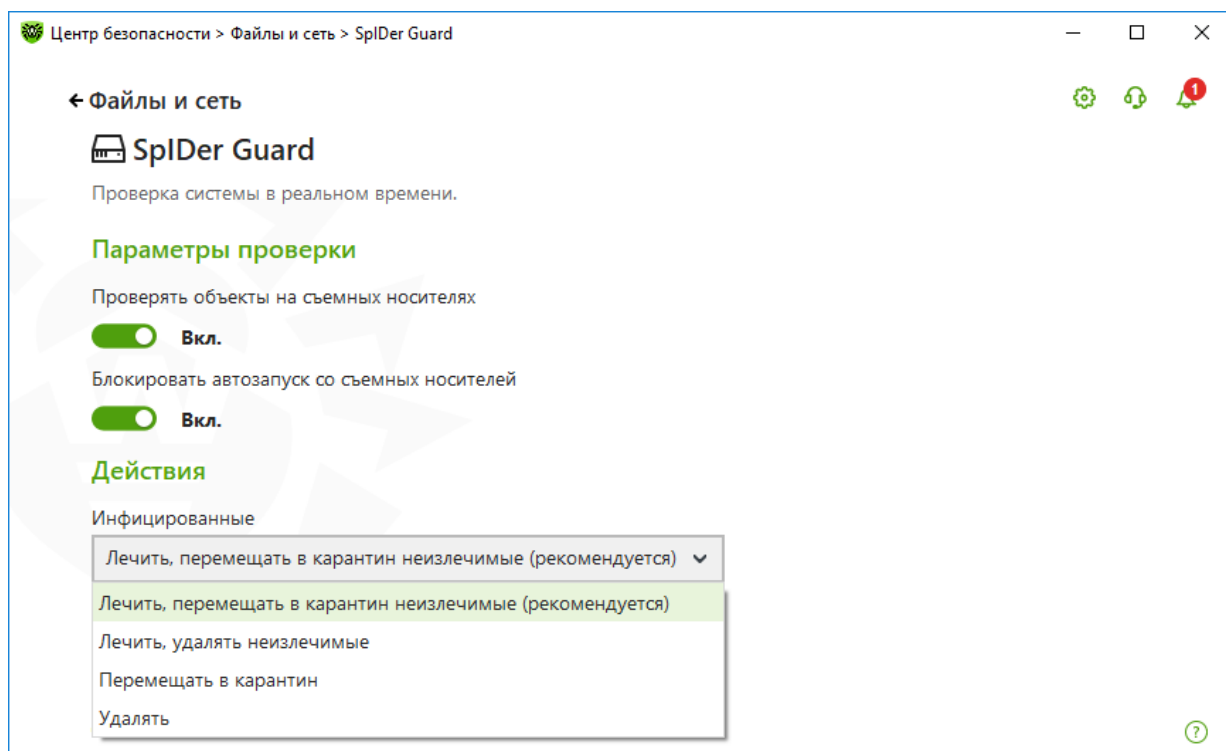
8.6.1.1. Обнаружение вредоносных скриптов

Используемая в Dr.Web Security Space технология ScriptHeuristic предотвращает исполнение вредоносных скриптов в браузере и PDF-документах, не нарушая при этом функциональности легитимных скриптов. Дополнительно к данной технологии для противодействия использованию вирусомисателями скриптовых языков JScript, JavaScript, VBScript и PowerShell используется модуль защиты Dr.Web Amsi-client, обеспечивающий проверку выполняемых скриптов, написанных на данных языках.

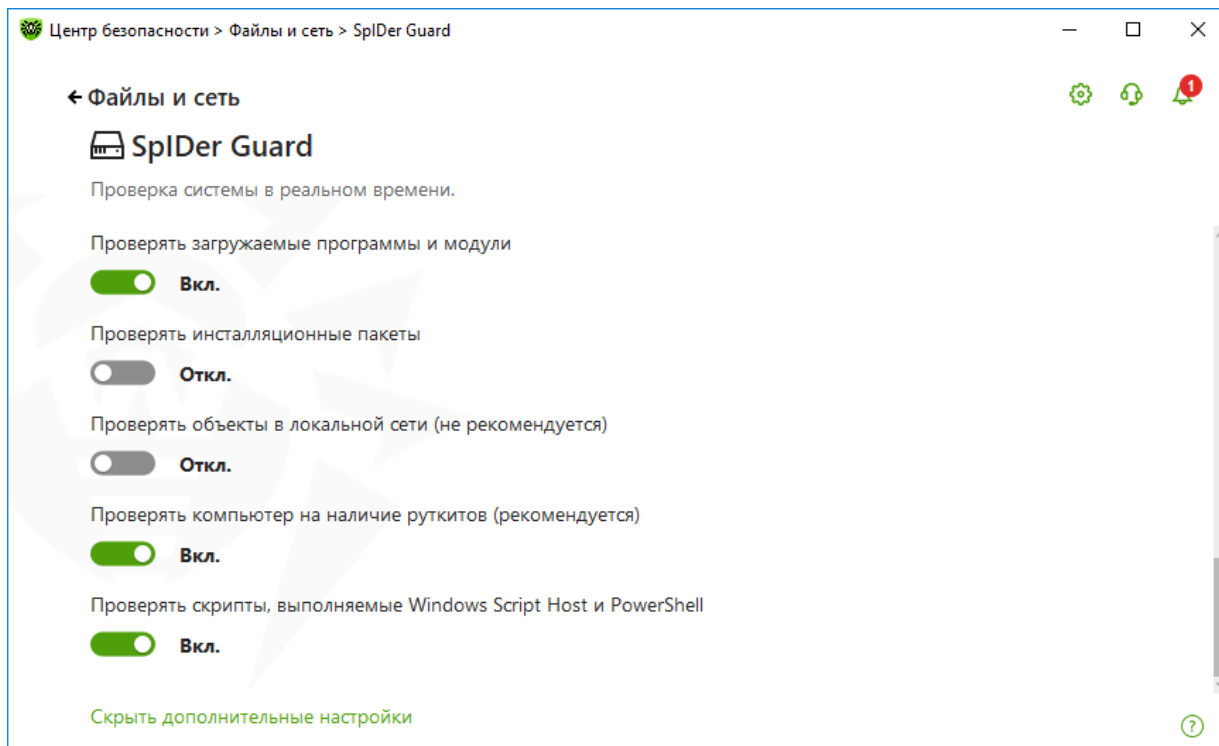
Включение антивирусной проверки модуля Dr.Web Amsi-client производится в разделе настроек **SpIDer Guard**. По умолчанию проверка включена. Для того чтобы проверить состояние модуля, кликните по значку значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).



В открывшемся окне **Центр безопасности** выберите **Файлы и сеть** и далее **SpIDer Guard**.



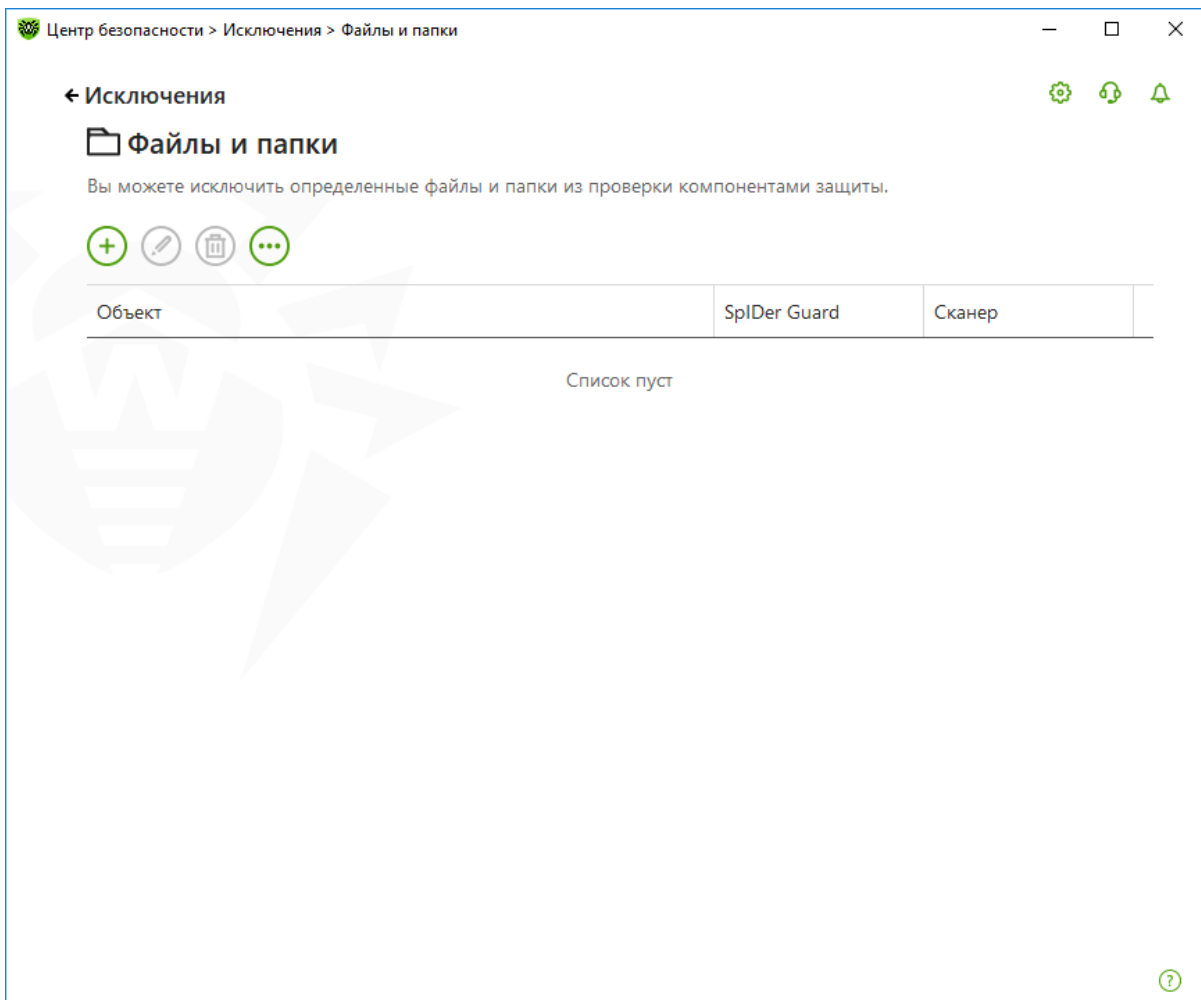
Кликните на пункт **Дополнительные настройки** и прокрутите окно до конца. Пункт **Проверять скрипты...** должен быть включен.



Внимание! Установка и удаление модуля Dr.Web Amsi-client производится совместно с модулем Dr.Web SpIDer Guard. Модуль доступен при использовании Антивируса Dr.Web и Dr.Web Security Suite в операционных системах начиная с Windows 10 (x86, x64), а также Windows Server 2016.

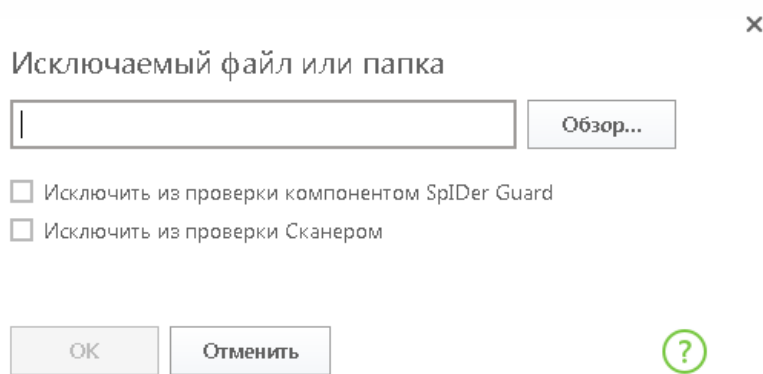
8.6.1.2. Настройка исключений

На странице настроек **Исключения** → **Файлы и папки** вы можете задать список файлов и папок, доступ к которым должен быть разрешен несмотря на установленные ограничения. В таком качестве могут выступать каталоги карантина антивируса, рабочие каталоги некоторых программ, временные файлы (файлы подкачки) и т. п. По умолчанию список пуст. Вы можете добавить к исключениям конкретные каталоги и файлы или использовать маски, чтобы запретить проверку определенной группы файлов.



Кнопка **Добавить** позволяет добавить к списку исключение, указанное в поле ввода:

- Чтобы указать конкретный существующий каталог или файл, нажмите кнопку **Обзор** и выберите каталог или файл в стандартном окне открытия файла. Или вручную введите полный путь к файлу или каталогу в поле ввода.



- Чтобы исключить из проверки все файлы или каталоги с определенным именем, введите это имя в поле ввода. Указывать путь к каталогу или файлу при этом не требуется.
- Чтобы исключить из проверки файлы или каталоги определенного вида, введите определяющую их маску в поле ввода. Маска задает общую часть имени объекта. При этом:
 - символ «*» заменяет любую, возможно, пустую последовательность символов;

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

- символ «?» заменяет любой, но только один символ;
- остальные символы маски ничего не заменяют и означают, что на данном месте в имени файла или каталога должен находиться именно этот символ.

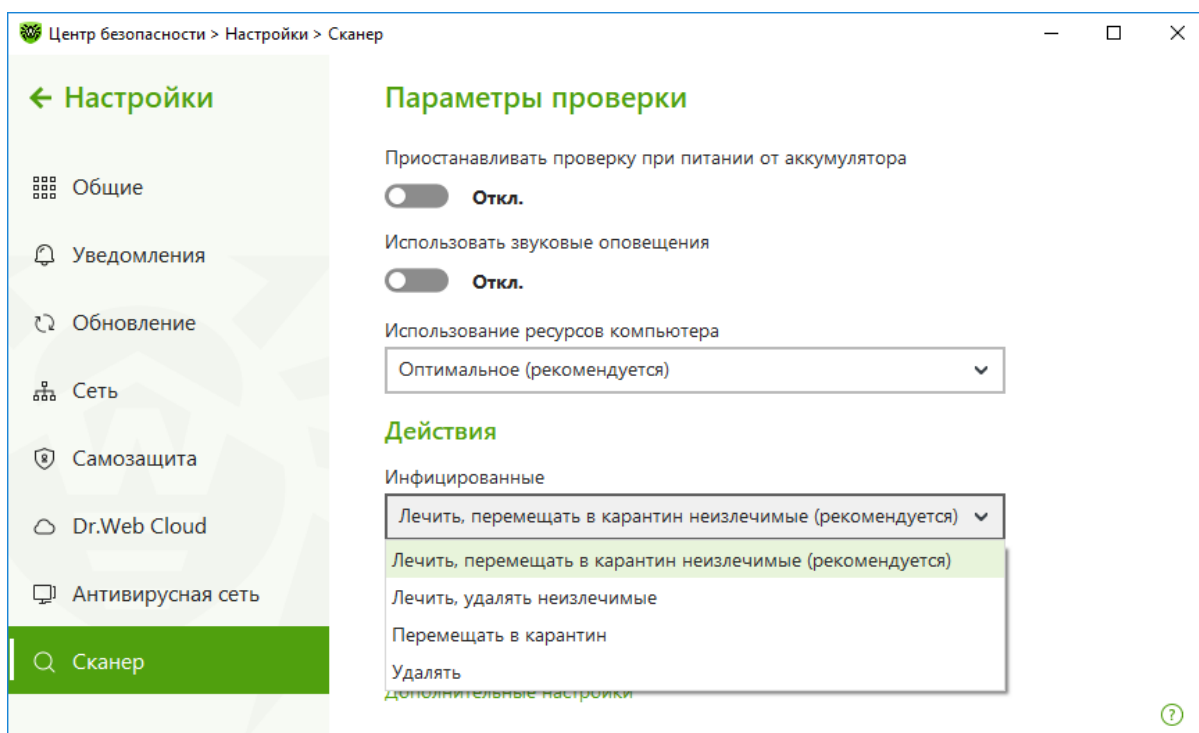
Пример:

- отчет*.doc — маска, задающая все документы Microsoft Word, название которых начинается с подстроки «отчет», например файлы отчет-февраль.doc, отчет121209.doc и т. д.;
- *.exe — маска, задающая все исполняемые файлы с расширением EXE, например setup.exe, iTunes.exe и т. д.;
- photo????09.jpg — маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных символа, например photo121209.jpg, photомама09.jpg или photo----09.jpg.

Кнопка **Удалить** позволяет удалить из списка выбранное исключение.

8.6.2. Настройка параметров работы антивирусного сканера

Для доступа к настройкам Сканера в окне **Центр безопасности** нажмите на кнопку  и далее выберите пункт **Сканер**.



8.6.3. Настройка проверки почтового трафика

Для защиты от вредоносных файлов установите настройки для модуля **SpIDer Mail**, антивирусного сканера аналогично тому, как это было рассказано выше.

Доступ к настройке параметров **SpIDer Mail** осуществляется также из окна **Центр безопасности**.

Почта являлась и является одним из основных путей проникновения вирусов на компьютер. Используя возможности почтового монитора **SpIDer Mail**, пользователь может не только

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

получать всегда чистую от вирусов почту, но и освободить свой почтовый ящик от гор спама.

Если пользователь хочет настроить действия, выполняемые при проверке почтовых сообщений, то рекомендуется следующий порядок действий.

Почтовый сторож **SpIDer Mail** по умолчанию включается в состав устанавливаемых компонентов, постоянно находится в памяти и автоматически запускается при загрузке операционной системы, однако его можно исключить из списка автоматически загружаемых компонентов. Для продуктов семейства Dr.Web Security Space почтовый сторож также может осуществлять проверку корреспонденции на спам с помощью Антиспама Dr.Web.

По умолчанию почтовый сторож **SpIDer Mail** автоматически перехватывает все обращения к почтовым серверам, выполняемые по стандартным для протоколов портам любыми почтовыми программами вашего компьютера. Стандартными являются следующие порты:

- для протокола POP3 — порт 110,
- для протокола SMTP — порт 25,
- для протокола IMAP4 — порт 143,
- для протокола NNTP — порт 119.

В ряде случаев автоматический перехват POP3-, SMTP-, IMAP4- и NNTP-соединений невозможен. В таком случае вы можете настроить перехват соединений вручную.

Почтовый сторож **SpIDer Mail** получает все входящие письма до почтового клиента и подвергает их антивирусному сканированию с максимальной степенью подробности. При отсутствии вирусов или подозрительных объектов они передаются почтовой программе «прозрачным» образом — так, как если бы письмо поступило непосредственно с сервера. Аналогично исходящие письма проверяются до отправки на сервер.

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

- Из зараженных писем удаляется вредоносная информация (это действие называется лечением письма), затем они доставляются обычным образом.
- Письма с подозрительными объектами перемещаются в виде отдельных файлов в **Карантин**, почтовой программе посылается сообщение об этом (это действие называется перемещением письма). Перемещенные письма удаляются с POP3- или IMAP4-сервера.
- Незараженные письма и письма, не прошедшие проверки, передаются без изменений (пропускаются).
- Инфицированные или подозрительные исходящие письма не передаются на сервер, пользователь извещается об отказе в отправке сообщения (как правило, почтовая программа при этом сохраняет письмо).

При наличии на компьютере неизвестного вируса, распространяющегося через электронную почту, почтовый сторож **SpIDer Mail** может определять признаки типичного для таких вирусов «поведения» (массовые рассылки). По умолчанию эта возможность включена.

Почтовый сторож **SpIDer Mail** предоставляет возможность проверки входящих писем на спам с помощью Антиспама Dr.Web. По умолчанию эта возможность включена.

Настройки **SpIDer Mail** по умолчанию являются оптимальными для начинающего пользователя, обеспечивая максимальный уровень защиты при наименьшем вмешательстве пользователя. При этом, однако, блокируется ряд возможностей почтовых программ (например, направление письма по многим адресам может быть воспринято как массовая

рассылка, полученный спам не распознается), а также утрачивается возможность получения полезной информации из автоматически уничтоженных писем (из незараженной текстовой части). Более опытные пользователи могут изменить параметры проверки почты и настройки реакции почтового сторожа **SpIDer Mail** на различные события.

Следует отметить, что не только почтовый сторож может распознавать вирусы, распространяемые по почте. Сканер Dr.Web также может обнаруживать вирусы в почтовых ящиках некоторых форматов, однако почтовый сторож **SpIDer Mail** имеет перед ним ряд преимуществ:

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

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

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

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

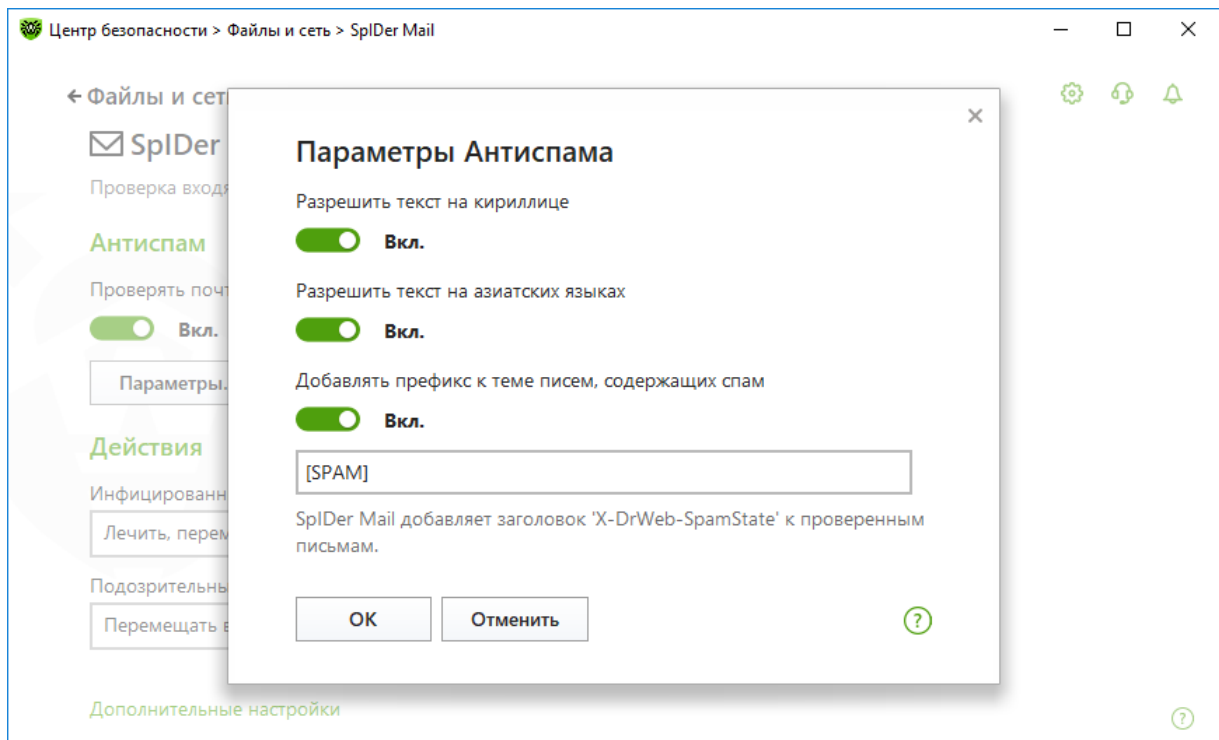
Вы можете временно отключать антивирусную проверку почтового трафика. Для этого в окне **Центр безопасности** выберите **Файлы и сеть**, далее **SpIDer Gate** и передвиньте переключатель компонента влево.

Удостоверьтесь, выбран ли пункт **Проверять почту на наличие спама**.

Почтовый сторож **SpIDer Mail** по умолчанию осуществляет проверку входящих писем на спам. Чтобы входящая корреспонденция не проверялась спам-фильтром, отключите режим **Проверять почту на наличие спама**.

Нажмите **Антиспам** → **Параметры**.

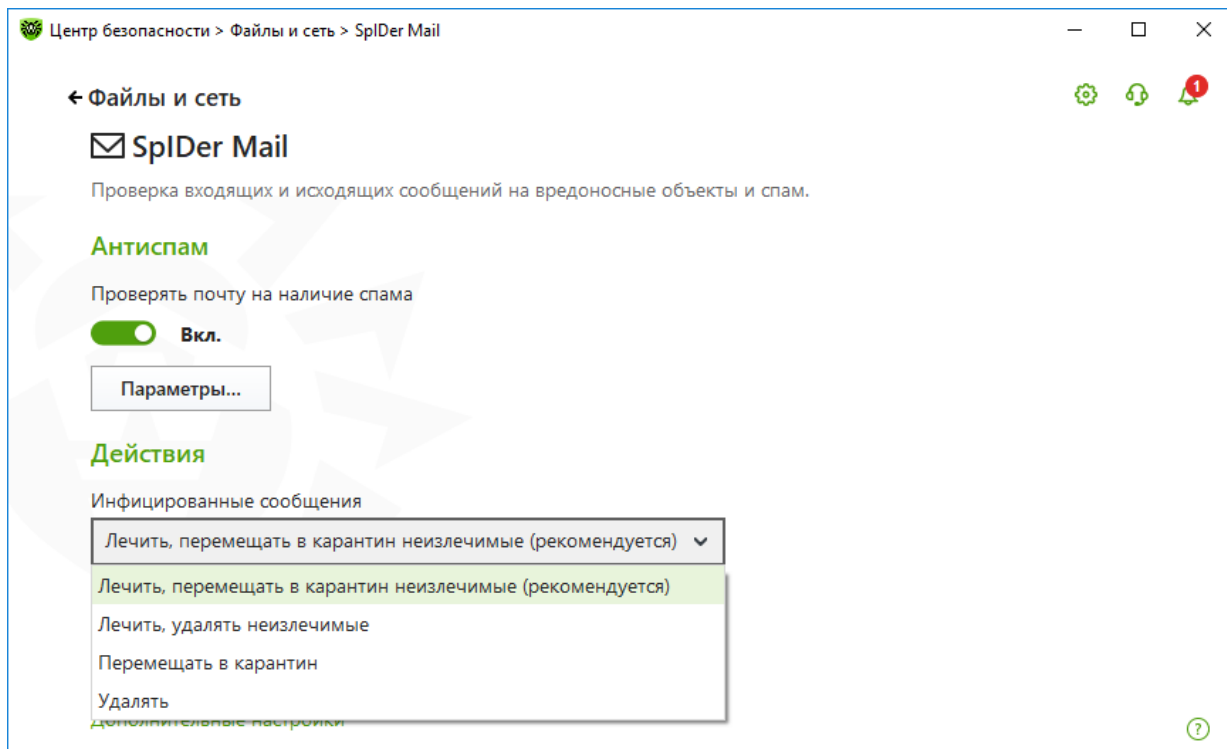
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию



В этой группе настроек проверки на спам вы можете указать, какие письма не следует причислять к спаму и каким образом пометить отфильтрованные сообщения. Определите, какой префикс будет присваиваться теме писем, определенных как спам-сообщения. Используя этот префикс, можно с помощью своего почтового клиента настроить действия со спам-сообщениями. Подробнее о настройках:

- **Разрешать текст на кириллице** (установлена по умолчанию) — данная настройка указывает почтовому сторожу **SpIDer Mail** без предварительного анализа не причислять к спаму письма, написанные в соответствии с установленной кириллической кодировкой. Если этот флажок снят, то такие письма с большой вероятностью будут отмечены фильтром как спам.
- **Разрешать текст на азиатских языках** (установлена по умолчанию) — данная настройка указывает почтовому сторожу **SpIDer Mail** без предварительного анализа не причислять к спаму письма, написанные в соответствии с наиболее распространенными кодировками азиатских языков. Если этот флажок снят, то такие письма с большой вероятностью будут отмечены фильтром как спам.
- **Добавлять префикс к полю Subject писем, содержащих спам** — по умолчанию данный флажок установлен, в начало темы спам-писем добавляется подстрока «[SPAM]». Данная настройка указывает почтовому сторожу **SpIDer Mail** добавлять указанный префикс к темам писем, распознаваемых как спам. Добавление префикса поможет вам создать правила для фильтрации почтовых сообщений, помеченных как спам, в тех почтовых клиентах (например, MS Outlook Express), в которых невозможно настроить фильтры по заголовкам писем.

С помощью группы настроек **Действия** укажите, что следует делать в том случае, если в письме были найдены инфицированные файлы и объекты.



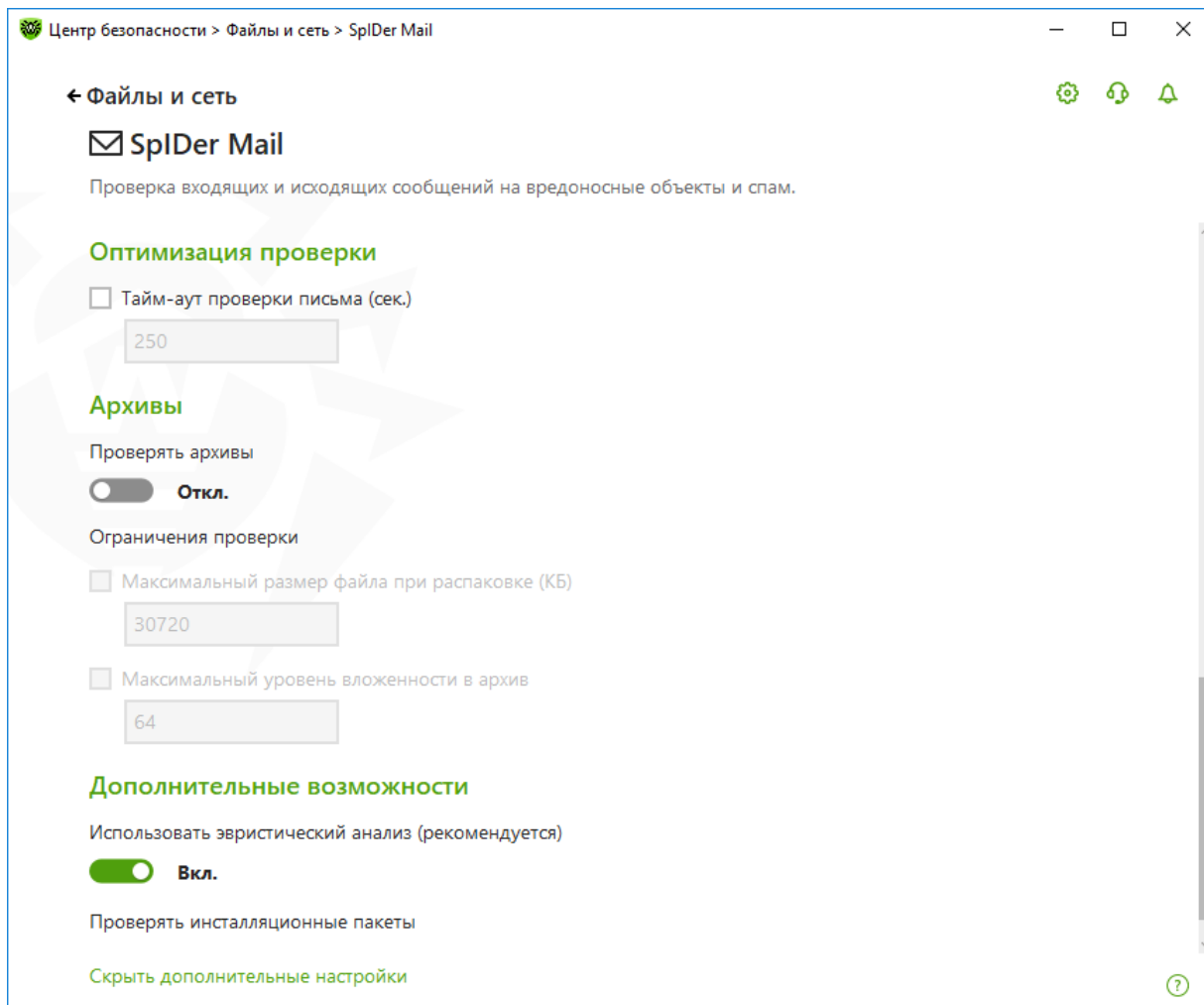
Реакция задается отдельно для каждой категории объектов, в том числе для таких, как:

- инфицированные письма, зараженные известным и (предположительно) излечимым вирусом;
- подозрительные письма, предположительно зараженные вирусом или содержащие вредоносный объект;
- письма, содержащие различные потенциально опасные объекты.

По умолчанию для большинства типов стоит действие **Перемещать в карантин**, что позволяет их сохранять для дальнейшего анализа.

В окне **Дополнительные настройки** режима проверки задаются дополнительные настройки режима проверки электронной почты, включая особенности сканирования, действия над письмом и параметры оптимизации.

Если требуется проверять получаемые вами архивы, нажмите **Дополнительные настройки** и отметьте пункт **Проверять архивы**.



Отказ от проверки содержимого архивов в условиях постоянной работы сторожа **SpIDer Guard** не ведет к проникновению вирусов на компьютер, а лишь откладывает момент их обнаружения. При распаковке зараженного архива операционная система производит попытку записать инфицированный объект на диск, при этом сторож **SpIDer Guard** неминуемо обнаруживает вредоносный объект.

Также можно определить максимальное время обработки каждого письма и правила обработки архивов. Если необходимо проверять только небольшие архивы (что увеличит скорость проверки), уменьшите числа, указанные в поле справа от пунктов **Максимальный размер файла при распаковке** (если почтовый сторож определяет, что после распаковки архив будет больше указанной длины, проверка и распаковка производиться не будет) и **Максимальный уровень вложенности в архив** (если уровень вложенности в архив превышает указанный, проверка будет производиться только до указанного уровня вложенности).

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

Действия над письмом — в данной группе настроек указываются дополнительные действия над электронными письмами, обработанными почтовым сторожем **SpIDer Mail**:

- **Добавлять заголовок 'X-Antivirus' к письмам** (установлена по умолчанию) — при использовании данной настройки в заголовок всех писем, обработанных почтовым

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

сторожем **SpIDer Mail**, добавляется информация о проверке электронного сообщения и версии Dr.Web. Вы не можете изменить формат добавляемого заголовка.

- **Удалять измененные письма на сервере** — при использовании данной настройки входящие письма, удаленные или перемещенные в карантин почтовым сторожем **SpIDer Mail**, удаляются с почтового сервера независимо от настроек почтовой программы. Снимите этот флажок для удаления таких писем вручную или с использованием более гибких настроек почтовой программы.

Почтовый сторож **SpIDer Mail** добавляет ко всем проверенным письмам следующие заголовки:

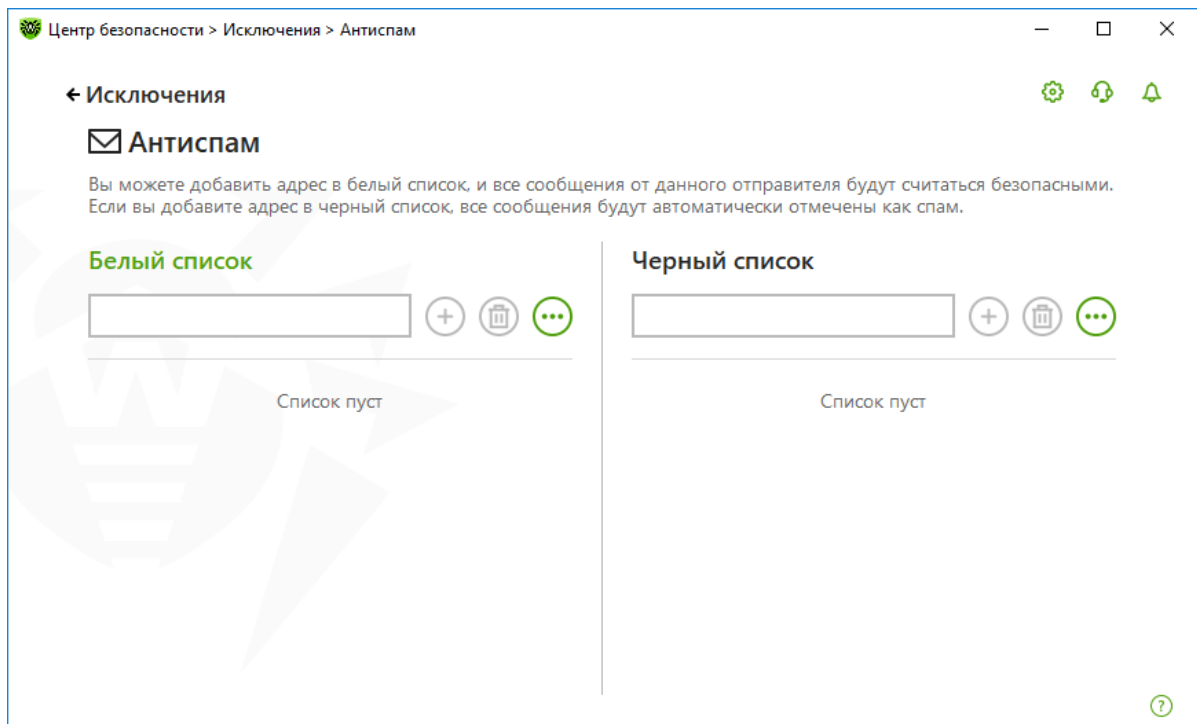
- X-DrWeb-SpamState: <значение>, где <значение> указывает на то, является ли письмо спамом (Yes), по мнению почтового сторожа **SpIDer Mail**, или нет (No).
- X-DrWeb-SpamVersion: <версия>, где <версия> — версия библиотеки Антиспама Dr.Web.
- X-DrWeb-SpamReason: <рейтинг спама>, где <рейтинг спама> —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

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

Так как **SpIDer Mail**, кроме добавления префикса к теме письма, всегда добавляет в служебные поля (скрытую в служебной области письма невидимую пользователю информацию) строку X-DrWeb-SpamState, то можно осуществлять дополнительную фильтрацию как по заголовку письма (message header), так и его теме (Subject'у).

8.6.3.1. Настройка исключений проверяемых адресов

В окне **Исключения** → **Антиспам** вы можете задать **Белый список** (список адресатов, чьи электронные письма вы хотите гарантированно пропускать без проверки на спам) и **Черный список** (список адресатов, чьи электронные письма вы хотите гарантированно блокировать).



Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

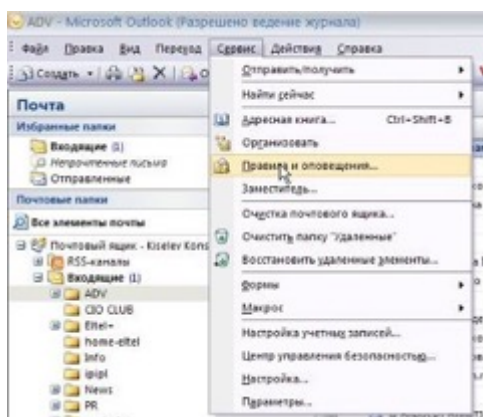
В окнах **Белый** и **Черный списки** задаются списки отправителей, почтовые сообщения которых пропускаются почтовым сторожем **SpIDer Mail** без проведения анализа, и списки отправителей, почтовые сообщения которых расцениваются почтовым сторожем **SpIDer Mail** как спам без проведения анализа, соответственно.

Если адрес отправителя добавлен в белый список, письмо не подвергается анализу на содержание спама. Однако если доменное имя адресов получателя и отправителя письма совпадают, и это доменное имя занесено в белый список с использованием маски ***@<имя.домена>**, то письмо подвергается проверке на спам. По умолчанию список пуст. Если адрес отправителя добавлен в черный список, письму без дополнительного анализа присваивается статус спама. По умолчанию список пуст.

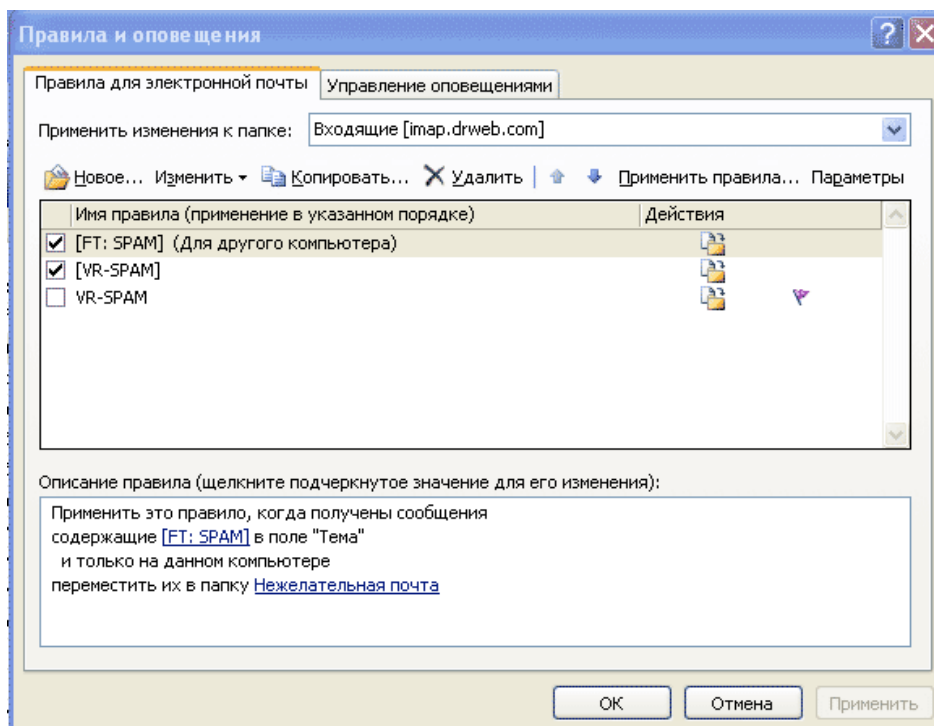
8.6.4. Настройка правил фильтрации в Microsoft Outlook

Для настройки правил фильтрации в Microsoft Outlook 2007:

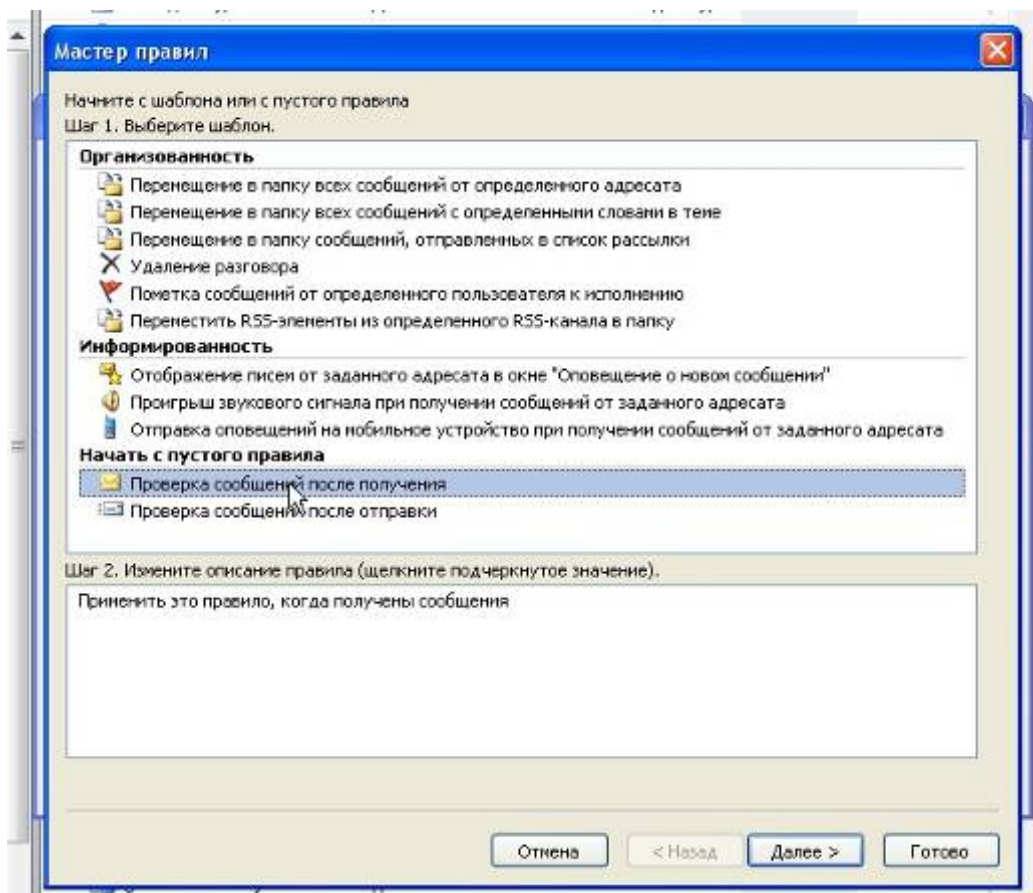
В меню Microsoft Outlook **Сервис** (Tools) откройте вкладку **Правила и оповещения** (Rules and Alerts).



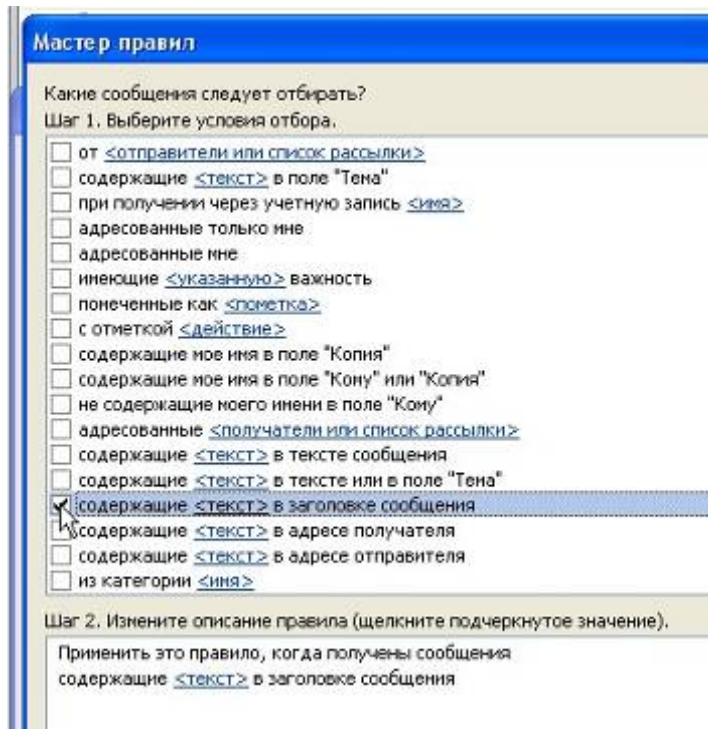
Перейдите на закладку **Правила для электронной почты** и выберите пункт **Новое** (New Rule).



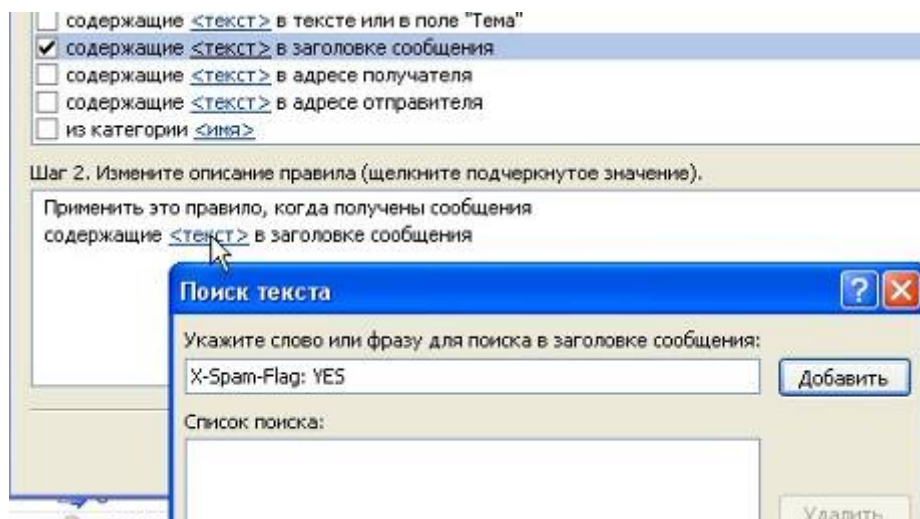
Выберите пункт **Начать с пустого правила** (Start from a blank rule) и, отметив параметр **Проверка сообщений после получения** (Check messages when they arrive), нажмите кнопку **Далее** (Next).



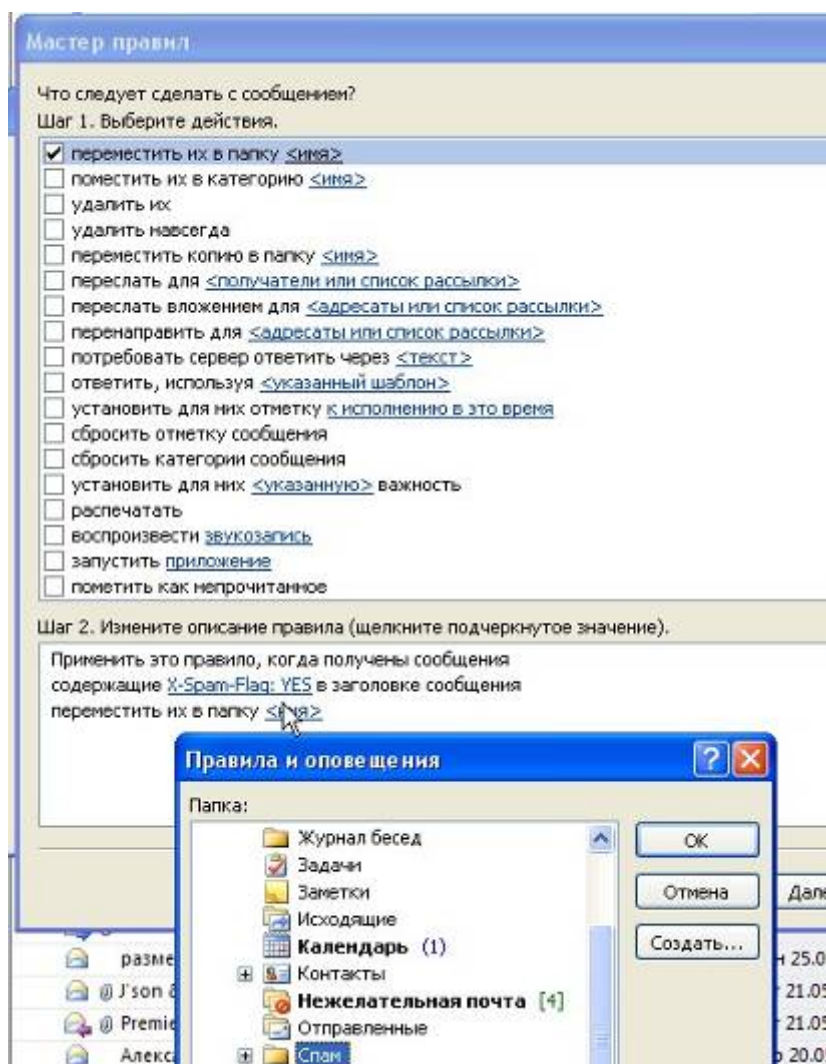
В открывшемся списке условий выберите пункт **Содержащие <текст> в заголовке сообщения** (with specific words in the message header).



В нижнем окне условий щелкните по фразе <текст> (specific words) и в открывшемся окне введите без кавычек фразу «X-DrWeb-SpamState: YES». Нажмите последовательно кнопки **Добавить** (Add), **ОК**, **Далее** (Next).



Отметьте действие **Переместить их в папку** <имя> (move it to specified folder) и выберите, в какую папку будет перемещен спам, нажав на подсвеченную фразу в нижнем окне <имя> (specified folder). Если необходимо сохранять спам в новой папке, создайте ее, нажав в этом же окне кнопку **Создать**. После этого последовательно нажмите **Далее** (Next) и **Готово** (Finish).



Для завершения настройки закройте окно правил. Настройка правил фильтрации для других почтовых клиентов производится аналогично.

Для проверки правильности работы почтового фильтра создайте новое письмо и в его тело вставьте строчку XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X. Это так называемый GTUBE (Generic Test for Unsolicited Bulk Email) — аналог тестового вируса EICAR, применяемый для тестирования функций антиспама.

Для повышения качества работы спам-фильтра вы можете сообщать об ошибках распознавания спама. Если происходят ошибки распознавания:

1. При обнаружении ошибки в работе спам-фильтра создайте новое письмо и приложите к нему неправильно распознанное сообщение. Письма, отправленные в тексте письма, анализироваться не будут.
2. Отправьте письмо с вложением на один из следующих адресов:
 - письмо, ошибочно оцененное как спам, — на адрес vrnonspam@drweb.com;
 - спам, не распознанный системой, — на адрес vrspam@drweb.com.

Отчет почтового сторожа **SpIDer Mail** записывается в файл `netfilter.log`, который находится в каталоге `%allusersprofile%\Application Data\Doctor Web\Logs\` (в Windows 7, `%allusersprofile%\Doctor Web\Logs\`).

8.6.5. Настройка проверки интернет-трафика

В окне **Центр безопасности** выберите **Файлы и сеть** и далее **SpIDer Gate**.

Внимание! Доступ к изменению настроек антивируса может быть защищен паролем.

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

SpIDer Gate — один из наиболее интенсивно развивающихся модулей антивируса. Во многом это связано с постоянным ростом трафика на компьютерах пользователей. В версии 12 работа системы проверки трафика была оптимизирована для обеспечения плавности загрузки больших файлов, онлайн-просмотра видео, прослушивания радио в сети Интернет. Проверка трафика осуществляется непосредственно во время его загрузки. Это также позволило снизить нагрузку на процессор — как при работе пользователей через популярные браузеры, так и через менеджеры закачек.

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

При базовых настройках **SpIDer Gate** блокирует получаемые по сети объекты, содержащие вредоносные программы.

Программа постоянно находится в оперативной памяти компьютера и автоматически перезапускается при загрузке Windows. При необходимости вы можете изменить режим запуска веб-антивируса при загрузке операционной системы.

Вы можете временно отключать антивирусную проверку трафика. Для этого в окне **Центр безопасности** выберите **Файлы и сеть**, далее **SpIDer Gate** и передвиньте переключатель

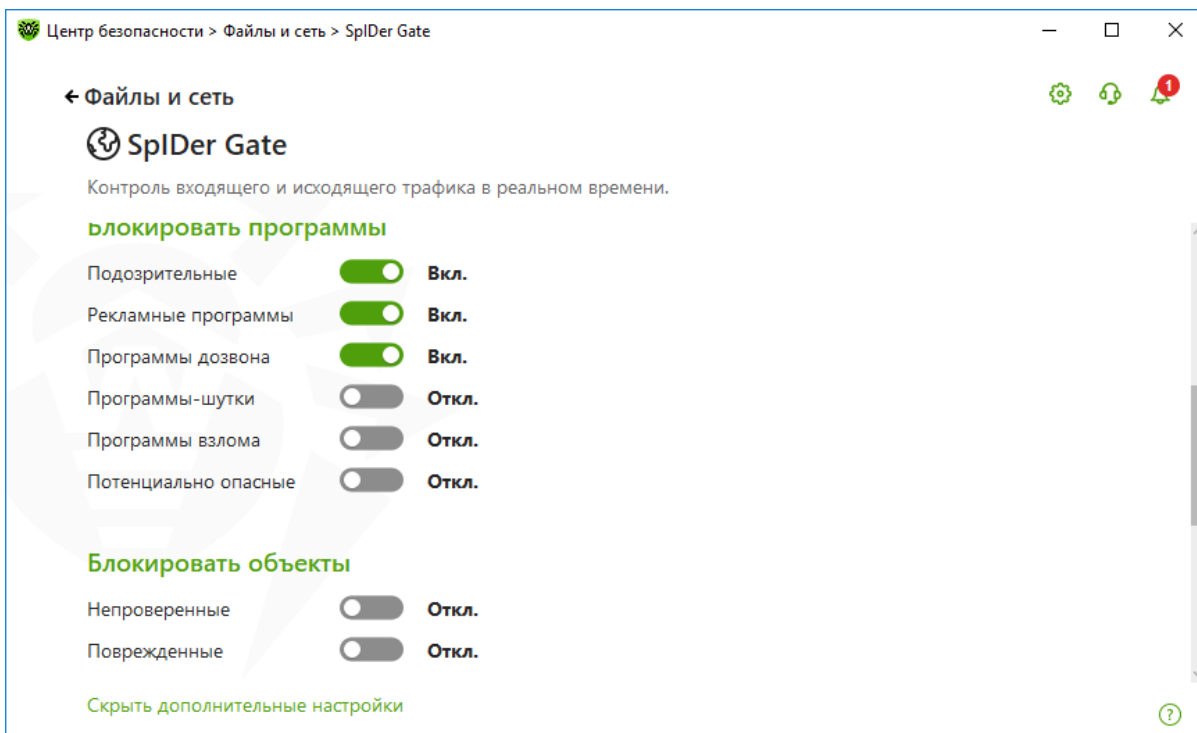
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

компонента влево.

В группе **Параметры блокировки** вы можете установить автоматическую блокировку доступа к известным веб-сайтам, с которых распространяются вирусы или вредоносные программы других типов, а также к нереккомендованным сайтам, известным как неблагонадежные (для этого установите флажок **Блокировать нереккомендуемые сайты**).

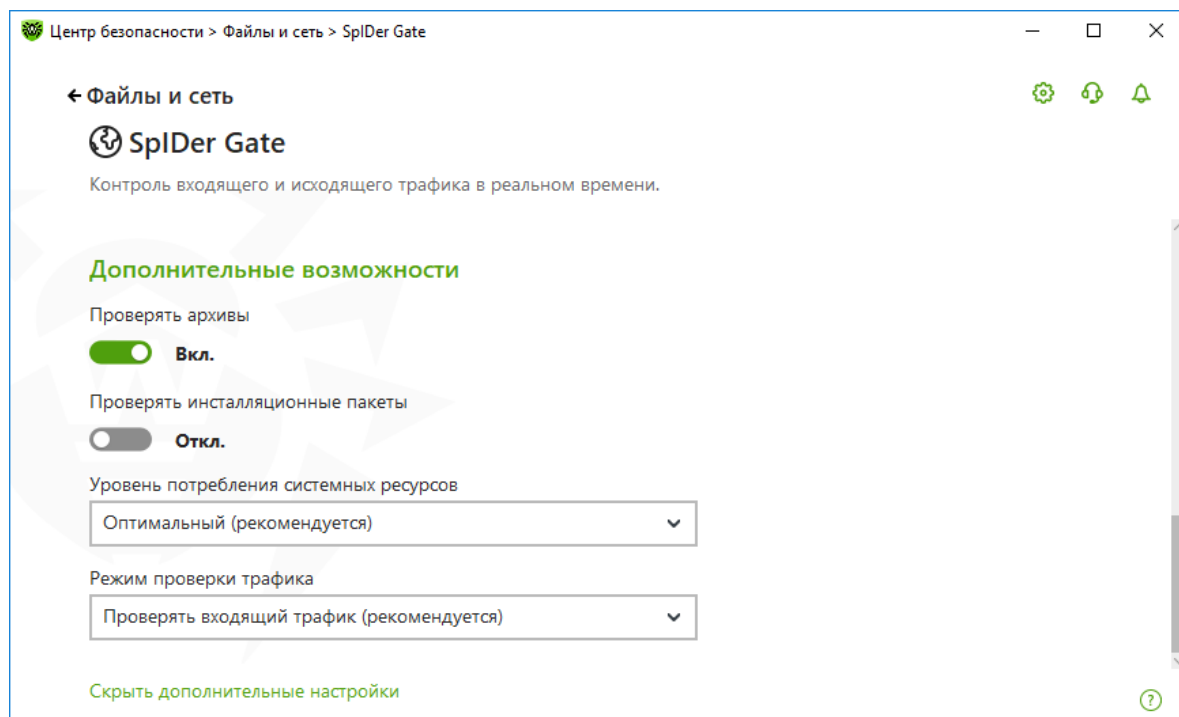
В окне настроек **SpIDer Gate**, также доступном из окна **Центр безопасности**, аналогично тому, как это было сделано выше, разрешите блокировку подозрительных и потенциально опасных файлов.

Кнопка **Дополнительные настройки** открывает доступ к окну выбора типов блокируемых объектов.

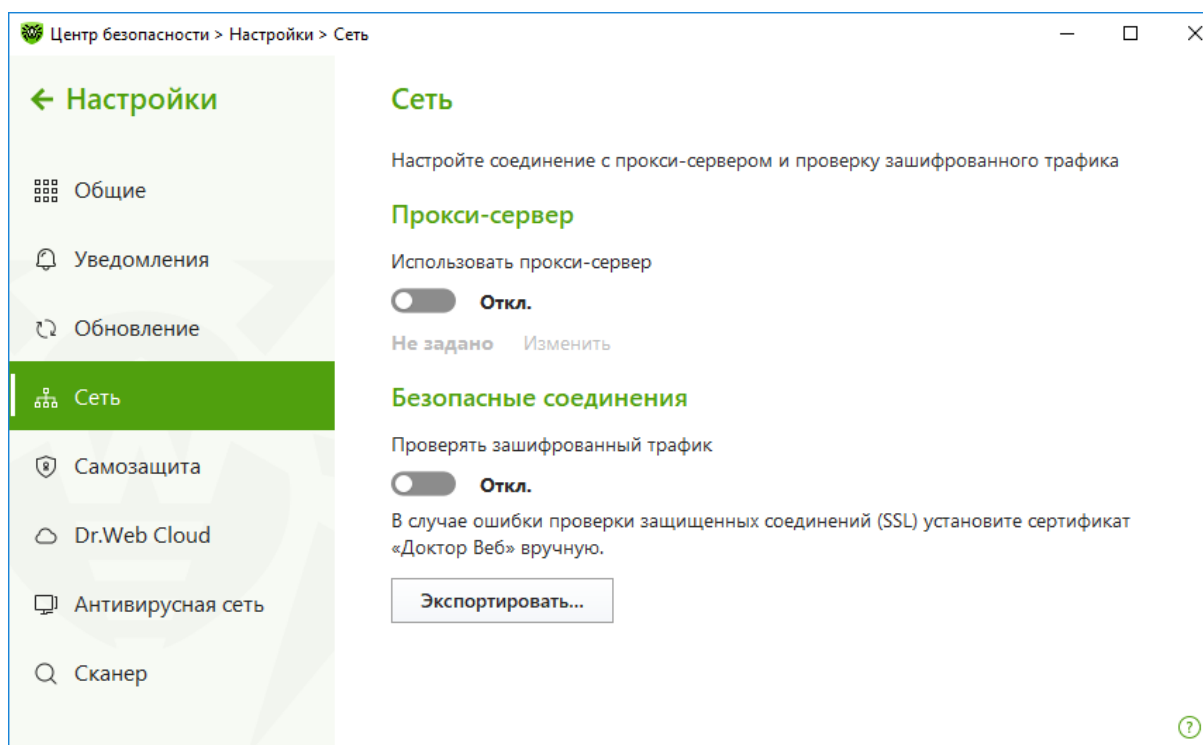


Здесь же вы можете настроить **Уровень потребления системных ресурсов** — распределение ресурсов в зависимости от приоритетности сканирования трафика. При меньшем приоритете проверки скорость работы с сетью Интернет уменьшается, поскольку веб-антивирусу **SpIDer Gate** приходится дольше ждать загрузки данных и проверять больший объем информации. При увеличении приоритета сканирования проверка производится чаще, что позволяет сторожу отдавать данные быстрее, тем самым повышая скорость работы с сетью. Однако при более частых проверках повышается нагрузка на процессор. Вы можете подобрать наилучший баланс опытным путем.

В разделе **Режим проверки** предоставляется возможность выбора типа проверяемого HTTP-трафика. По умолчанию проверяется только входящий трафик.







Вы можете включить в проверку данные, передаваемые по безопасным протоколам (HTTPS). Для этого включите соответствующую опцию на странице **Основные** → **Сеть**.



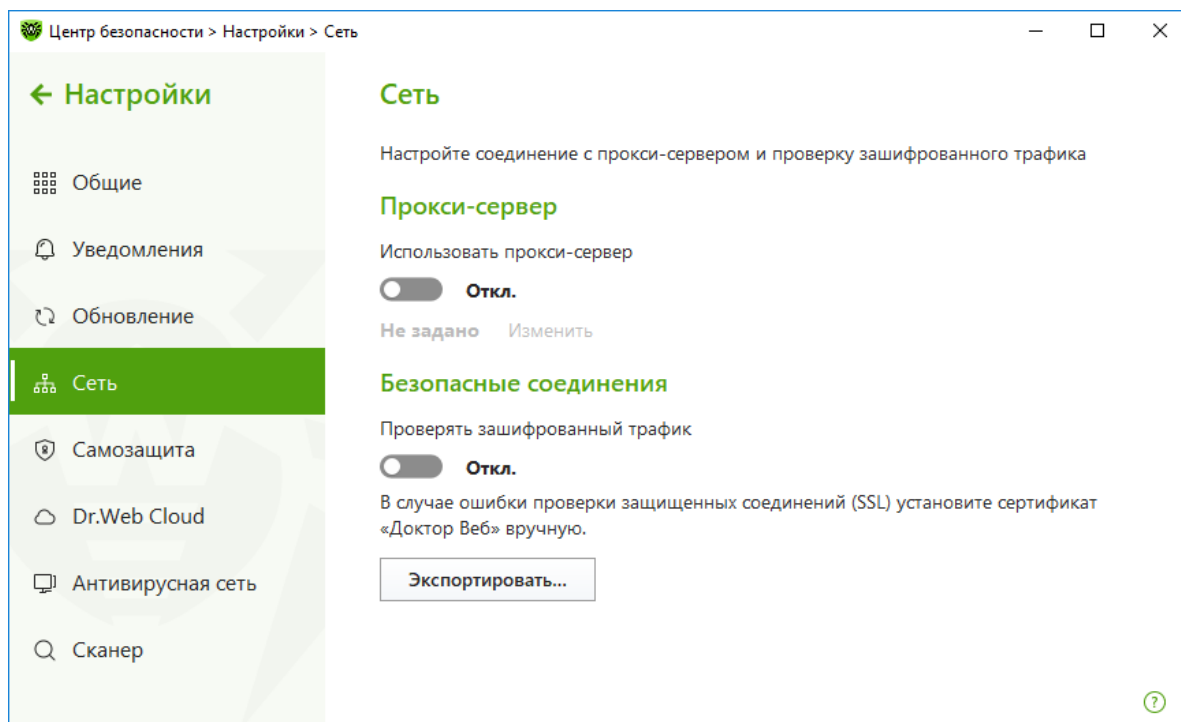
Если клиент, который получает и передает такие данные, не обращается к хранилищу сертификатов системы Windows, экспортируйте сертификат.

Если вы хотите включить в проверку данные, передаваемые по криптографическому протоколу SSL (например, в **SpIDer Mail** — по протоколам POP3S, SMTPS, IMAPS), то для работы некоторых клиентов, которые передают и получают такие данные и при этом не обращаются к хранилищу сертификатов системы Windows, может потребоваться сертификат компании «Доктор Веб». Нажмите кнопку **Экспортировать** и сохраните сертификат в удобную для вас папку.

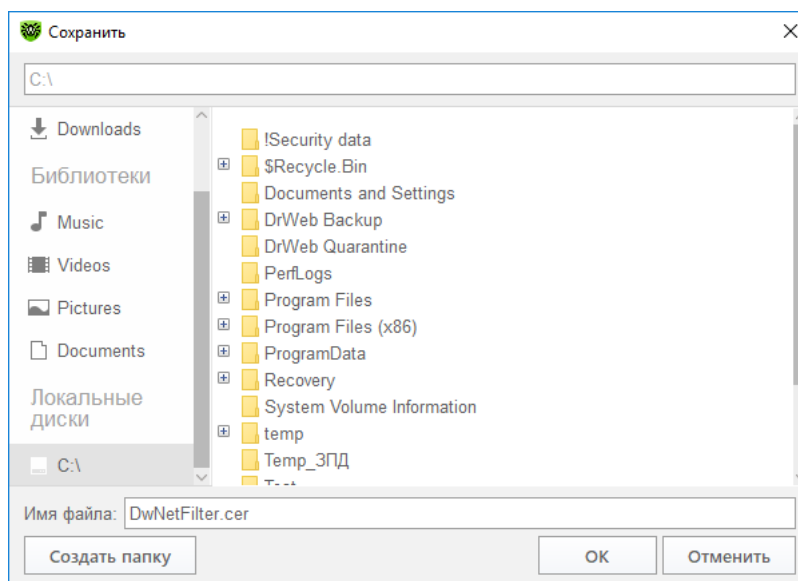
8.6.5.1. Настройка проверки зашифрованного трафика

На данный момент до половины интернет-трафика зашифровано, чем могут воспользоваться злоумышленники. В связи с этим включите проверку зашифрованного трафика (функционал доступен для Dr.Web Security Space): кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне последовательно нажмите на  (Режим администратора) (значок изменит вид на ) и ставший зеленым значок  в правом верхнем углу окна.

В открывшемся окне **Настройки** выберите пункт **Сеть**. Переключатель **Безопасные соединения** должен быть включен.

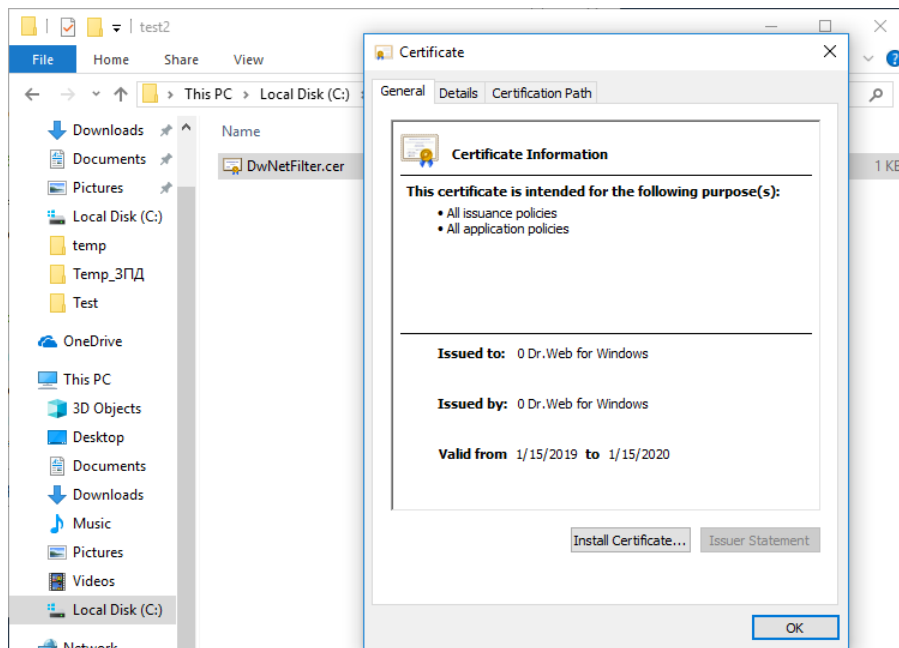


В случае необходимости установите сертификат Dr.Web в систему. Для этого в окне **Сеть** кликните на кнопку **Экспортировать** и сохраните предложенный файл в удобную вам папку.



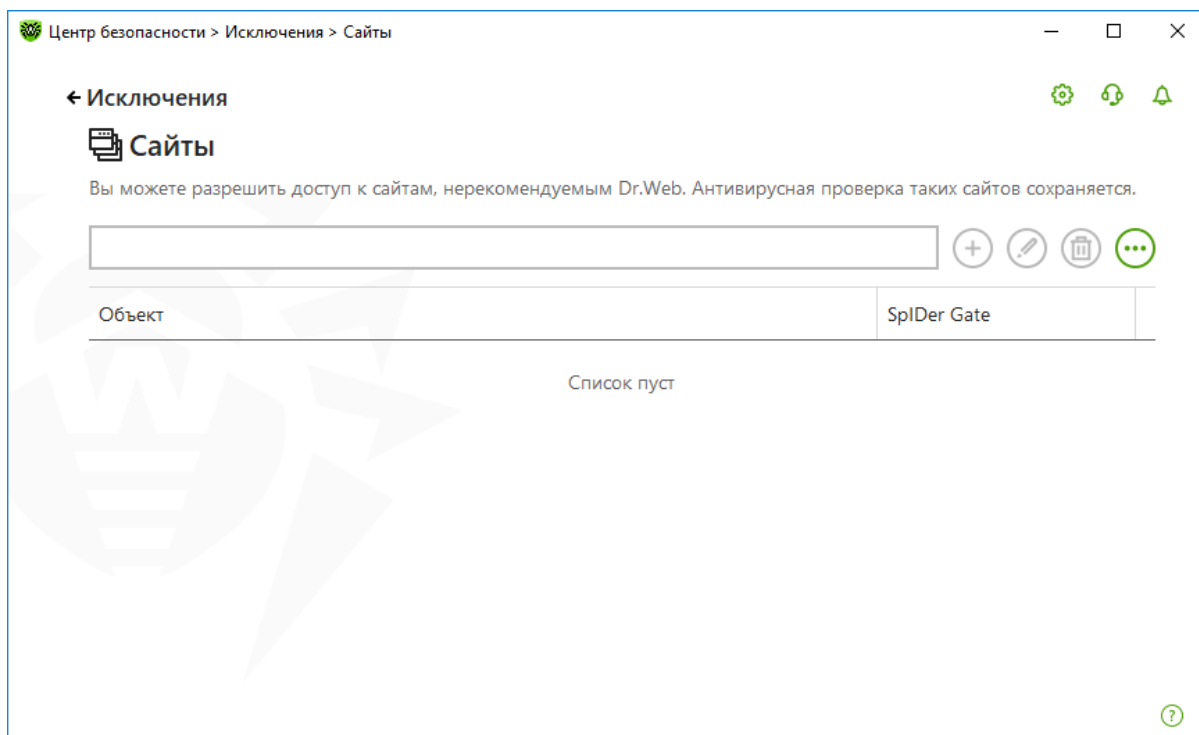
Произведите установку удобным для вас способом. Например, кликнув по сохраненному файлу и подтвердив установку.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию



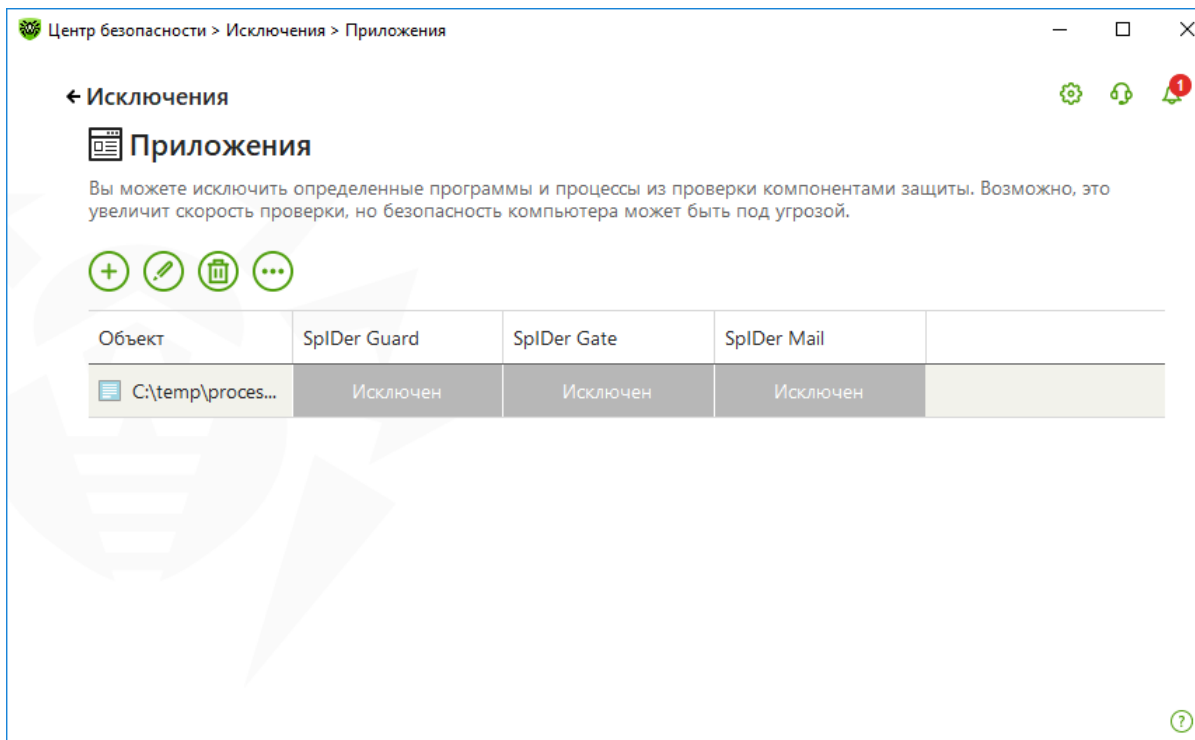
8.6.5.2. Настройка исключений доступа к сетевым ресурсам


На странице настроек **Исключения** → **Сайты** вы можете задать список сайтов, доступ к которым должен быть разрешен несмотря на установленные ограничения.



8.6.6. Настройка исключений для работающих приложений

В разделе **Исключения** → **Приложения** задаются программы и процессы, которые исключаются из проверки компонентами **SpIDer Guard**, **SpIDer Gate** и **SpIDer Mail**. По умолчанию список пуст.



Чтобы добавить программу или процесс к списку исключений, нажмите .

Исключаемые приложения


Исключить из проверки компонентом SpIDer Guard

Исключить из проверки компонентами SpIDer Gate и SpIDer Mail

▾

▾

▾



Чтобы указать программу, сетевую активность которой компонент контролировать не должен, в открывшемся окне нажмите кнопку **Обзор** и выберите файл в стандартном окне открытия файла. Далее в окне настройки укажите, какие компоненты не должны проводить проверку выбранного файла.

При использовании исключений допускается вводить путь к процессам вручную, а также использовать маски для задания исключений.

Для объектов, исключаемых из проверки компонентами **SpIDer Gate** и **SpIDer Mail**, укажите дополнительные условия.


- **Независимо от наличия цифровой подписи приложения.** Выберите эту настройку, если приложение должно быть исключено из проверки вне зависимости от наличия у него действительной цифровой подписи.


Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

- **При наличии действительной цифровой подписи приложения.** Выберите эту настройку, если приложение должно быть исключено из проверки только при наличии действительной цифровой подписи приложения. В противном случае приложение будет проверено компонентами.
- **Любой трафик.** Выберите эту настройку, чтобы исключить из проверки и зашифрованный, и незашифрованный трафик приложения.
- **Зашифрованный трафик.** Выберите эту настройку, чтобы исключить из проверки только зашифрованный трафик приложения.
- **По всем IP-адресам и портам.** Выберите эту настройку, чтобы исключить из проверки трафик, передаваемый на любые IP-адреса и порты.
- **По указанным IP-адресам и портам.** Выберите эту настройку, чтобы указать IP-адреса или порты для исключения из проверки переданного на них трафика. Трафик, переданный на остальные IP-адреса или порты, будет проверен (если не исключен другими настройками).

Для завершения настройки нажмите кнопку **ОК**. Выбранная программа или процесс появится в списке.

При необходимости повторите действия для других программ. Исключать из проверки следует только те приложения, действиям и защищенности которых вы полностью доверяете.

Для того чтобы отредактировать исключение, выберите нужный элемент в списке и нажмите .

Чтобы удалить элемент списка исключений, выберите соответствующий элемент в списке и нажмите .

8.7. Настройка системы обновлений Dr.Web Security Space

Внимание! Для обнаружения вредоносных объектов антивирусы компании «Доктор Веб» используют специальные вирусные базы Dr.Web, в которых содержится информация обо всех известных вредоносных программах. В связи с постоянным появлением новых угроз и разработкой алгоритмов противодействия им, реализованных в виде исполняемых файлов и программных библиотек, — эти базы требуют периодического обновления.

Обновление позволяет обнаруживать ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев — излечивать ранее неизлечимые зараженные файлы. Автоматическое обновление необходимо для поддержания выбранного в ходе настройки уровня безопасности компьютера.

Благодаря опыту эксплуатации антивирусов Dr.Web исправляются обнаруженные в программах ошибки, обновляется система помощи и документация, выпускаются усовершенствованные модули, позволяющие осуществлять поиск и лечение вредоносных программ с меньшими затратами системных ресурсов.

Для поддержания актуальности вирусных баз и программных алгоритмов компанией «Доктор Веб» реализована система распространения обновлений через сеть Интернет. Модуль обновления позволяет в течение срока действия лицензии загружать и устанавливать дополнения к вирусным базам и обновленные программные модули. Важно помнить, что для использования **Модуля обновления** необходимо иметь доступ в сеть Интернет.

Вы можете запустить обновление одним из следующих способов:

- из командной строки,
- с помощью **Модуля обновления SpIDer Agent**.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

При автоматическом запуске обновление проводится в «невидимом» режиме, отчет **Модуля обновления** записывается в файл `dwupdater.log` в каталоге `%allusersprofile%\Doctor Web\Logs`.

Успешность поиска и удаления вирусов во многом зависит от состояния вирусных баз. Работа модуля обновления определяется структурой вирусных баз и методикой обновления баз и комплекса в целом:

- В состав программного комплекса входит основная вирусная база (файл `drwebase.vdb`) и ее расширения. Все вместе они содержат вирусные записи, позволяющие определять вредоносные программы, известные в момент выпуска данной версии программного комплекса.
- Еженедельно выпускаются дополнения — файлы с вирусными записями для обнаружения и обезвреживания вирусов, выявленных за время, прошедшее с выпуска предыдущего еженедельного обновления. Еженедельные дополнения представлены файлами, наименование которых выглядит так: `drwXXXYY.vdb`, где `XXX` — номер текущей версии антивирусного ядра, а `YY` — порядковый номер еженедельного дополнения.
- По мере необходимости (обычно несколько раз в сутки) выпускаются горячие дополнения, содержащие вирусные записи для обнаружения и обезвреживания всех вирусов, выявленных после выхода последнего еженедельного дополнения. Эти дополнения выпускаются в виде файла с именем `drwtoday.vdb`. В конце дня содержимое этого файла добавляется в файл накопительного обновления `drwdaily.vdb`. Содержимое файла `drwdaily.vdb` в конце недели выпускается в виде очередного еженедельного обновления.
- В состав программного комплекса входят дополнительные базы вредоносных программ `drwnasty.vdb` и `drwrisky.vdb`. Записи, предназначенные для обнаружения рекламных программ и программ дозвона, включаются в состав вирусной базы `drwnasty.vdb`. Записи для обнаружения программ-шутков, потенциально опасных программ и программ несанкционированного доступа включаются в состав вирусной базы `drwrisky.vdb`.
- Время от времени выпускаются кумулятивные дополнения баз вредоносных программ. Горячие дополнения для этих баз могут выпускаться значительно реже, чем для основной вирусной базы.
- Время от времени выпускаются радикальные обновления самих компонентов антивирусной защиты.

Для запуска обновления можно:

- в режиме командной строки вызвать исполняемый файл `drwupsrv.exe` из каталога установки программы (`%PROGRAMFILES%\Common Files\Doctor Web\Updater`);
- выбрать пункт **Обновление** меню значка **SpIDer Agent** в области уведомлений Windows.

Внимание! При отсутствии ключевого файла обновление Dr.Web невозможно.

При наличии ключевого файла **Модуль обновления** проверяет, не является ли имеющийся у вас ключевой файл заблокированным на сайте компании «Доктор Веб». В случае блокировки вам выдается соответствующее сообщение, обновление не производится, а компоненты программы могут быть заблокированы. Если ваш ключевой файл был заблокирован по ошибке, свяжитесь с продавцом, у которого вы приобрели Dr.Web.

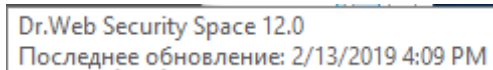
После успешной проверки ключевого файла **Модуль обновления** автоматически загружает все обновленные файлы, соответствующие вашей версии Dr.Web.

При обновлении исполняемых файлов и библиотек может потребоваться перезагрузка
Dr.Web® Security Space. Руководство по быстрой установке и разархивированию





компьютера. Пользователь извещается об этом при помощи информационного окна. **Сканер и SpIDer Guard** начинают использовать обновленные базы автоматически.

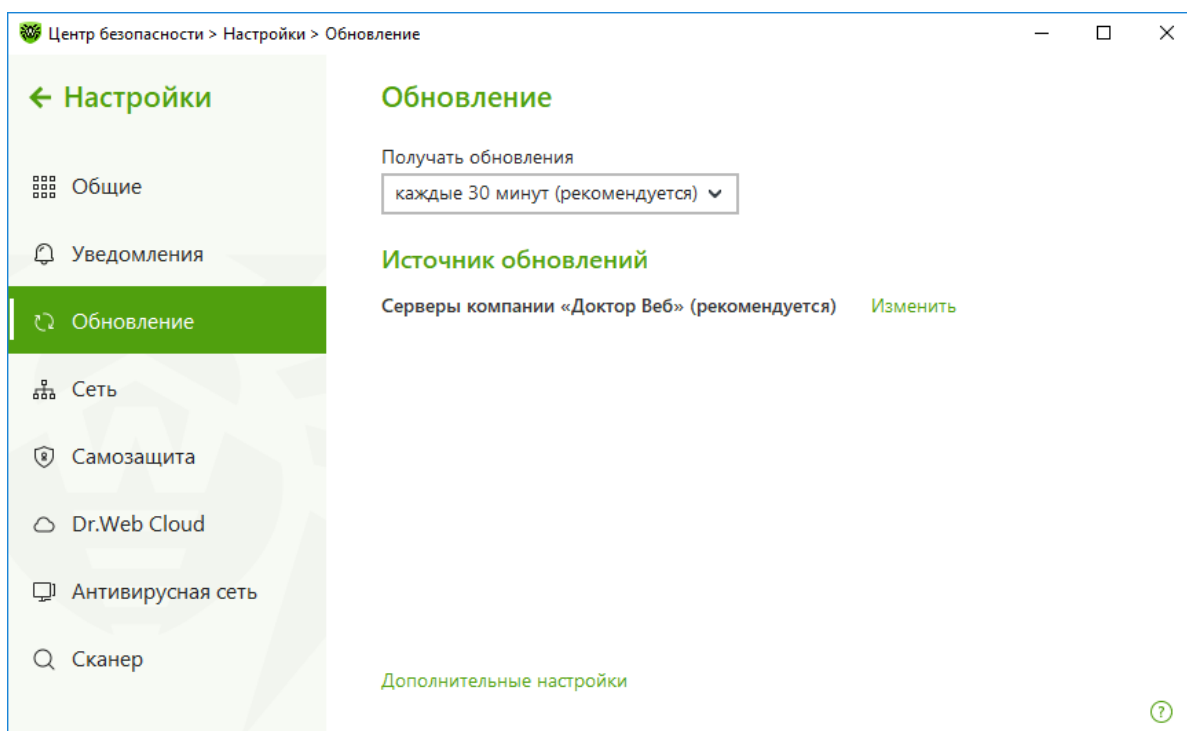
Хотя инсталляционный пакет содержит вирусные базы, рекомендуется сразу после установки провести обновление — в случае необходимости настроив параметры доступа в Интернет.

Проверьте актуальность вирусных баз. При наведении курсора мыши на значок в правом нижнем углу экрана появляется всплывающая подсказка с датой последнего обновления антивируса.



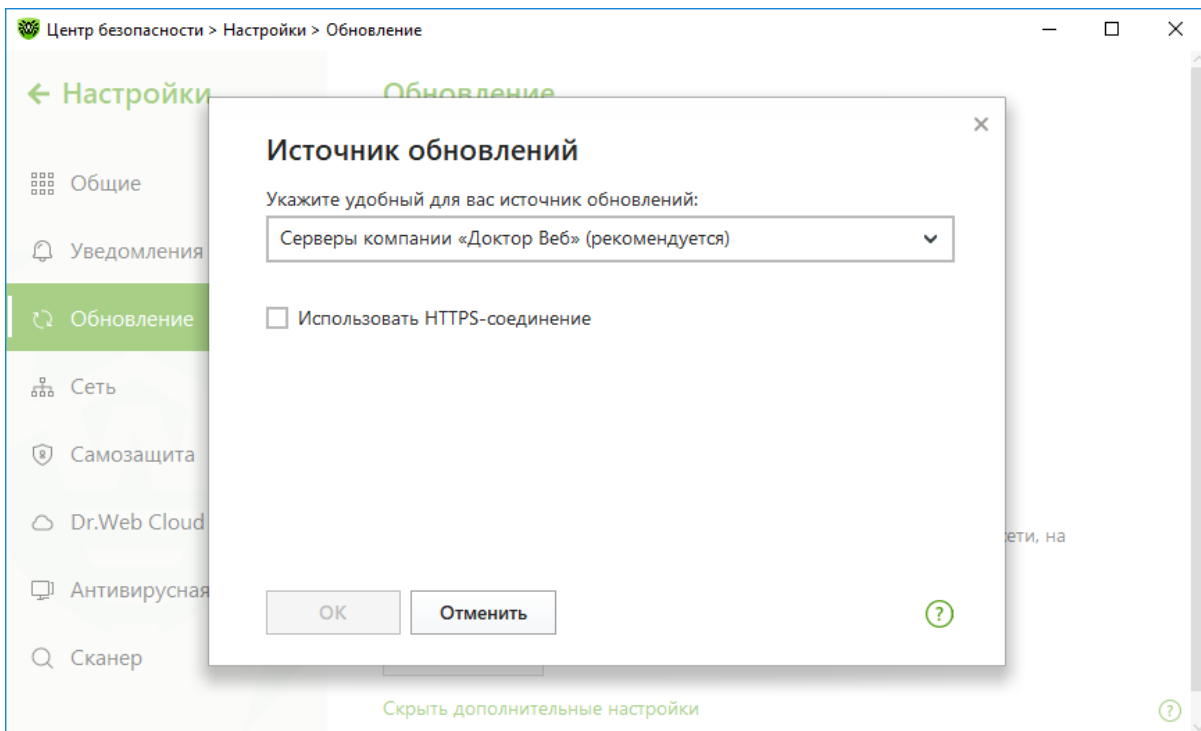
Щелкните на значок . Статус обновлений будет показан в открывшемся меню.

Для настройки параметров обновлений щелкните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне последовательно нажмите на  (Режим администратора) (значок изменит вид на , ставший зеленым значок  в правом верхнем углу окна и выберите в меню **Настройки** пункт **Обновление**.

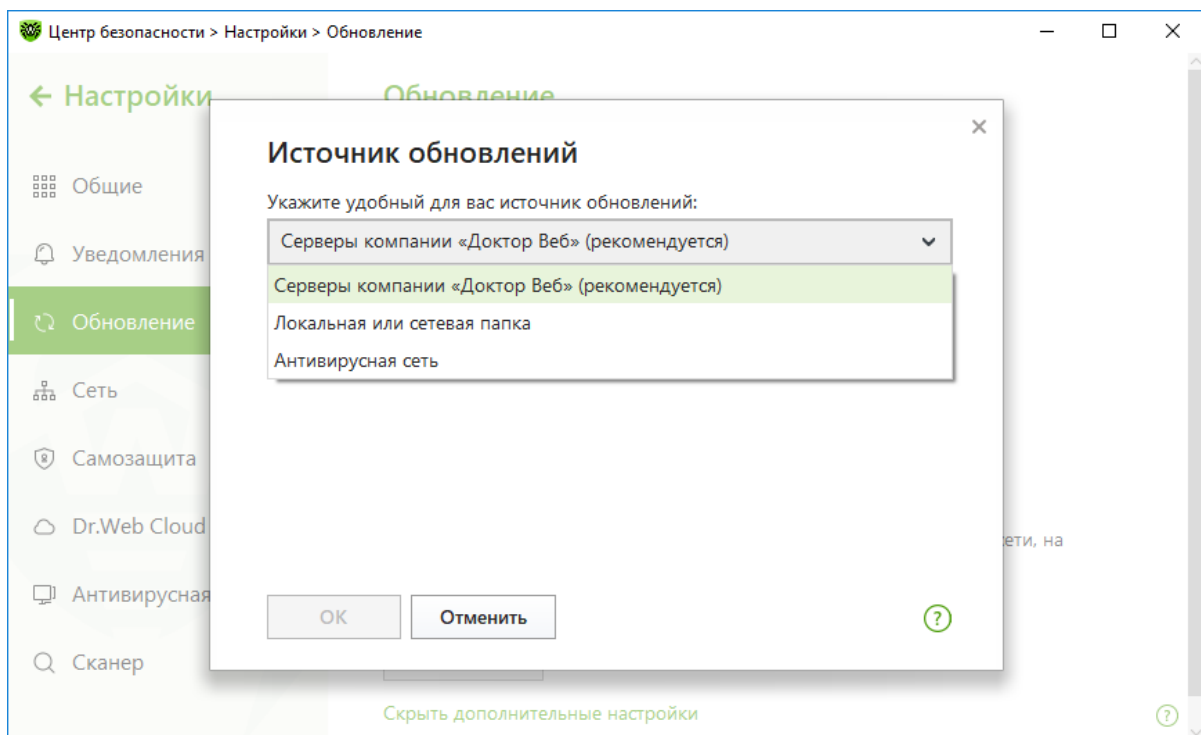


В данном окне можно указать источник обновлений и периодичность их проведения. По умолчанию антивирус обновляется с серверов компании «Доктор Веб».

Чтобы изменить источник обновлений, выберите **Изменить**.

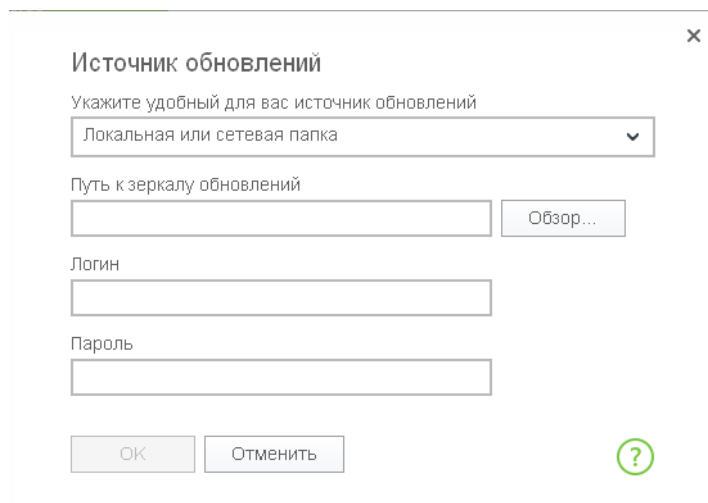


Доступны три варианта:

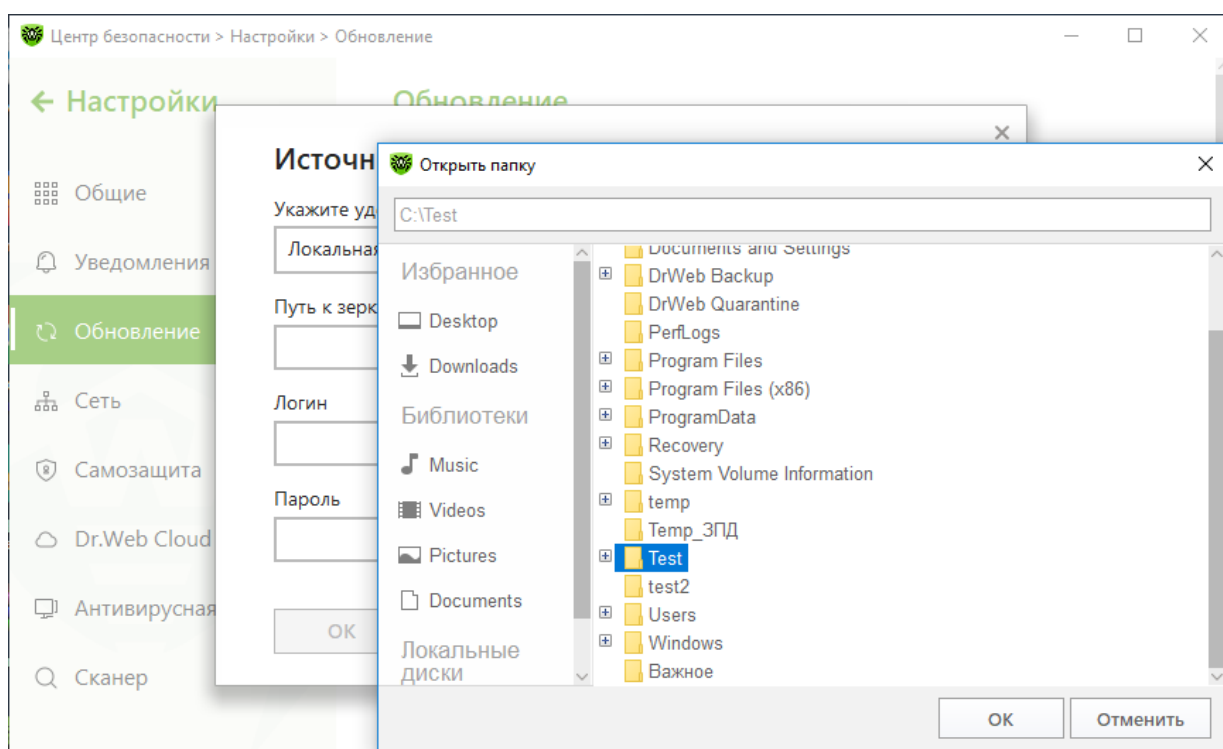


Если обновления не планируется получать с ВСО (серверов Всемирной системы обновлений компании «Доктор Веб»), можно указать локальный источник обновлений. Программа может получать обновления из локальной или сетевой папки. Для этого в выпадающем списке в качестве источника обновлений укажите вариант **Локальная или сетевая папка**.

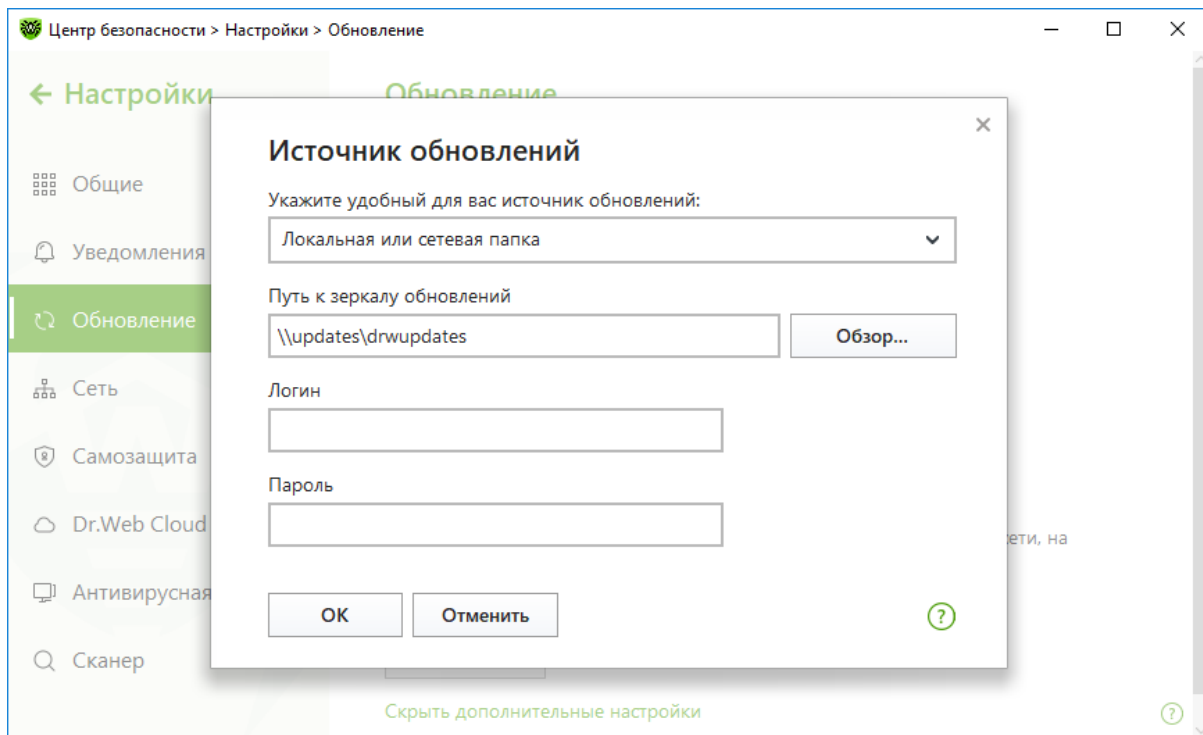
Если обновление выполняется из локальной папки, укажите ее адрес и параметры доступа к ней.



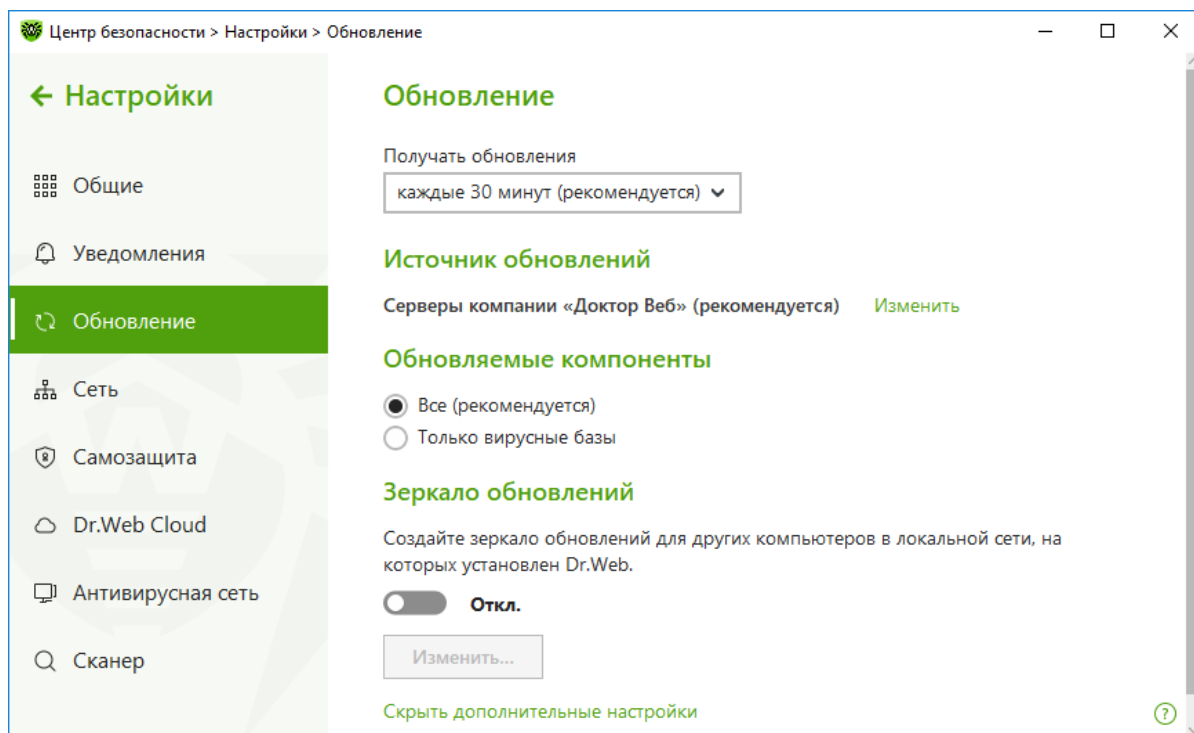
С помощью кнопки **Обзор** выберите место размещения источника обновления — папку или сетевой ресурс — и нажмите **ОК**. В поле **Путь** отобразится полный путь к папке с обновлениями:



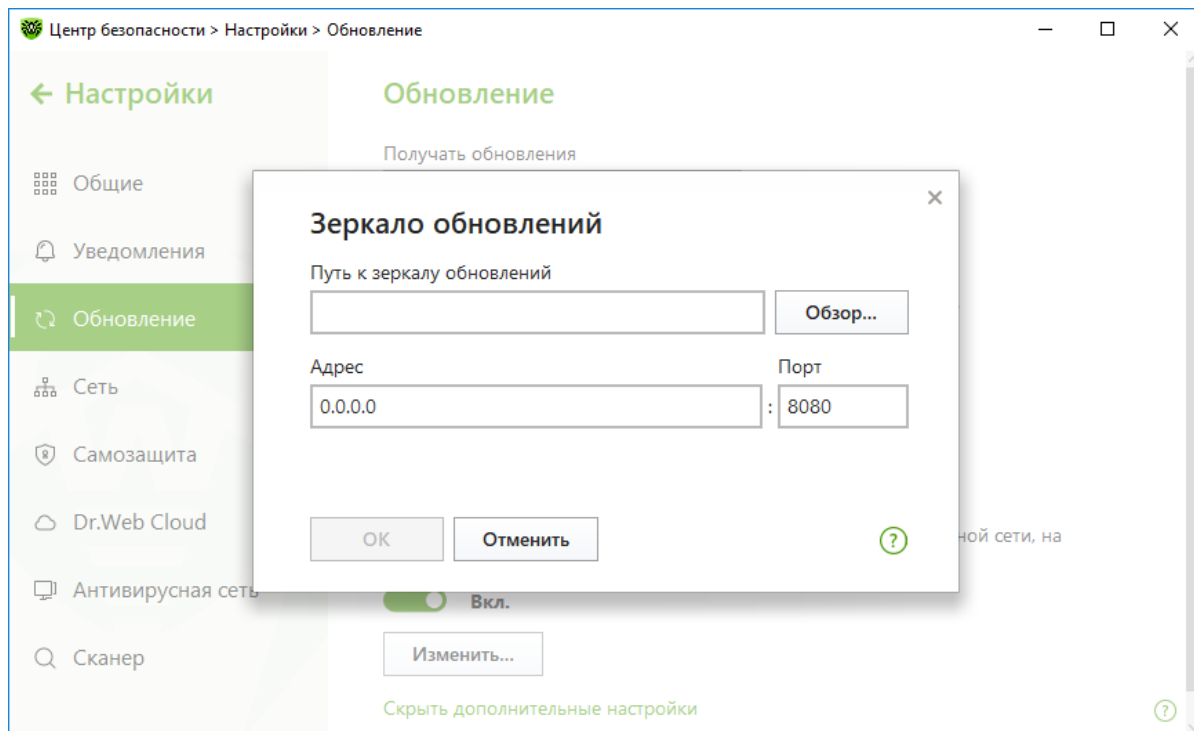
Источники обновления могут быть локальными и сетевыми. В случае нахождения источника обновления на разделяемом общем ресурсе задайте путь к папке в формате сетевых адресов.



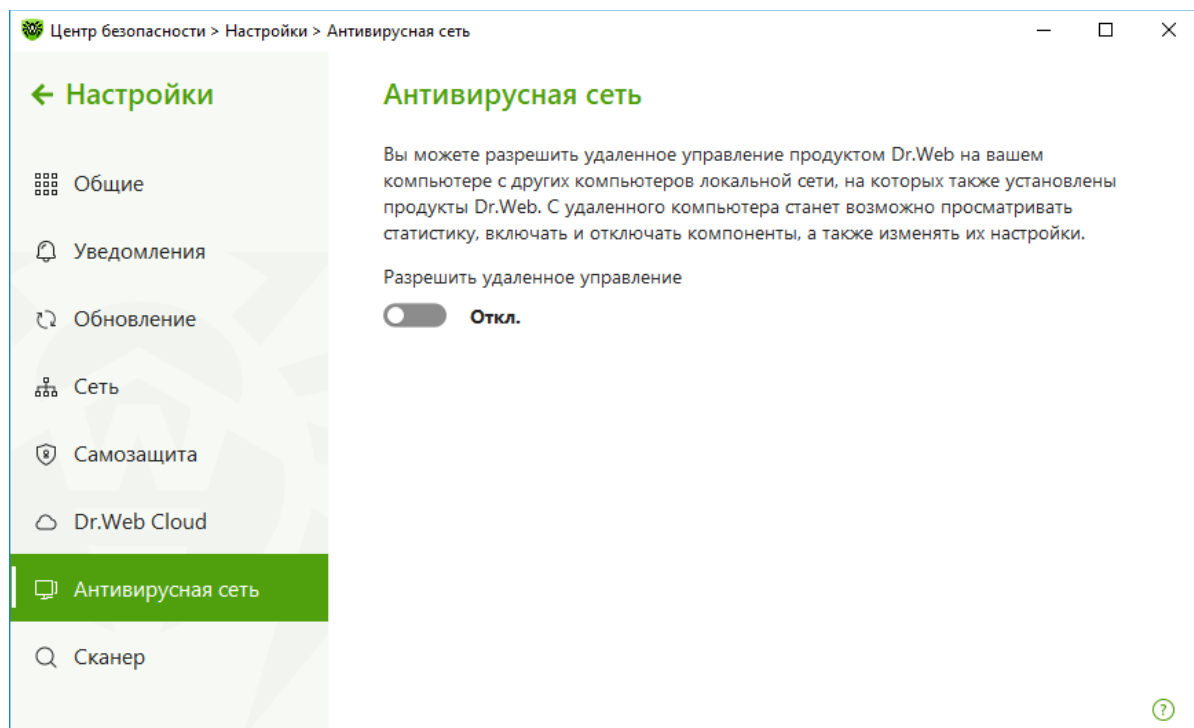
Если обновления в сети предполагается проводить с локально созданного зеркала, то можно задать параметры его создания. В окне **Обновления** щелкните на **Дополнительные настройки** и переместите выключатель **Зеркало обновлений**.



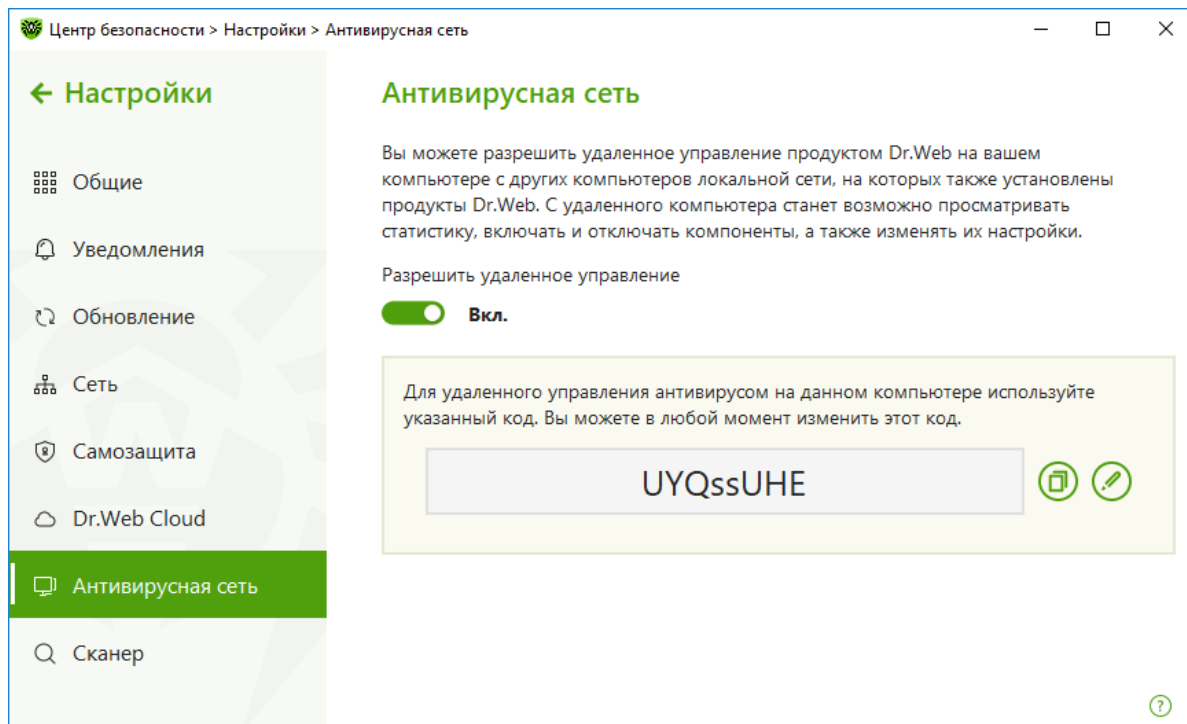
Нажмите **Изменить**.



При загрузке необходимых файлов с одного из компьютеров в сети на компьютере, с которого будет производиться обновление, включите поддержку удаленного управления по сети и функцию создания локального зеркала обновлений. В окне **Настройки** → **Основные** перейдите в пункт **Антивирусная сеть** и включите опцию **Разрешить удаленное управление**.



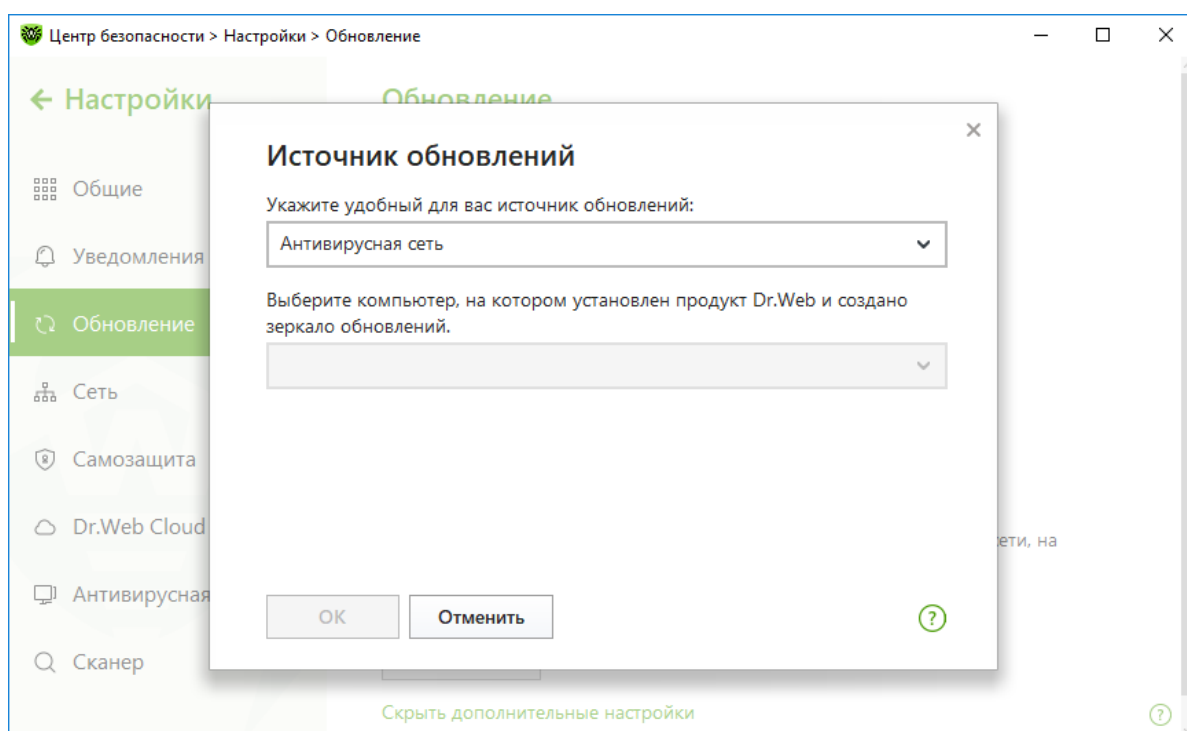
В открывшемся окне введите пароль, который будет использоваться для удаленного доступа к настройкам Dr.Web по сети, и нажмите **ОК**.



После определения параметров зеркала вернитесь в пункт **Обновление**. Нажмите **Изменить** и в окне **Зеркало обновлений** в поле **Путь** пропишите путь к предварительно созданной папке для загрузки обновлений. Эту папку также можно найти с помощью кнопки **Обзор**. Нажмите **ОК**.

Наведите курсор мыши на значок **Dr.Web** в системном трее, нажмите правую или левую клавишу мыши и выберите пункт **Обновление**. Начнется процесс обновления программы, в ходе которого будет создан локальный репозиторий.

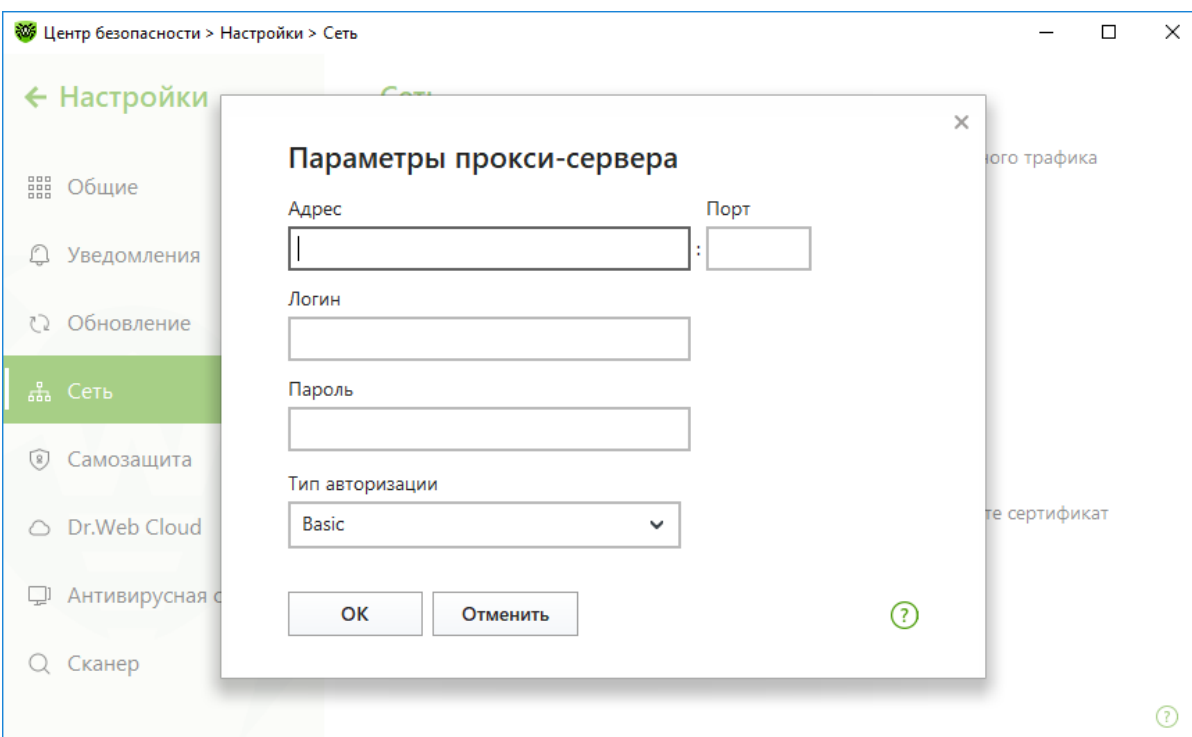
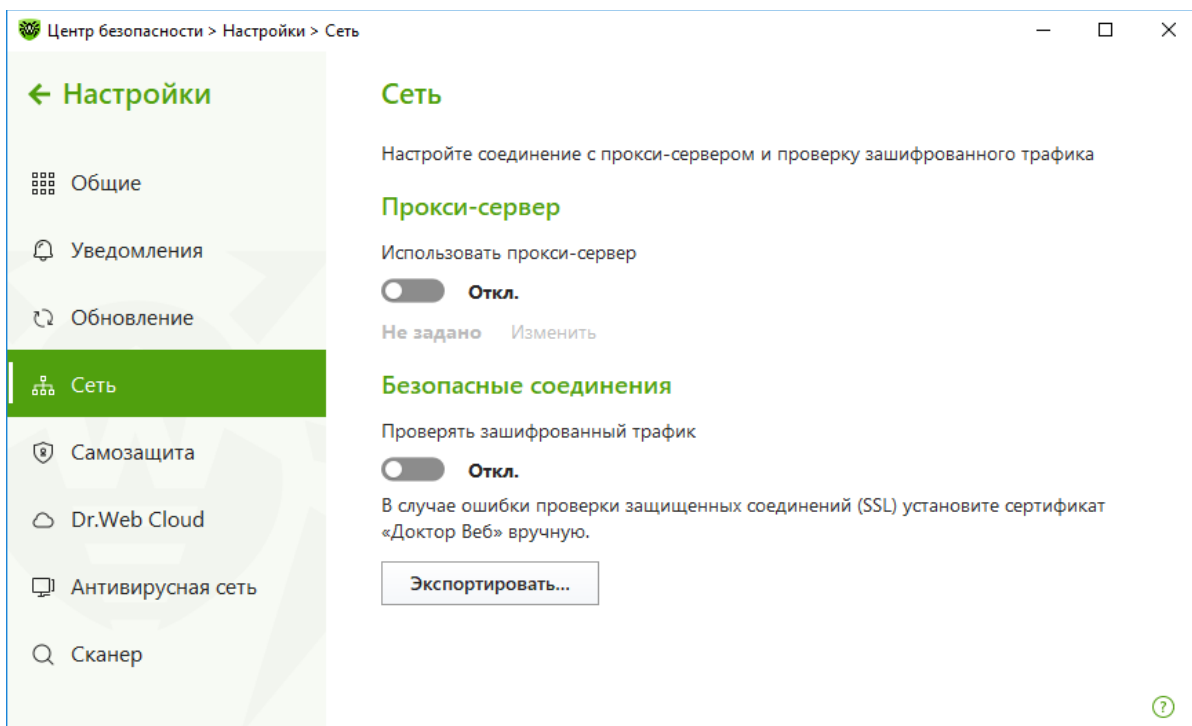
На всех компьютерах, которые должны получать обновления из компьютера — источника обновлений, сделайте следующие настройки. Перейдите в пункт **Обновление** и нажмите **Источник обновлений** → **Изменить**. В окне **Источник обновлений** отметьте опцию **Антивирусная сеть**. С помощью выпадающего списка выберите компьютер-источник.



Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Аналогичным образом следует поступить при обновлении с антивирусного сервера.

Также вы можете настроить параметры доступа к сети. Для этого в окне **Основные** выберите пункт **Сеть**, отметьте переключатель **Прокси-сервер** и нажмите **Изменить**.



- **Адрес** — укажите адрес прокси-сервера.
- **Порт** — укажите порт прокси-сервера.
- **Пользователь** — укажите имя учетной записи для подключения к прокси-серверу.
- **Пароль** — укажите пароль учетной записи, используемой для подключения к прокси-серверу.

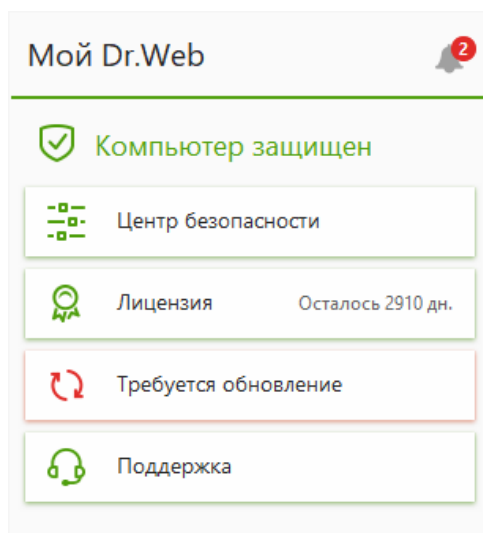
- **Тип авторизации** — выберите тип авторизации, требуемый для подключения к прокси-серверу.

Если не возникло проблем с подключением к Интернету, настройки на этой странице рекомендуется оставить без изменений.

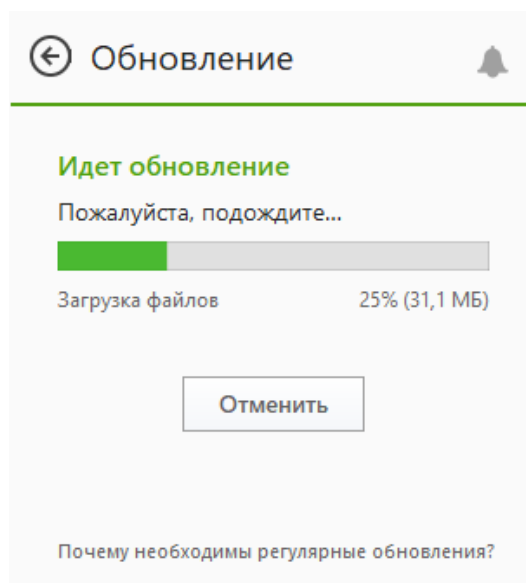
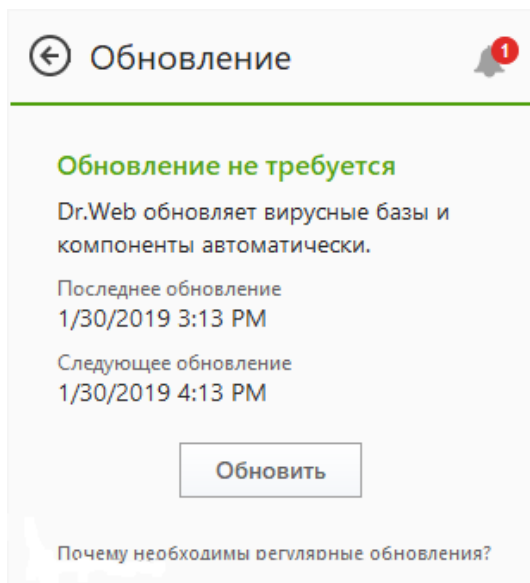
Чтобы провести обновление вручную или проверить статус обновлений, нажмите на значок



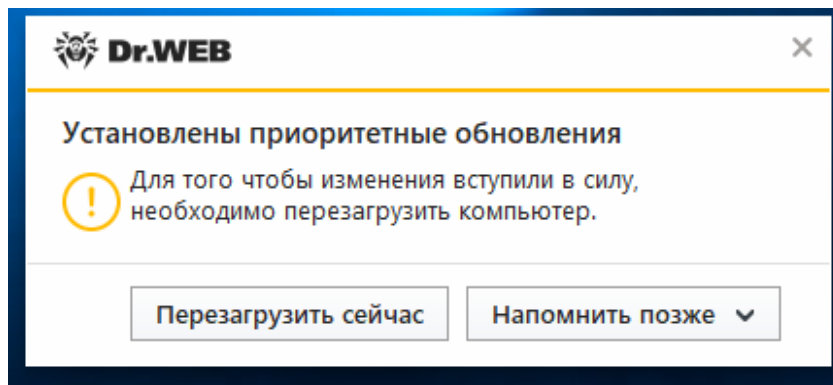
в системном меню, затем в открывшемся меню агента на кнопку



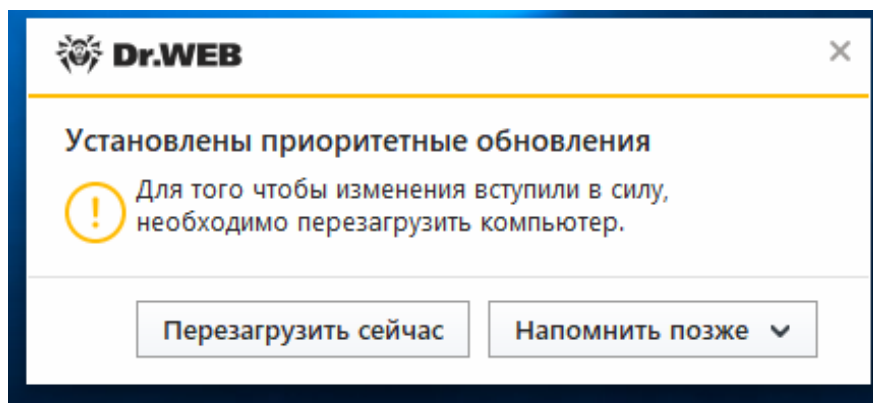
Для обновления вручную нажмите на кнопку **Обновить**.



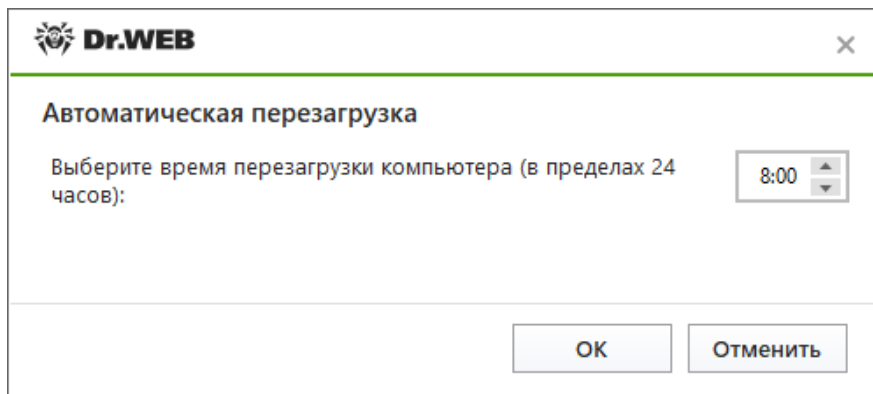
В том случае, если полученные обновления требуют для своей установки перезагрузки, будет показано окно, в котором вы сможете указать удобное время перезагрузки:



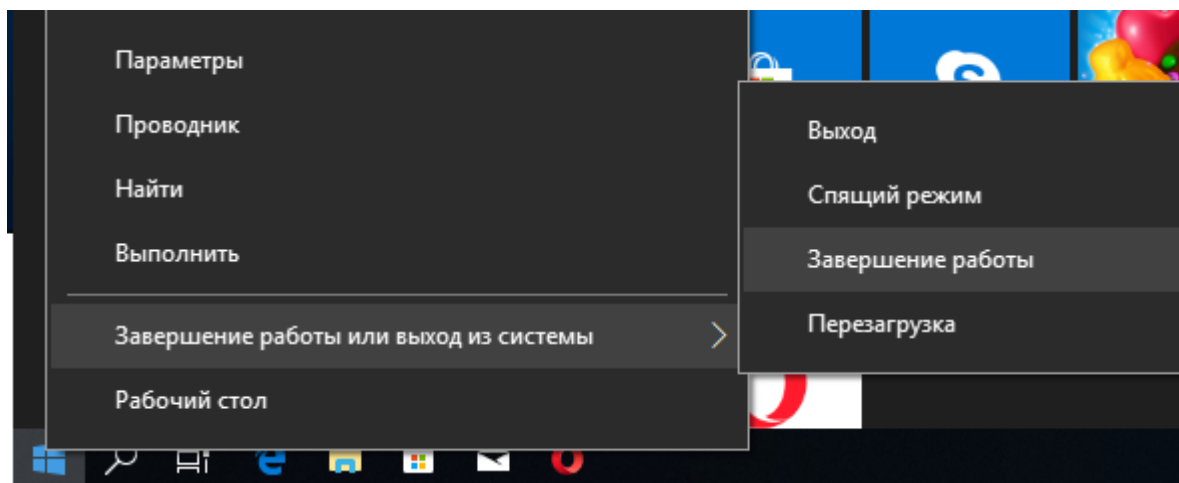
Пользователь может перезагрузиться немедленно — завершив все используемые приложения и нажав кнопку **Перезагрузить сейчас**, выбрать время следующего уведомления или назначить время перезагрузки. Для выполнения двух последних действий нажмите кнопку **Напомнить позже**.



Автоматическая перезагрузка может быть назначена в пределах ближайших 24 часов.



Также пользователь может перезагрузить систему самостоятельно. Например, выбрав последовательно **Пуск** → **Завершение работы** или **Выход из системы** → **Завершение работы** или **Перезагрузка**.



Внимание! Выбор перехода в сменный режим или смены учетной записи не приводит к перезагрузке системы и ее обновлению.

Внимание! Нажатие кнопки выключения планшета или ноутбука переводит его в спящий режим. Для применения обновлений перезагрузите его любым доступным способом, в том числе выбрав вариант перезагрузки в уведомлении антивируса.

8.7.1. Поисковый модуль Dr.Web

Поисковый модуль Dr.Web (файл drweb32.dll) является одним из основных модулей антивируса Dr.Web.

Этот компонент служит для обнаружения наличия в сканируемом объекте инфекции.

Поисковый модуль использует вирусные базы, расположенные в файлах с расширением *.vdb, которые автоматически обновляются в соответствии с текущими настройками компонентов антивируса. Вирусные базы являются неотъемлемой частью поискового модуля. Помимо записей для обнаружения инфекций, в вирусных базах Dr.Web могут содержаться процедуры, отвечающие за функции непосредственно поискового модуля, например некоторые функции эвристического анализатора.

Подробно о структуре и частоте выпуска обновлений вирусной базы Dr.Web можно прочитать в документации на антивирусный комплекс.

Поисковый модуль используют многие компоненты Dr.Web, а именно: сканеры, сторожи **SpIDer Guard** и **SpIDer Mail**. Это позволяет этим компонентам использовать одинаковые алгоритмы поиска вирусов. Более того, этот же самый поисковый модуль используется в версиях антивируса Dr.Web для операционных систем, отличных от Windows.

Взаимодействие компонентов антивируса Dr.Web с поисковым модулем происходит следующим образом.

1. Поисковый модуль производит первичное сканирование, при котором изучается общая структура сканируемого файла: упакован он или нет, является ли файловым контейнером или файловым архивом, производится сканирование контейнера или файлового архива как единого объекта. Если на этом этапе обнаруживается инфекция, то результаты сканирования возвращаются компоненту Dr.Web и сканирование заканчивается.
2. Если инфекция не обнаружена и если файл является контейнером или файловым архивом, то поисковый модуль возвращает компоненту название контейнера или файлового архива для записи их в файл отчета компонента.
3. Для составных объектов (файловых контейнеров и файловых архивов) последовательно распаковываются и сканируются вложенные объекты.

4. Если какой-то файл был вылечен, то процедура сканирования файла начинается сначала, т. к. существуют случаи многократного заражения файлов различными вирусами или одним и тем же вирусом.

Поисковый модуль может обновляться внутри одной и той же версии Dr.Web, таким образом возможно динамически добавлять проверку содержимого новых типов архивов и исполняемых файлов, сжатых новыми упаковщиками.

В поисковом модуле Dr.Web реализован эвристический анализатор для определения неизвестных вирусов по косвенным признакам. Так, в поисковом модуле реализованы алгоритмы для следующих типов неизвестных вирусов:

- COM — вирус, заражающий com-файлы (MS-DOS);
- EXE — вирус, заражающий exe-файлы (MS-DOS);
- TSR — резидентный вирус (MS-DOS);
- WIN.EXE — вирус, заражающий exe-файлы (Windows: NE, PE и т. д.);
- MACRO — вирус, заражающий документы Microsoft Office;
- BOOT — вирус, заражающий загрузочные секторы дисков;
- CRYPT — зашифрованный или полиморфный вирус;
- SCRIPT — вирус, содержащийся в скрипте;
- BATCH — вирус, содержащийся в командном файле;
- IRC — вирус, поражающий программы немедленного обмена сообщениями;
- DLOADER — неизвестная модификация вируса типа Trojan.DownLoader.xxx;
- MULDROP — неизвестная модификация вируса типа Trojan.MulDrop.xxx;
- STPAGE — неизвестная модификация вируса типа Trojan.StartPage.xxx;
- BACKDOOR — неизвестная модификация вируса типа BackDoor.xxx;
- PWS — неизвестная модификация вируса типа Trojan.PWS.xxx;
- WORM и MAIL.WORM — почтовые черви;
- прочее.

Данный список не претендует на полноту.

В большинстве случаев отключать эвристический анализатор не рекомендуется, т. к. часто с помощью эвристического анализа можно обнаружить новые вирусы или модификации уже известных вредоносных программ. Отправьте подозрительный файл на анализ в антивирусную лабораторию ООО «Доктор Веб», после чего новый вирус будет в кратчайшие сроки добавлен в вирусную базу.

Отключение данной настройки можно рекомендовать лишь в том случае, когда было обнаружено ложное срабатывание на определенный тип файлов. После корректировки вирусной базы настройку рекомендуется включить и повторить сканирование.

Начиная с версии Dr.Web 4.44 в состав эвристического анализатора встроена технология Origins Tracing, которая основана на поиске вредоносных программ, некоторым образом похожих на программы, записи о которых уже имеются в вирусных базах Dr.Web. При обновлении вирусных баз Dr.Web технология Origins Tracing использует сразу же новые вирусные записи в качестве отправных точек для нахождения сходства. Данная технология практически не имеет ложных срабатываний. Все вредоносные файлы, найденные с помощью технологии Origins Tracing, считаются неизлечимыми, к ним применяются действия,

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

соответствующие настройкам для неизлечимых объектов. В наименовании найденных с помощью данной технологии вирусов используется суффикс .origin. Хотя данная технология является частью несигнатурного анализа антивируса Dr.Web, файлы, обнаруженные с помощью этой технологии, не следует отправлять на анализ в вирусную лабораторию, т. к. в компонентах антивируса Dr.Web данная технология по весу приравнена к сигнатурному анализу. Исключения составляют файлы, обнаруженные с помощью этой технологии и являющиеся заведомо чистыми. Данные файлы следует отправлять на анализ в вирусную лабораторию с целью устранения ложного срабатывания.

Начиная с версии Dr.Web 5.0 в состав эвристического анализатора встроен универсальный распаковщик FLY-CODE. Данная технология позволяет распаковать файлы, упакованные неизвестными Dr.Web упаковщиками, и на основе специальных записей вирусной базы делать предположение о наличии опасного кода. Универсальный распаковщик FLY-CODE является эффективным средством против использования вирусомисателями полиморфных (постоянно видоизменяющихся) упаковщиков.

В поисковом модуле Dr.Web реализована поддержка распаковки различных архивов. Это дает возможность проверять содержимое большинства архивов на наличие инфекций.

Следует помнить, что лечение, удаление, переименование и перемещение объектов, находящихся внутри архивов, невозможно. Если нужно проделать одну из этих операций, предварительно распакуйте соответствующие файлы из архива во временную папку, а после проведения необходимых действий запакуйте обратно.

Без специальной настройки в конфигурационном файле удаление архива целиком тоже невозможно.

В настоящее время поддерживаются архиваторы: ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP.

Также поддерживаются следующие типы самораспаковывающихся архивов: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy.

Также поддерживаются следующие типы инсталляторов: Agentix Installer, Agency SFX, Commodore, FilePacker, File2Pack SFX, SFXFactory (ZIP-SFX), Stardust Setup Package и некоторые другие.

В поисковом модуле Dr.Web реализована проверка файлов почтовых форматов.

Поддерживается проверка писем, соответствующих формату ARPA Internet Text Messages (RFC822), в том числе с расширениями MIME, в кодировке форматов UUENCODE, BASE64, Quoted Printable.

Поддерживаются открытые форматы почтовых архивов, создаваемые почтовыми программами Mozilla, Netscape, The Bat! и др.

Не поддерживаются форматы почтовых архивов, созданных в программах Microsoft Outlook, Microsoft Outlook Express и других проприетарных форматов.

В поисковом модуле Dr.Web реализована поддержка файловых контейнеров следующих форматов: 1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM.

При настройке модулей антивируса Dr.Web следует различать файловые контейнеры и файловые архивы. Например, нельзя отключить проверку файловых контейнеров, но можно при необходимости отключить проверку файловых архивов.

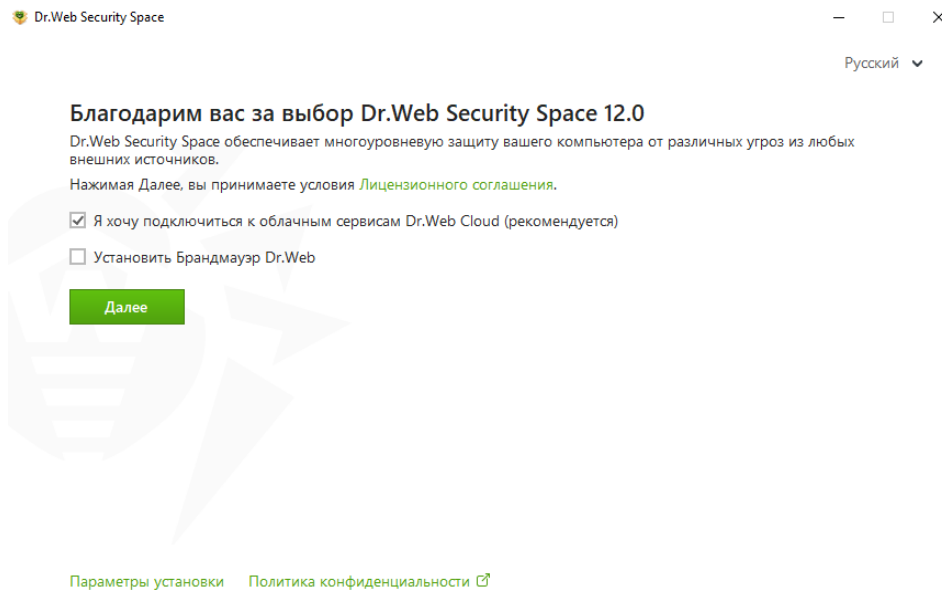
В поисковом модуле Dr.Web реализована поддержка большинства известных программ сжатия исполняемых файлов, среди которых ASPACK, UPX, FSG, MORPHINE, YODA и многие
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию



другие.

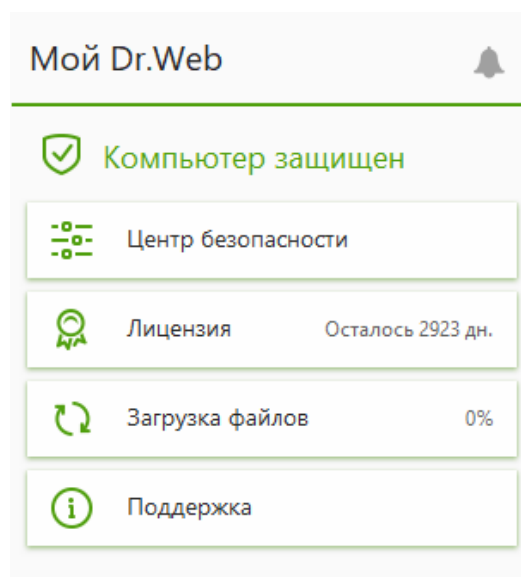
Не все из этих программ служат только для уменьшения объема файлов. Некоторые из них созданы, например, для защиты программ от взлома, другие — для затруднения детектирования вирусов.

8.8. Настройка компонента Dr.Web Cloud

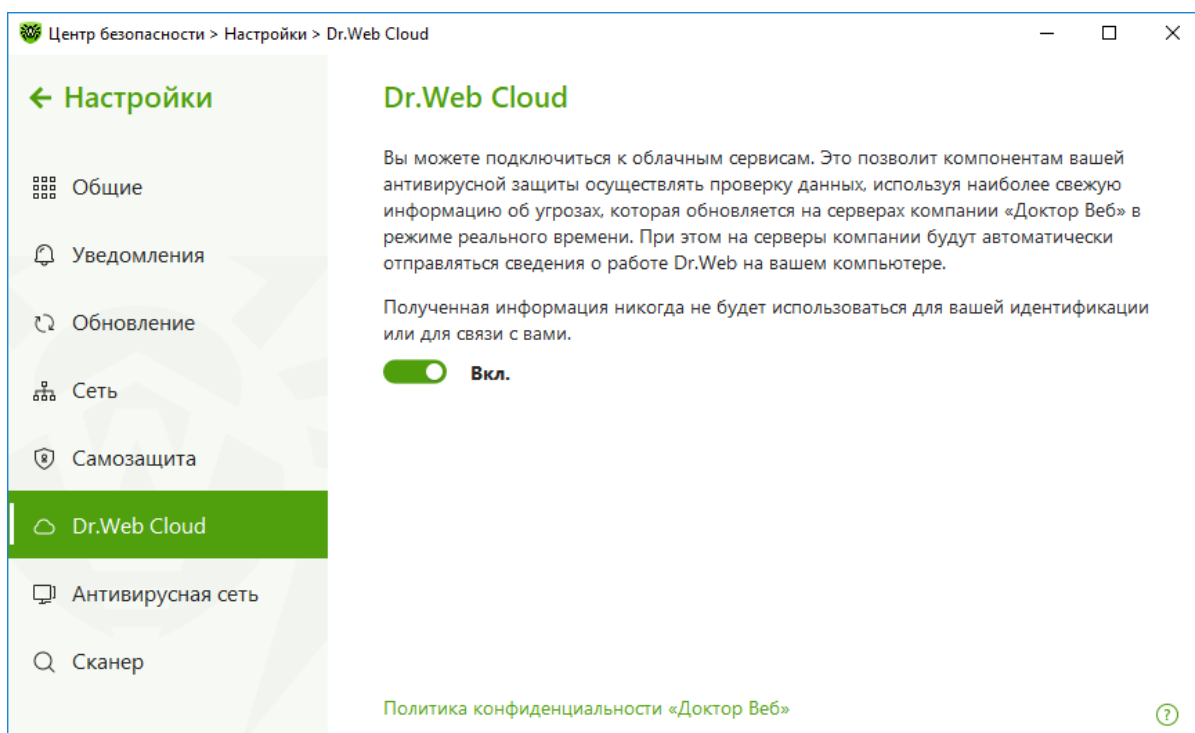
Использование компонента Dr.Web Cloud предлагается уже в процессе инсталляции продукта Dr.Web Security Space. Для работы компонента достаточно оставить по умолчанию значение параметра **Я хочу подключиться к облачным сервисам Dr.Web Cloud**. После завершения установки запрос репутации для каждого проверяемого объекта будет происходить автоматически и практически не требует расхода ресурсов защищаемого компьютера.



Если в ходе инсталляции компонент Dr.Web Cloud не был включен, кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне последовательно нажмите на  (Режим администратора) (значок изменит вид на ) и ставший зеленым значок  в правом верхнем углу окна.



В открывшемся окне **Настройки** выберите пункт меню **Основные** → **Dr.Web Cloud**.



В открывшемся окне передвиньте переключатель в положение **Вкл.**


8.9. Настройка параметров Dr.Web Security Space, обеспечивающих обнаружение ранее неизвестных вредоносных файлов

Обнаружение еще неизвестных представителей семейства Trojan.Encoder обеспечивается модулем **Превентивной защиты**, контролирующим попытки злоумышленников выполнить нужное им действие, а также поведенческим анализатором, «на лету» сравнивающим поведение запускаемых программ с поведением троянцев-шифровальщиков.



При подсоединении нового носителя информации (съёмного устройства) в современных операционных системах по умолчанию срабатывает система автозапуска. Она сканирует содержимое носителя и предлагает пользователю список возможных действий. Существует целый ряд вредоносных программ, загружающихся в память ПК при установке в привод инфицированного диска или флеш-накопителя. Чтобы предотвратить активацию таких вирусов, запретите автозапуск со всех съёмных носителей с помощью возможностей **Превентивной защиты**.

Обнаружение ранее неизвестных вредоносных программ обеспечивается модулем фоновой проверки запущенных процессов, а также проведением периодической антивирусной проверки.

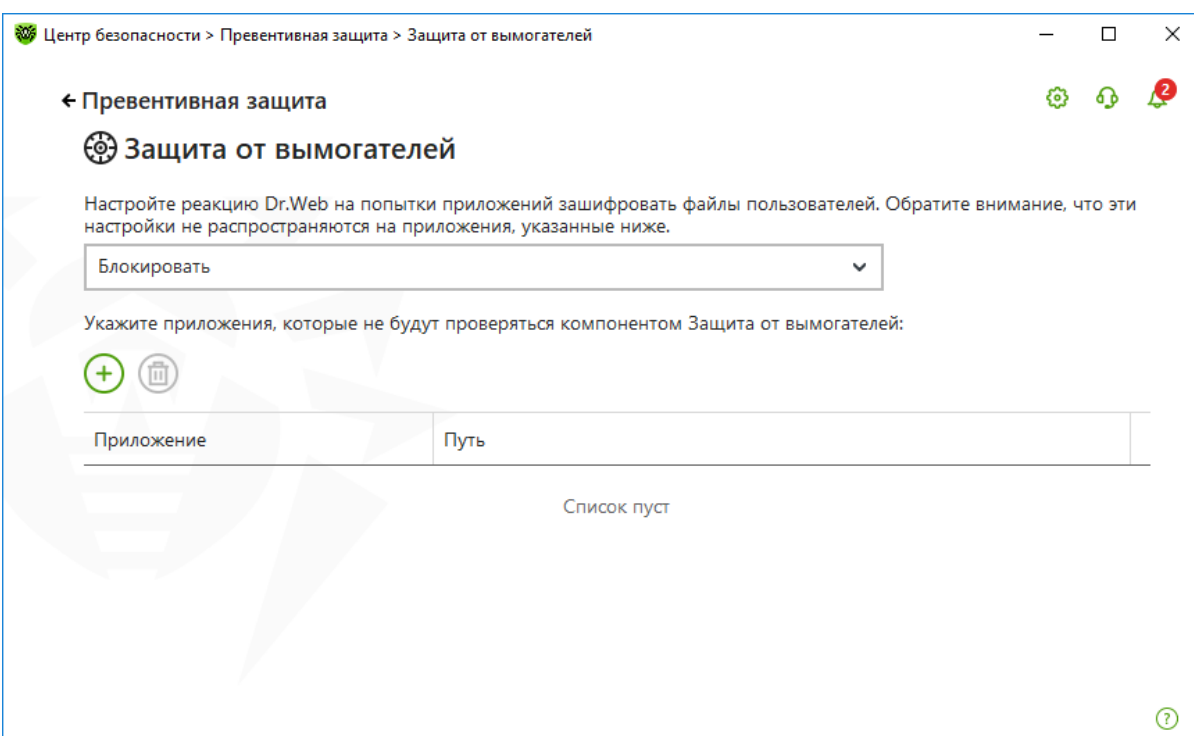
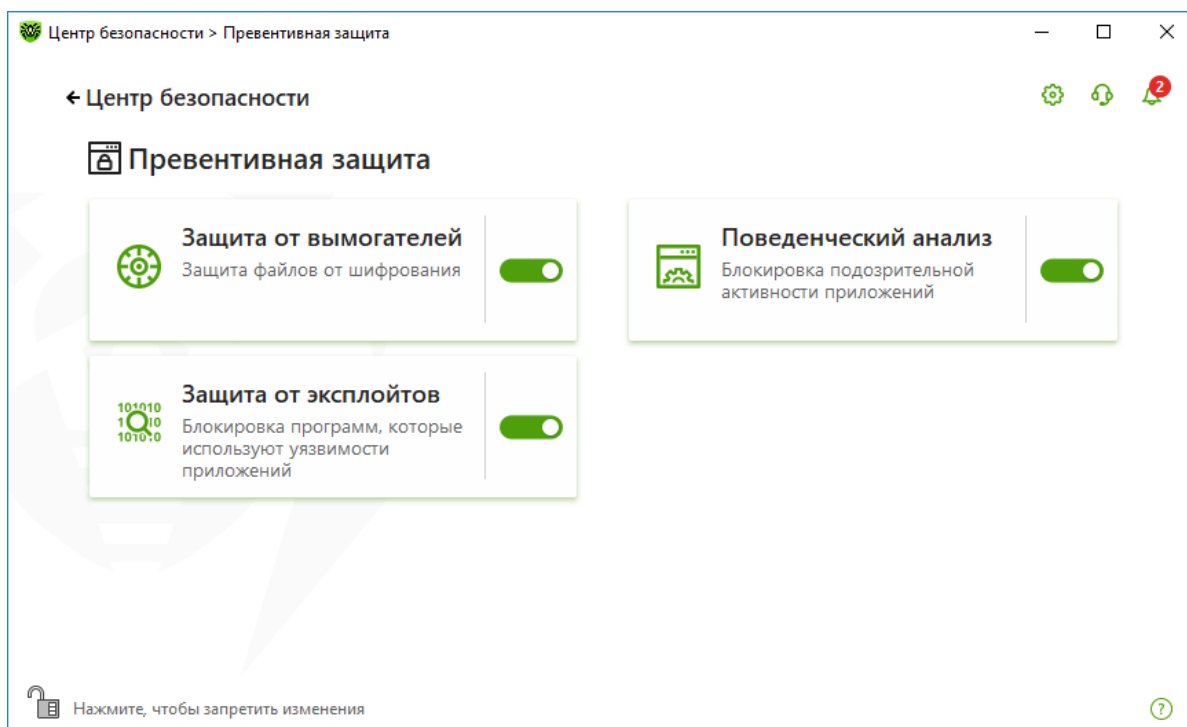
Подсистема фоновое сканирование и нейтрализации активных угроз реализована в рамках Антируткита **Dr.Web Shield**. Данная подсистема постоянно находится в памяти и осуществляет поиск активных угроз в следующих критических областях Windows: объекты автозагрузки, запущенные процессы и модули, эвристики системных объектов, оперативная память, MBR/VBR дисков, системный BIOS компьютера. При обнаружении угроз данная подсистема может оповещать об опасности пользователя, осуществлять лечение и блокировать опасные воздействия.

Для настройки параметров **Превентивной защиты** кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

открывшемся окне нажмите на  (Режим администратора) (значок изменит вид на ).


В окне **Центр безопасности** выберите **Превентивная защита** и далее **Защита от вымогателей**.

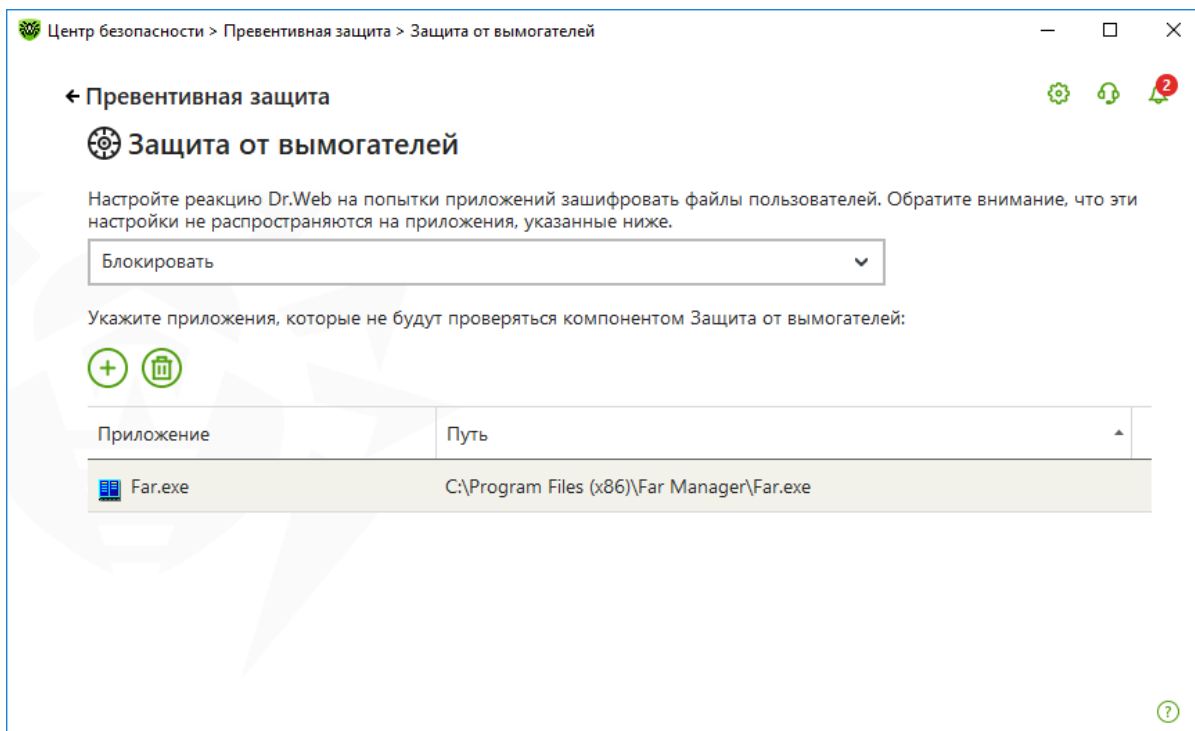


Внимание! Крайне не рекомендуется выключать данный компонент, так как многочисленные ошибки в коде троянцев-вымогателей часто повреждают файлы пользователей без возможности их восстановления.

Защита от вымогателей действует на основе правил, описывающих действия, характерные для вредоносных программ, что позволяет эффективно обнаруживать угрозы, неизвестные вирусной базе.

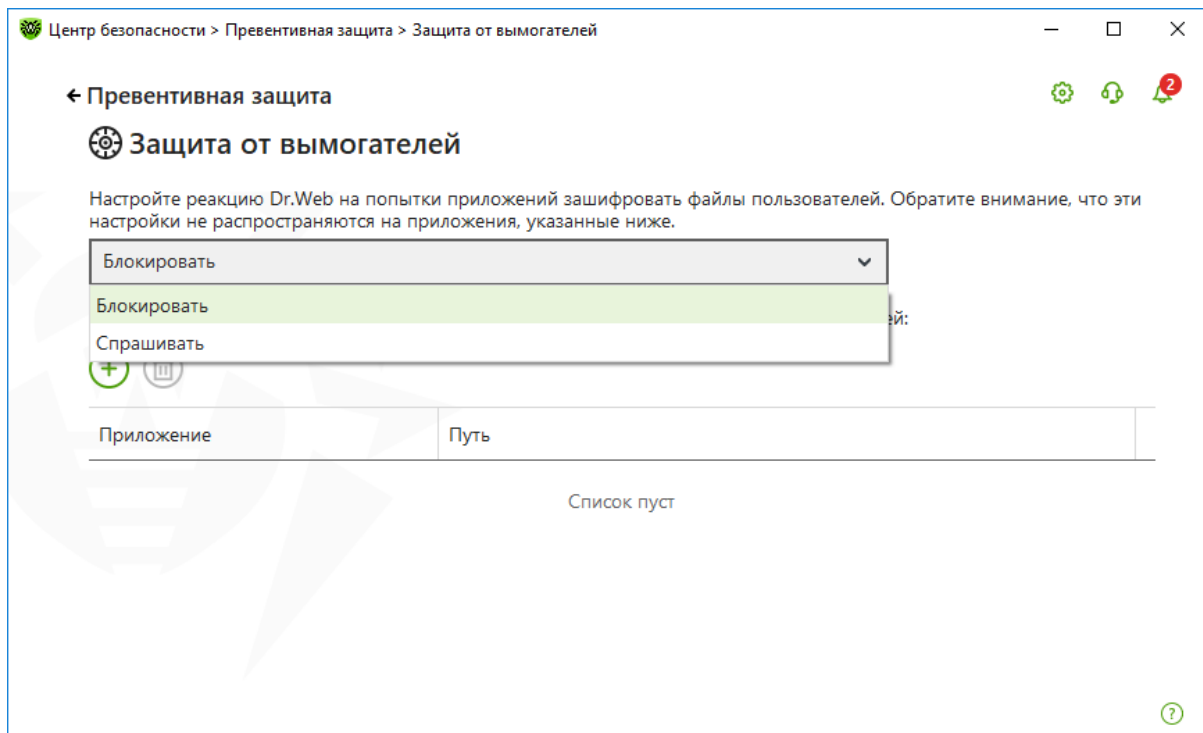
Dr.Web® Security Space. Руководство по быстрой установке и разворачиванию

В том случае, если вам необходимо дать полный доступ к вашим данным используемым вами программам, добавьте их в список доверенных приложений. Для этого нажмите  и в открывшемся окне выберите программу для включения в список.

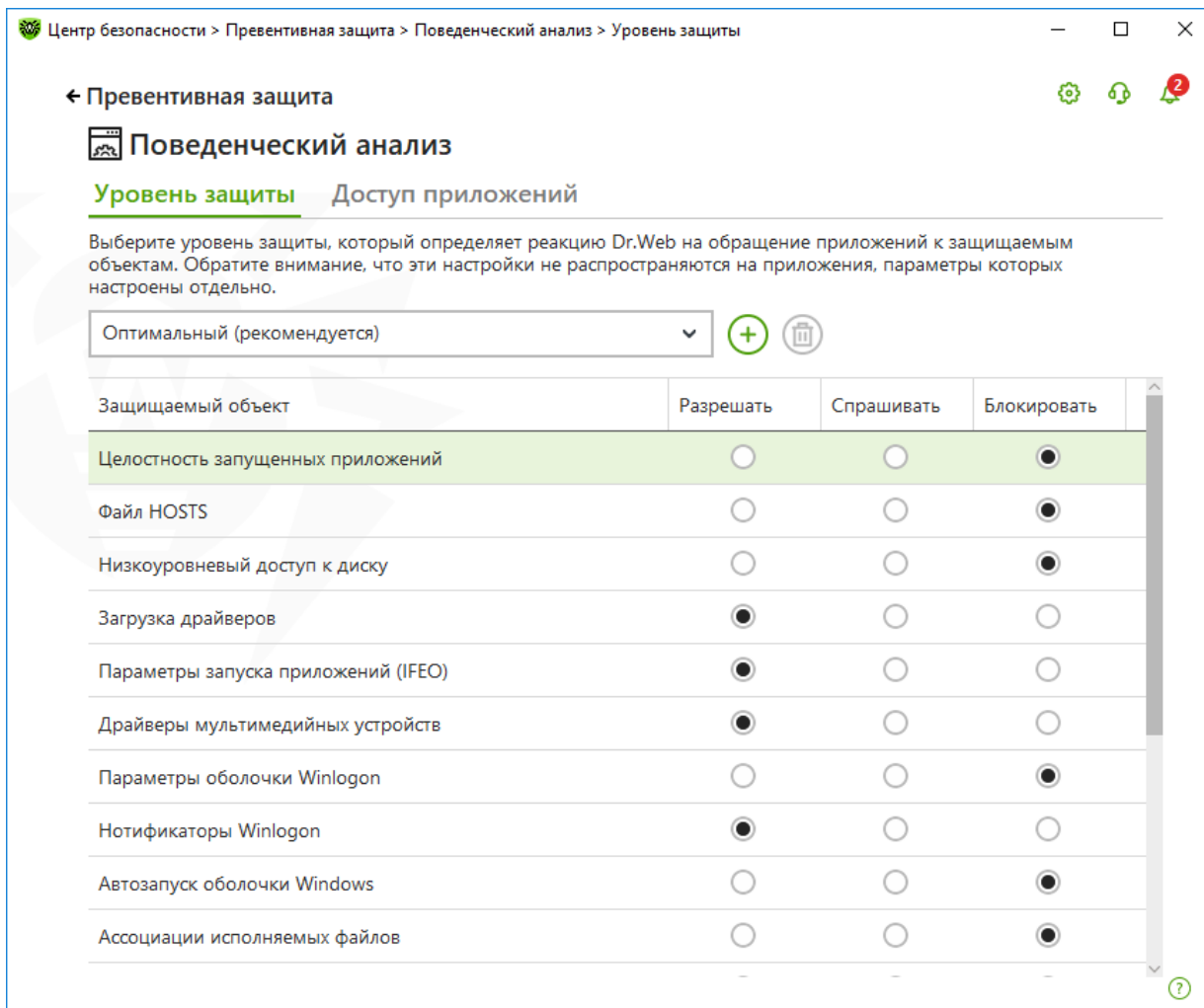


Внимание! Злоумышленники создают вредоносные приложения, имитирующие действия известных программ, или встраивают свой код в имеющиеся приложения. Известны случаи размещения взломанных приложений даже на сайтах их создателей. Поэтому крайне не рекомендуется давать полный доступ к данным без консультации с технической поддержкой Dr.Web.

Защита от вымогателей включена в Dr.Web с реакцией **Блокировать**. Вы можете изменить реакцию на **Спрашивать**. Будьте внимательны! В этом случае при каждом срабатывании системы защиты вам потребуется самостоятельно принять решение о том, является ли программа, обратившаяся к вашему файлу, вредоносной или нет.



Чтобы настроить реакцию антивируса на действия сторонних приложений, которые могут привести к заражению вашего компьютера, вернитесь в окно **Превентивная защита** и, выбрав **Поведенческий анализ**, установите необходимый уровень блокировки подозрительных действий.



Настройка данных параметров Preventивной защиты позволяет держать под контролем все попытки изменения критических областей Windows. В частности, настройки Preventивной защиты не должны позволять внедрение эксплойтов в работающие приложения.

- **Файл HOSTS**

Этот файл позволяет определить соответствие между доменным именем хоста и его IP-адресом. Приоритет обработки файла HOSTS выше, чем приоритет обращения к DNS-серверу.

Файл HOSTS позволяет злоумышленникам блокировать доступ к сайтам антивирусных компаний и перенаправлять пользователей на поддельные сайты.

Preventивная защита Dr.Web не дает возможность вредоносным программам вносить изменения в файл HOSTS и перенаправлять пользователей на фишинговые ресурсы.

- **Целостность запущенных приложений**

Процесс — это набор ресурсов и данных, которые находятся в оперативной памяти компьютера. Процесс, принадлежащий одной программе, не должен изменять процесс другой программы. Но вредоносные программы, например Trojan.Encoder.686 (CTB-Locker), нарушают это правило.

- **Низкоуровневый доступ к диску**

При штатной работе операционной системы Windows доступ к файлам происходит путем обращения к файловой системе, которая подконтрольна ОС. Троянцы-буткиты,

изменяющие загрузочные области диска, обращаются к диску напрямую, минуя файловую систему Windows — обращаясь к определенным секторам диска.

Внедрение троянца в загрузочную область существенно затрудняет как его обнаружение, так и процесс обезвреживания.

Превентивная защита Dr.Web блокирует возможность изменения вредоносными программами загрузочных областей диска и предотвращает запуск троянцев на компьютере.

- **Загрузка драйверов**

Многие руткиты скрытно запускают свои драйверы и службы для маскировки своего присутствия на компьютере и выполнения несанкционированных пользователем действий, например отправки логинов и паролей, а также иных идентификационных сведений злоумышленникам.

Превентивная защита Dr.Web не дает возможности загрузки новых или неизвестных драйверов без ведома пользователя.

- **Параметры запуска приложений**

В реестре ОС Windows существует ключ (entry) Image File Execution Options, с помощью которого для любого приложения Windows можно назначить отладчик — программу, которая помогает программисту в отладке написанного кода, в том числе позволяя модифицировать данные отлаживаемого процесса. С помощью данного ключа вредоносное ПО, будучи назначенным отладчиком какого-нибудь системного процесса или приложения (например, того же Internet Explorer или проводника), получает полный доступ к тому, что интересует злоумышленников.

Превентивная защита Dr.Web блокирует доступ к ключу реестра Image File Execution Options. Реальной необходимости отлаживать приложения «на лету» у обычных пользователей нет, а риск от использования ключа Image File Execution Options вредоносными программами очень высок.

- **Драйверы мультимедийных устройств**

Известны некоторые вредоносные программы, которые создают исполняемые файлы и регистрируют их как виртуальные устройства.

Превентивная защита Dr.Web блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможным установку нового виртуального устройства.

- **Параметры оболочки Winlogon, нотификаторы Winlogon**

Интерфейс Winlogon notification package реализует возможность обрабатывать события, назначаемые на вход и выход пользователей, включение и выключение операционной системы, и некоторые другие. Вредоносные программы, получив доступ к Winlogon notification package, могут перезагружать ОС, выключать компьютер, препятствовать входу пользователей в рабочую среду ОС. Так поступают, например, Trojan.Winlock.3020, Trojan.Winlock.6412.

Превентивная защита Dr.Web запрещает изменение веток реестра, отвечающих за Winlogon notification package, и не дает вредоносным программам возможности добавлять исполнение новых задач, нужных злоумышленникам, в логику работы операционной системы.

- **Автозапуск оболочки Windows**

Опция блокирует сразу несколько параметров в реестре Windows в ветке [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows]: например, AppInit_DLLs (заставляет Windows загружать указанные DLL каждый раз, когда запускается какая-либо программа), AppInit_DLLs (может использоваться для внедрения руткита в Windows), Run (необходим для запуска программ в минимизированном виде после запуска операционной системы), IconServiceLib (отвечает за загрузку библиотеки IconCodecService.dll, которая необходима для нормального отображения рабочего стола и значков на экране).

Превентивная защита Dr.Web блокирует ряд параметров в реестре Windows, например, запрещая вирусам изменить нормальное отображение Рабочего стола или не позволяя руткиту скрыть присутствие троянца в системе.

- **Ассоциации исполняемых файлов**

Некоторые вредоносные программы нарушают ассоциации исполняемых файлов, в результате чего программы не запускаются — или вместо нужной пользователю программы запускается программа, назначенная вредоносным ПО.

Превентивная защита Dr.Web не позволяет вредоносному ПО изменить правила запуска программ.

- **Политики ограничения запуска программ (SRP)**

В Windows можно настроить систему ограничения запуска программ (SRP) таким образом, чтобы разрешить запуск программ только из определенных папок (например, ProgrammFiles) и запретить выполнение программ из прочих источников. Блокировка ветки реестра, отвечающей за настройку политик SRP, запрещает вносить изменения в уже настроенные политики, таким образом усиливая уже реализованную защиту.

Превентивная защита Dr.Web позволяет защитить систему от вредоносного ПО, попадающего на компьютер через почту и съемные носители — и запускающегося, например, из временного каталога. Опция рекомендуется к использованию в корпоративной среде.

- **Плагины Internet Explorer (ВНО)**

С помощью данной настройки можно запретить установку новых плагинов для Internet Explorer путем блокирования соответствующей ветки реестра.

Превентивная защита Dr.Web защищает браузер от вредоносных плагинов, например от блокировщиков браузера.

- **Автозапуск программ**

Запрещает изменение нескольких веток реестра, ответственных за автозапуск приложений.

Превентивная защита Dr.Web позволяет предотвратить автозапуск вредоносных программ, не давая им зарегистрироваться в реестре для последующего запуска.

- **Автозапуск политик**

Опция блокирует ветку реестра, с помощью которой можно запустить любую программу при входе пользователя в систему.

Превентивная защита Dr.Web позволяет предотвратить автозапуск определенных программ, например анти-антивирусов.

- **Конфигурация безопасного режима**

Некоторые троянцы отключают безопасный режим Windows для затруднения лечения компьютера.

Превентивная защита Dr.Web предотвращает отключение безопасного режима путем блокировки изменения реестра.

- **Параметры менеджера сессий**

Опция защищает параметры диспетчера сеансов Windows — системы, от которой зависит стабильность работы операционной системы. При отсутствии такой блокировки вредоносные программы получают возможность инициализации переменных окружения, запуска ряда системных процессов, выполнения операций по удалению, перемещению или копированию файлов до полной загрузки системы и т. п.

Превентивная защита Dr.Web защищает операционную систему от внедрения вредоносных программ, их запуска до полной загрузки операционной системы — и, следовательно, до завершения запуска антивируса.

- **Системные службы**

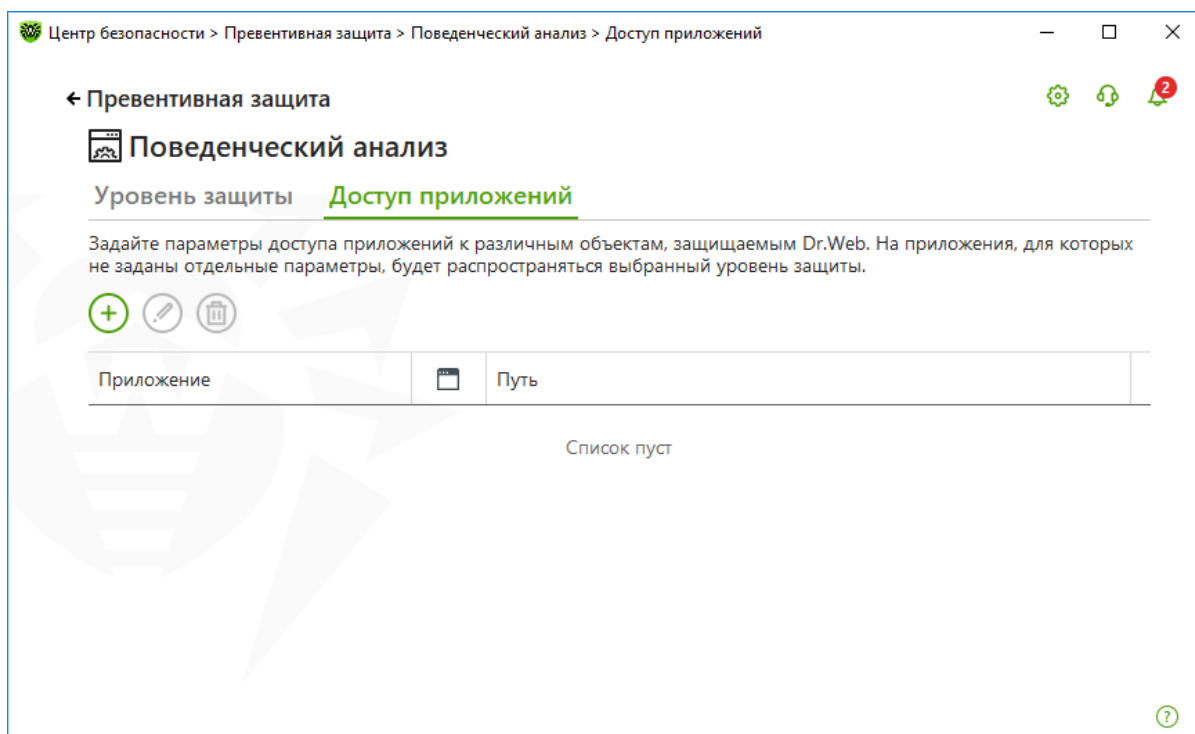
Опция защищает изменение параметров реестра, отвечающих за нормальную работу системных служб.

Некоторые вирусы могут блокировать редактор реестра, затрудняя нормальную работу пользователя. Например, очищают Рабочий стол от ярлыков установленных программ или не дают перемещать файлы.


Превентивная защита Dr.Web не позволяет вредоносному ПО нарушить нормальную работу системных служб, например вмешаться в штатное создание резервных копий файлов.

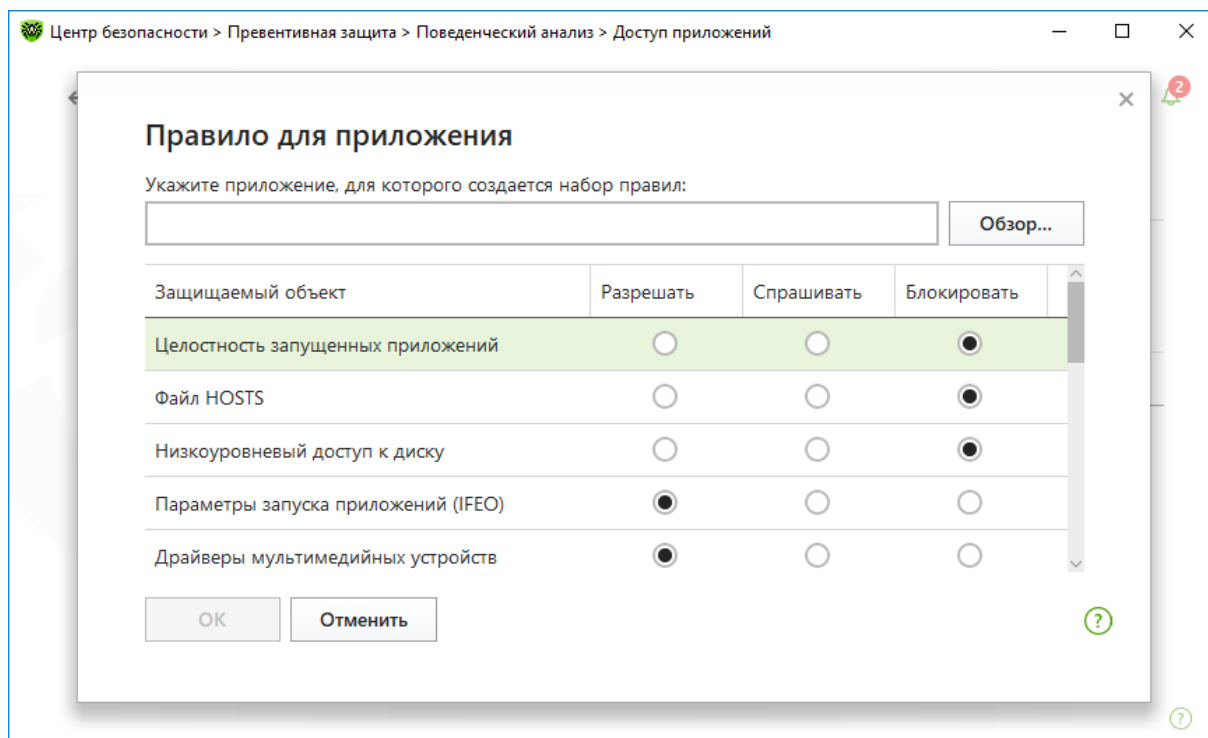
Статус **Разрешать** позволяет пользователям и злоумышленникам вносить изменения в соответствующие ресурсы.

Перейдя на закладку **Доступ приложений**, вы можете задать ограничения для доступа к системе для конкретных программ, установленных у вас на компьютере.



Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Для этого нажмите , в открывшемся окне выберите программу и настройте ограничения для нее.




В режиме работы **Оптимальный**, установленном по умолчанию, запрещается автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему. Также запрещается низкоуровневый доступ к диску для защиты системы от заражения буткитами и троянками-блокировщиками, которые заражают главную загрузочную запись диска. Для предотвращения блокировки доступа к обновлениям антивируса через Интернет и блокировки доступа на сайты производителей антивирусов запрещается модификация файла HOSTS.

При повышенной опасности заражения повысьте уровень защиты до **Среднего**. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.

Внимание! В этом режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.

При необходимости полного контроля за доступом к критическим объектам Windows можно поднять уровень защиты до **Параноидального**. В данном случае будет доступен интерактивный контроль за загрузкой драйверов и автоматическим запуском программ.

Чтобы самостоятельно настроить параметры работы **Превентивной защиты**, отметьте необходимый уровень доступа к защищаемым объектам. Режим автоматически сменится на **Пользовательский**. Пользовательский режим позволяет гибко настроить реакцию антивируса на определенные действия, которые могут привести к заражению компьютера.

Вы также можете, нажав , создать новый профиль и переключаться на него в случае необходимости.

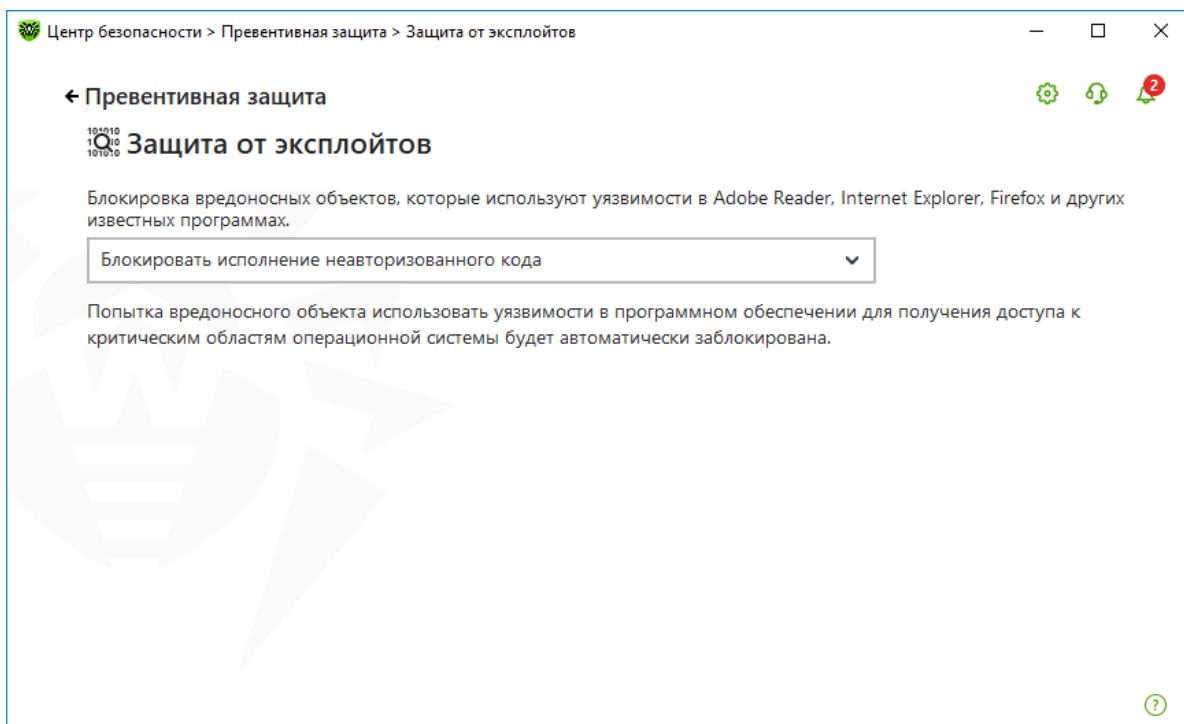
Напоминаем! Для пользователей Dr.Web [расшифровка](#) файлов, зашифрованных троянцем-вымогателем, бесплатна, если на момент инцидента были соблюдены эти [условия](#) использования Dr.Web.

Еще один компонент **Превентивной защиты** — **Защита от эксплойтов**.

Эксплойт (от англ. exploit — использовать, эксплуатировать) — вредоносная программа, последовательность команд или специально написанный вредоносный код, использующие уязвимости, в том числе для доставки троянцев в систему или для взлома определенного ПО. Существуют также наборы эксплойтов — «эксплойт-паки», предназначенные для использования целого ряда уязвимостей.

Эксплойт позволяет злоумышленнику внедриться в систему незаметно. Даже если ОС настроена так, что при запуске программ (одна из которых может быть и вредоносной) она выдает предупреждение о старте приложения, вредоносный код может исполниться незаметно для пользователя, благодаря эксплуатации уязвимостей.

Компонент **Защита от эксплойтов** уберет от вредоносных объектов, пытающихся для проникновения в систему использовать уязвимости в популярных приложениях, в том числе еще не известные никому, кроме вирусописателей (так называемые уязвимости нулевого дня). При обнаружении попытки проникновения через уязвимость Dr.Web принудительно завершает процесс атакуемой программы.



В выпадающем списке выберите подходящий уровень защиты от эксплойтов:

- **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.

Это интересно! Антивирус предназначен для «ловли» вредоносных программ. Но зачастую именно внедрение вредоносного кода есть цель злоумышленников, использующих

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

уязвимости. И если антивирус перехватывает внедряемую через даже еще никому не известную уязвимость программу — он выполняет роль защиты от уязвимостей!

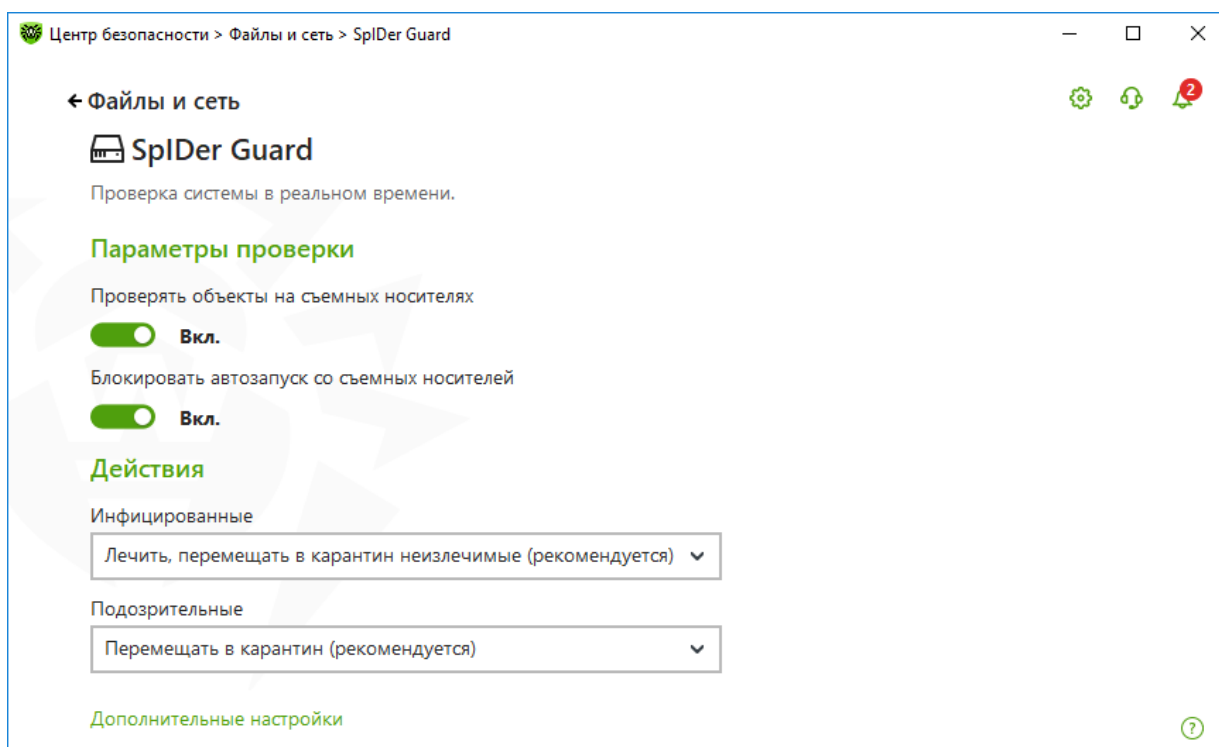
Неуязвимых систем не существует!

Разработчики ПО стараются оперативно выпускать «заплаты» к известным уязвимостям. Например, компания Microsoft достаточно часто выпускает обновления безопасности. Но часть из них пользователи устанавливают с большим запозданием (или не устанавливают вовсе), что стимулирует злоумышленников как на поиск все новых уязвимостей, так и на использование уже известных, но не закрытых на стороне потенциальных жертв.

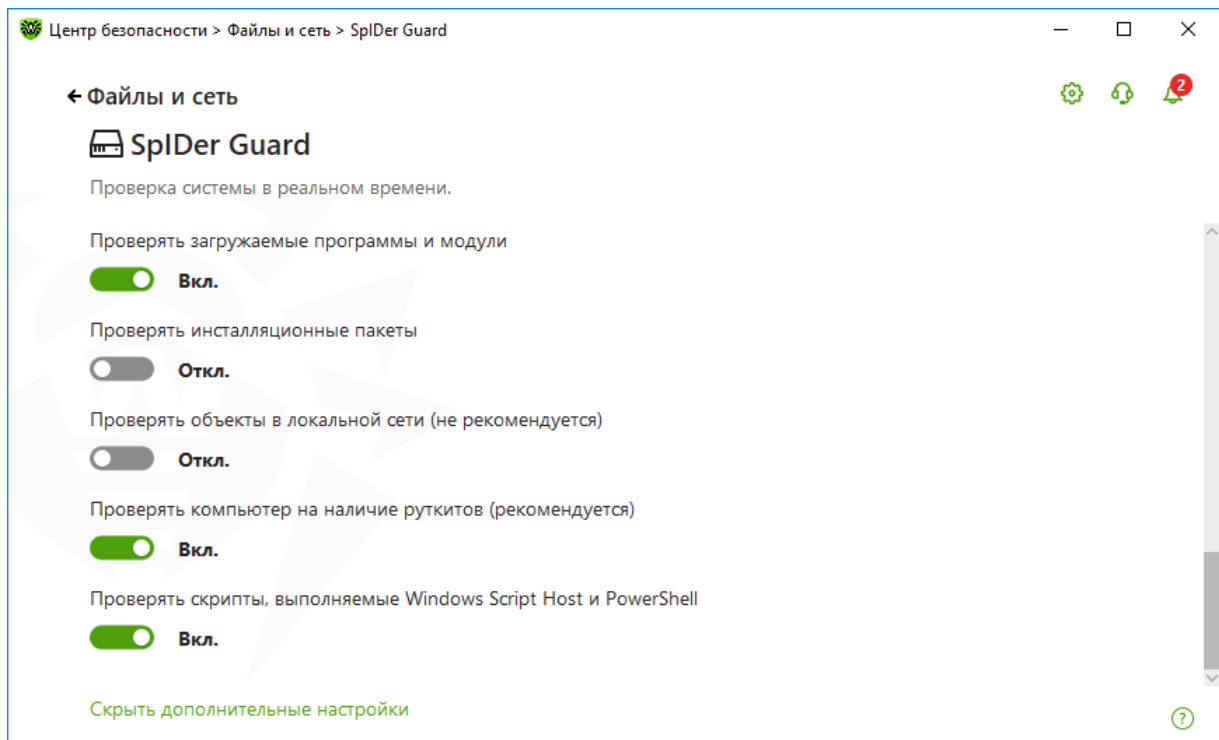
О том, как злоумышленники проникают в якобы защищенные системы, как создаются эксплойты, читайте в выпусках рубрики «[Уязвимые](#)» и «[Незваные гости](#)» проекта «Антивирусная правДА!».

Также обнаружение ранее не известных вредоносных программ обеспечивается модулем фоновой проверки запущенных процессов и нейтрализации активных угроз, а также проведением периодической антивирусной проверки. Данная подсистема реализована в рамках Антируткита Dr.Web. Подсистема постоянно находится в памяти и осуществляет поиск активных угроз в следующих критических областях Windows: объекты автозагрузки, запущенные процессы и модули, эвристики системных объектов, оперативная память, MBR/VBR дисков, системный BIOS компьютера. При обнаружении угроз данная подсистема может оповещать пользователя об опасности, осуществлять лечение и блокировать опасные действия.

Для включения режима проверки на руткиты в окне **Центр безопасности** выберите **Файлы и сеть** и далее **SpIDer Guard**. Нажмите на **Дополнительные настройки**.



Прокрутите бегунок справа до появления строки **Проверить компьютер на наличие руткитов**.



Данный параметр включен по умолчанию.


8.10. Ограничения возможности проникновения программ-шифровальщиков на компьютер

Троянец-шифровальщик может проникнуть в локальную сеть или на отдельный компьютер через спам (как правило, сообщение содержит вложение или специально сформированную ссылку), с помощью сообщения мессенджера (также содержащего ссылку), с зараженного сайта или принесен на зараженной флешке. Для снижения риска заражения используйте антиспам, а также ограничьте возможность работы с потенциально опасными ресурсами сети Интернет и сменными носителями.

С помощью модуля **Родительского (Офисного) контроля** осуществляется ограничение доступа пользователей к аппаратному обеспечению компьютера и различным программным ресурсам, содержащимся как на самом компьютере, так и на веб-сайтах, а также контролируется время работы в сети Интернет и за компьютером. Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность и конфиденциальность важных данных и защитить файлы от заражения. Существует возможность защиты как отдельных файлов, так и папок целиком, расположенных как на локальных дисках, так и на внешних носителях информации. Для предотвращения несанкционированного доступа к данным или их кражи можно ограничить доступ к таким устройствам, как USB-порты, жесткие диски, дисководы и т. п. Контроль доступа к интернет-ресурсам позволяет как оградить пользователей от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т. п.), так и разрешить пользователю доступ только к тем сайтам, которые определены настройками модуля Родительского (Офисного) контроля.

По умолчанию для всех учетных записей разрешен неограниченный доступ к ресурсам сети Интернет и к локальным ресурсам, ограничения по времени отсутствуют.

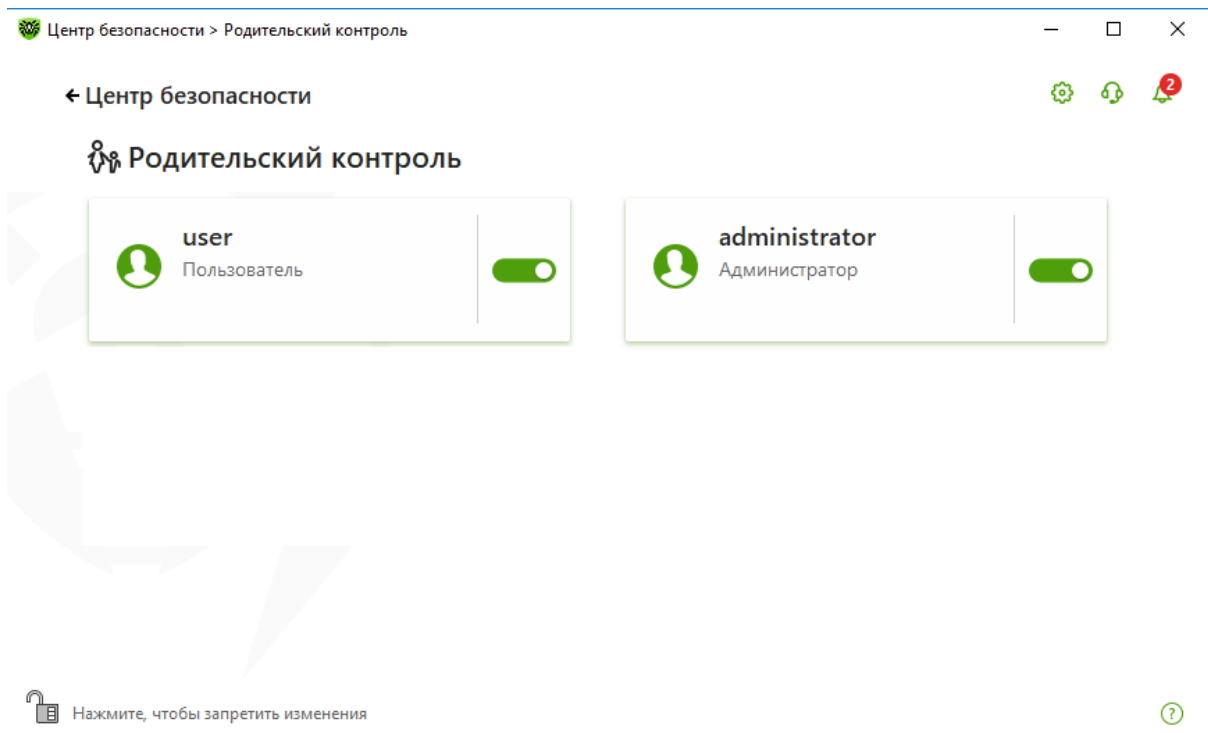
Настройки **Родительского контроля** индивидуальны для каждого пользователя на одном компьютере. Настройки других модулей Dr.Web одинаковы для всех пользователей.

Для настройки режима доступа к ресурсам сети Интернет, а также ограничения доступа к файлам и папкам кликните на значок  в системном меню, затем в открывшемся меню

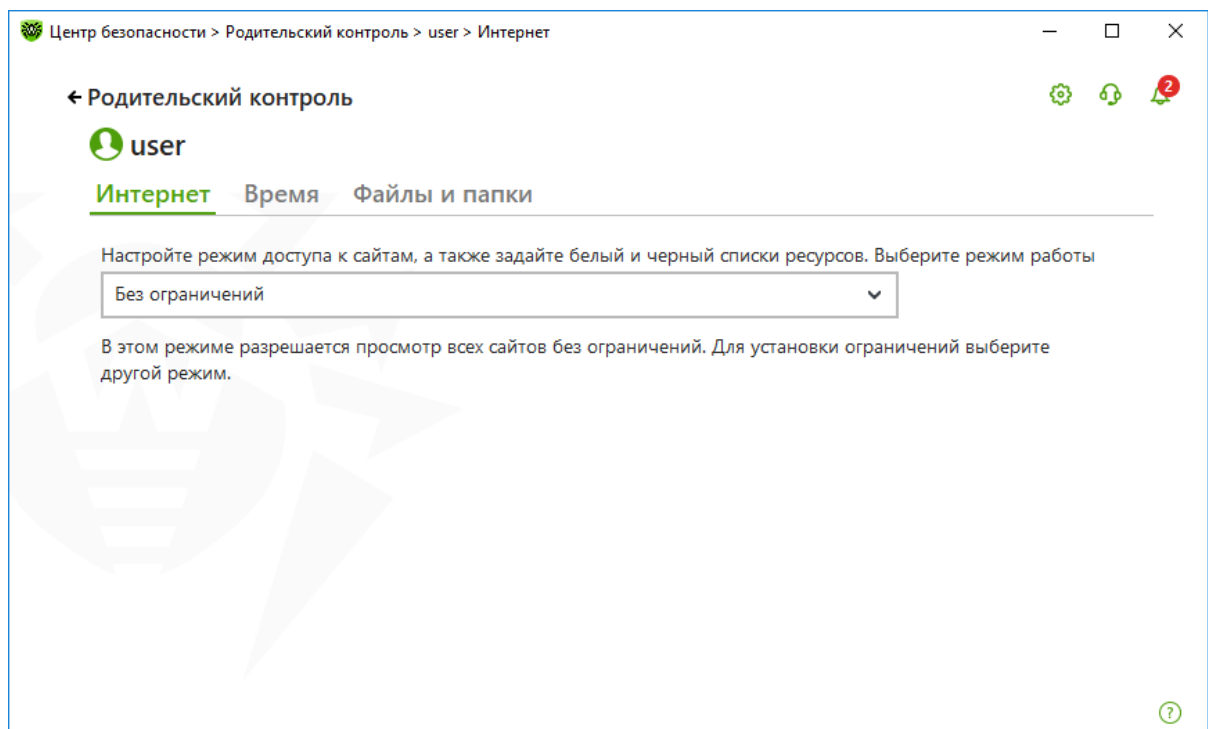
Dr.Web® Security Space. Руководство по быстрой установке и разворачиванию

агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).

В окне **Центр безопасности** выберите **Родительский контроль**.



В открывшемся окне выберите пользователя, для которого необходимо настроить ограничения и сделать необходимые настройки.



По умолчанию ограничения отключены.

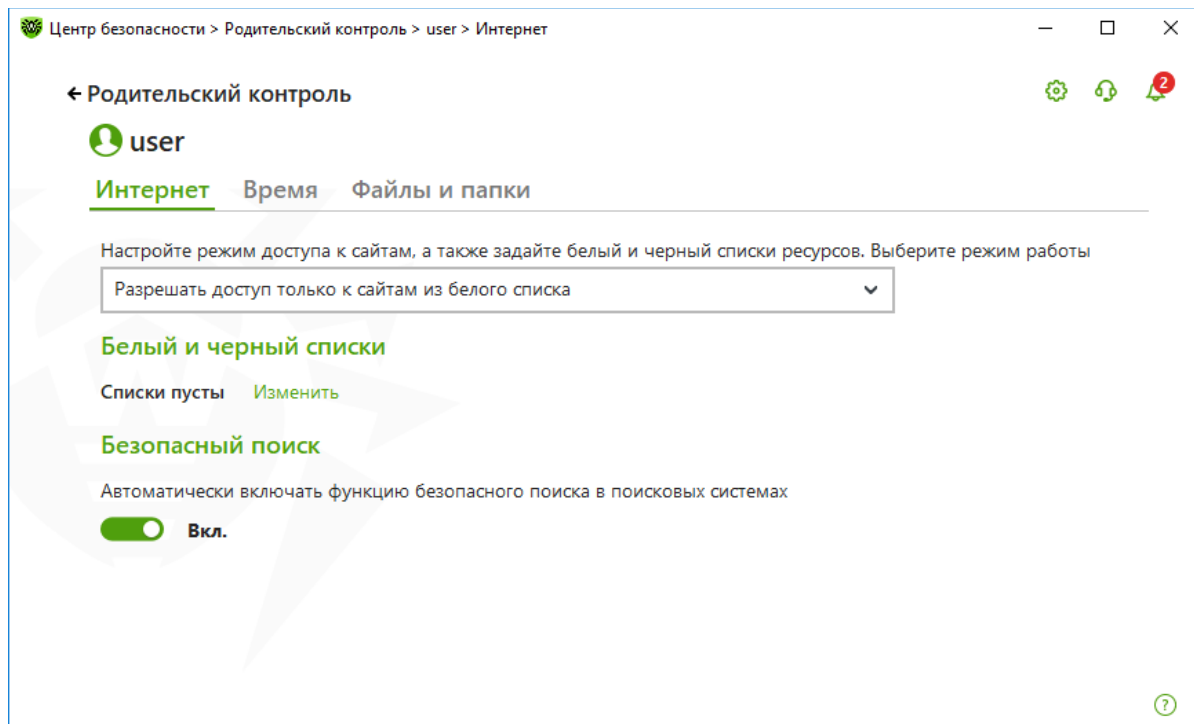
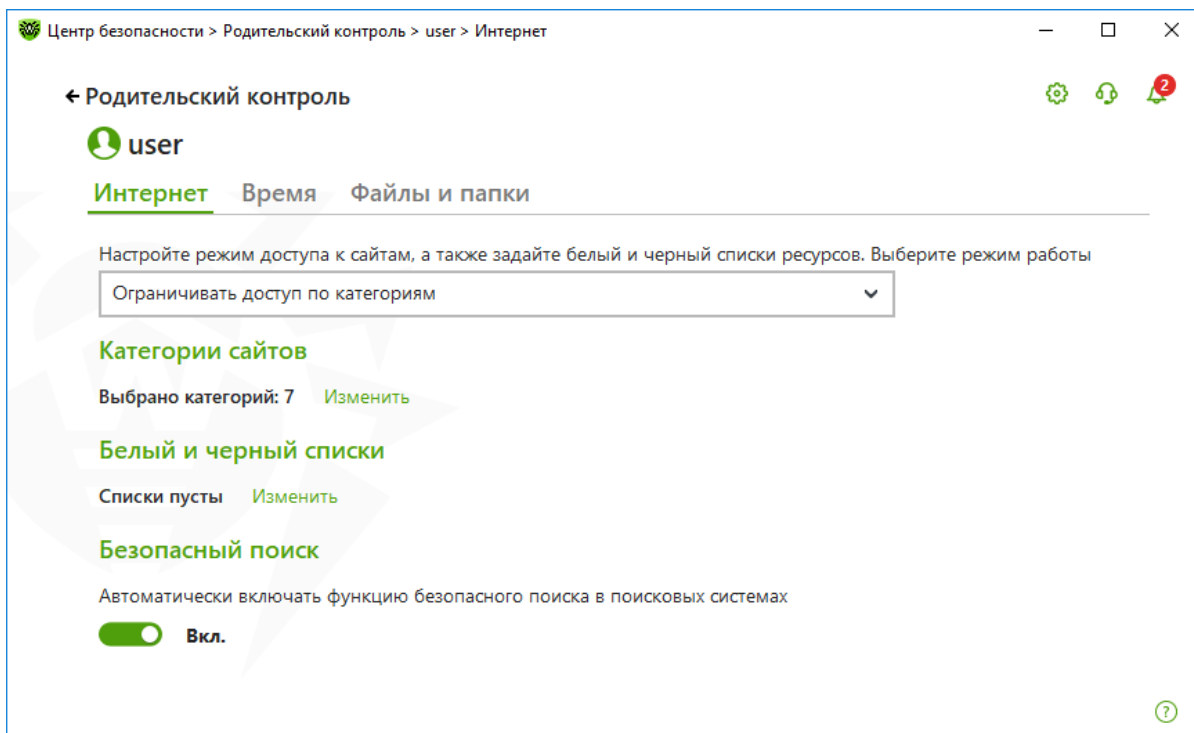
8.10.1. Ограничения времени доступа к сетевым ресурсам

Выберите вкладку **Интернет** для настройки правил доступа к интернет-ресурсам. Здесь

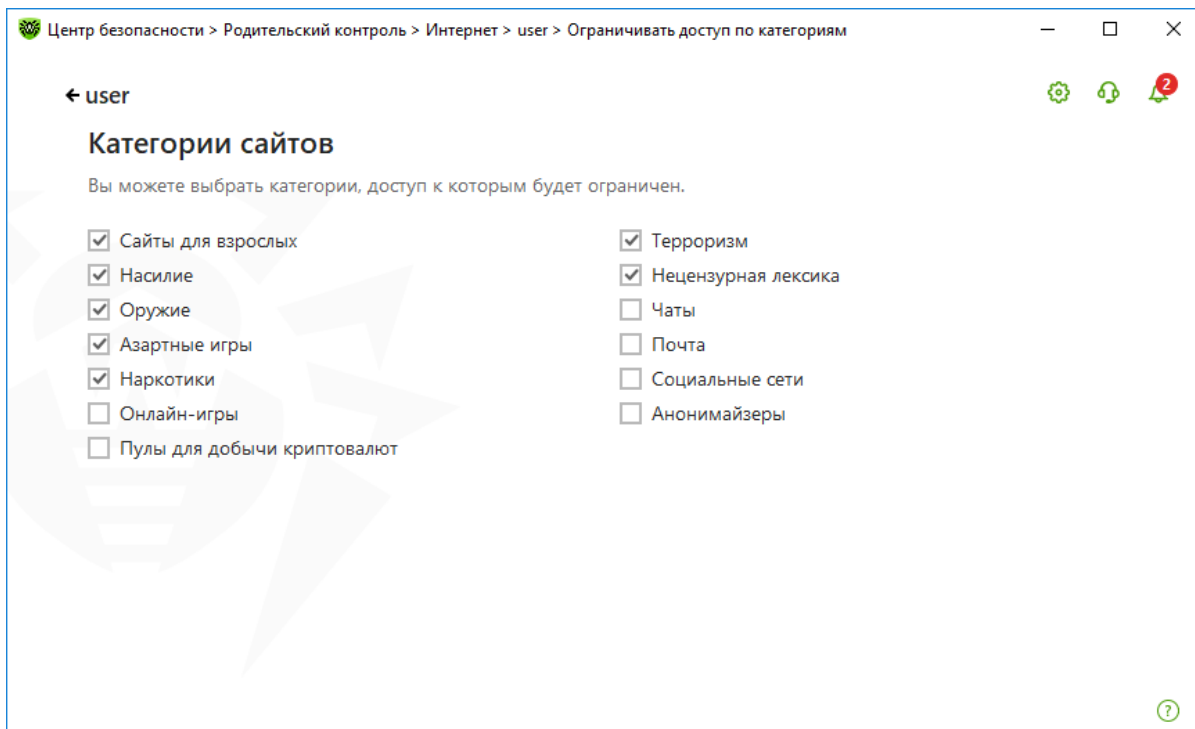
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

можно запретить доступ к сайтам, посвященным насилию, азартным играм и т. п., а также разрешить посещение указанных сайтов. Рекомендуется использовать режимы **Ограничить доступ по категориям** или **Разрешать доступ только к сайтам из белого списка**.

Если для пользователя не установлены ограничения на посещение определенных веб-ресурсов, то в окне **Интернет** будет отображено значение **Без ограничений**.



Выбрав режим **Ограничить доступ по категориям** и кликнув на **Изменить**, выберите категории ресурсов, доступ к которым нужно блокировать.



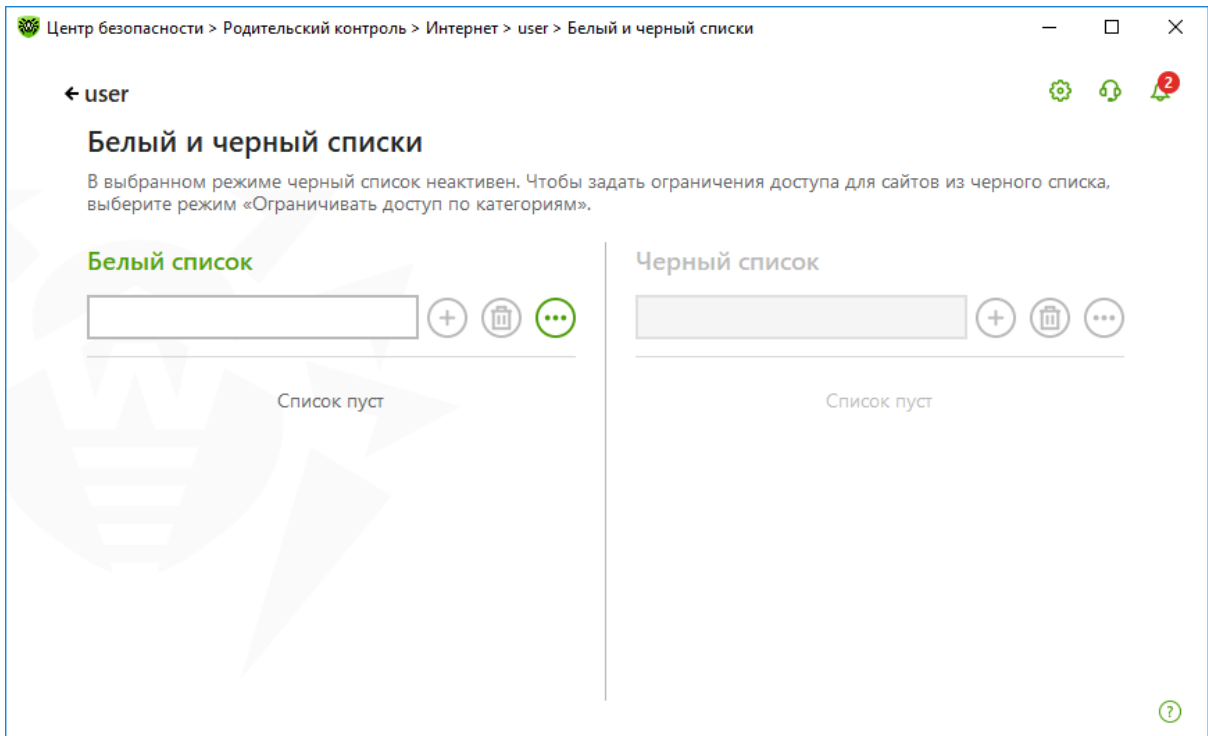
В случае такого выбора пользователю доступен выбор групп сайтов (сайты для взрослых, насилие, оружие и т. п.), к которым необходимо ограничить доступ.

Отметьте необходимые категории, доступ к которым нужно запретить.

Можно также запретить посещение всех веб-ресурсов, кроме добавленных в белый список. Для этого выберите режим **Разрешать доступ только к сайтам из белого списка**.

Приоритет списков выше приоритета предустановленных групп. Например, можно выбрать группу **Социальные сети**, но адрес сети «ВКонтакте» добавить в белый список. Тогда доступ ко всем социальным сетям, за исключением «ВКонтакте», будет запрещен.

В обоих рекомендуемых режимах вы можете настроить белые и черные списки доступа к ресурсам, нажав на кнопку **Изменить** в группе настроек **Белый и черный списки**.

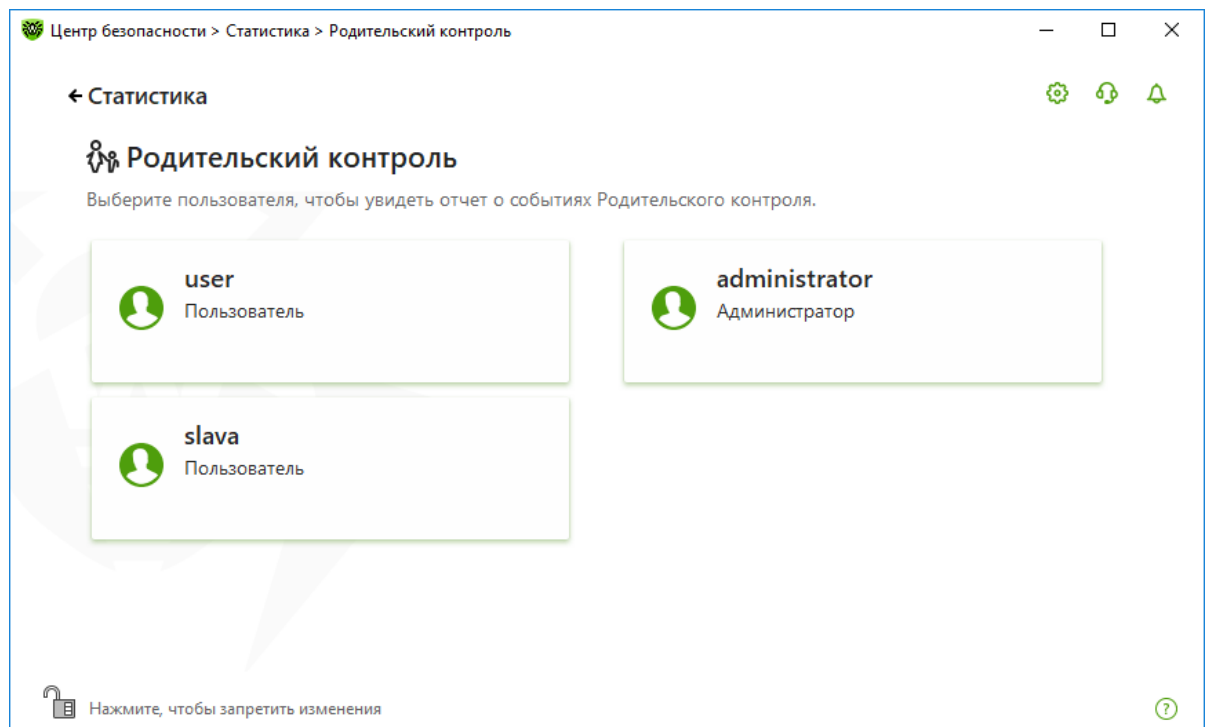


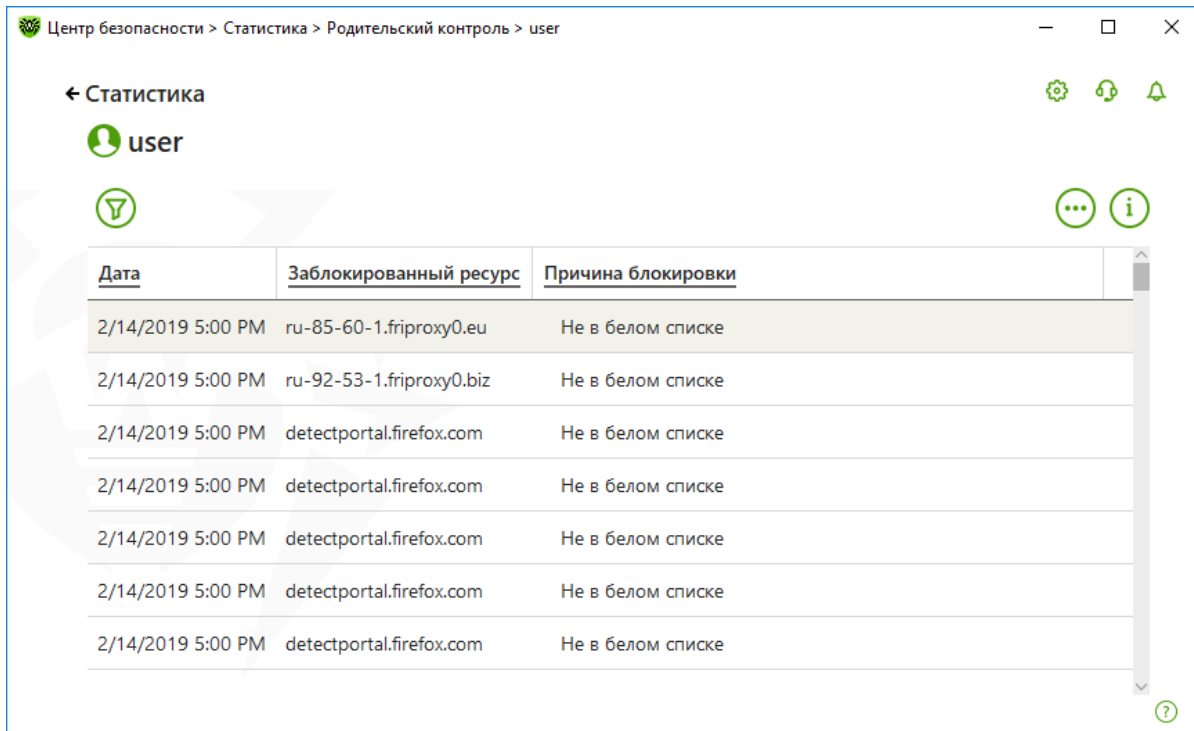
Для добавления ресурса нажмите  для соответствующего списка.

Для обоих списков можно использовать доменные имена ресурсов или части доменных имен, а также маски.



Опция **Безопасный поиск** позволяет исключить нежелательные ресурсы из результатов поиска, используя средства поисковых систем.

Для просмотра статистики обращений к различным ресурсам перейдите на закладку **Статистика** в **Центре безопасности**. Далее выберите **Родительский контроль** и имя пользователя.



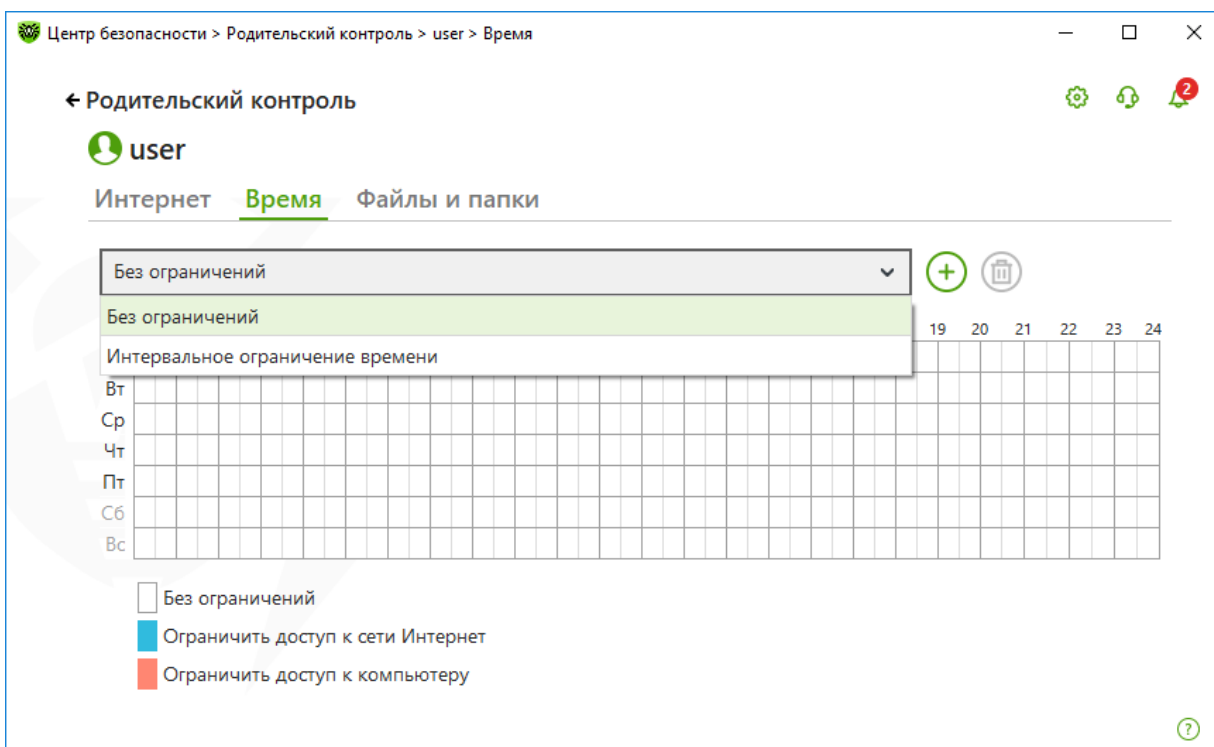


8.10.2. Ограничения времени доступа к Интернету и учетной записи


Для настройки времени доступа к Интернету и учетной записи кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).

В окне **Центр безопасности** выберите **Родительский контроль** и далее пользователя.

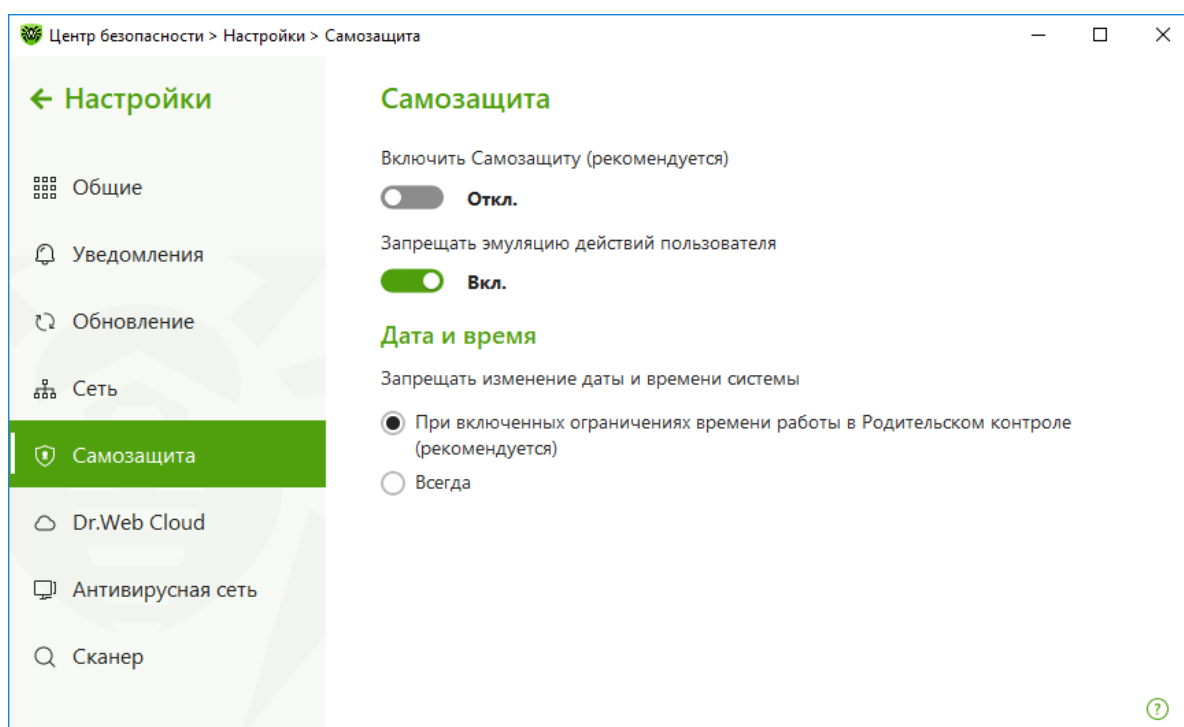
На вкладке **Время** вы можете ограничить время работы пользователей за компьютером и в Интернете. Данная возможность позволяет исключить неконтролируемый доступ к ресурсу в неразрешенное время.



С помощью временной сетки настройте расписание доступа. Для этого наведите курсор на любой белый квадрат. При однократном щелчке левой клавиши мыши квадрат окрасится в голубой цвет, при двойном щелчке — в бордовый цвет, при тройном щелчке — в белый цвет. Синий цвет означает, что в заданный период времени будет заблокирован доступ в Интернет, бордовый — блокировка на пользование учетной записью (невозможно использовать компьютер под учетной записью, для которой настроена такая блокировка), белый — ограничения отсутствуют. Добившись нужного цвета квадрата, удерживайте левую клавишу мыши нажатой и проведите курсором таким образом, чтобы нужные квадраты изменили цвет. Таким образом настраивается расписание работы пользователя для конкретной учетной записи. В данном примере пользователь не сможет пользоваться компьютером по воскресеньям, сможет работать на компьютере в будни, но не все время сможет выйти в Интернет.



Нажав , создайте профиль настроек. В профиле сохранятся настоящие настройки таблицы. В дальнейшем при изменении настроек профиля они будут также автоматически сохраняться.

При включении ограничений времени работы за компьютером или в сети Интернет, автоматически включается опция **Запрещать изменение даты и времени системы** в разделе **Самозащита** основных настроек.



8.10.3. Контроль доступа к локальным ресурсам

Пользователь может ограничить доступ к сменным носителям, файлам и папкам, тем самым уменьшив риск проникновения вредоносных программ.

Для настройки времени доступа к Интернету и учетной записи кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).

В окне **Центр безопасности** выберите **Родительский контроль** и далее пользователя.

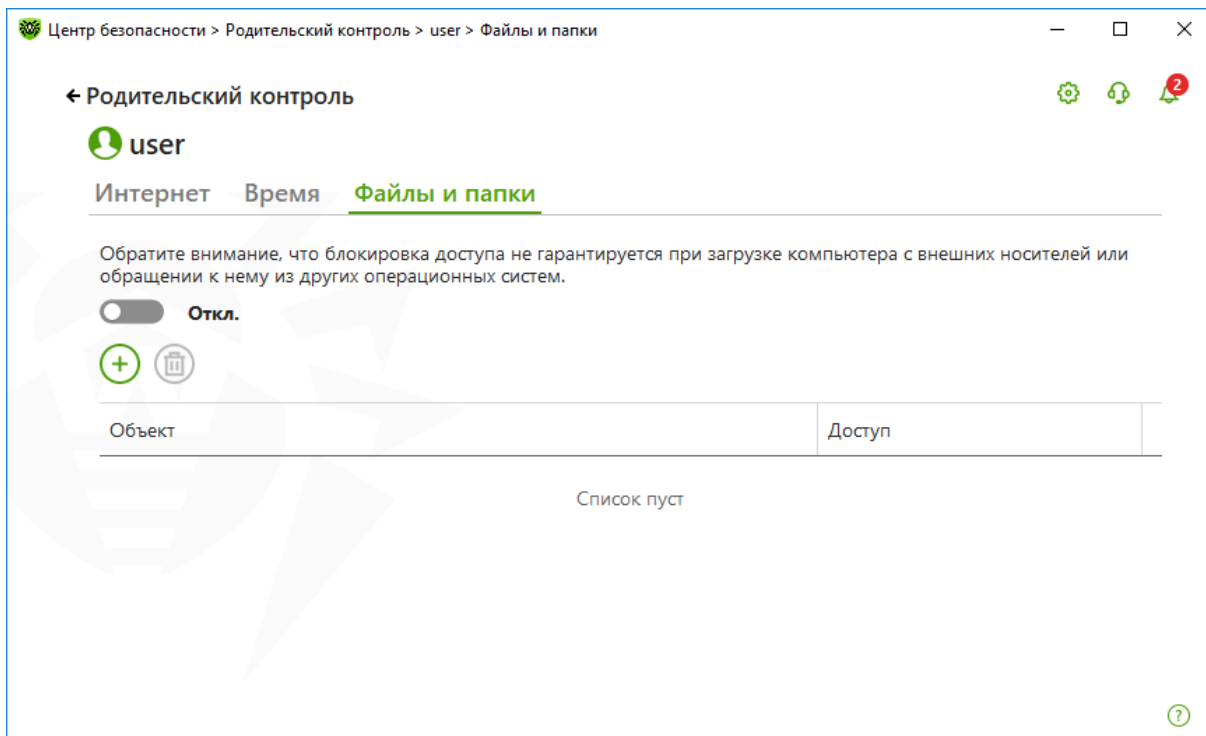
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Доступ к изменению настроек модуля может быть защищен паролем. Изменить пароль можно в окне **Настройки** → **Общие**.


Внимание! Все используемые пароли должны быть достаточной длины. В паролях не должны использоваться простые сочетания букв. Использование простых паролей делает возможным злонамеренное проникновение через перебор паролей.

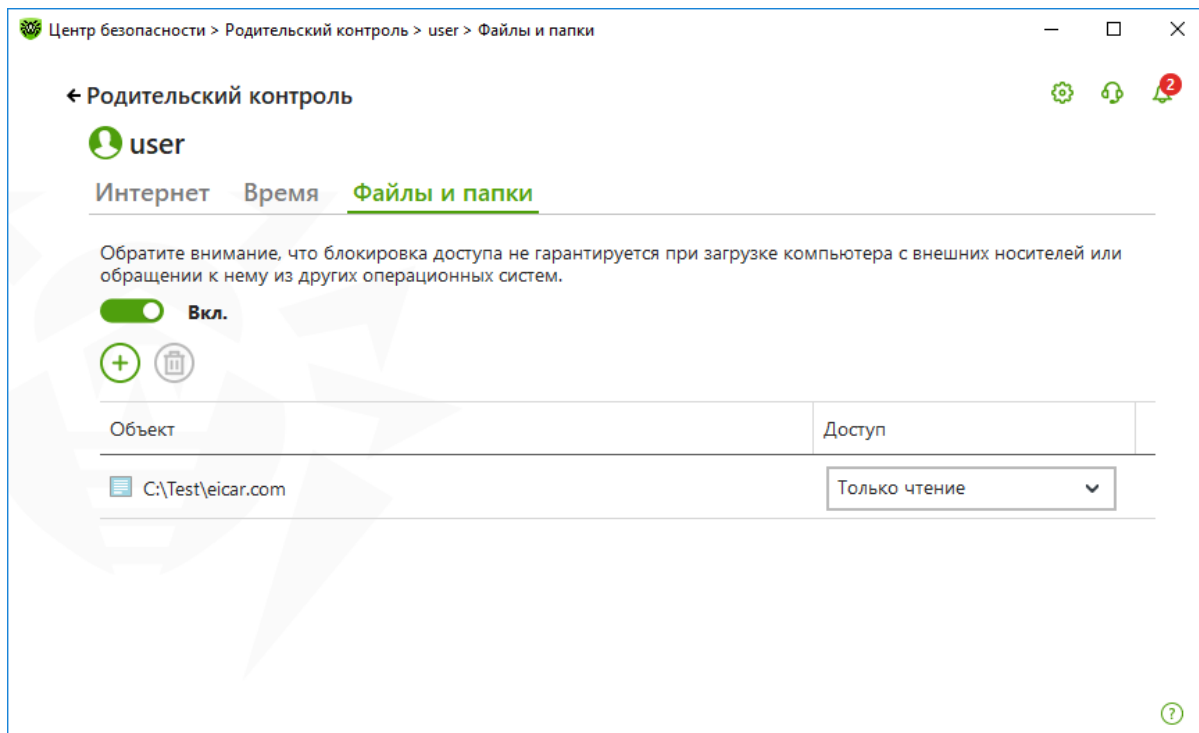
На вкладке **Файлы и папки** ограничьте доступ к файлам и папкам на локальных дисках и на съемных носителях.

Включите ограничение доступа к файлам и папкам, передвинув переключатель.



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

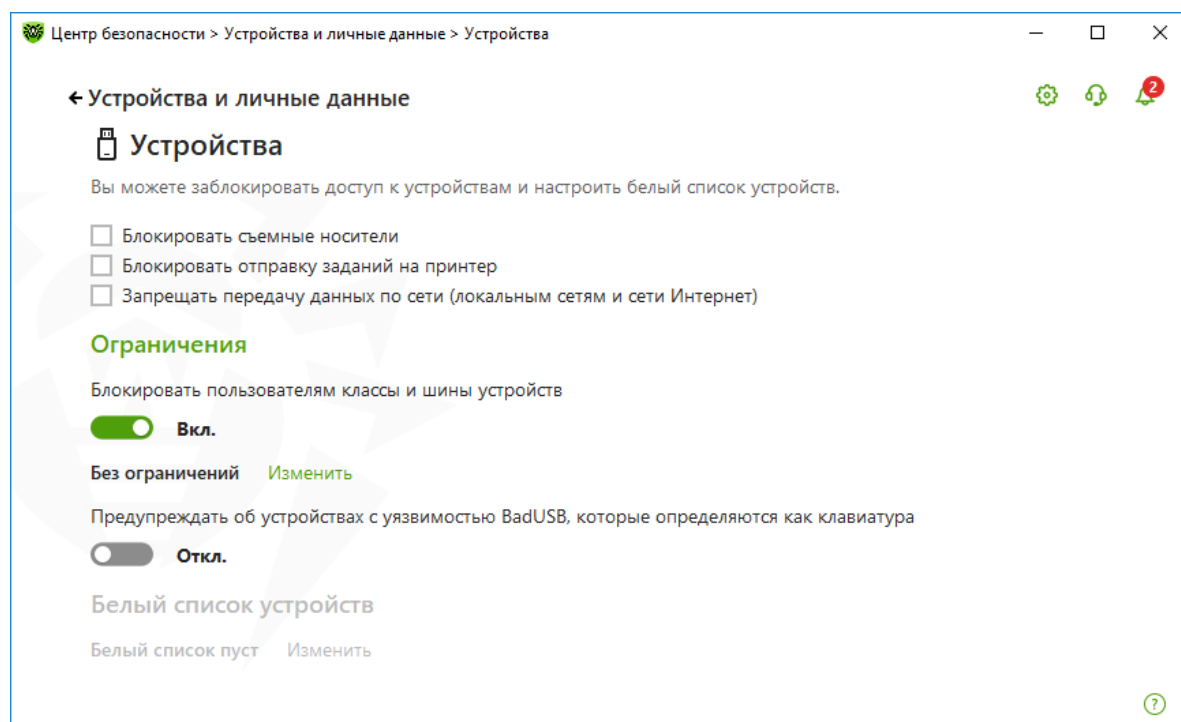
Нажав , добавьте необходимые папки и файлы в список ресурсов, доступ к которым будет ограничен.



Выберите режим доступа для добавленного объекта:

- **Заблокирован** — для полной блокировки доступа к объекту.
- **Только чтение** — для того, чтобы разрешить доступ к объекту без его изменения, удаления или перемещения (например, просмотр документа, изображения, запуск исполняемого файла).

Для настройки ограничений действий со сменными носителями в окне **Центр безопасности** выберите **Устройства и личные данные** и далее **Устройства**.



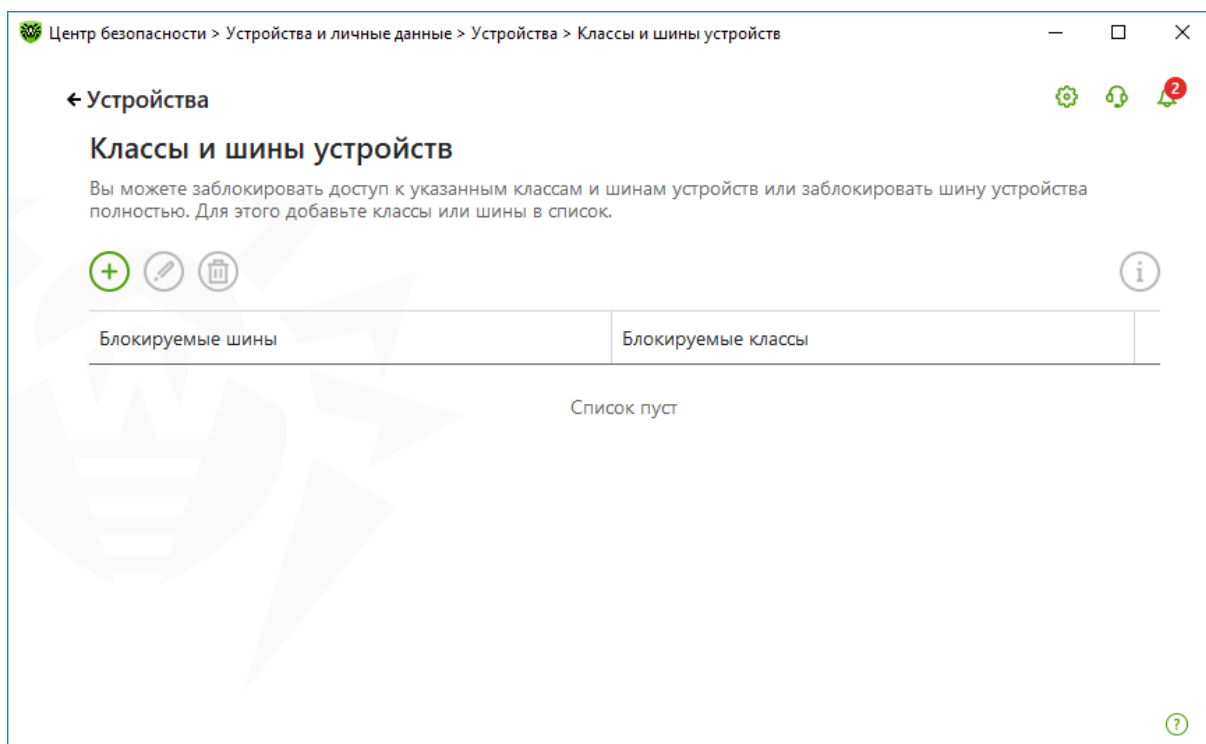
В данном окне вы можете полностью заблокировать доступ к данным на съемных носителях (USB флеш-накопителях, дискетах, CD/DVD приводах, ZIP-дисках и т. п.), выбрав **Блокировать съемные носители**.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Если вы хотите заблокировать доступ к отдельным устройствам и типам устройств, передвиньте переключатель **Блокировать указанные устройства для всех пользователей**, нажмите кнопку **Изменить** и в открывшемся окне составьте список классов и шин устройств, доступ к которым хотите заблокировать.

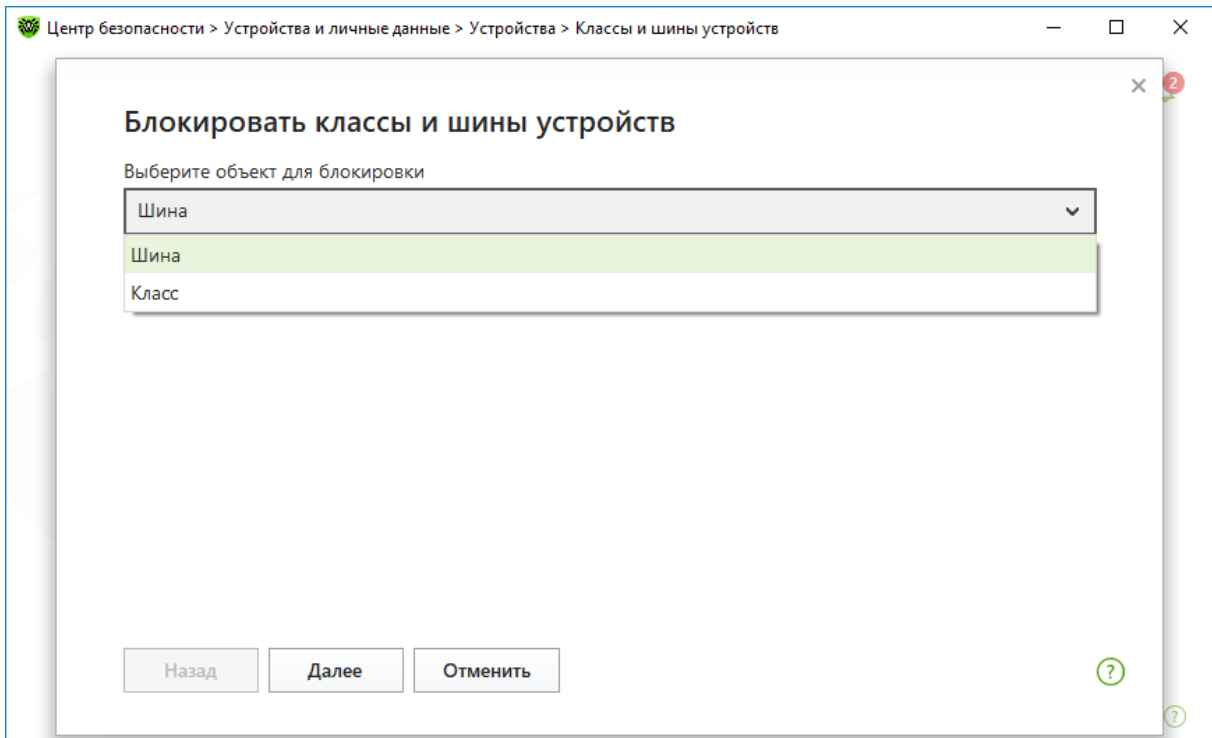
Класс устройства — специальный код, передаваемый устройством операционной системе, позволяющий операционной системе выбрать правильный драйвер и определить перечень функционала, предоставляемый устройством (аудиоустройства ввода/вывода, биометрические устройства, дисковые устройства, DVD/CD-ROM, дисководы, устройства GPS, камеры/фотоаппараты, инфракрасные устройства, клавиатуры, мыши и иные подобные устройства, модемы, сетевые карты, принтеры и т. д.).

Шина устройства — способ подключения к компьютеру (Bluetooth, IEEE 1394, USB, последовательный/параллельный порт, устройства чтения смарт-карт, PCMCIA, шина PCI и т. д.).

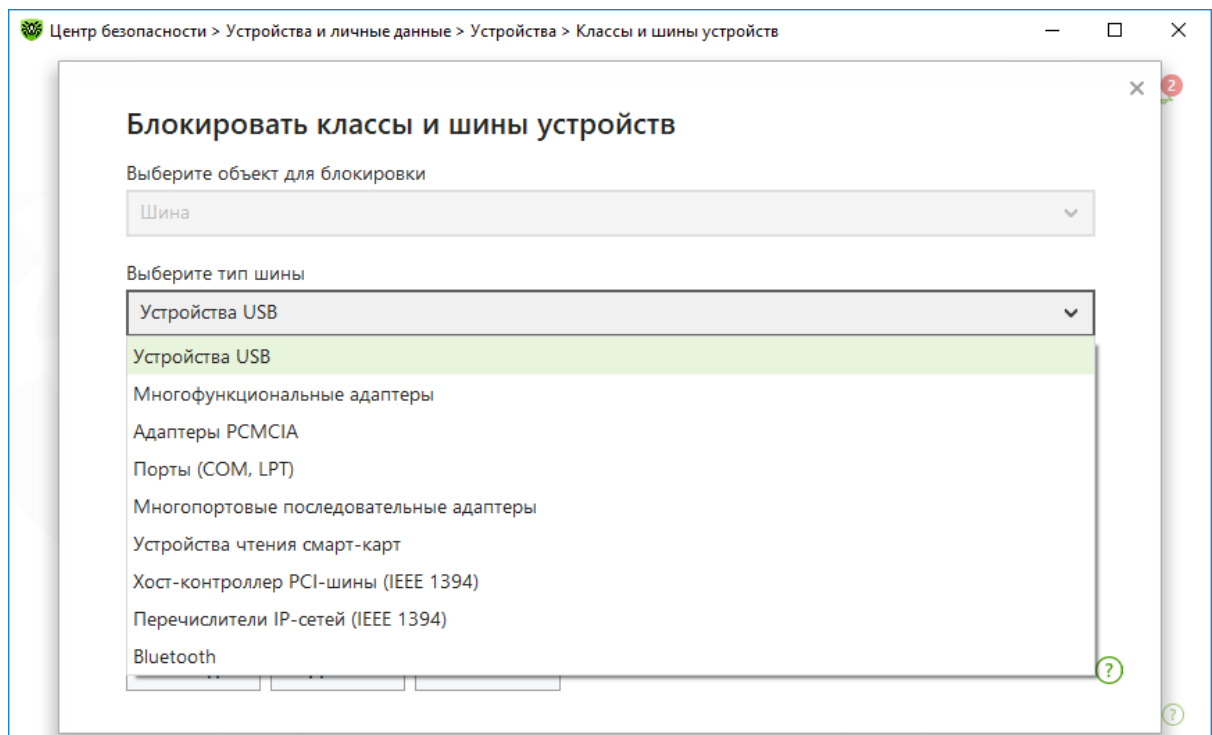


Для добавления шины полностью или некоторого устройства на определенной шине в список используйте **+**.

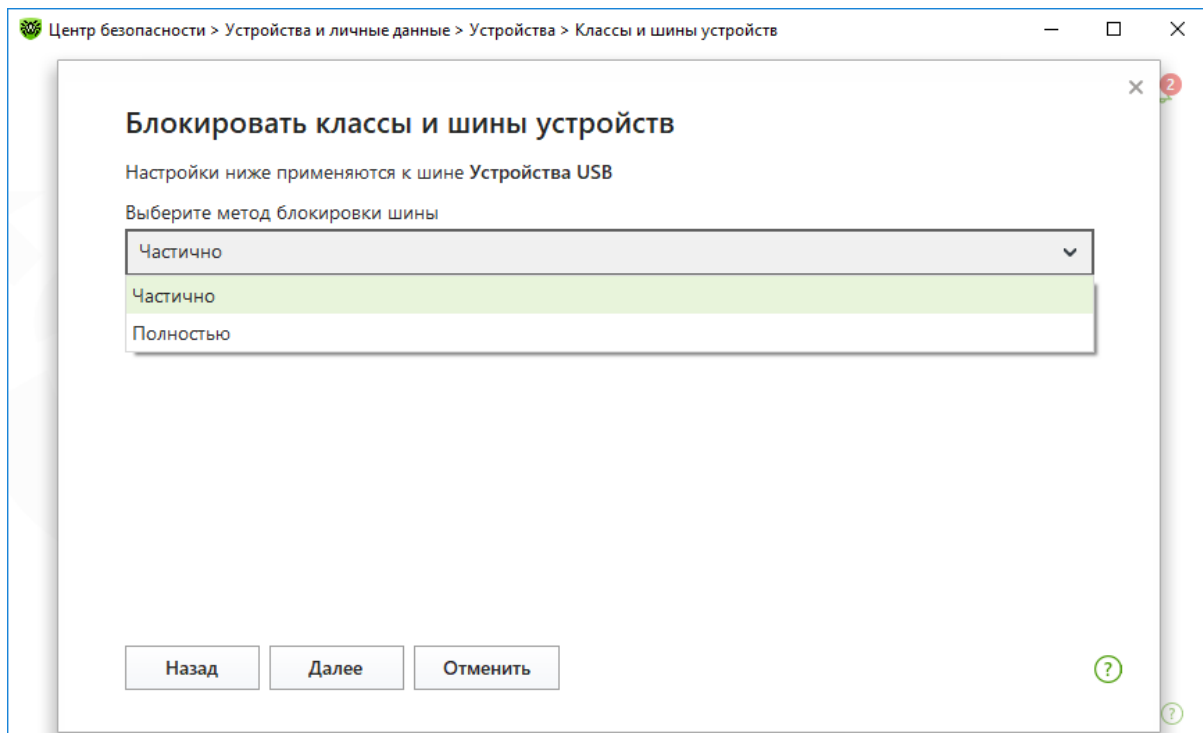
Если вы хотите заблокировать шину, то из выпадающего списка выберите **Шина** и нажмите **Далее**.



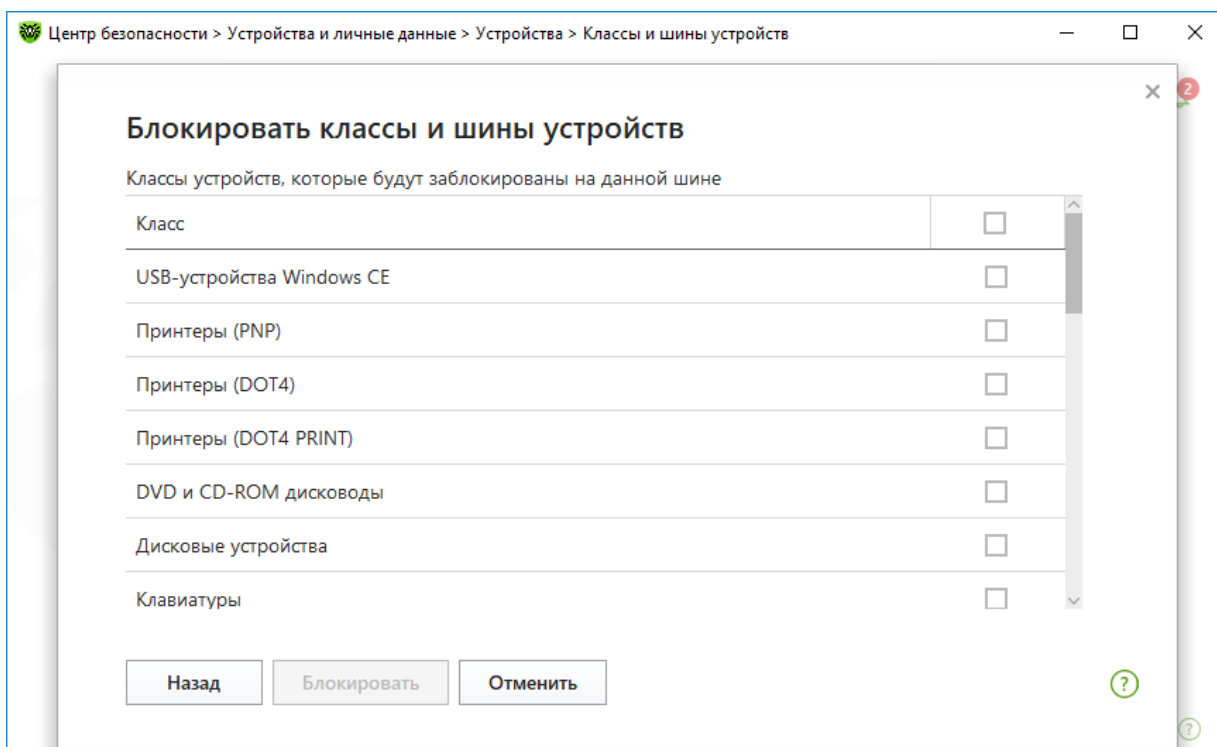
Выберите тип шины.

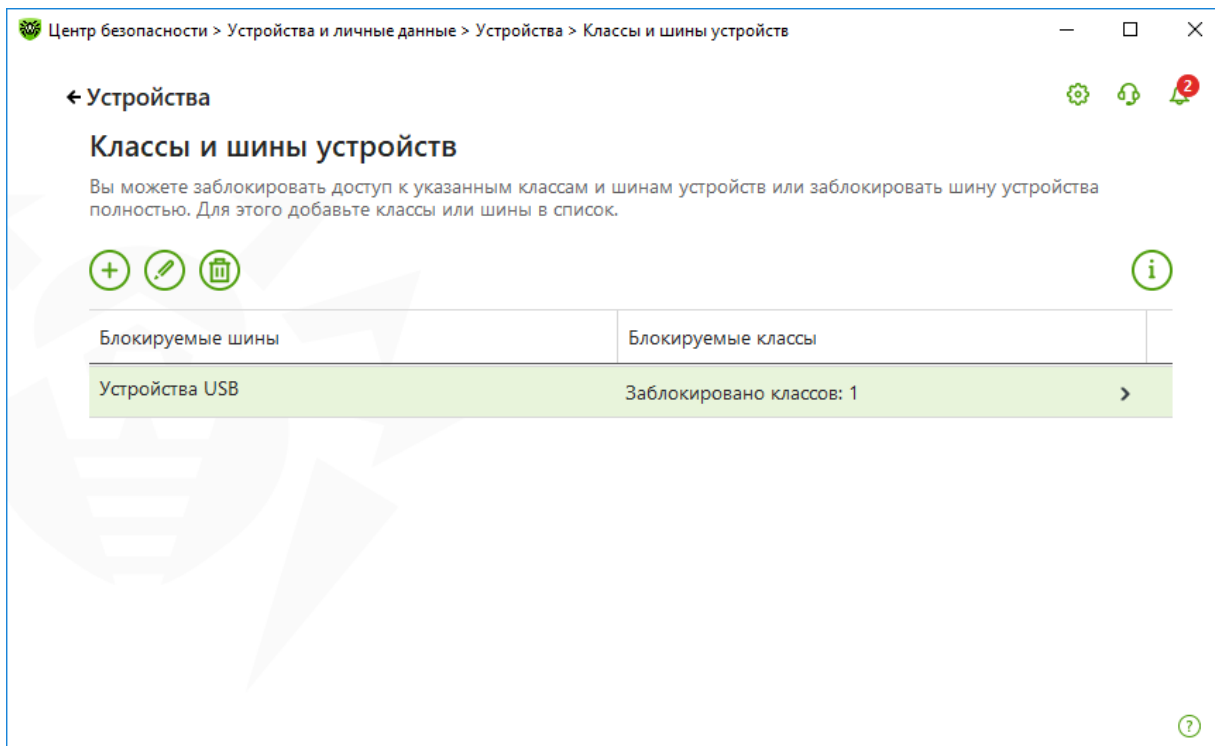


Выберите тип блокировки (**Полностью** — будут заблокированы все классы устройств на данной шине или **Частично** — откроется окно выбора классов устройств для блокировки на данной шине) и нажмите **Далее**.




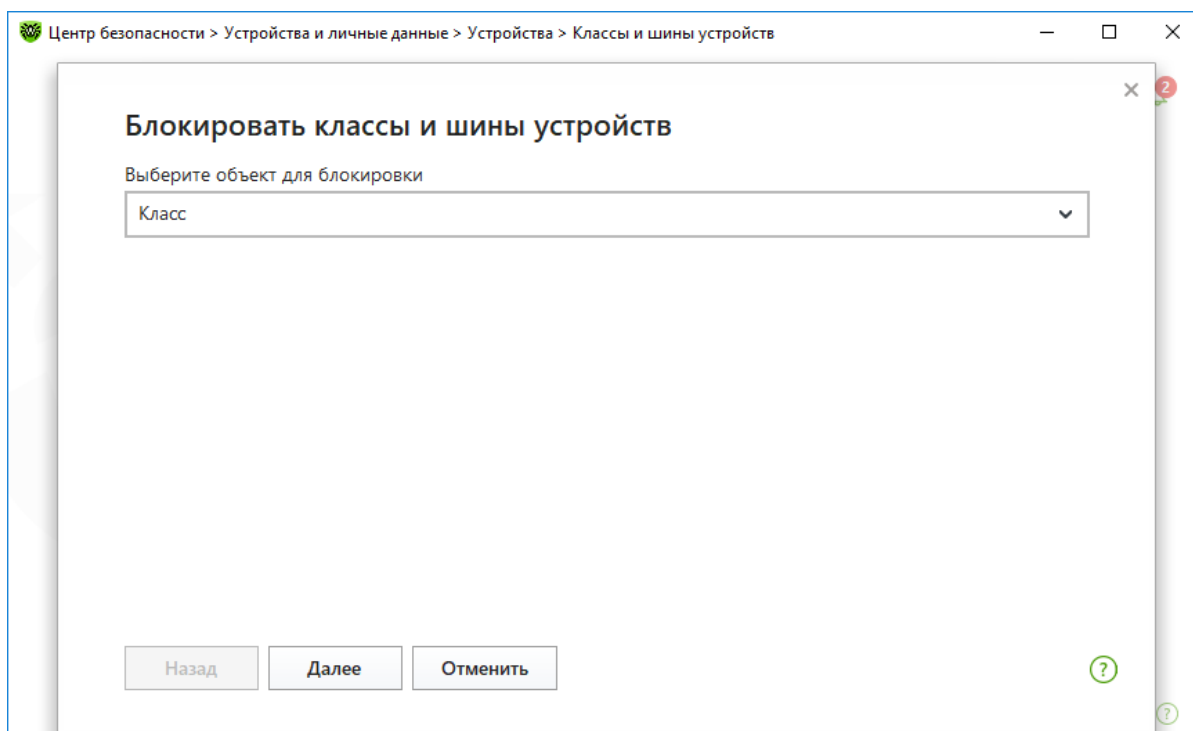
Отметьте классы из списка, которые вы хотите заблокировать. Нажмите **Блокировать**.



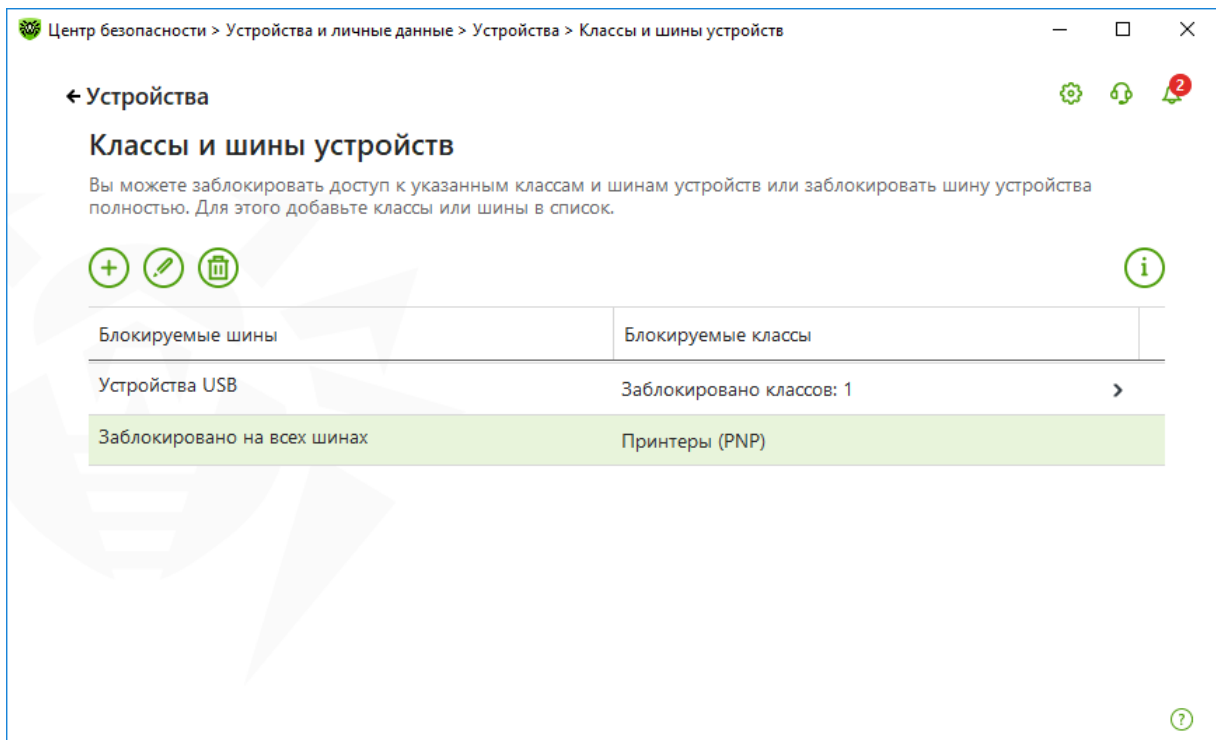
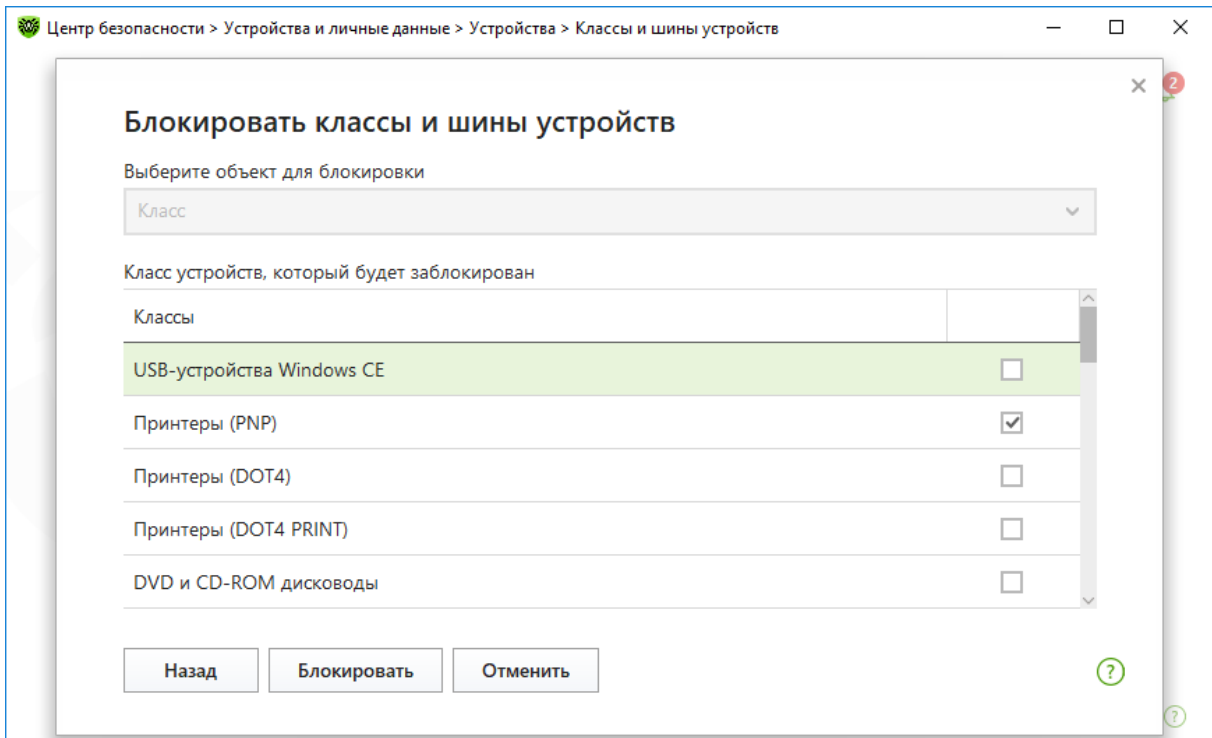


Внимание! При блокировке шины USB-клавиатура и мышь вносятся в исключения.

Чтобы заблокировать один или несколько классов устройств, нажмите кнопку . В открывшемся окне из выпадающего списка выберите **Класс** и нажмите **Далее**.



Отметьте те классы из списка, которые вы хотите заблокировать. Нажмите **Блолировать**.



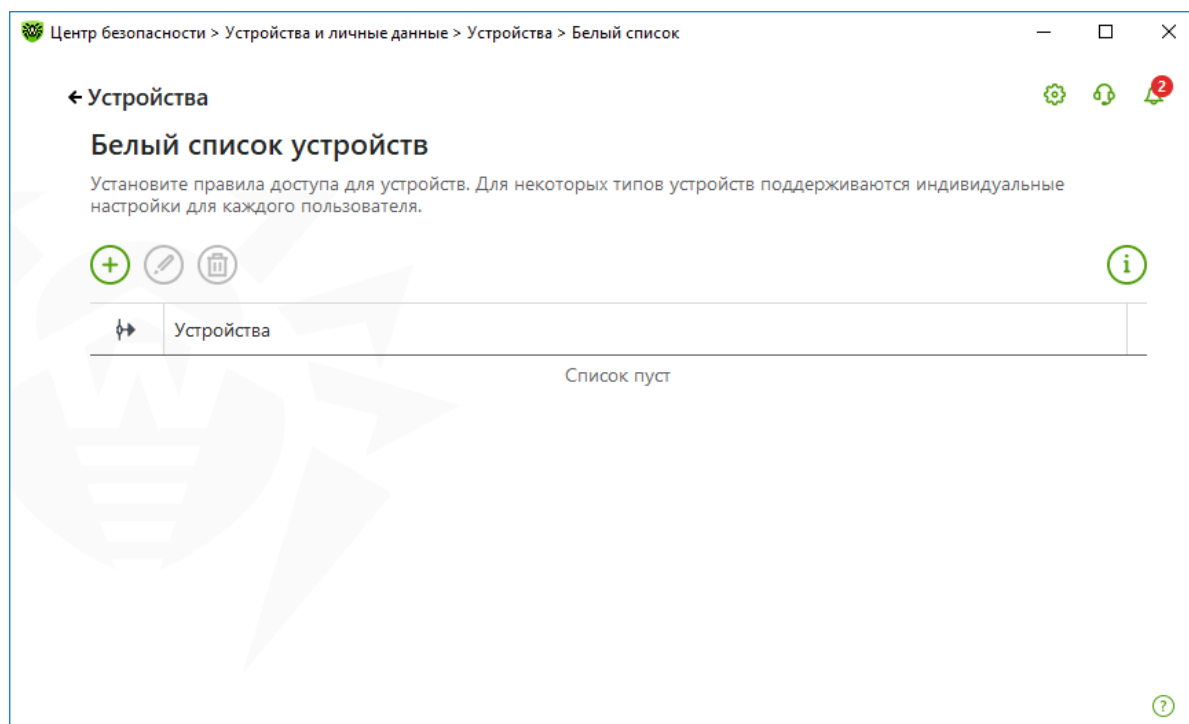
Внимание! При активации блокировки уже подключенного устройства требуется либо подключить устройство заново, либо перезагрузить компьютер. Блокировка работает только для устройств, подключенных после активации функции.

С помощью функций Родительского (Офисного) контроля на вкладке **Устройства** можно запретить запись данных на съемные носители, ограничить доступ к конкретным устройствам — либо разрешить доступ только с определенных устройств, запретить передачу данных по локальным сетям и сети Интернет.

Внимание! Настройки контроля доступа применяются для всех учетных записей Windows.

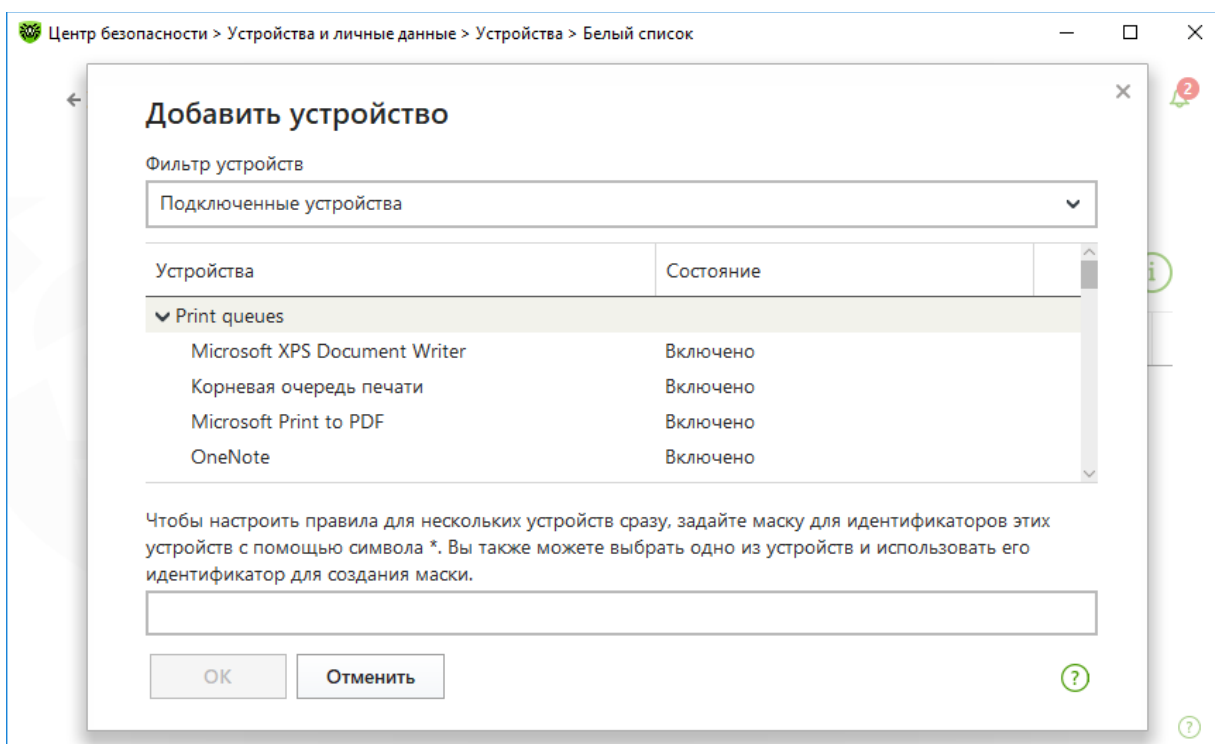
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

Для формирования белого списка устройств в группе настроек **Белый список устройств** нажмите кнопку **Изменить**.

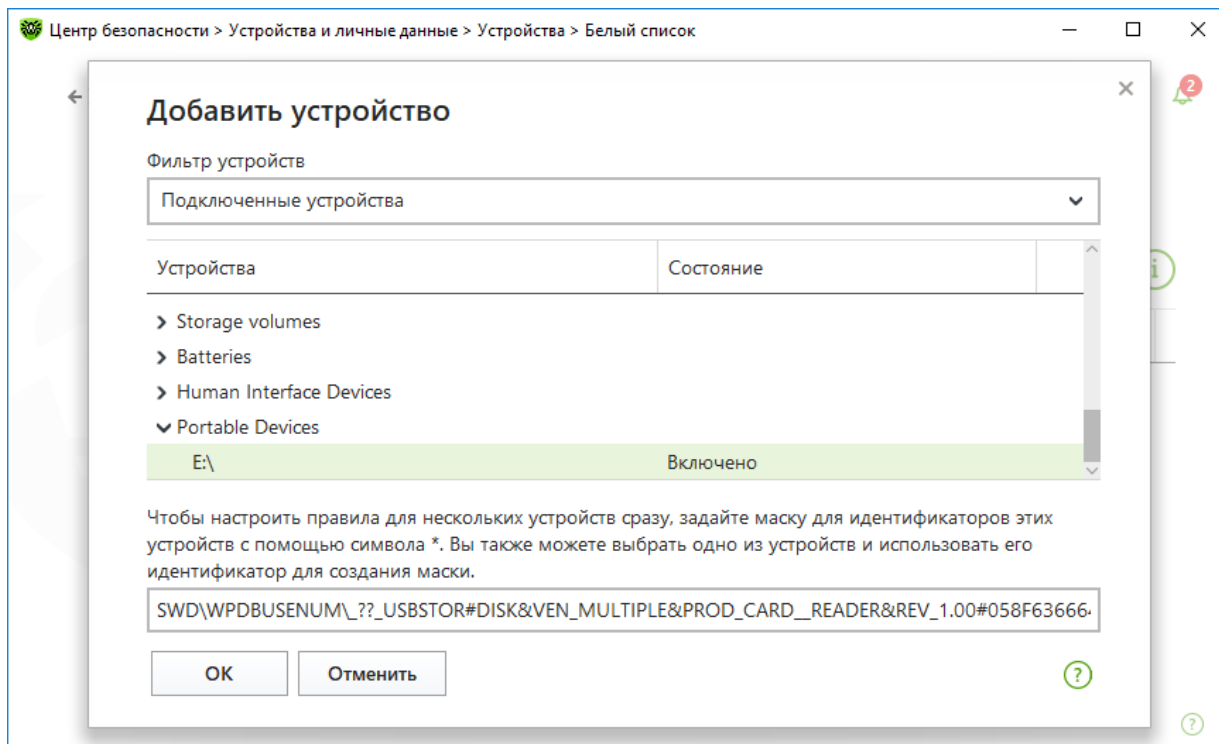


Окно **Белый список устройств** содержит информацию обо всех устройствах, добавленных в белый список.

Для добавления устройства в белый список подключите его к компьютеру и нажмите **+**.



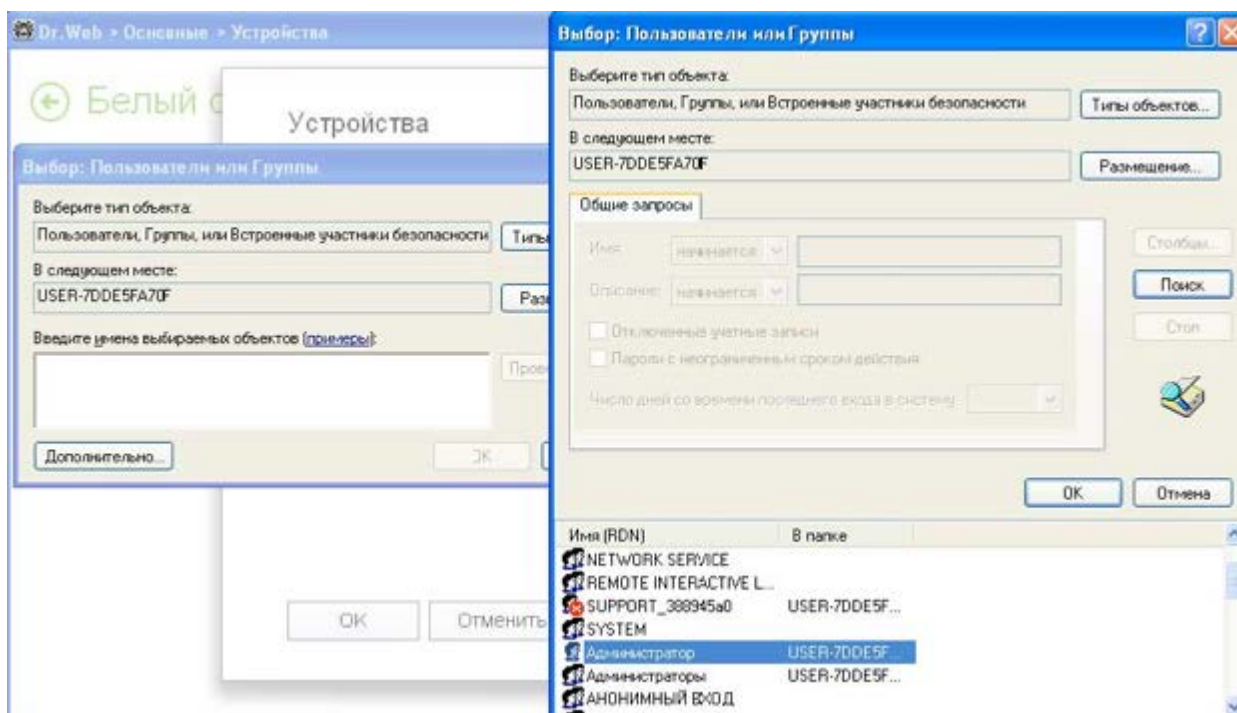
В открывшемся окне нажмите кнопку **Обзор** и выберите нужное устройство. В выпадающем списке выберите показ только подключенных или только отключенных устройств.

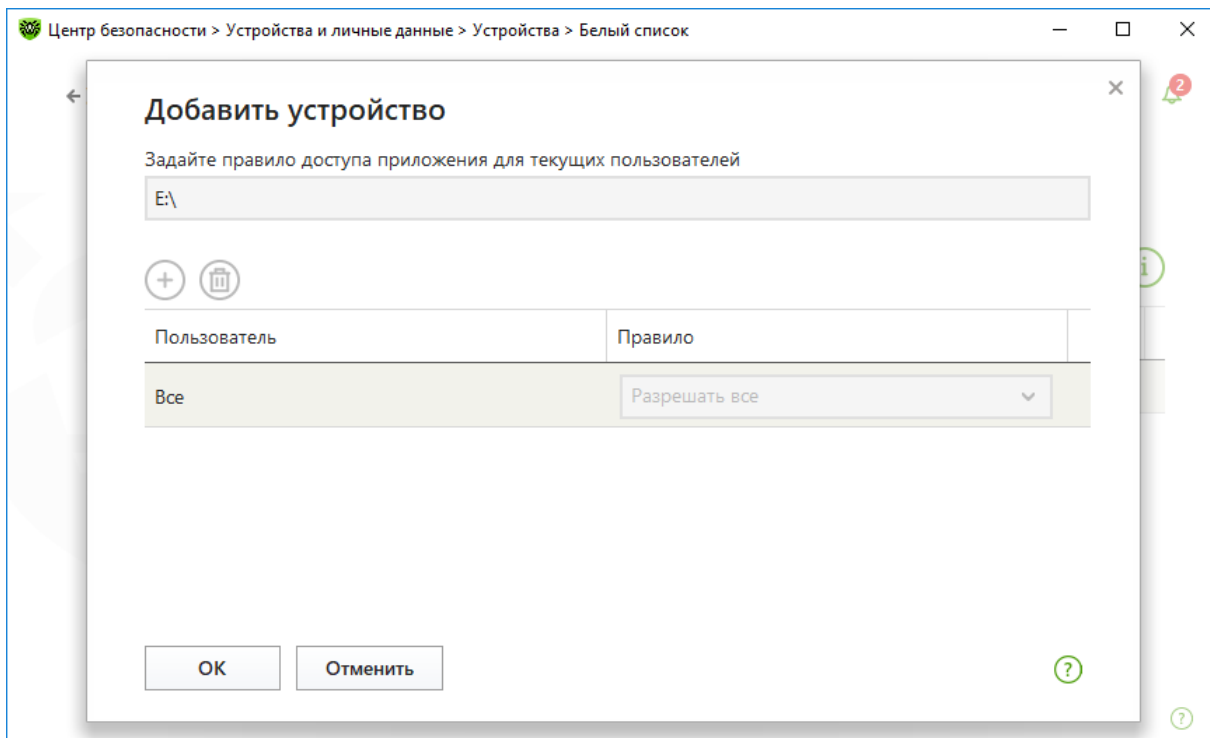


Нажмите кнопку **ОК**.

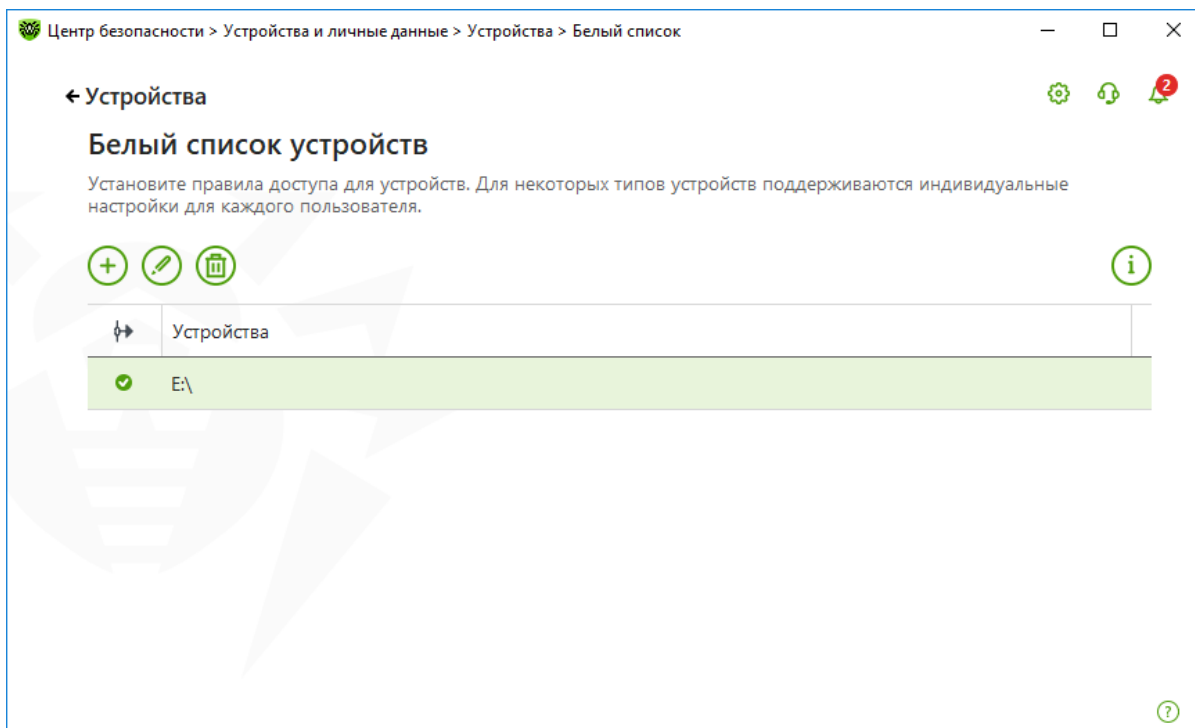
Для устройств с файловой системой вы можете настроить правила доступа. Для этого в столбце **Правило** выберите один из режимов: **Разрешать все** или **Только чтение**.

Чтобы добавить новое правило для конкретного пользователя, нажмите **+**, **Поиск** и выберите необходимого пользователя.







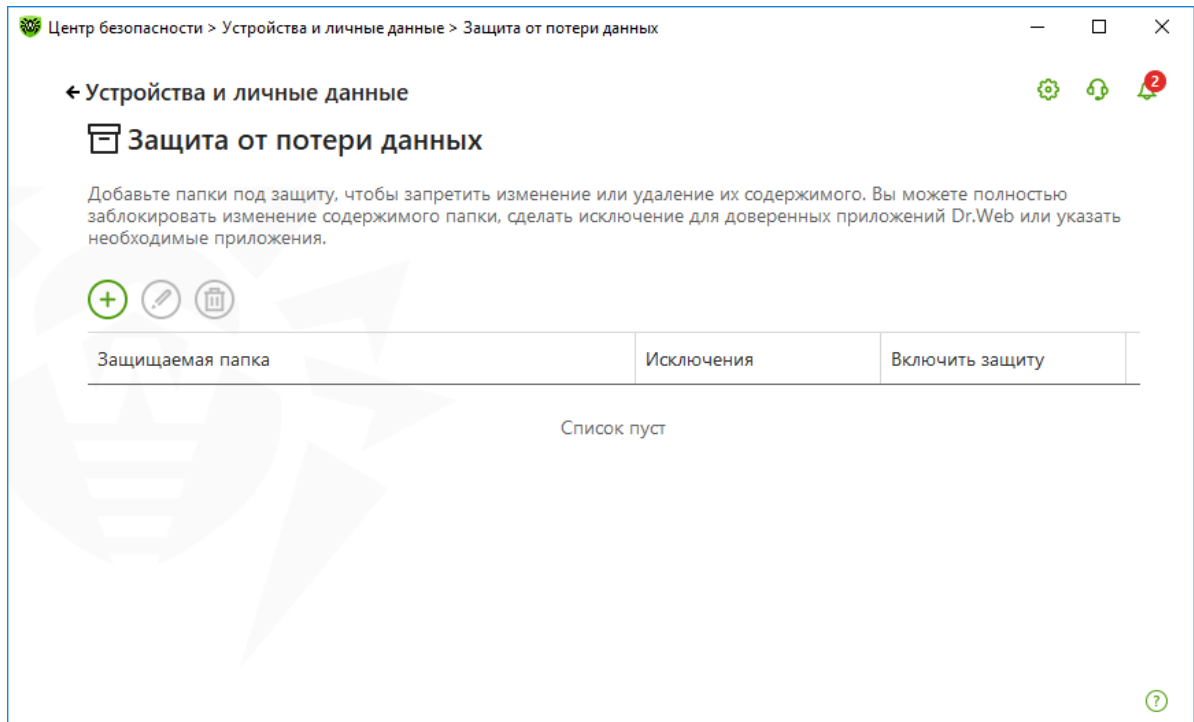
Нажмите кнопку **ОК**.



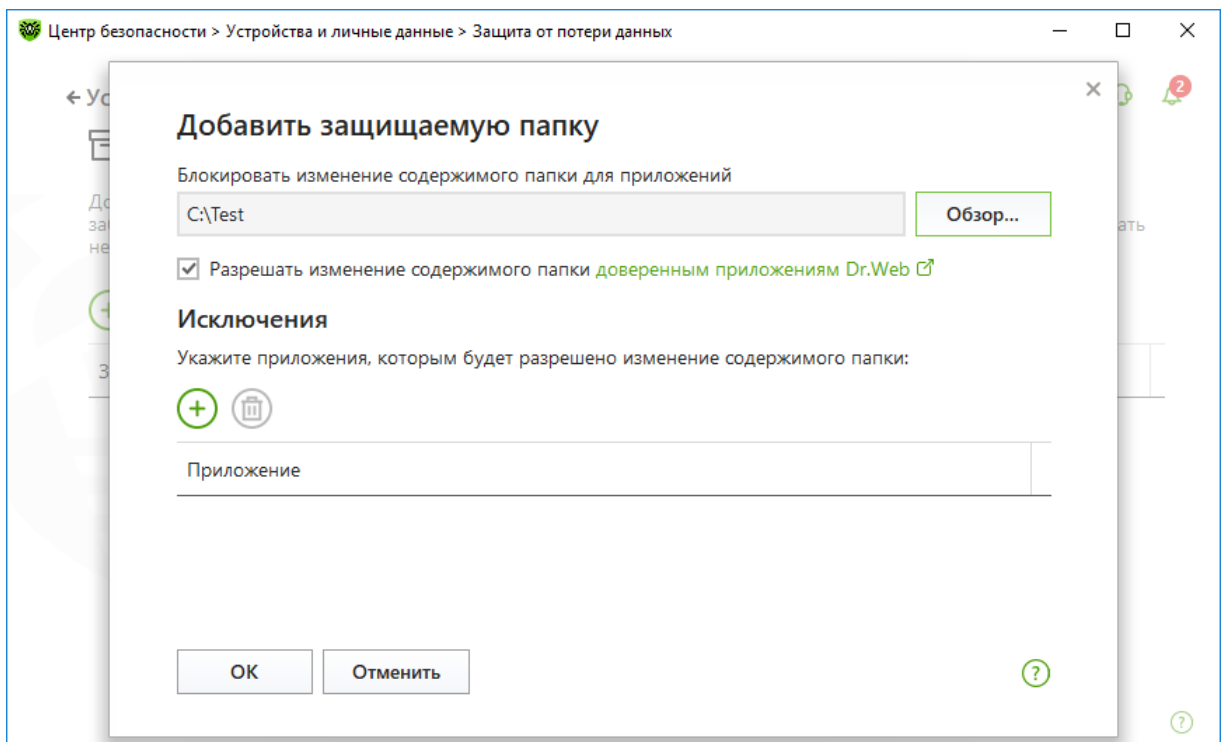
8.11. Функционал «Защита от потери данных»


Для настройки параметров «Защиты от потери данных» кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).

В окне **Центр безопасности** выберите **Устройства и личные данные** и далее **Защита от потери данных**.



В открывшемся окне нажмите  и сформируйте список папок, помещенных под защиту.



В том случае, если вы хотите вручную сформировать список программ, имеющих доступ к защищаемым данным, — нажмите  и укажите имена программ, которым вы даете такое право.

8.12. Проверка работоспособности продукта

Пользователь всегда может убедиться в работоспособности выбранного продукта. Для этого необходимы следующие действия.

1. Проверьте, что антивирус установлен и работает. Самый простой тест — для его проведения посмотрите в трей и убедитесь в наличии значка Dr.Web. Если значок есть — антивирус запущен.

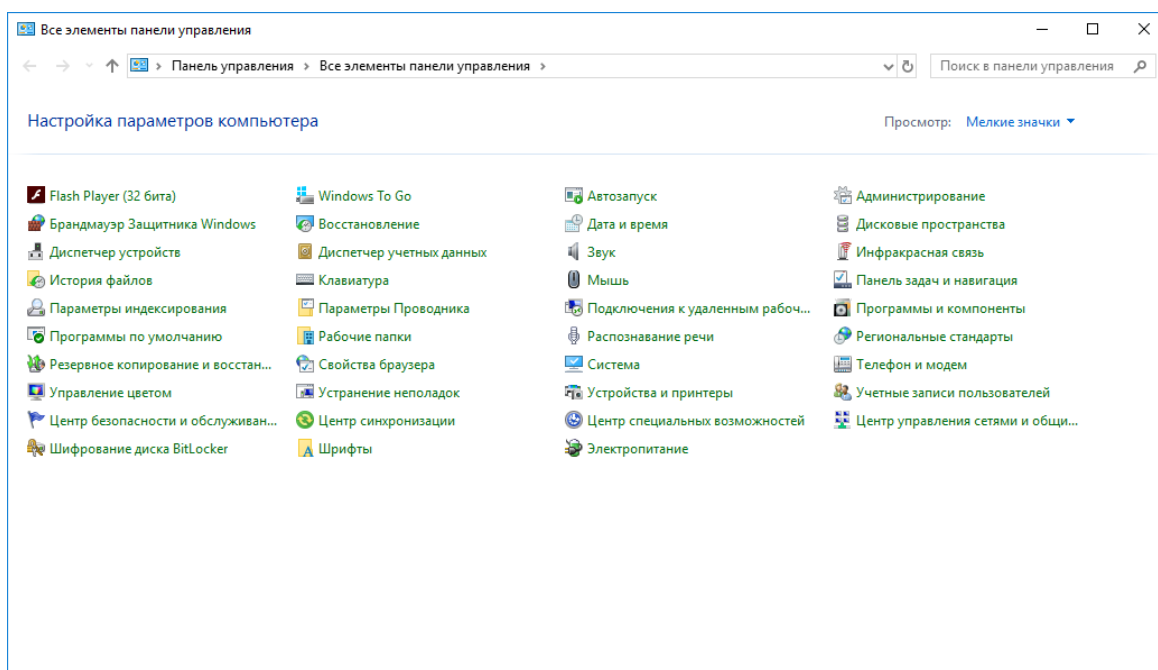
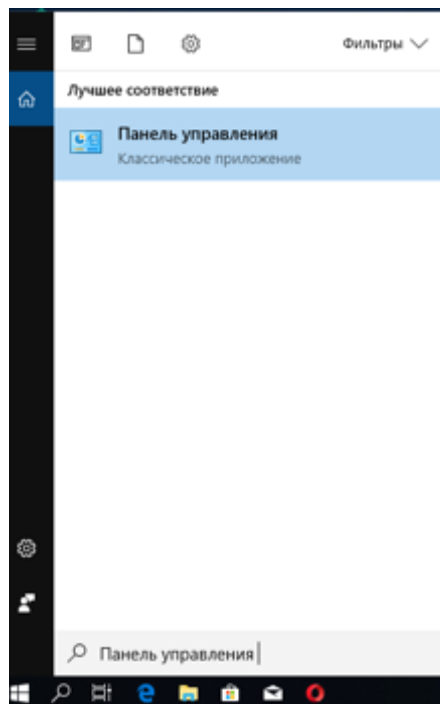
Тест необходим в связи с тем, что установка антивируса может не завершиться успехом — например, по причине того, что файловая система ОС имеет проблемы или установке препятствует иное ПО. Ситуация редкая, крайне маловероятная, но всё когда-либо может случиться и у тестировщика. А вот у пользователей, кстати, иногда обнаруживается, что антивируса на их машине нет, хотя они думают иначе.

Изображения иконки в различных версиях антивируса Dr.Web несколько отличаются, но в любом случае на иконке должен присутствовать узнаваемый паучок

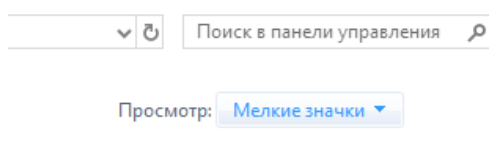


Если иконка отсутствует, проверьте наличие антивируса в установленных программах. Тут порядок действий отличается для разных ОС:

- для Windows XP (в зависимости от вида меню «Пуск»):
 - Меню «Пуск»: **Пуск** → **Панель управления** → **Установка и удаление программ**.
 - Классическое меню «Пуск»: **Пуск** → **Настройка** → **Панель управления** → **Установка и удаление программ**.
- для Windows Vista (в зависимости от вида меню «Пуск»):
 - Меню «Пуск»: **Пуск** → **Панель управления**, далее в зависимости от вида Панели управления:
 - Классический вид: **Программы и компоненты**.
 - Домашняя страница: **Программы** → **Программы и компоненты**.
 - Классическое меню «Пуск»: **Пуск** → **Настройка** → **Панель управления** → **Программы и компоненты**.
- для Windows 7 выберите **Пуск** → **Панель управления**, далее в зависимости от вида Панели управления:
 - Мелкие/крупные значки: **Программы и компоненты**.
 - Категория: **Программы** → **Удаление программ**.
- для Windows 8/8.1/10 откройте **Панель управления** любым удобным способом, например через пункт **Панель управления** в контекстном меню, вызываемом правым щелчком мыши по левому нижнему углу экрана.

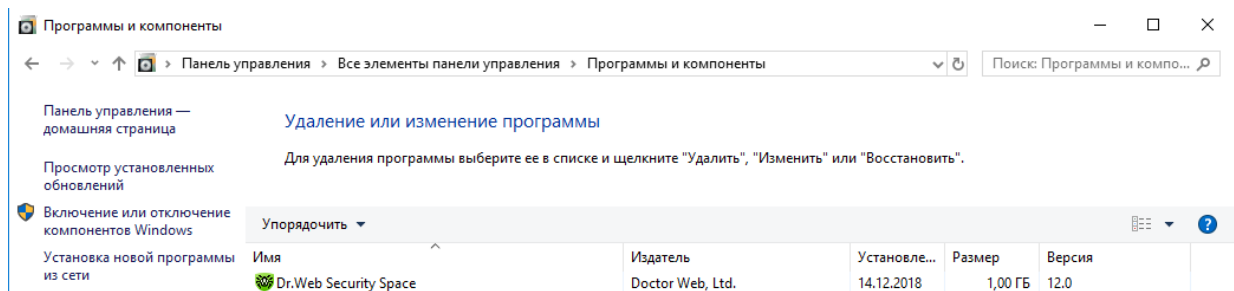


Далее, в зависимости от установленного типа отображения **Просмотр**:



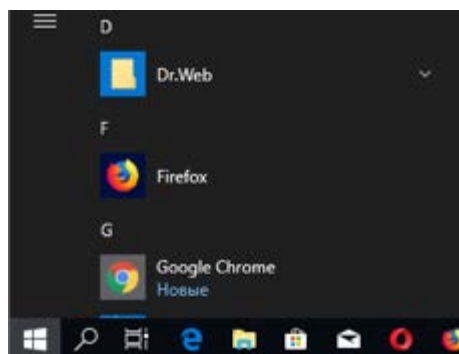
- Мелкие/крупные значки: **Программы и компоненты.**
- Категория: **Программы** → **Удаление программ.**

В открывшемся списке должен отображаться установленный вами продукт.



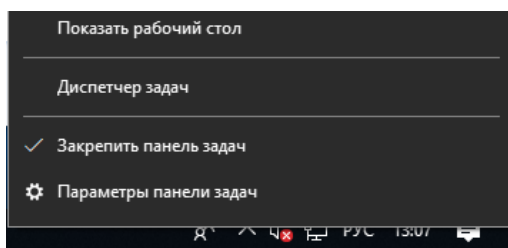
Отметим важную информацию. Столбец **Версия** списка установленных программ показывает версию установленного антивируса.

Если программа установлена, то она также должна присутствовать в меню **Пуск**.



2. Если программа установлена, проверьте список процессов.

Для того чтобы его запустить, например, кликните по Панели задач (полоске с иконками запущенных программ, как правило, располагающейся внизу экрана) и выберите пункт **Диспетчер задач**.



В нем должны отображаться процессы запущенного антивируса (для показа всех процессов в зависимости от версии ОС отметьте чекбокс **Отображать процессы всех пользователей** или **Подробнее**).

Диспетчер задач						
Файл Параметры Вид						
Процессы Производительность Журнал приложений Автозагрузка Пользователи Подробности Службы						
Имя	Состояние	52% ЦП	73% Память	3% Диск	0% Сеть	
Dr.Web Anti-Rootkit Server		49,5%	50,4 МБ	0,1 МБ/с	0 Мбит/с	
Dr.Web Anti-Spam (32 бита)		0%	0,1 МБ	0 МБ/с	0 Мбит/с	
> Dr.Web Control Service		0%	49,4 МБ	0,1 МБ/с	0 Мбит/с	
> Dr.Web Firewall for Windows se...		0%	1,1 МБ	0 МБ/с	0 Мбит/с	
> Dr.Web Scanning Engine (32 би...		0%	70,7 МБ	0 МБ/с	0 Мбит/с	
Dr.Web Scanning Watcher (32 б...		0%	0,2 МБ	0 МБ/с	0 Мбит/с	
Dr.Web Updater		0%	3,0 МБ	0,1 МБ/с	0,1 Мбит/с	

3. Убедитесь, что антивирус актуален и в его функционировании проблем не отмечено. Для этого проверьте вид значка в трее.

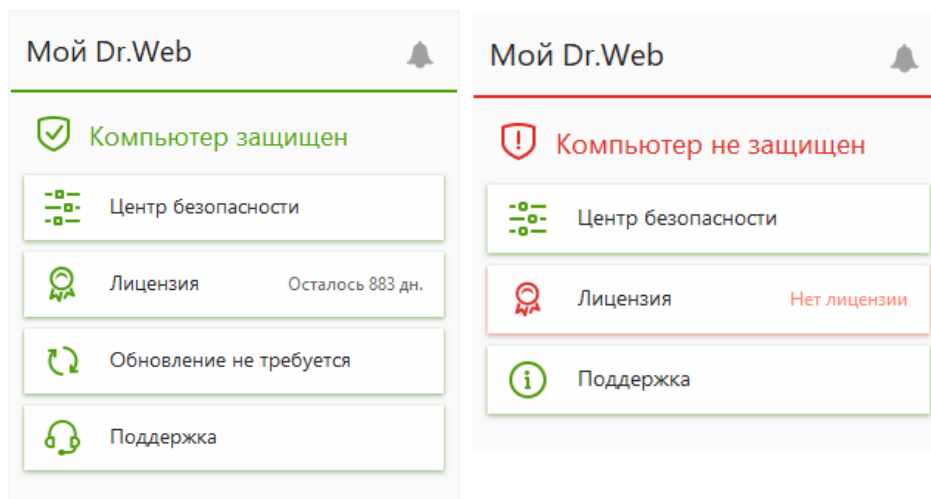
- все компоненты, необходимые для защиты компьютера, запущены и работают правильно;
- самозащита или важный компонент (сторож **SpIDer Guard**, **Брандмауэр**) отключены, что ослабляет защиту антивируса и компьютера. Включите самозащиту или отключенный компонент;
- в процессе запуска одного из ключевых компонентов возникла ошибка. Компьютер находится под угрозой заражения. Проверьте наличие действительного ключевого файла и при необходимости установите его или обратитесь в техническую поддержку.

Проверьте актуальность лицензии — не истекла ли она. Очевидно, что в случае отсутствия актуальной лицензии антивирус не будет обеспечивать полной защиты.

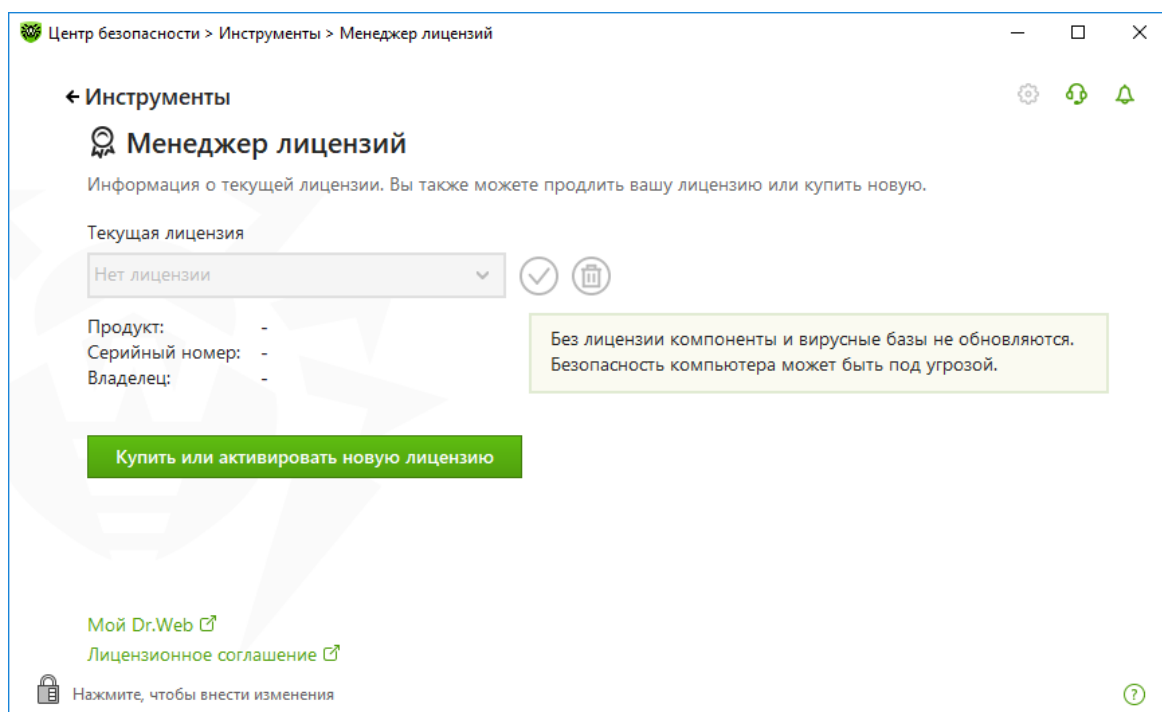
- С помощью левой или правой клавиши мыши щелкните по пиктограмме Dr.Web (пауку) в трее (как правило, в правом в нижнем углу экрана).

Меню с еще действующей лицензией

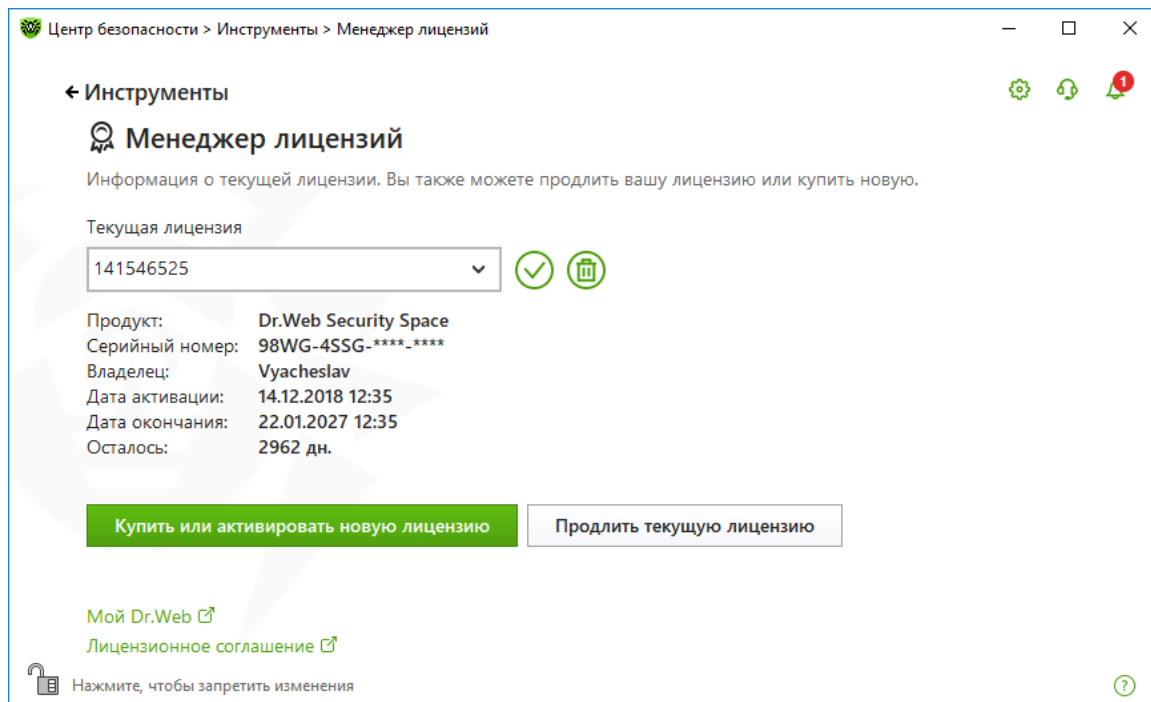
Меню с истекшей лицензией



2. Выберите в меню пункт **Лицензия**. Если на компьютере не использовалась ранее ни одна лицензия, окно Менеджера лицензий будет выглядеть следующим образом:



Если у вас есть предыдущая лицензия и она еще действует, то в **Менеджере лицензий** будет показан ее номер.

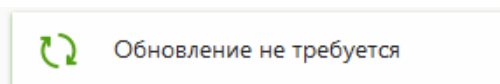


В пункте **Осталось** показывается количество дней до срока истечения лицензии.

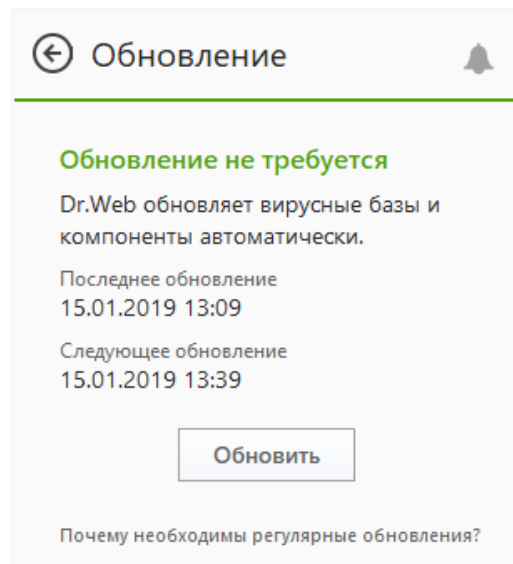
3. Если у вас имеется не активированная лицензия, нажмите в меню антивируса пункт **Лицензия** → **Купить или активировать новую лицензию** и введите ваш серийный номер лицензии.

Бывает, что купленная (или полученная) лицензия не совпадает с установленным продуктом. Скажем, установлен продукт Dr.Web KATANA, а лицензия — на Dr.Web Security Space. В этом случае переустановите продукт или попытайтесь изменить лицензию, обратившись к поставщику.

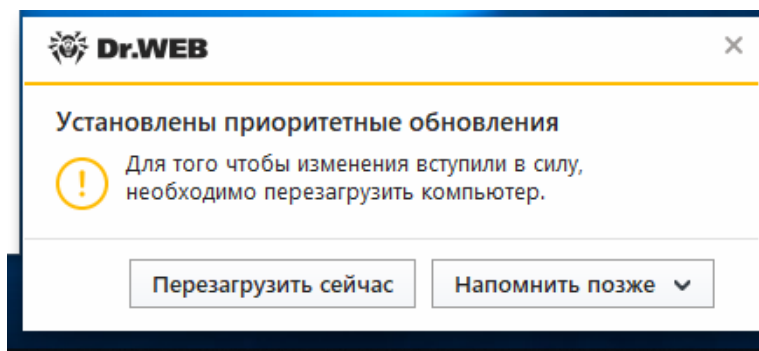
Проверьте актуальность продукта и в случае необходимости обновите его. Если продукт актуален (установлены все обновления антивирусных баз), то меню антивируса должно содержать надпись **Обновление не требуется**.




Если надпись на кнопке с двумя стрелками иная, кликните на нее и нажмите кнопку **Обновить**. В случае проблем с обновлениями проверьте доступность сети Интернет.

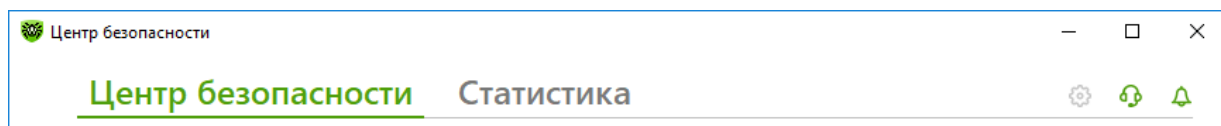


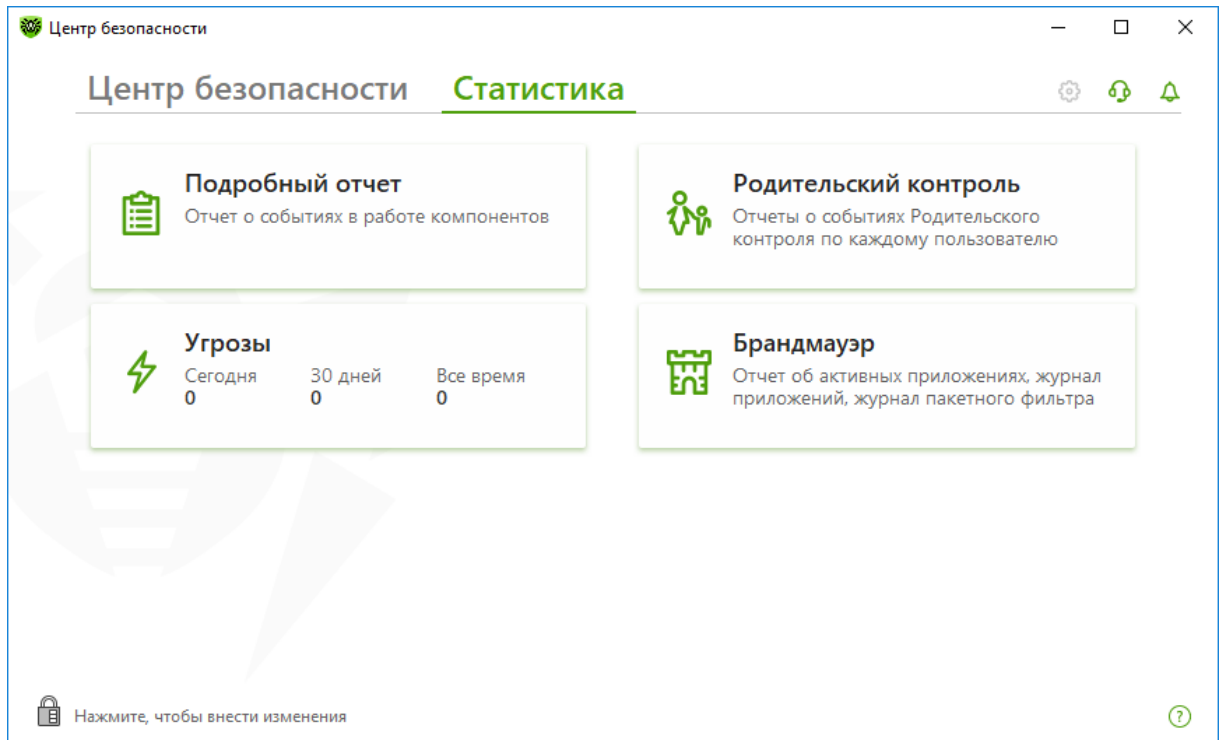
Если обновление потребует перезагрузки, на экран будет выведено предупреждение.



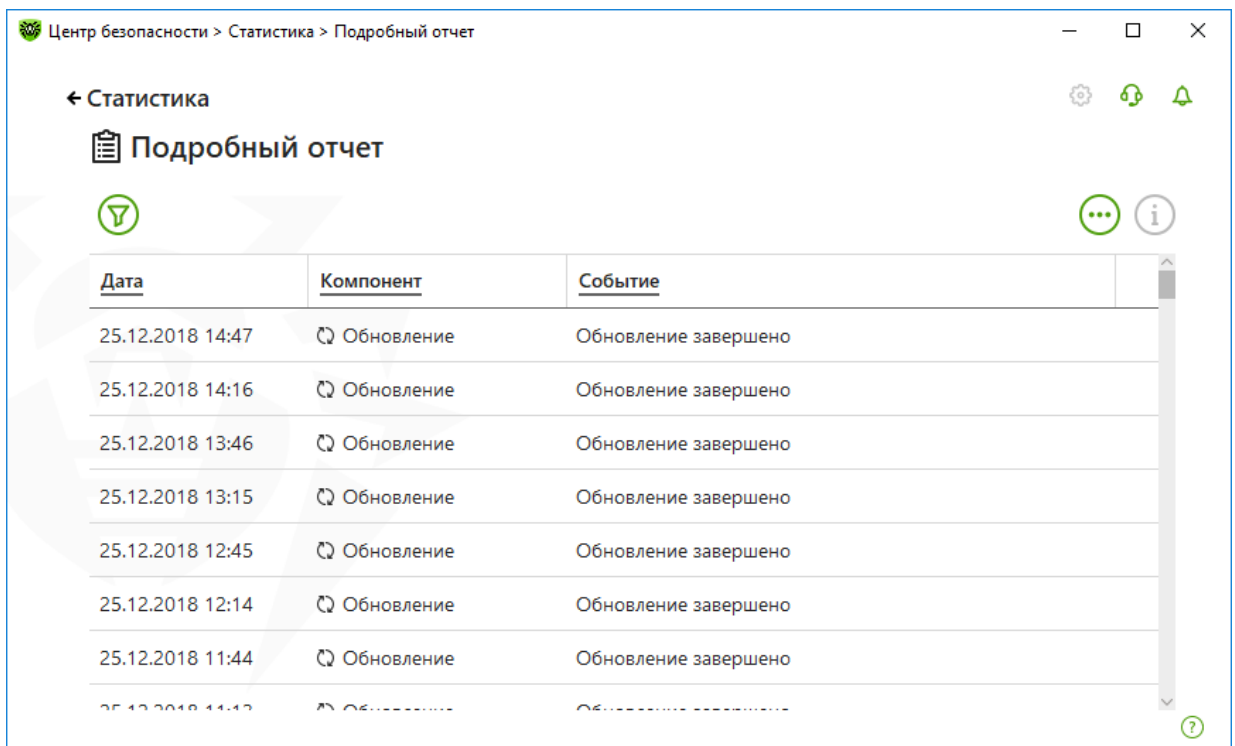
4. После того как вы убедились в актуальности продукта, проведите базовую проверку с помощью специального файла EICAR.

Щелкните по значку  в трее, выберите пункт **Центр безопасности** и перейдите на закладку **Статистика**.

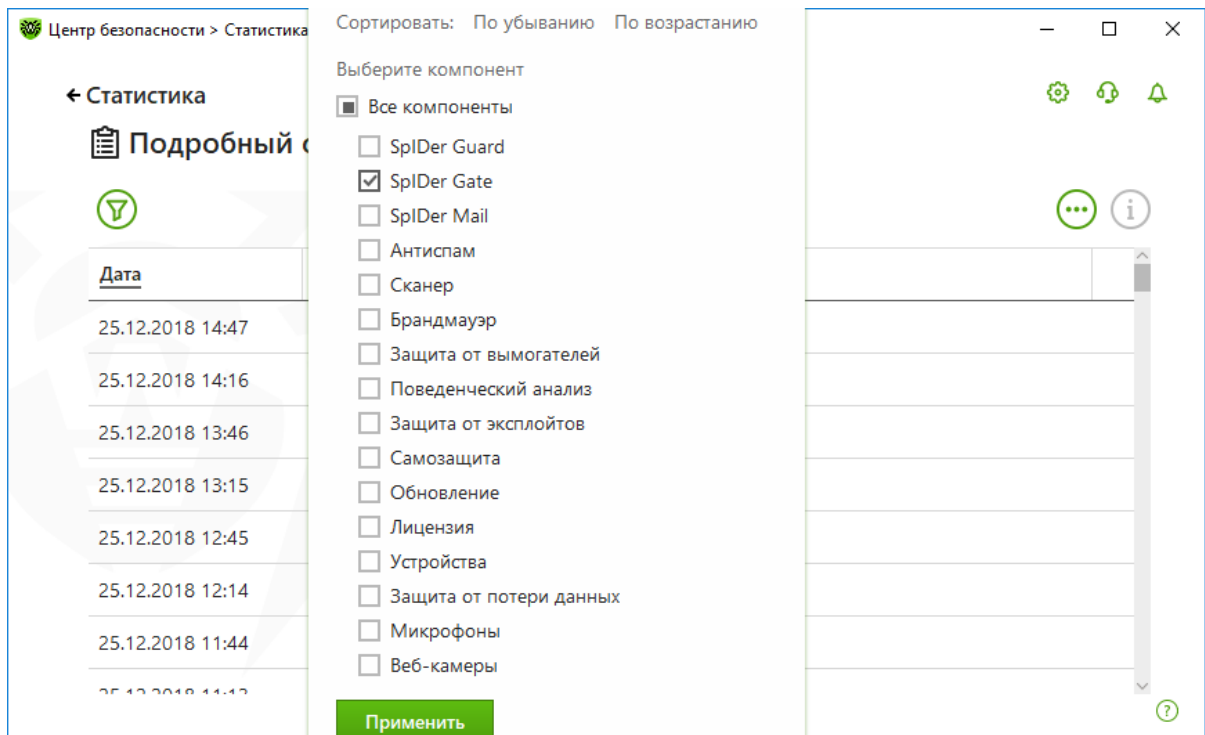




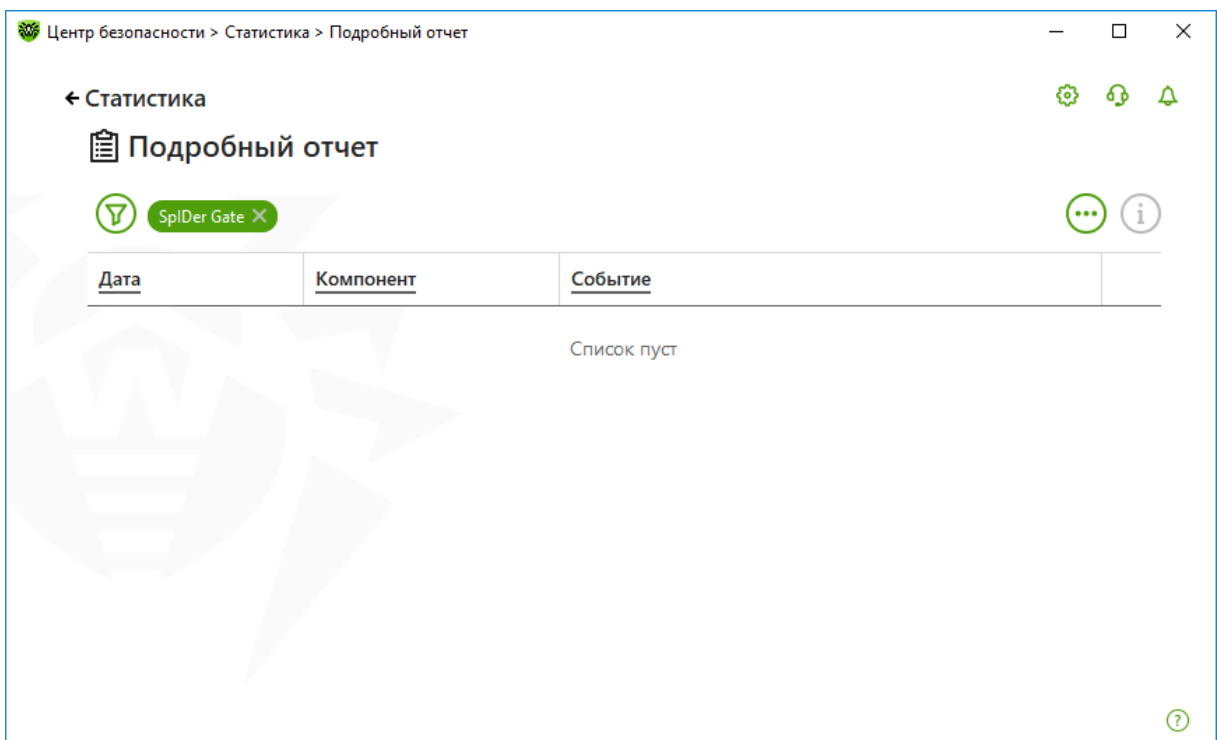
Запомнив количество угроз, нажмите **Подробный отчет**.



Для проверки модуля проверки трафика кликните на колонку **Компонент** и отметьте **SpIDer Gate**.



Нажмите **Применить**.



Запомните количество обнаруженных инфицированных объектов в строке с данными по компоненту.

Откройте браузер и перейдите по адресу <http://2016.eicar.org/85-0-Download.html>.

На открывшейся странице найдите текст:

Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.bxt 68 Bytes	eicar_com.zip 184 Bytes	eicar.com 308 Bytes
--	--	---	---

Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.bxt 68 Bytes	eicar_com.zip 184 Bytes	eicar.com 308 Bytes
---	---	--	--

и выберите для скачивания любой из предложенных вариантов, например первый — eicar.com.

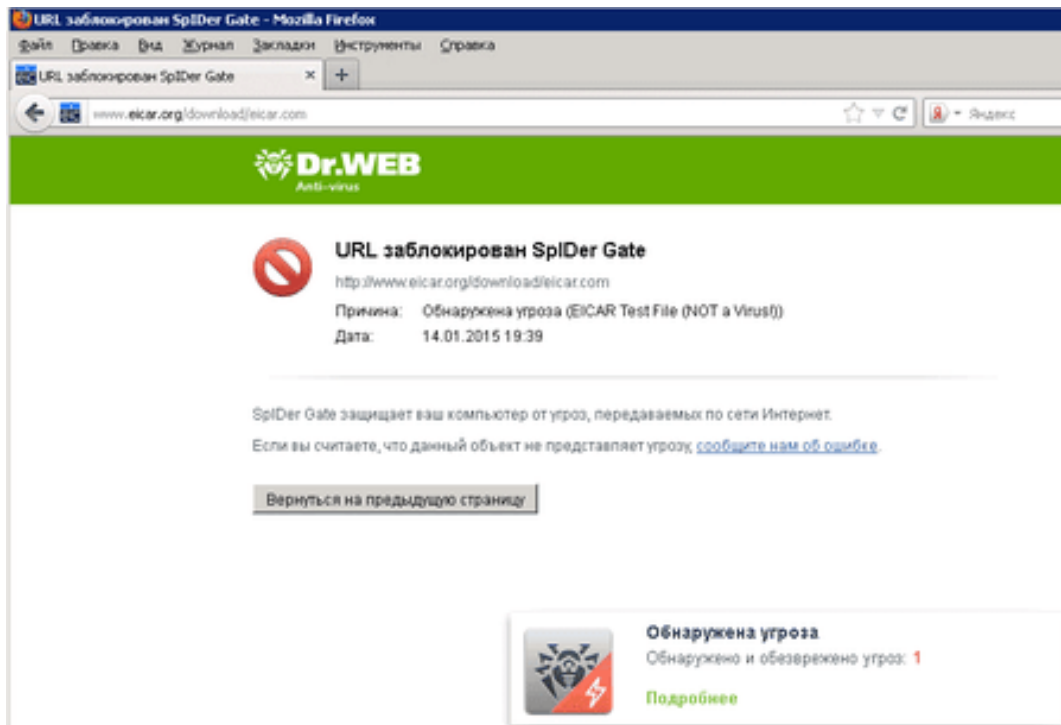
Данная «программа» (EICAR — European Institute for Computer Anti-Virus Research) была специально разработана для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении вируса. Программа не является вредоносной, но специально обрабатывается большинством антивирусных программ как вирус. Dr.Web называет этот «вирус» EICAR Test File (Not a Virus!). Примерно так его называют и другие антивирусные программы. Программа представляет собой 68-байтный COM-файл, в результате исполнения которого выводится текстовое сообщение EICAR-STANDARD-ANTIVIRUS-TEST-FILE! В 64-битных Windows 10 данная программа не запускается.

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

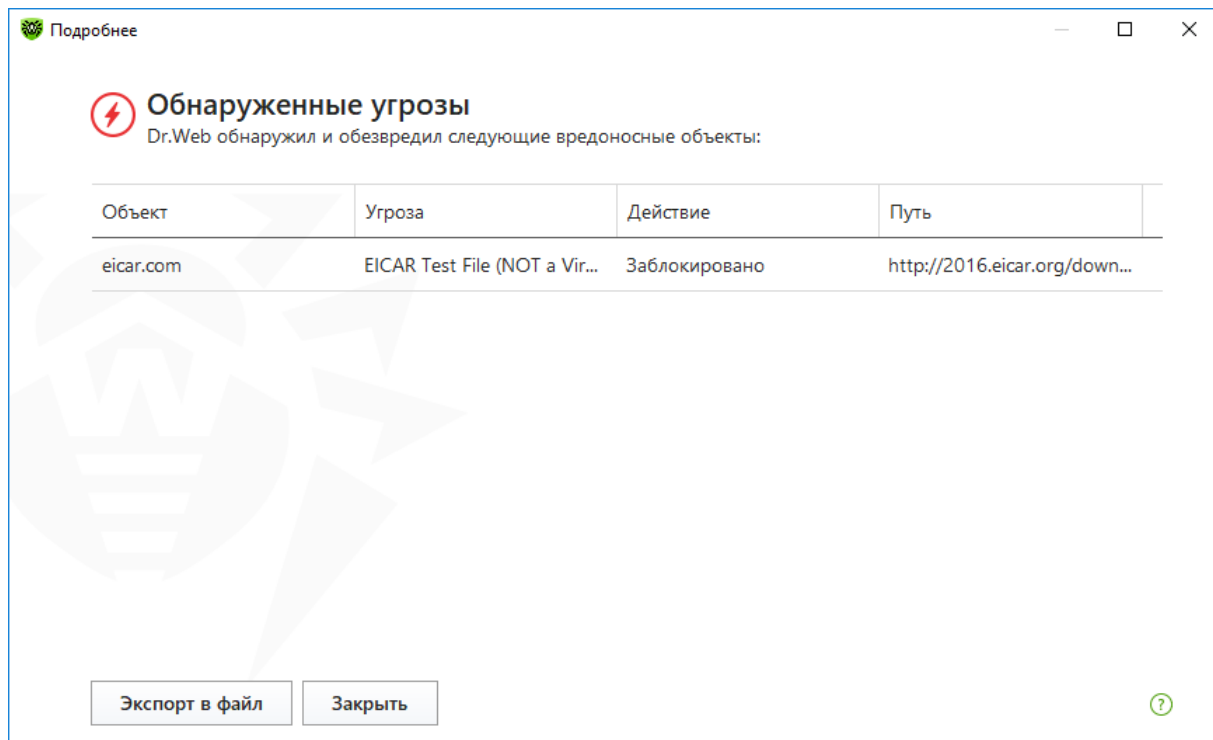
```
X5O!P% @AP[4PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

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

Если защита работает корректно, браузер должен показать следующее окно:

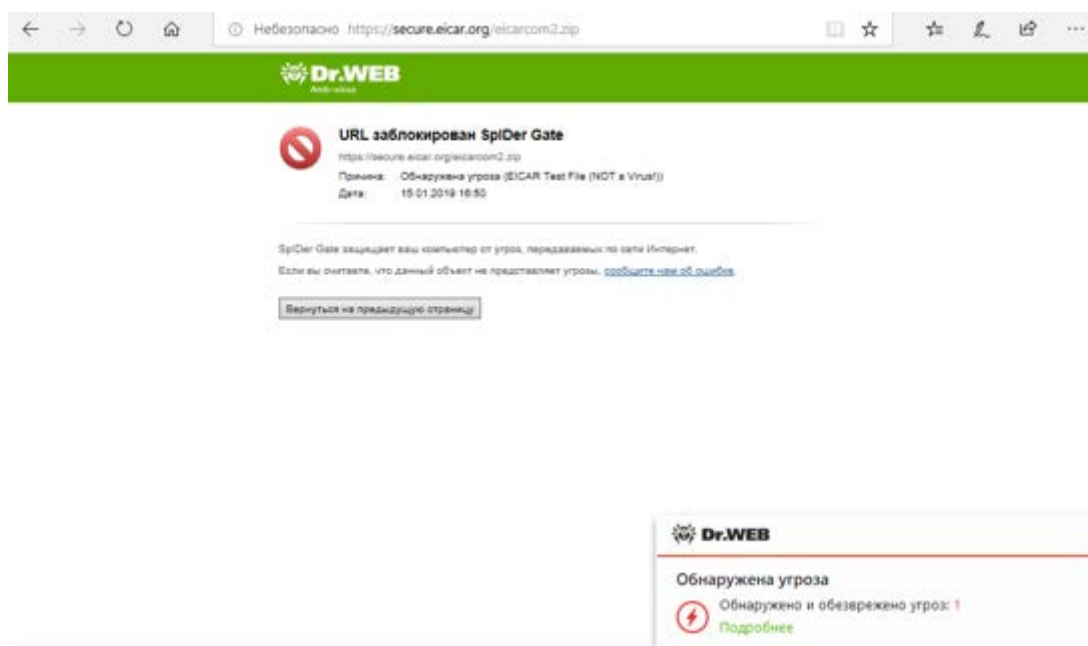


Нажмите на кнопку **Подробнее** всплывающего окна, чтобы получить более подробную информацию.

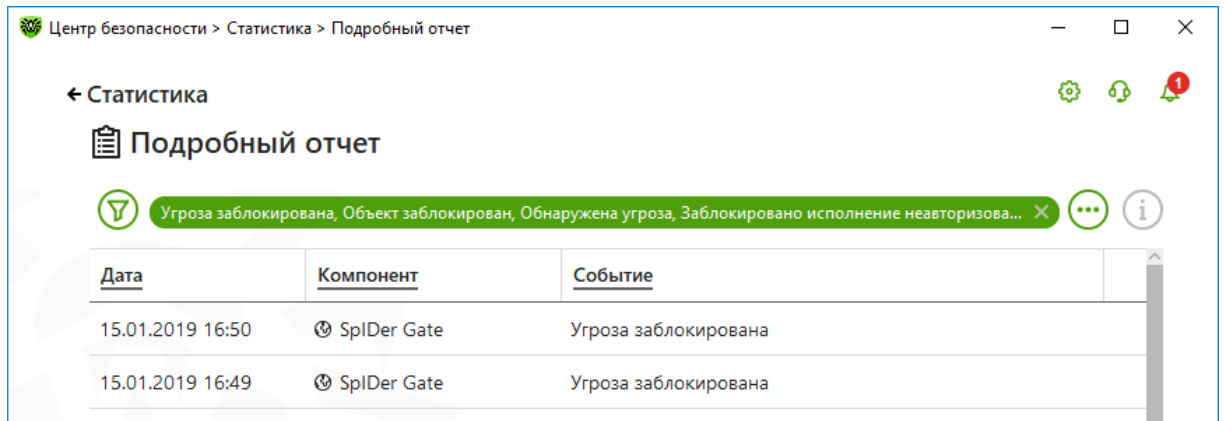


Для проверки того, что модуль проверки трафика проверяет архивы, выберите eicar_com.zip или eicarcom2.zip. В случае обнаружения угрозы будет получено окно предупреждения, аналогичное предыдущему.

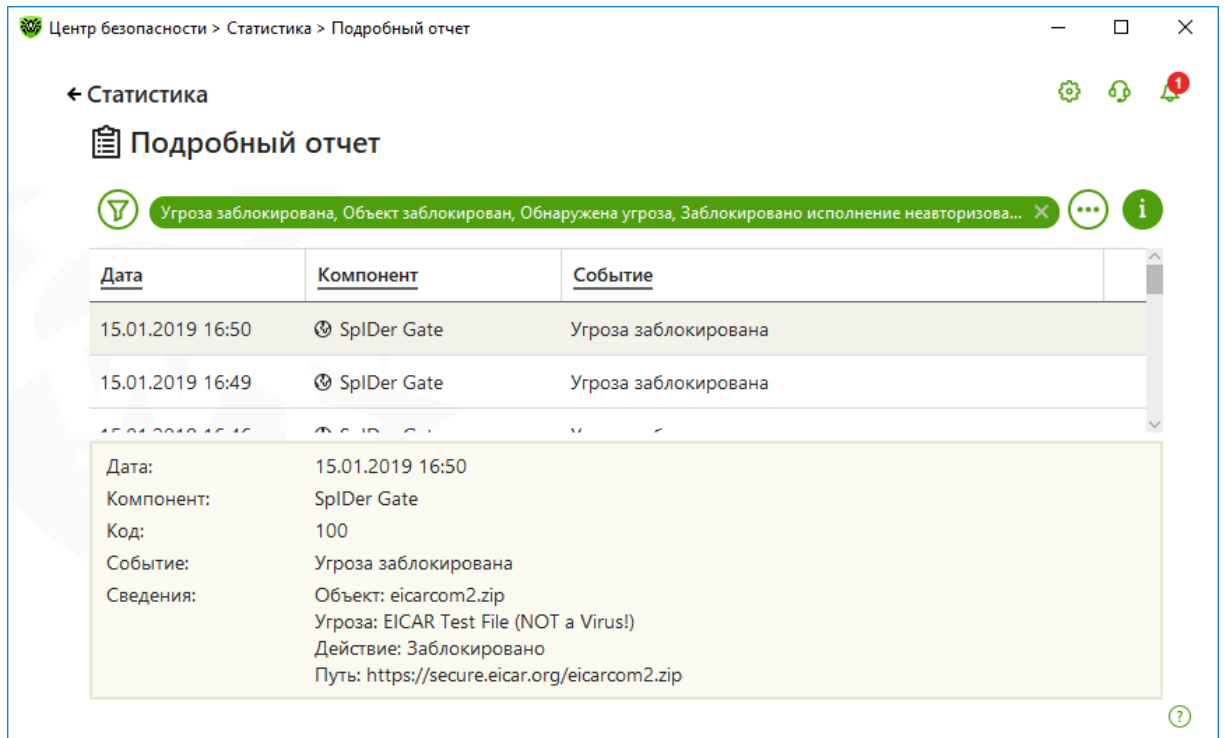
Для того чтобы проверить, проверяется ли зашифрованный трафик, выберите файлы Eicar из раздела Download area using the secure, SSL enabled protocol https.



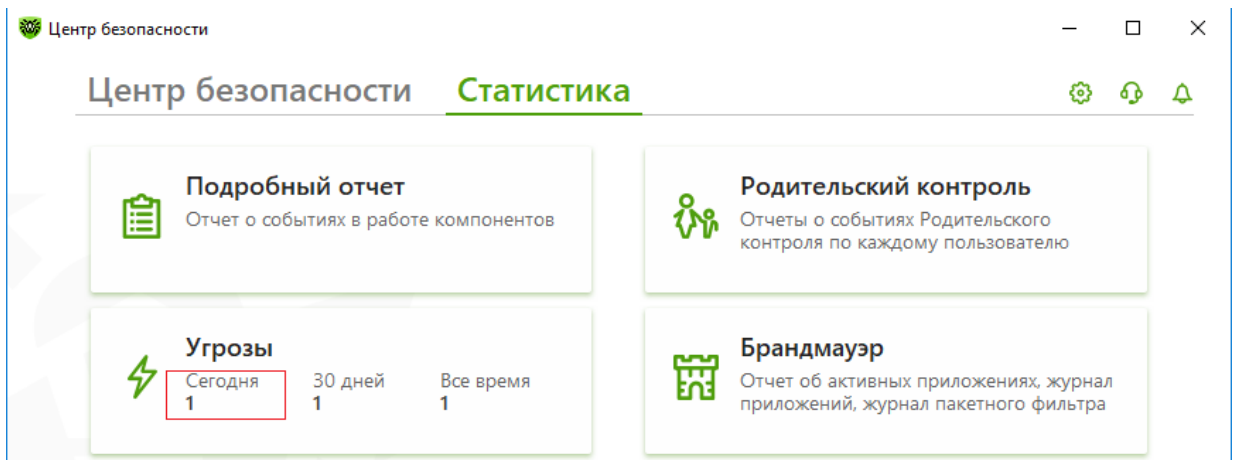
Вернитесь в раздел **Статистика**. Подробный отчет должен содержать строку **Угроза заблокирована**.



Нажав на **i**, вы получите подробную информацию об инциденте.



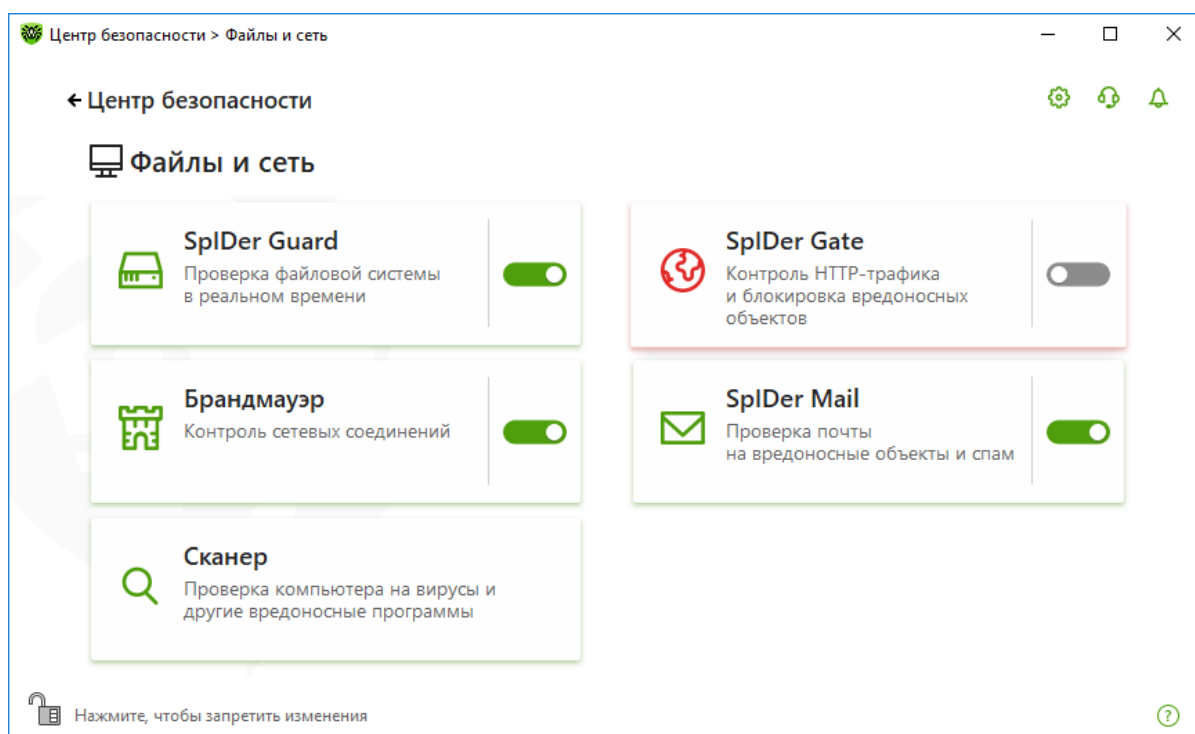
Количество обнаруженных инфицированных объектов компонентом **SpIDer Gate** должно увеличиться. Ниже приведен скриншот для теста одного вредоносного файла.



Переходим к тестированию файлового монитора.

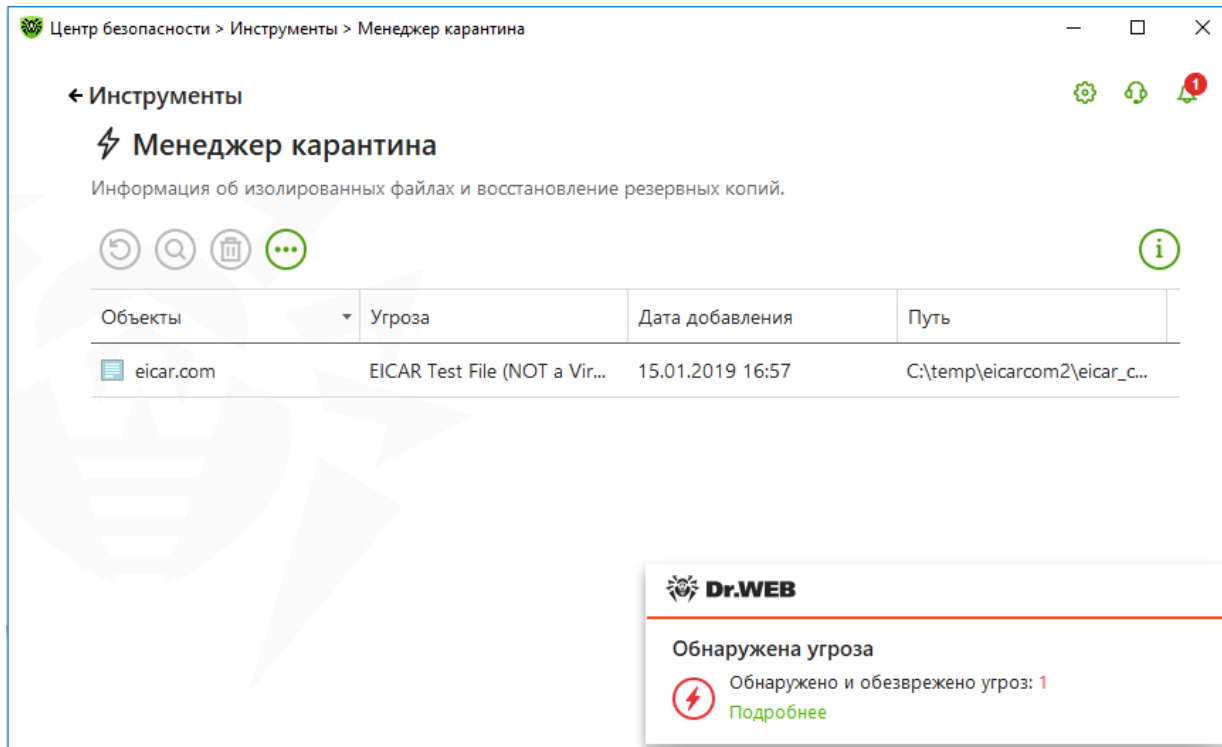
Если необходимо проверить работу файлового монитора, сначала получите файл с тестовым вирусом. Для этого отключите **SpIDer Gate** — иначе он заблокирует попытки его скачать.

Кликните на иконке паучка в трее, выберите **Центр безопасности**, зайдите в **Файлы и сеть**, нажмите на замочек в нижнем левом углу окна для того, чтобы разрешить внесение изменений, и передвиньте бегунок **SpIDer Gate**.



Вернитесь на сайт eicar.org и снова попытайтесь загрузить тестовый «вирус». Итогом попытки должно стать уведомление **Обнаружена угроза** в правом нижнем углу экрана.

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 попытке открыть такой файл на компьютере **SpIDer Guard** автоматически обрабатывает файл как вредоносную программу и по умолчанию перемещает его в **Карантин** — точно так же, как это сделал **SpIDer Gate**.

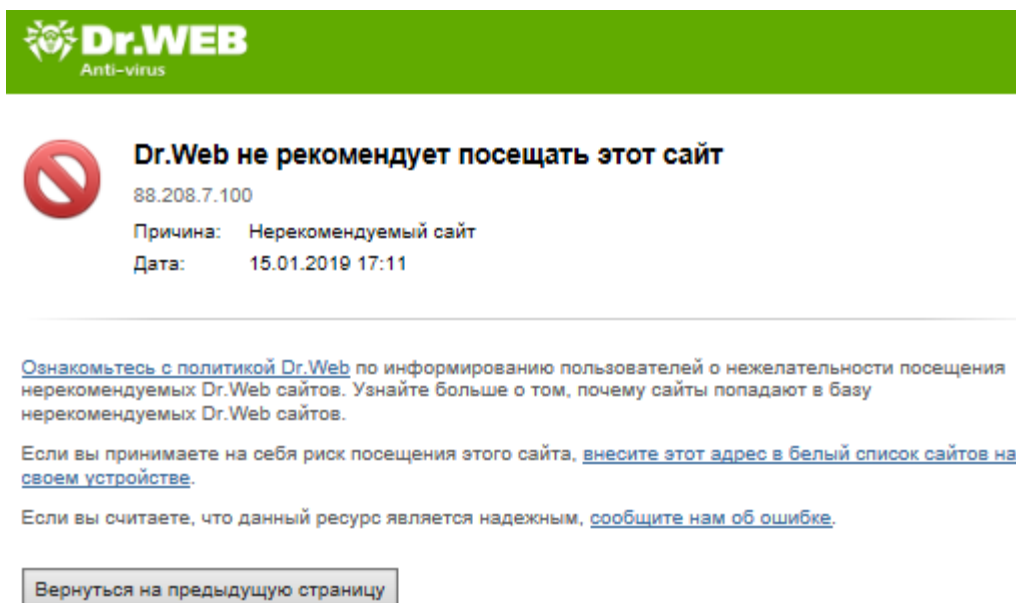


После завершения проверки включите **SpIDer Gate**, нажав на переключатель в соответствующем разделе.

Для тестирования работы системы проверки почтового трафика Eicar можно послать в виде вложения.

Чтобы проверить работу модуля **Родительского контроля**, пополните черный список в настройках модуля.

Затем откройте браузер и введите адрес, добавленный в черный список **Родительского контроля**. Запрашиваемая страница не будет открыта, вместо этого в окне браузера появится информационное сообщение:



8.13. Настройка Брандмауэра Dr.Web

Брандмауэр необходим для защиты от несанкционированного доступа извне и



Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

предотвращения утечки важных данных по сети. Этот компонент позволяет контролировать подключение и передачу данных по сети Интернет и блокировать подозрительные соединения на уровне пакетов и приложений. Основные функции этого компонента:

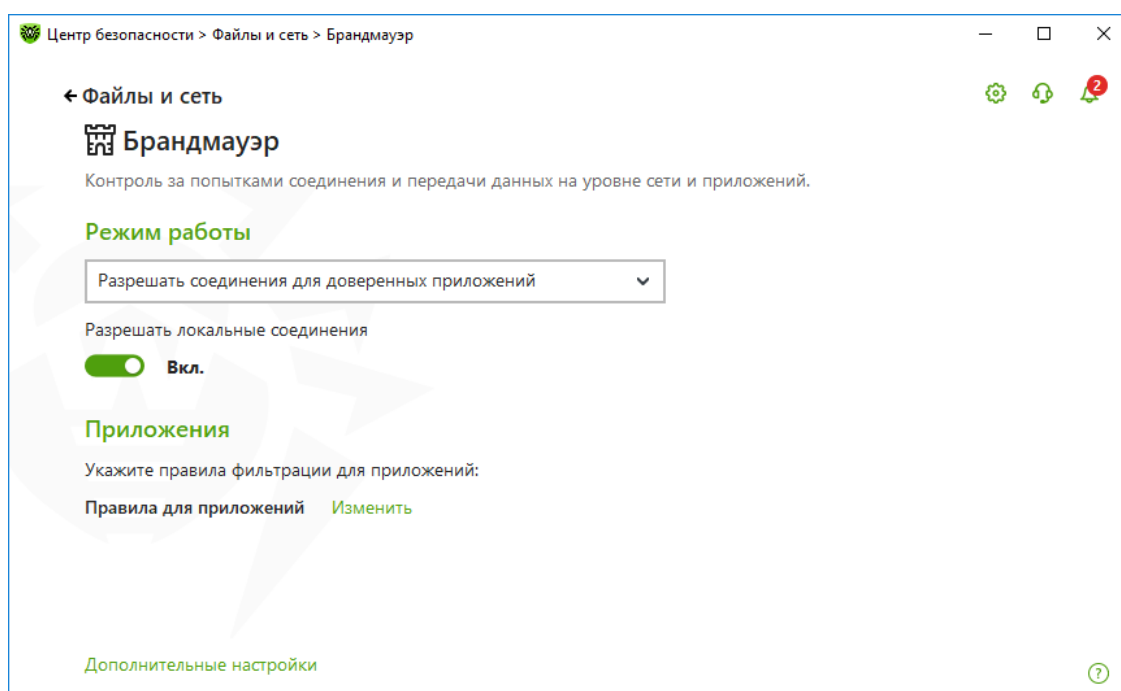
- Контроль и фильтрация всего входящего и исходящего трафика
- Контроль подключения на уровне приложений
- Фильтрация пакетов на сетевом уровне
- Быстрое переключение между наборами правил. Наборы правил определяются пользователем
- Регистрация событий

В настройках этого компонента вы можете выбрать один из режимов его работы, наиболее удобный для вас в данный момент.

Брандмауэр запускается автоматически при старте операционной системы. Вы можете временно приостановить работу **Брандмауэра** (однако в обычных условиях отключать какие-либо компоненты антивируса не рекомендуется), просмотреть статистику фильтрации и изменить настройки программы.

Для настройки параметров работы **Брандмауэра** щелкните кнопкой мыши по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).

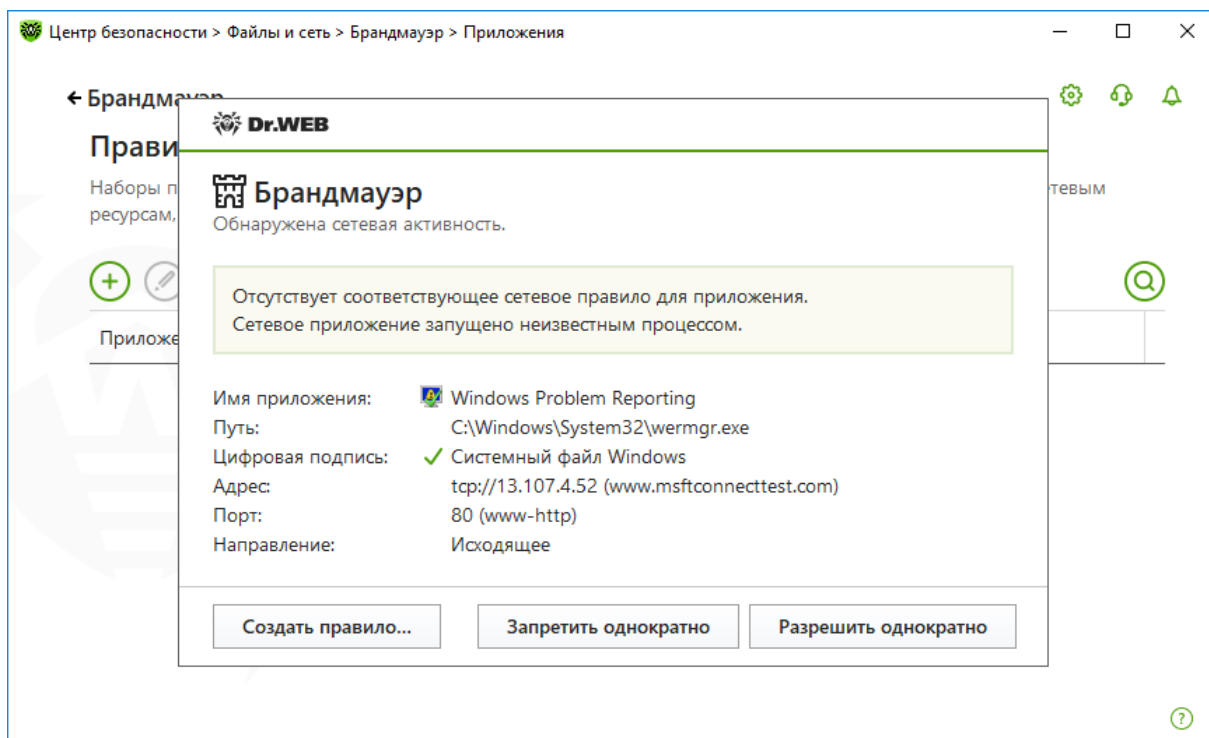
В окне **Центр безопасности** выберите **Файлы и сеть** и далее **Брандмауэр**.



Выберите один из следующих режимов работы:

- **Разрешать неизвестные соединения** — режим, при котором всем неизвестным приложениям предоставляется доступ к сетевым ресурсам;
- **Разрешать соединения для доверенных приложений** — режим, при котором всем доверенным приложениям предоставляется доступ к сетевым ресурсам (используется по умолчанию), для всех остальных приложений выдается предупреждение, где вы можете задать правило;

- **Интерактивный режим** — режим, в котором при обнаружении попытки системы или приложений подключиться к сети **Брандмауэр** проверяет, заданы ли для этих программ правила фильтрации. Если правила отсутствуют, то выводится соответствующее предупреждение, где вы можете задать правило.



Внимание! При работе под учетной записью с ограниченными правами (Гость) **Брандмауэр Dr.Web** не выдает пользователю предупреждения о попытках доступа к сети. Предупреждения будут выдаваться под учетной записью с правами администратора, если такая сессия активна одновременно с гостевой.

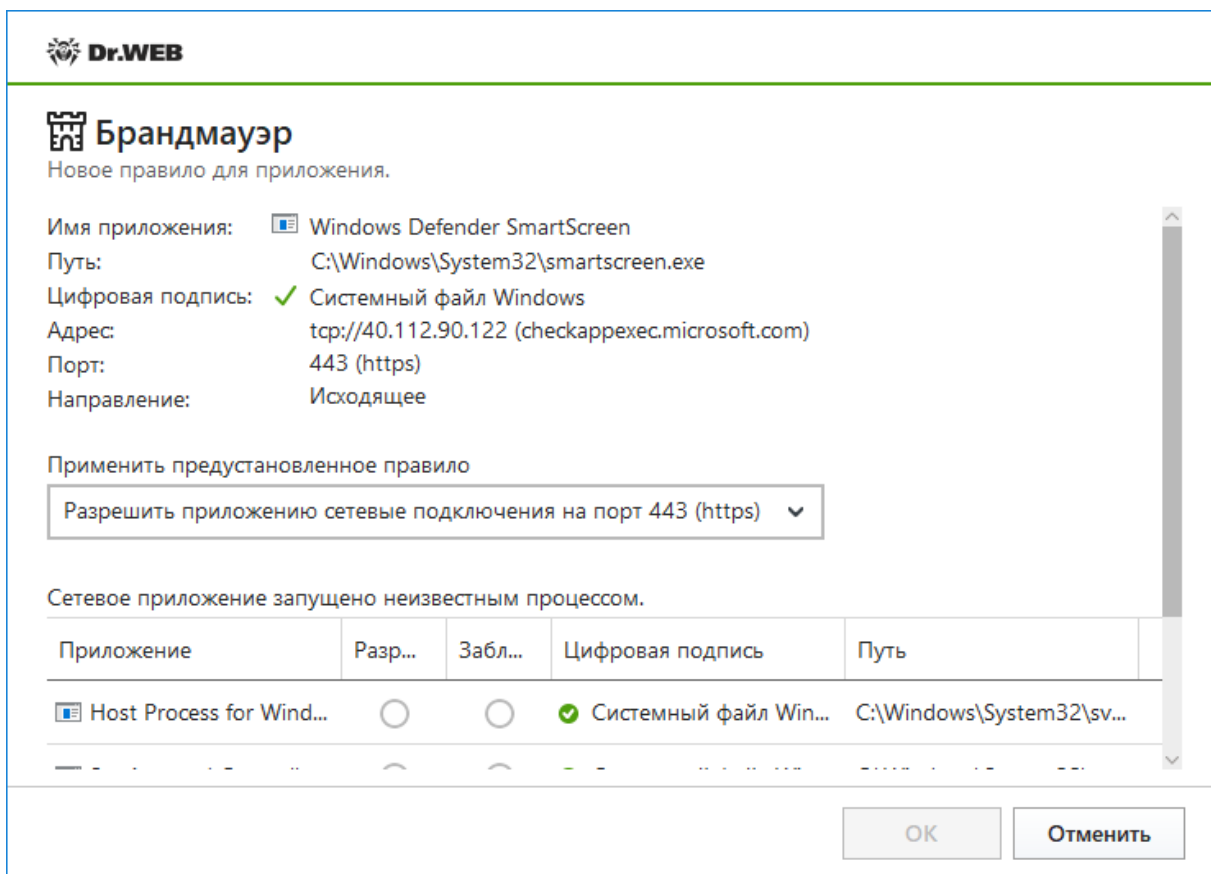
Будьте внимательны при работе с приложениями, запрашивающими доступ к сети. При обнаружении попытки подключения к сети со стороны приложения обязательно ознакомьтесь со следующей информацией:

- **Имя приложения** (наименование программы) — удостоверьтесь, что путь к нему, указанный в поле **Путь**, соответствует правильному расположению программы.
- **Путь** — полный путь к исполняемому файлу приложения и его имя.
- **Цифровая подпись** — цифровая подпись приложения.
- **Адрес** — протокол и адрес хоста, к которому совершается попытка подключения.
- **Порт** — порт, по которому совершается попытка подключения.
- **Направление** — тип соединения.

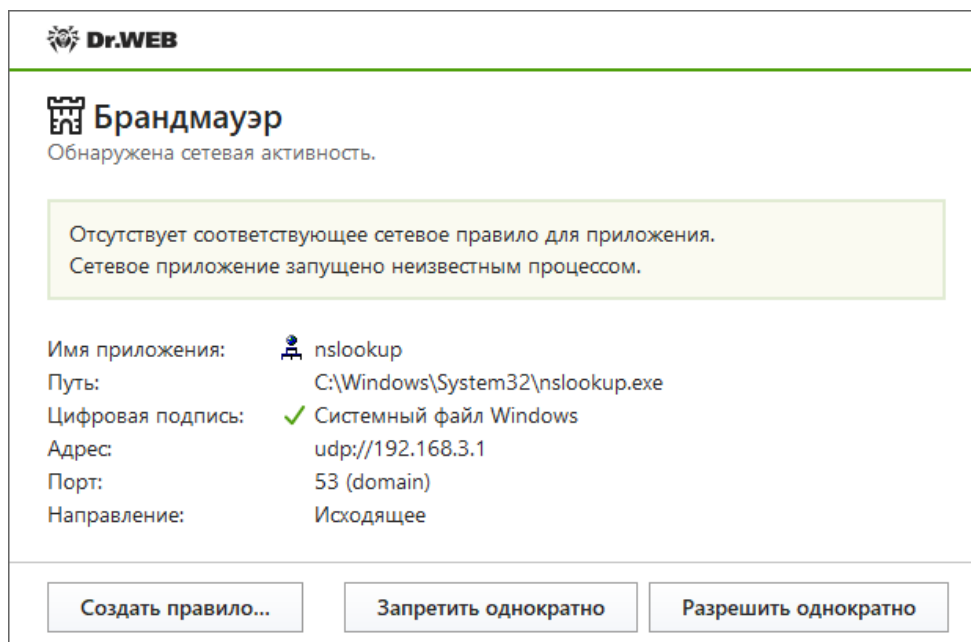
После ознакомления примите решение о подходящей для данного случая операции и выберите соответствующее действие нижней части окна:

- Блокировать данное подключение — выберите действие **Запретить однократно**.
- Позволить приложению данное подключение — выберите действие **Разрешить однократно**.
- Перейти к форме создания правила фильтрации — выберите **Создать правило**. Откроется окно, в котором вы можете либо выбрать предустановленное правило, либо вручную создать правило для приложений:

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию



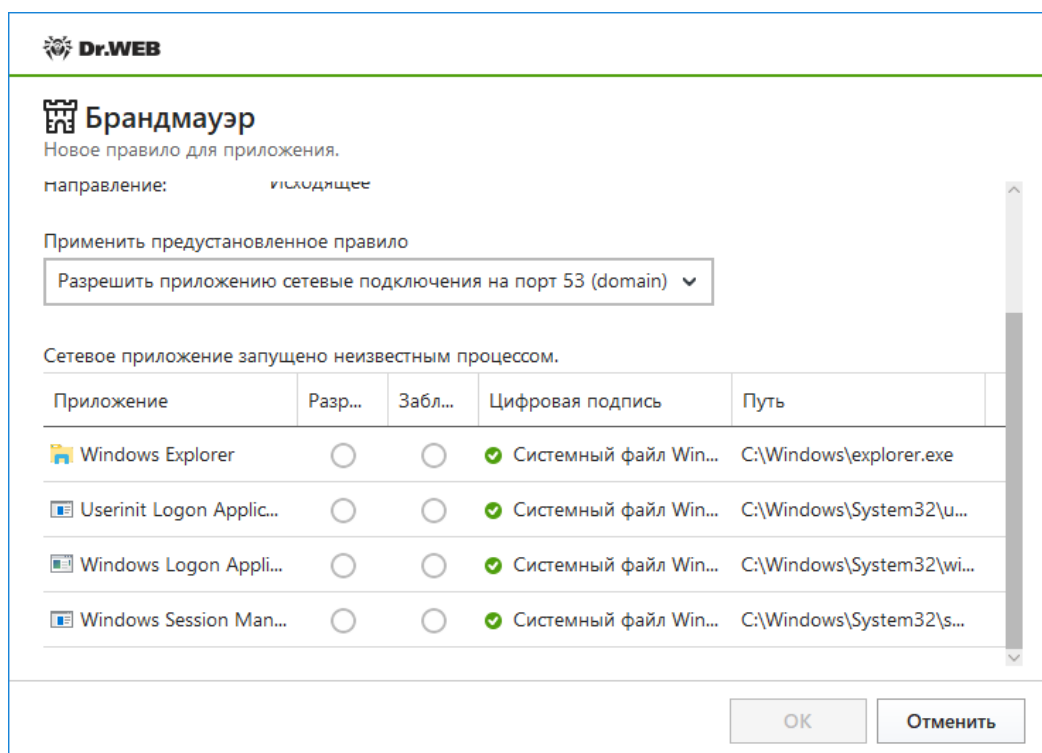
Внимание! В некоторых случаях операционная система Windows не позволяет однозначно идентифицировать службу, работающую как системный процесс. При обнаружении попытки подключения со стороны системного процесса обратите внимание на порт, указанный в сведениях о соединении. Если вы используете приложение,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



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

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

соответствующее предупреждение.



Правила для родительских процессов

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

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

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

По умолчанию **Брандмауэр** автоматически создает правила для известных приложений. Вне зависимости от режима работы производится регистрация событий. Настройки программы

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

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

Настройка **Разрешать локальные соединения** позволяет всем приложениям беспрепятственно устанавливать соединения на вашем компьютере. К таким подключениям правила применяться не будут. Снимите этот флажок, чтобы применять правила фильтрации вне зависимости от того, происходит ли соединение по сети или в рамках вашего компьютера.

8.13.1. Ограничение прав сетевых приложений

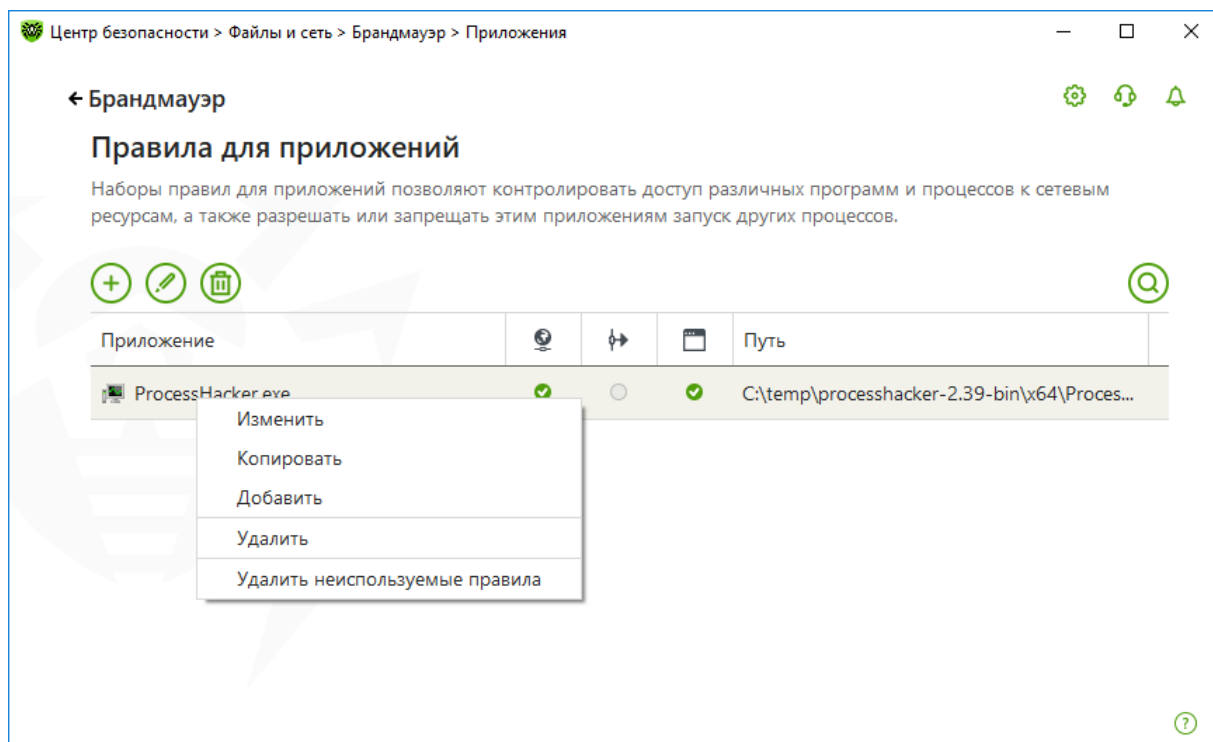
С помощью **Брандмауэра** можно ограничить доступ приложений в Интернет. Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам.

Для ограничения доступа приложения к сетевым ресурсам, а также запрета для них запуска других сетевых приложений в разделе настроек **Приложения** нажмите **Изменить**. На данной странице вы можете формировать наборы правил фильтрации, создавая новые, редактируя существующие или удаляя ненужные правила. Приложение однозначно идентифицируется полным путем к исполняемому файлу.

Если файл приложения, для которого было создано правило, изменился (например, было установлено обновление), то **Брандмауэр** предложит подтвердить, что приложение может обращаться к сетевым ресурсам.

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


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

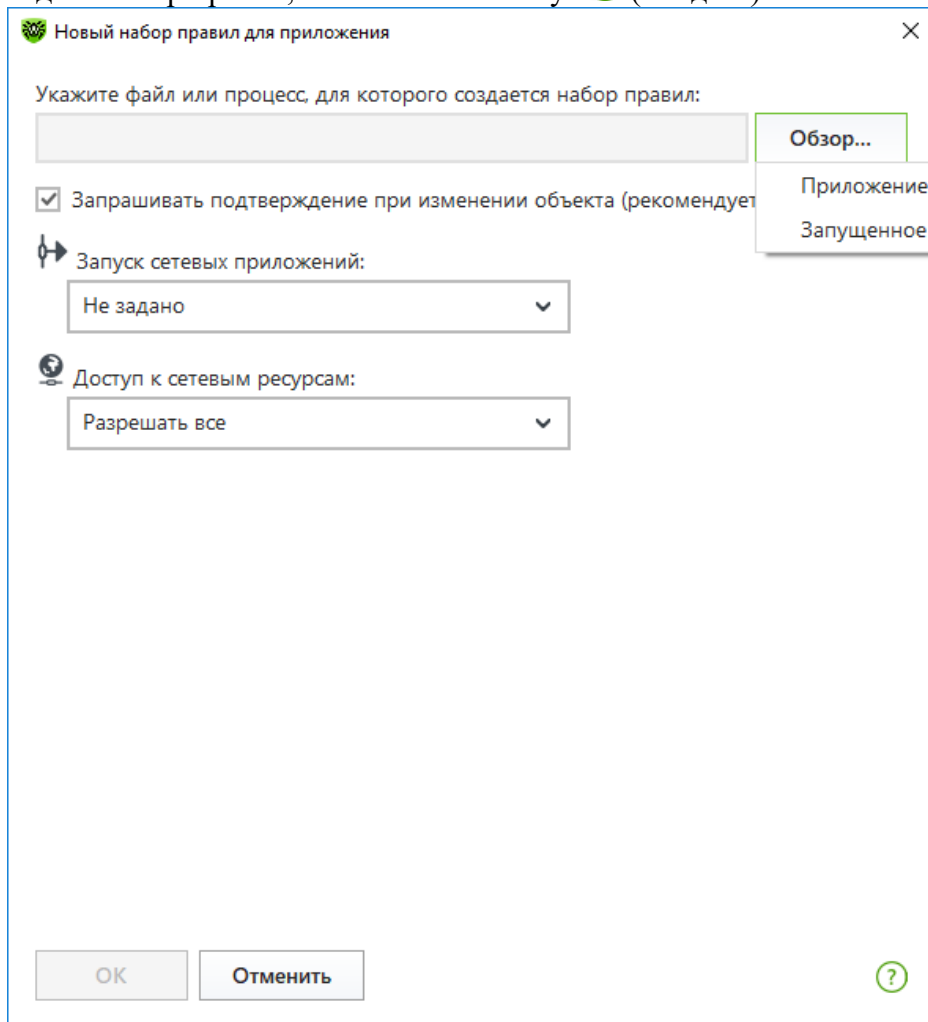


Внимание! Для каждой программы может быть не более одного набора правил фильтрации.

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

Для формирования набора правил выполните одно из следующих действий:

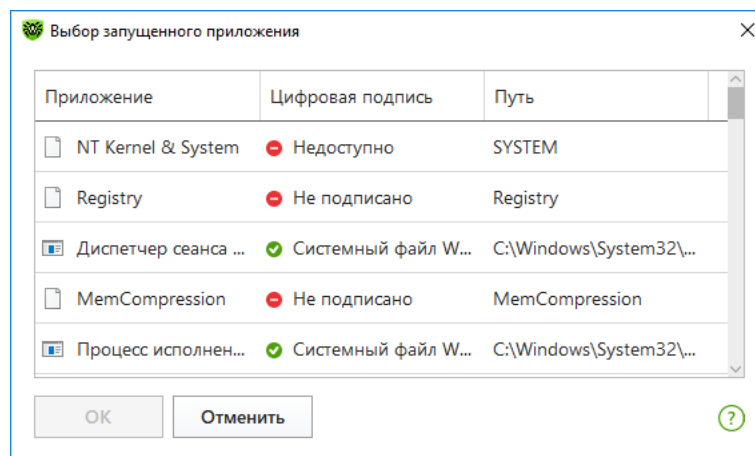
- Чтобы создать набор правил, нажмите на кнопку  (Создать).





В окне **Новый набор правил для приложения** (или **Редактирование набора правил**) отображается тип правила для конкретного приложения или процесса, а также список правил. Вы можете изменять тип правила, формировать список, добавляя новые или редактируя существующие правила фильтрации, а также изменяя порядок их выполнения. Правила применяются последовательно, согласно очередности в списке.

Если вы выбрали создание или редактирование набора правил, в открывшемся окне задайте программу или процесс, для которых будет применяться набор правил. Нажав **Обзор**, вы можете выбрать два варианта поиска приложения по месту размещения на диске и среди запущенных приложений.

- Чтобы задать набор правил для программы, нажмите кнопку **Обзор** и выберите исполняемый файл программы.



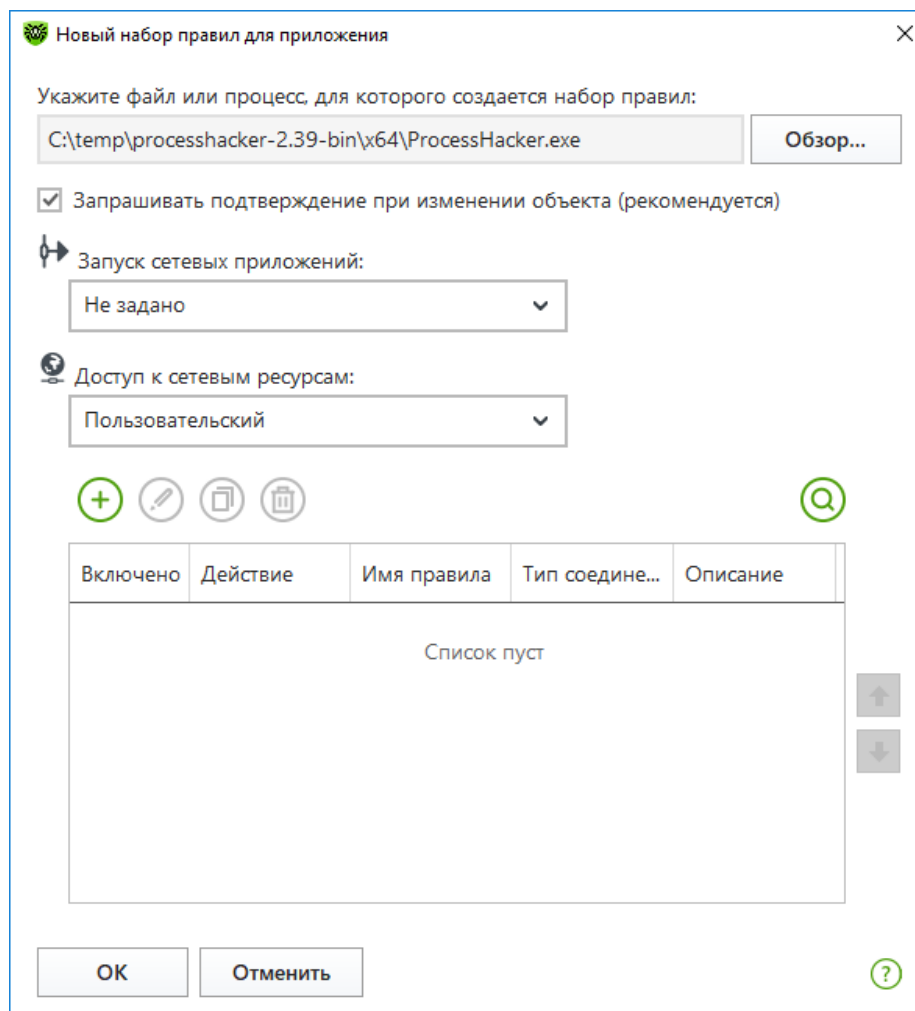
- Чтобы задать набор правил для процесса, нажмите стрелку на кнопке **Обзор**, выберите **Запущенное приложение** и укажите процесс.
- Чтобы отредактировать существующий набор правил, выберите его в списке и нажмите на кнопку  (Изменить).
- Чтобы добавить копию существующего набора правил, выберите **Копировать** в контекстном меню. Копия добавляется под выбранным набором.
- Чтобы удалить все правила для программы, выберите соответствующий набор в списке и нажмите на кнопку  (Удалить).

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

Чтобы разрешить или запретить приложению запускать другие приложения, в выпадающем списке **Запуск сетевых приложений** выберите **Разрешать** или **Запрещать**. При выборе **Не задано** на это приложение будут распространяться настройки выбранного режима работы **Брандмауэра**.



Выберите режим доступа к сетевым ресурсам **Разрешать все** (все соединения приложения будут разрешены), **Блокировать все** (все соединения приложения запрещены), **Не задано** (на это приложение будут распространяться настройки выбранного режима работы **Брандмауэра**) или **Пользовательский** — в этом режиме вы можете создать набор правил, разрешающих или запрещающих те или иные соединения приложения.

Если вы выбрали **Пользовательский режим**, то вид окна создания правила изменяется, и вы можете определить правила фильтрации, регулирующие сетевое взаимодействие программы с конкретными хостами сети.



Для каждого правила в списке предоставляется следующая информация:

- **Включено** — состояние правила.
- **Действие** — указывает на действие, выполняемое **Брандмауэром** при попытке программы подключиться к сети Интернет:
 - **Блокировать пакеты** — блокировать попытку подключения;
 - **Разрешать пакеты** — разрешить подключение.
- **Имя правила** — название правила.
- **Тип соединения** — указывает на инициатора подключения:
 - **Входящее** — правило применяется, если иницируется подключение из сети к программе на вашем компьютере;
 - **Исходящее** — правило применяется, если подключение иницирует программа на вашем компьютере;
 - **Любое** — правило применяется вне зависимости от того, кто является инициатором подключения.
- **Описание** — пользовательское описание правила. Имеет смысл добавлять краткий комментарий к каждому правилу, чтобы легче было в них ориентироваться.

Для редактирования правил выберите правило и нажмите . Для добавления правила используйте кнопку  (Создать).

Задайте следующие параметры правила:

- **Имя правила** — имя создаваемого/редактируемого правила.
- **Описание** — краткое описание правила.
- **Действие** — действие, выполняемое **Брандмауэром** при попытке программы подключиться к сети Интернет:
 - **Блокировать пакеты** — блокировать попытку подключения;
 - **Разрешать пакеты** — разрешить подключение.
- **Состояние** — статус правила:
 - **Включено** — правило применяется;
 - **Отключено** — правило временно не применяется.
- **Тип соединения** — направление соединения:
 - **Входящее** — правило применяется, если соединение инициируется из сети к программе на вашем компьютере;
 - **Исходящее** — правило применяется, если соединение инициируется программой на вашем компьютере;
 - **Любое** — правило применяется вне зависимости от направления соединения.
- **Ведение журнала** — режим ведения журнала:
 - **Включено** — регистрировать события;
 - **Отключено** — не сохранять информацию о правиле.
- **Протокол** — протоколы сетевого и транспортного уровня, по которым осуществляется подключение.
 - IPv4;
 - IPv6;

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

- IP all — протокол IP любой версии;
 - TCP;
 - UDP;
 - TCP & UDP — протокол TCP или UDP;
 - RAW.
- **Локальный адрес / Удаленный адрес** — IP-адрес удаленного хоста, участвующего в подключении. Вы можете указывать как конкретный адрес (**Равен**), так и диапазон адресов (**В диапазоне**), а также маску конкретной подсети (**Маска**) или маски всех подсетей, в которых ваш компьютер имеет сетевой адрес (**MY_NETWORK**). Чтобы задать правило для всех хостов, выберите вариант **Любой**.

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

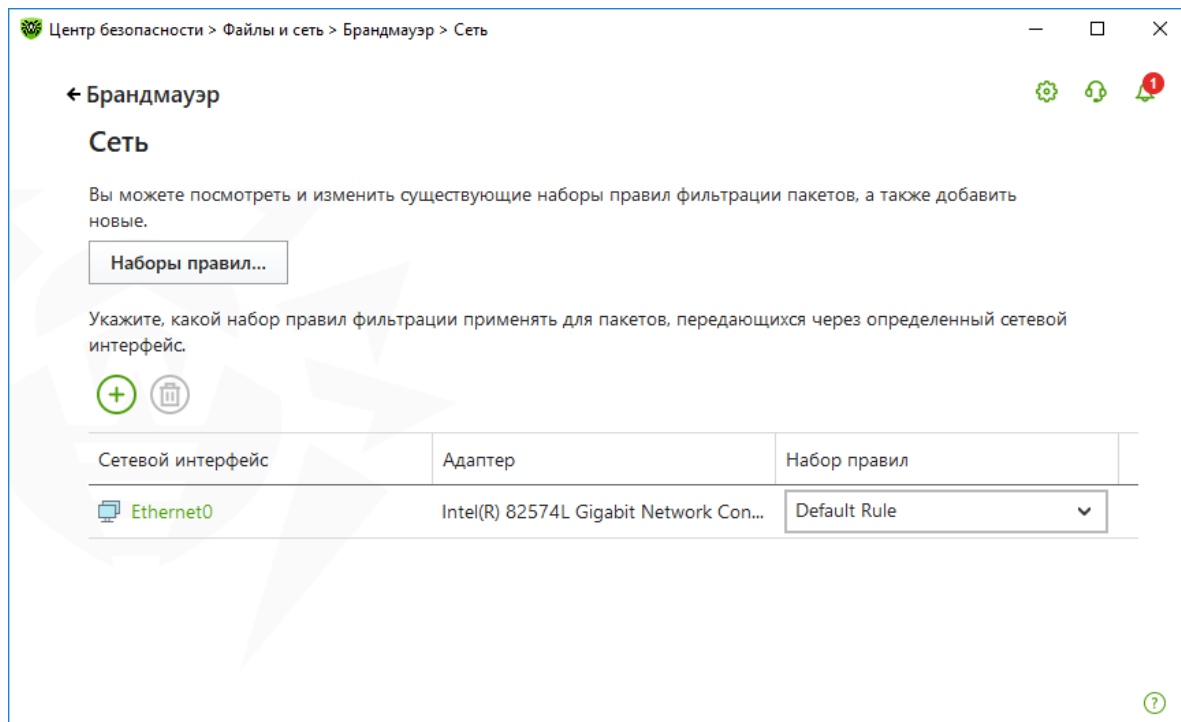
По окончании редактирования набора правил нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для отказа от изменений. Изменения, внесенные в набор правил, сохраняются при переключении на другой режим.


8.13.2. Настройка параметров работы известных сетей

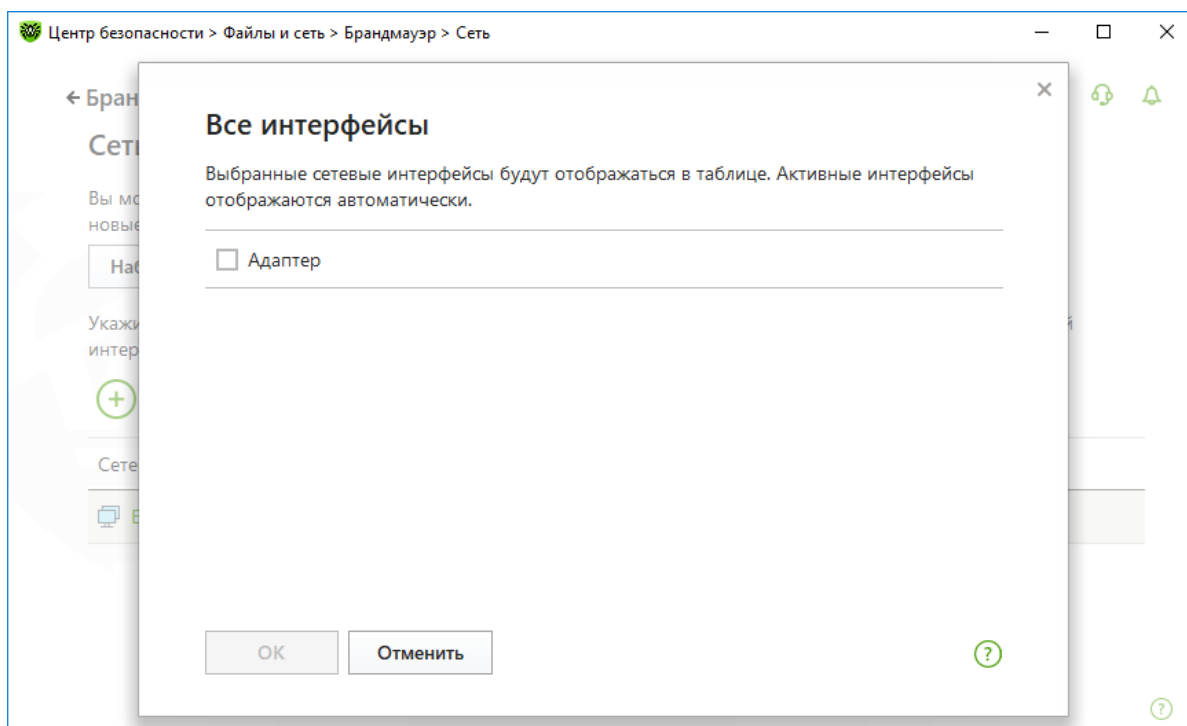
Фильтрация на уровне пакетов позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение. Правила применяются ко всем сетевым пакетам определенного типа, которые передаются через один из сетевых интерфейсов вашего компьютера. Данный вид фильтрации предоставляет вам общие механизмы контроля, в отличие от фильтра приложений. На странице настроек сетевых интерфейсов вы можете указать, какой набор правил фильтрации применять для пакетов, передающихся через определенный сетевой интерфейс.

В окне **Брандмауэр** кликните по строчке **Дополнительные настройки** и в разделе настроек **Параметры работы для известных сетей** нажмите **Изменить**.

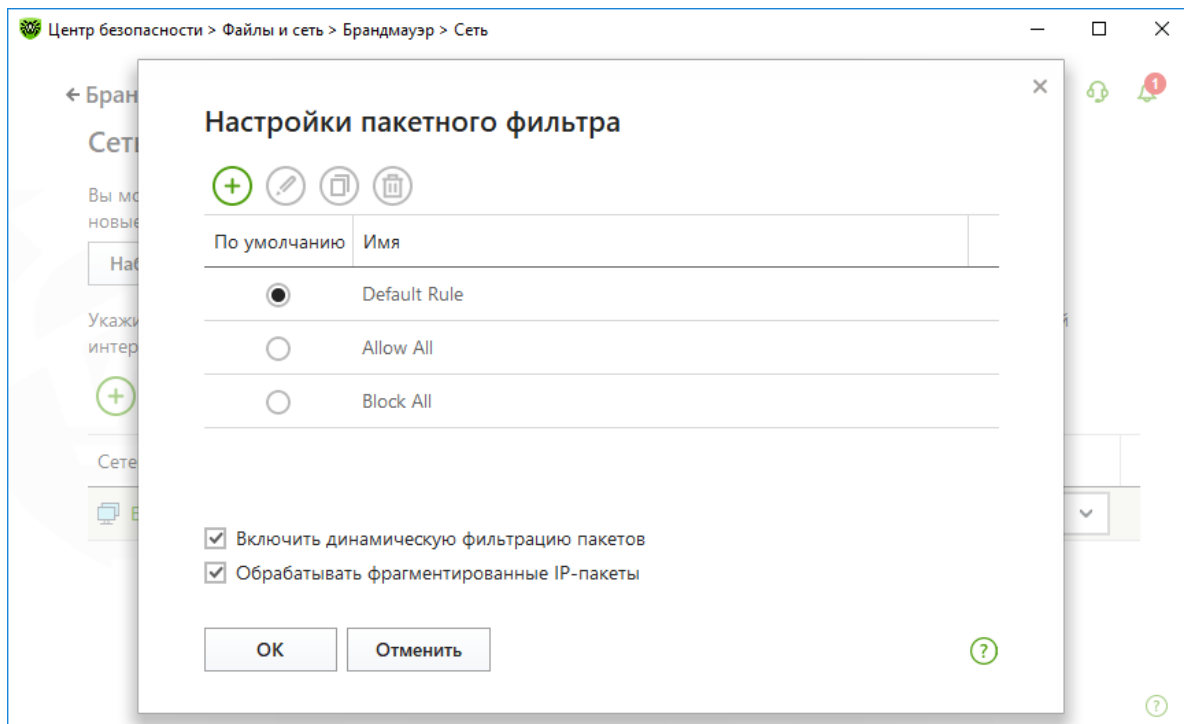
Откроется окно со списком сетевых интерфейсов, для которых заданы правила.



Для того чтобы увидеть все доступные интерфейсы, нажмите кнопку . В открывшемся окне при необходимости укажите, какие интерфейсы должны всегда отображаться в таблице. Активные интерфейсы будут отображаться в таблице автоматически.




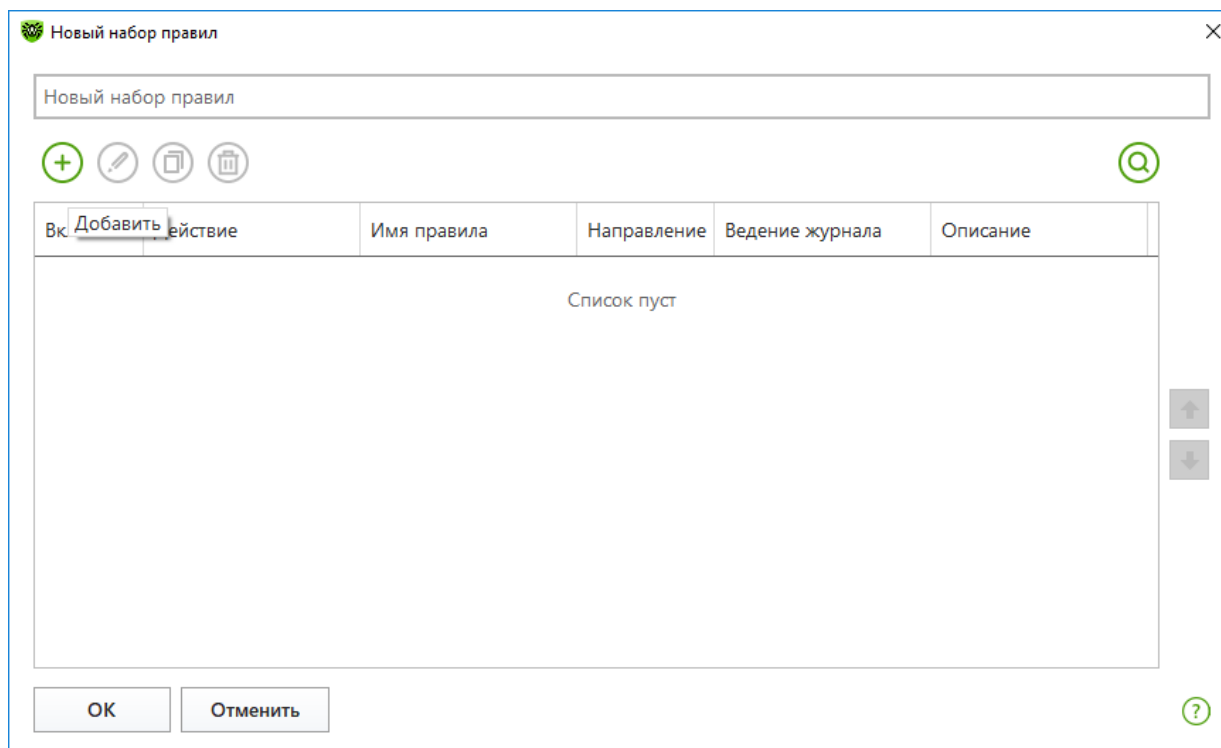
Для управления существующими наборами правил и добавления новых перейдите в окно **Настройки пакетного фильтра**, нажав кнопку **Наборы правил**.



Брандмауэр поставляется со следующими предустановленными наборами правил:

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

Для удобства использования и быстрого переключения между режимами фильтрации вы можете задать дополнительные наборы правил, нажав на кнопку  (Создать) или скопировав существующий набор и изменив его в режиме редактирования.



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

- Чтобы отредактировать существующий набор правил, выберите его в списке и нажмите кнопку **Изменить**.
- Чтобы добавить копию существующего набора правил, нажмите кнопку **Копировать**. Копия добавляется под выбранным набором.
- Чтобы удалить выбранный набор правил, нажмите кнопку **Удалить**.

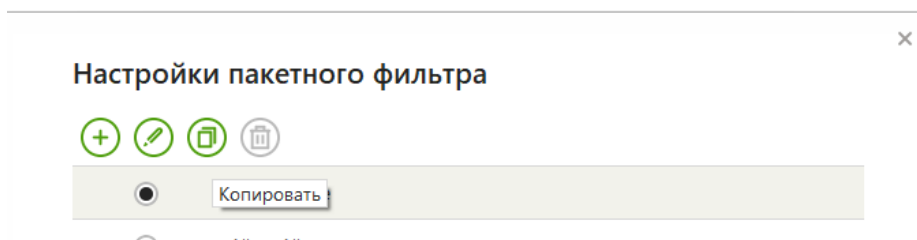
Чтобы задать дополнительные настройки фильтрации пакетов, в окне **Настройки пакетного фильтра** установите следующие флажки:

- **Включить динамическую фильтрацию пакетов.** Установите этот флажок, чтобы учитывать при фильтрации состояние TCP-соединения и пропускать только те пакеты, содержимое которых соответствует текущему состоянию. В таком случае все пакеты, передаваемые в рамках соединения, но не соответствующие спецификации протокола, блокируются. Этот механизм позволяет лучше защитить ваш компьютер от DoS-атак (отказ в обслуживании), сканирования ресурсов, внедрения данных и других злонамеренных операций. Также рекомендуется устанавливать этот флажок при использовании протоколов со сложными алгоритмами передачи данных (FTP, SIP и т. п.). Снимите этот флажок, чтобы фильтровать пакеты без учета TCP-соединений.
- **Обрабатывать фрагментированные IP-пакеты.** Установите этот флажок, чтобы корректно обрабатывать передачу больших объемов данных. Размер максимального пакета (MTU — Maximum Transmission Unit) для разных сетей может варьироваться, поэтому часть IP-пакетов при передаче может быть разбита на несколько фрагментов. При использовании данной опции ко всем фрагментарным пакетам применяется одно и то же действие, предусмотренное правилами фильтрации для головного (первого) пакета. Снимите этот флажок, чтобы обрабатывать все пакеты по отдельности.

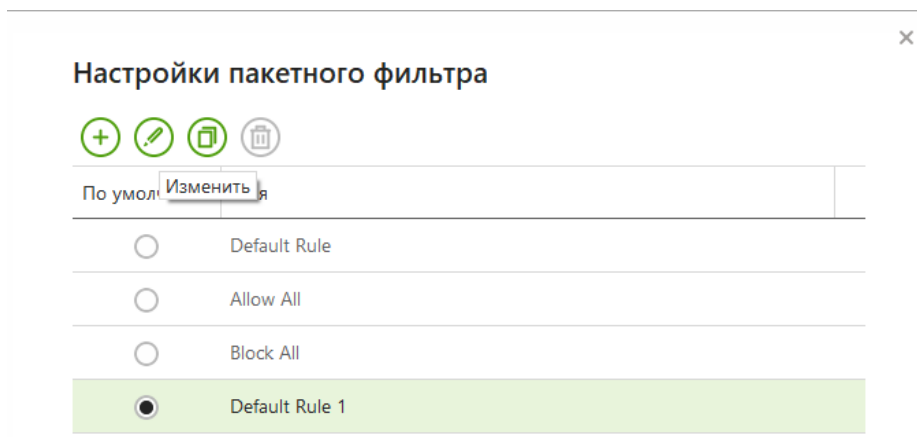
Рассмотрим пример создания нового правила на примере редактирования текущего набора.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

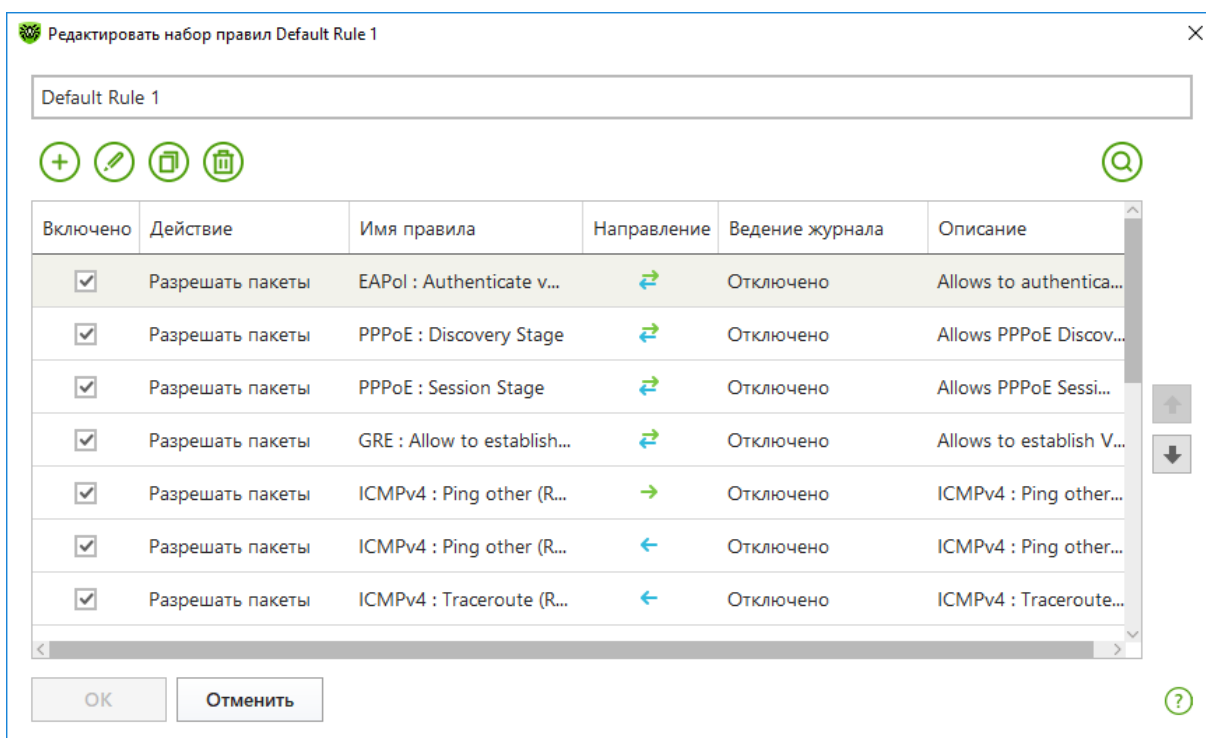
Кликните на **Default rule** и далее на кнопку **Копировать**.



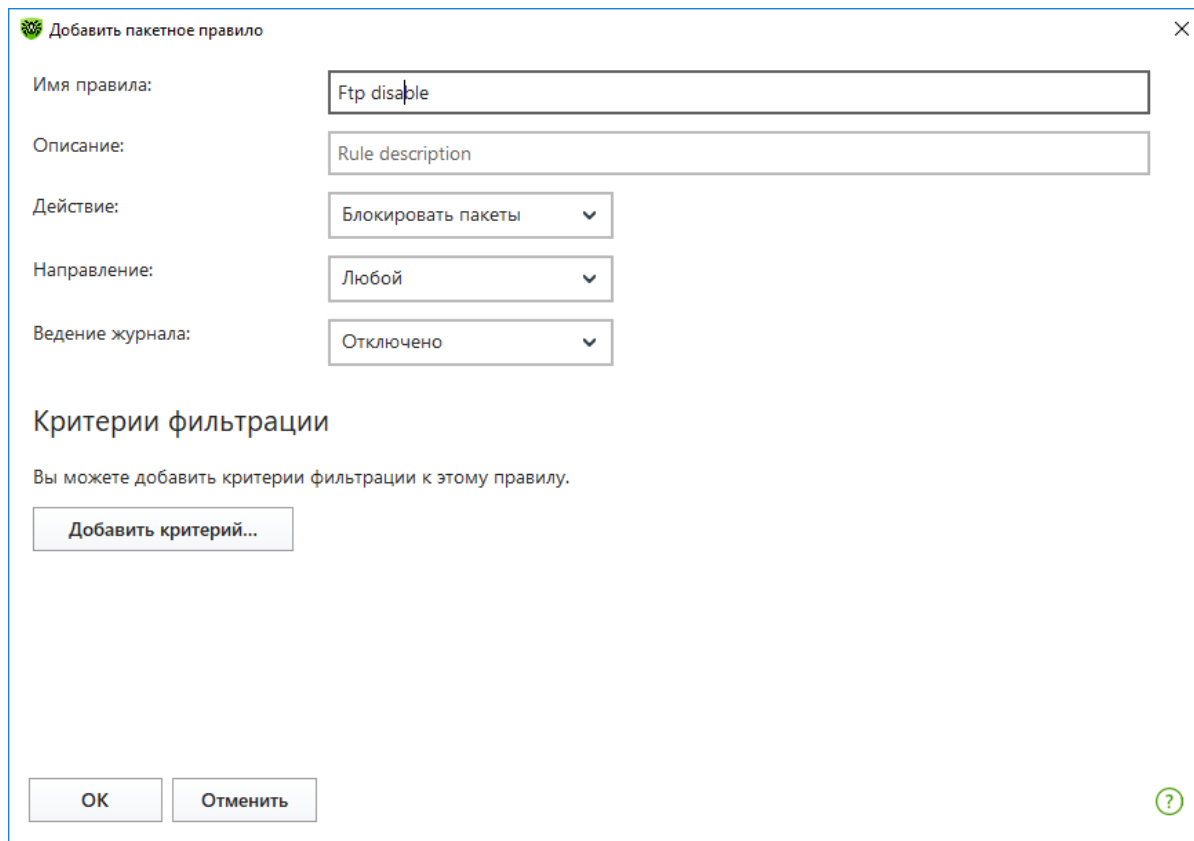
Перейдите на новый набор и нажмите на кнопку **Изменить**.



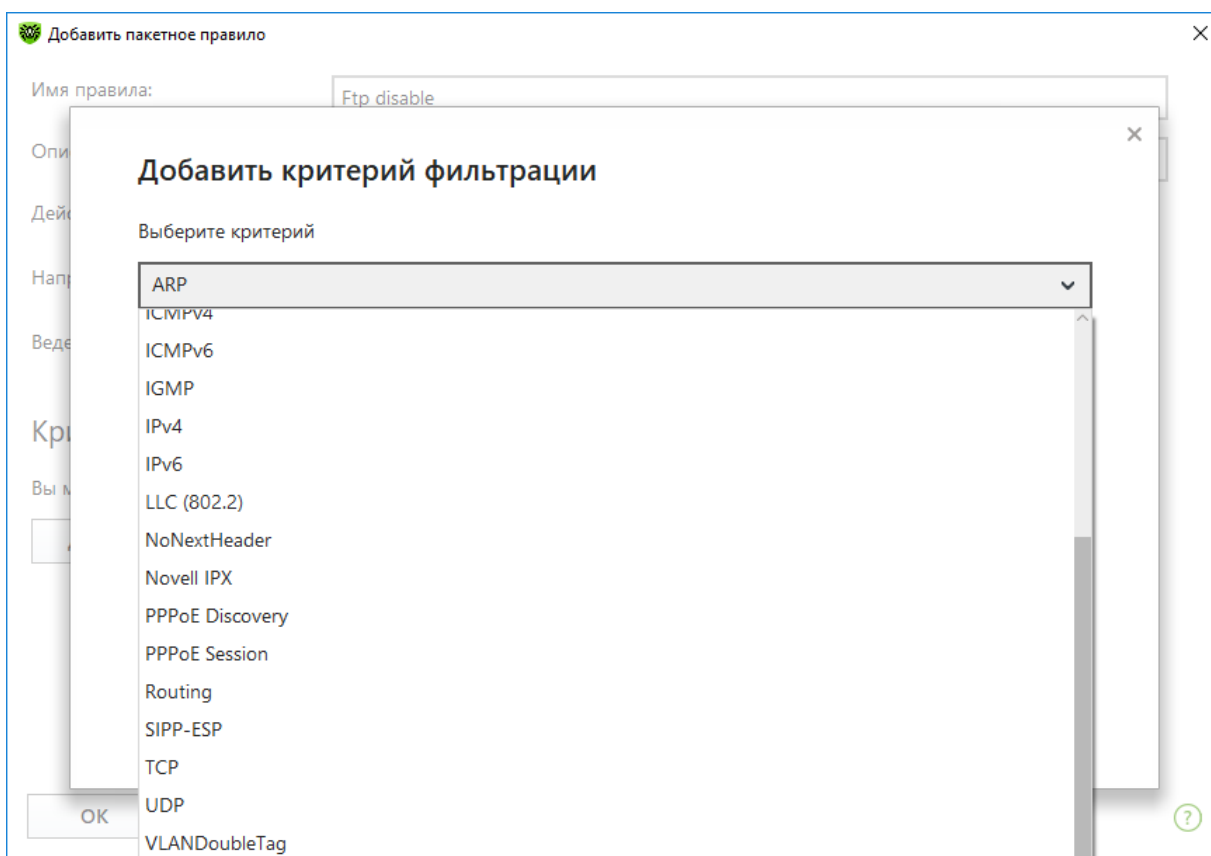
В открывшемся окне кликните на **плюс** для создания нового правила.



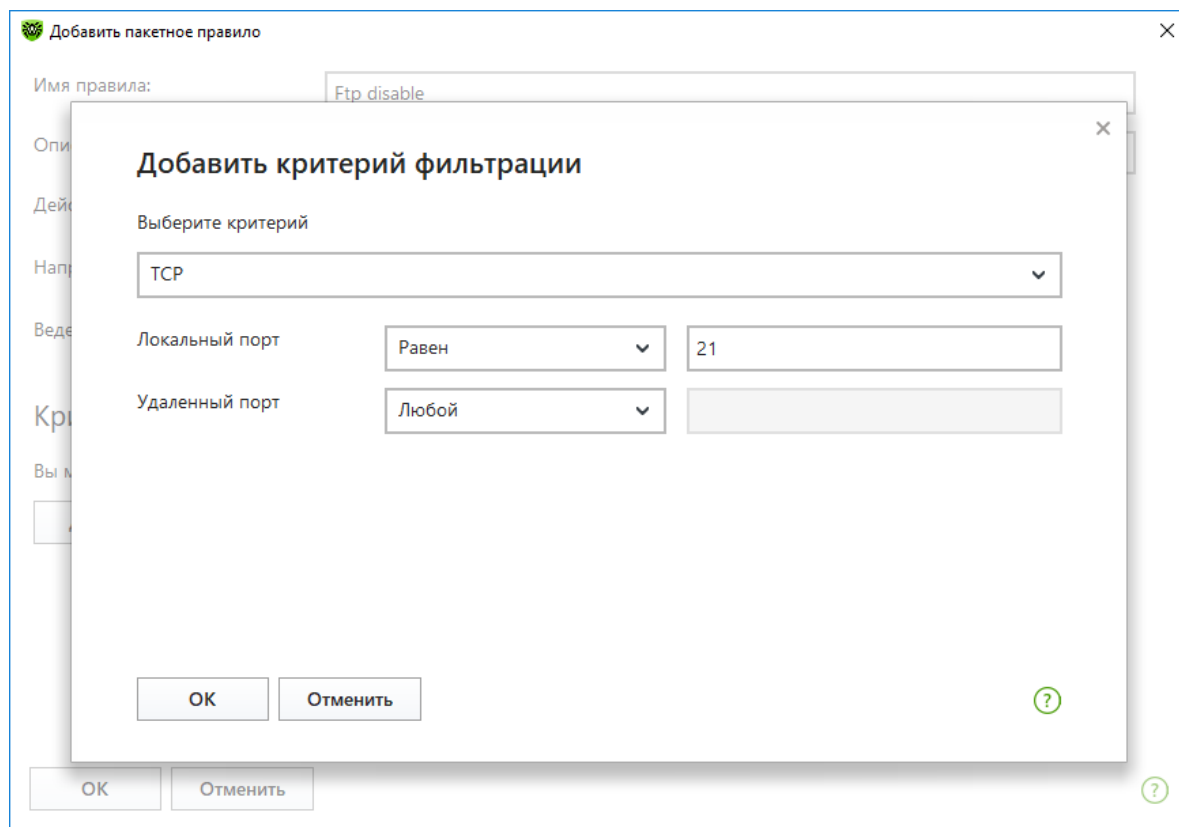
Задайте **Имя правила**, **Действие** (Блокировать пакеты) и **Направление** (Любой).



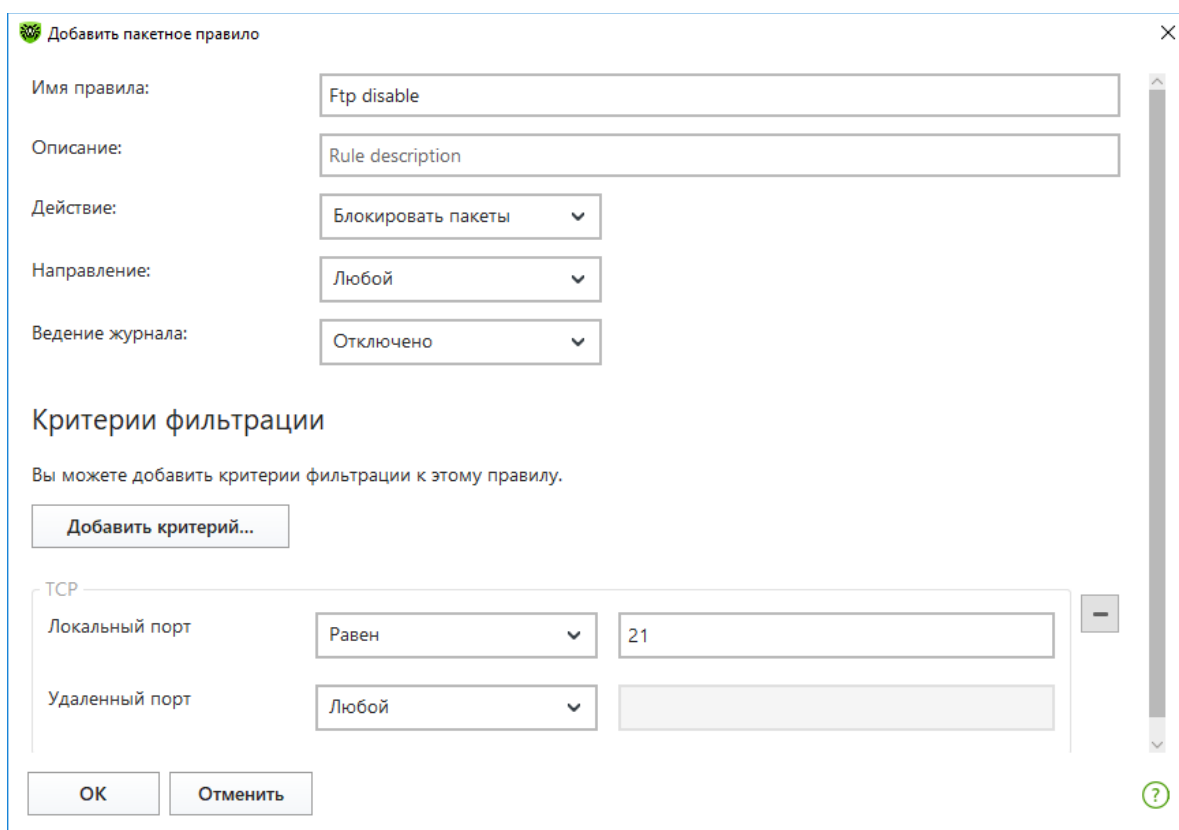
Кликните **Добавить критерий**.



В выпадающем списке выберите **TCP**, в выпадающем списке **Локальный порт** выберите **Любой** и в соседнем окне укажите порт 21, через который работает по умолчанию ftp.



Нажмите **ОК**.







И еще два раза нажмите **ОК**.

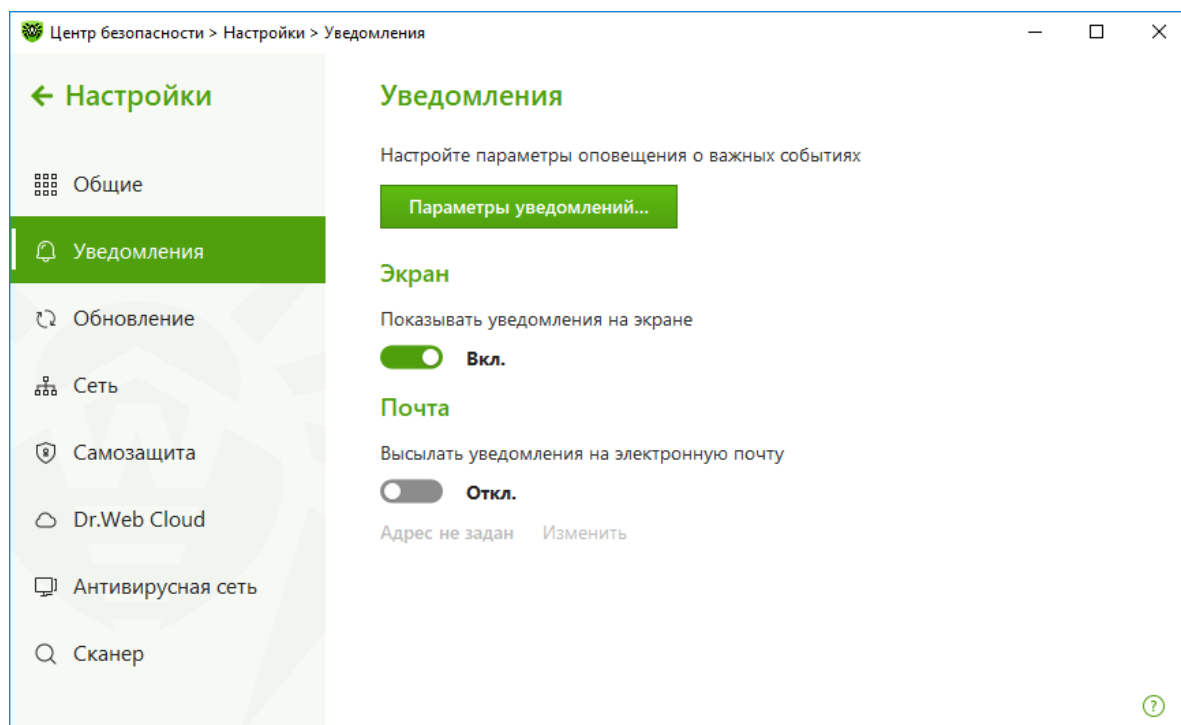
Настройка завершена.

8.13.3. Игровой режим

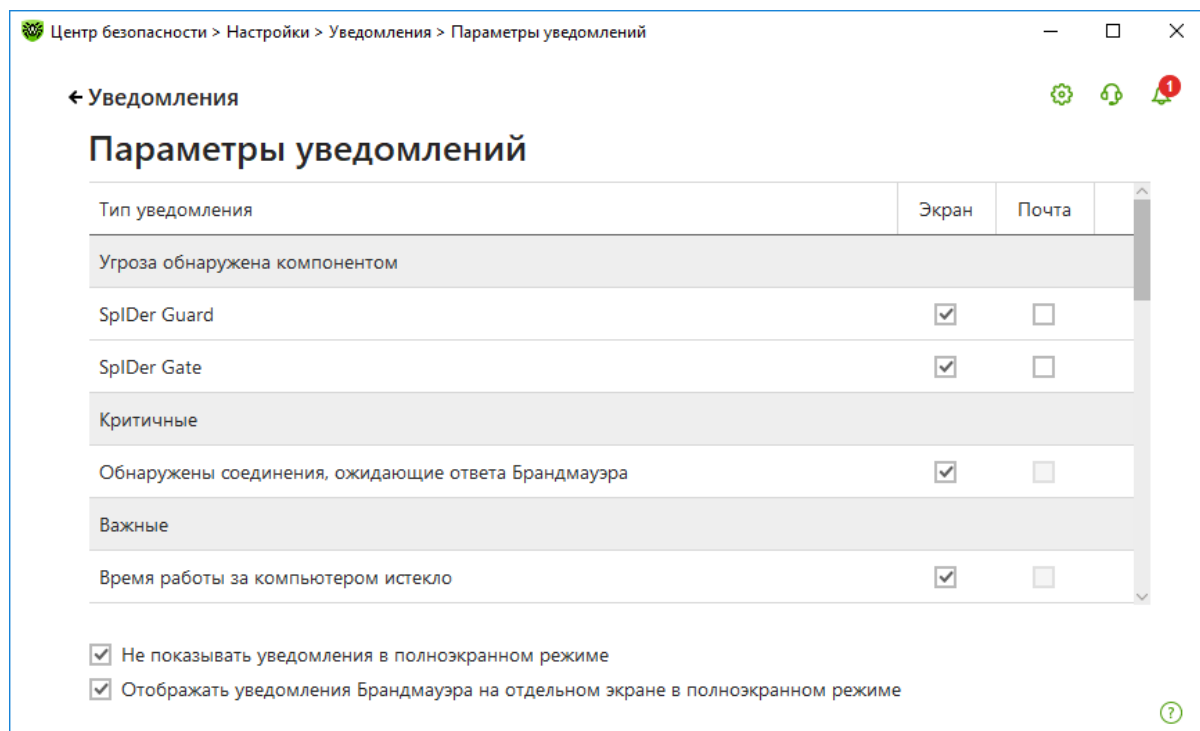
Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

В настоящей версии антивируса появилась возможность использовать так называемый «игровой режим» **Брандмауэра**, при включении которого окно с запросом на создание правила появляется поверх любого приложения, запущенного в полноэкранном режиме. Расширенные настройки позволяют отобразить уведомления **Брандмауэра** на альтернативном рабочем столе.

Для включения **Игрового режима** кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . Нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Уведомления**.







Нажмите кнопку **Параметры уведомлений**.

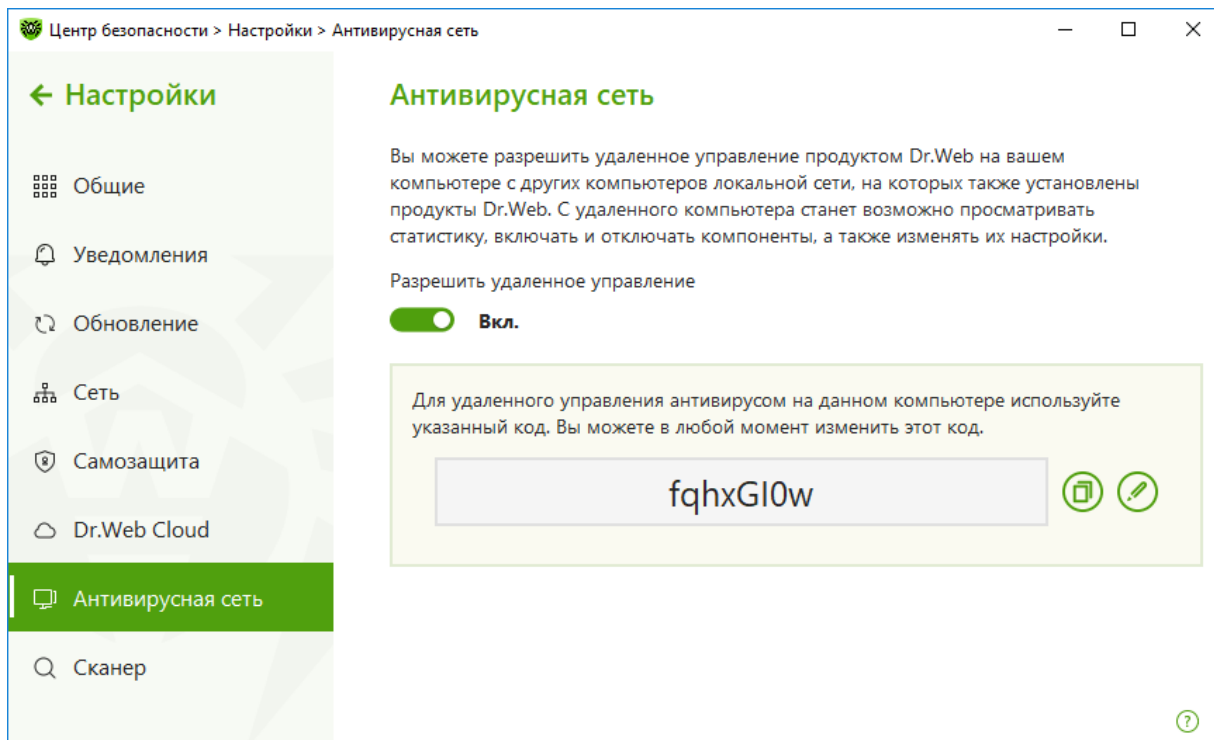


Установите флажок **Отображать уведомления Брандмауэра на отдельном экране в полноэкранном режиме**, чтобы уведомления от **Брандмауэра** отображались на отдельном рабочем столе во время работы приложений в полноэкранном режиме (игры, видео). В противном случае уведомления выводятся на том же рабочем столе, на котором запущено приложение в полноэкранном режиме.

8.14. Управление антивирусной защитой удаленного компьютера

Удаленное управление позволяет осуществлять управление продуктами Dr.Web на других компьютерах в пределах одной локальной сети.




Чтобы разрешить удаленное управление продуктом Dr.Web, кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . Нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Антивирусная сеть**.

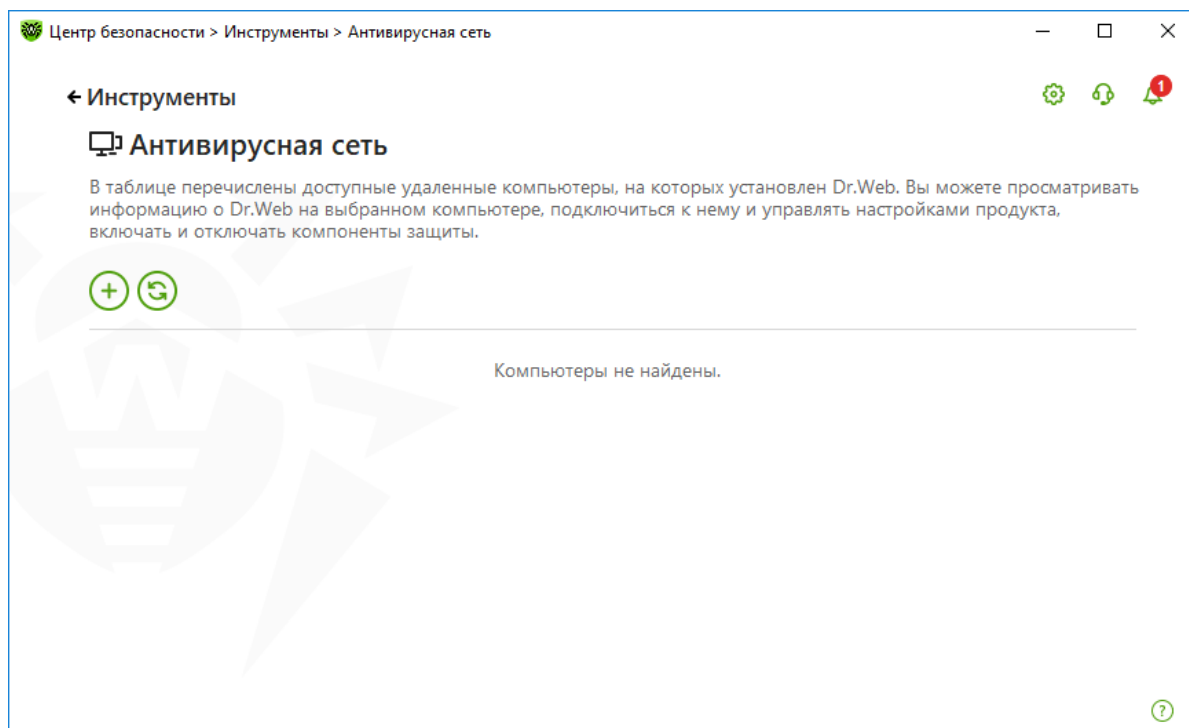


Разрешите удаленное управление продуктом Dr.Web при помощи переключателя.

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


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

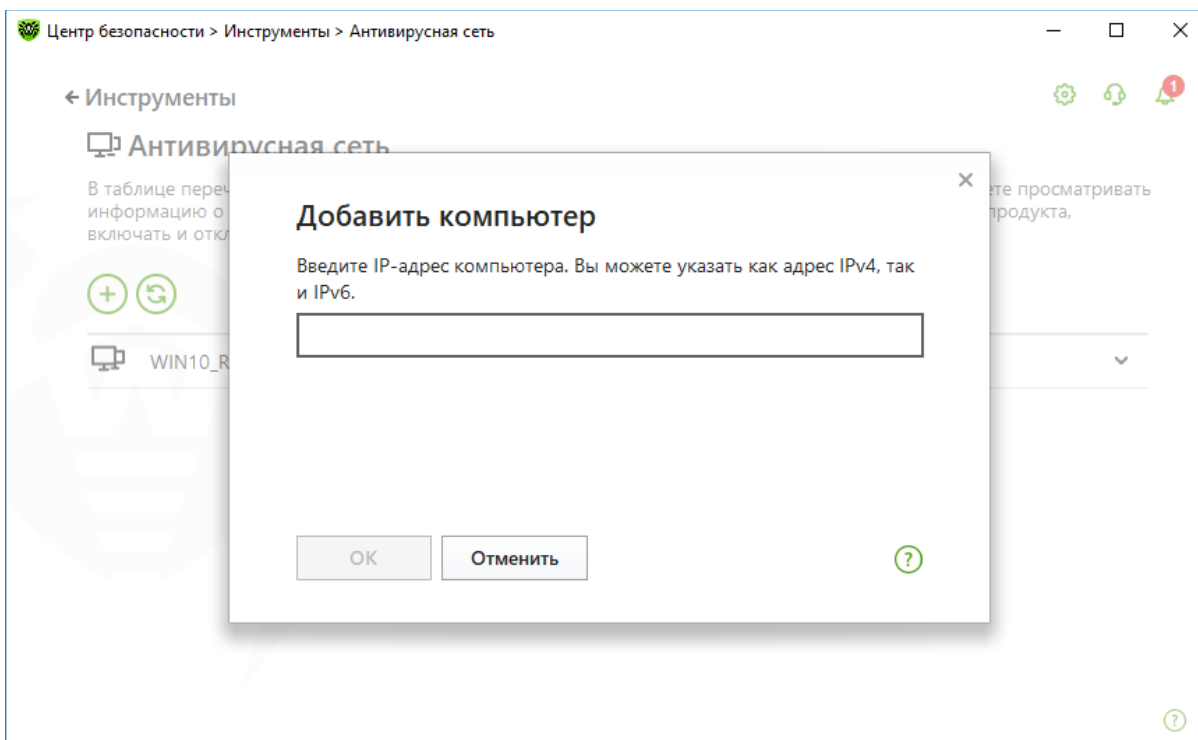
Чтобы запустить удаленное управление компьютером, кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . В окне **Центр безопасности** последовательно выберите **Инструменты** → **Антивирусная сеть**. Этот компонент позволяет управлять программами Dr.Web на других компьютерах в пределах одной локальной сети.



Компьютеры в локальной сети отображаются в списке только в том случае, если в установленном на них продукте Dr.Web разрешено удаленное управление.

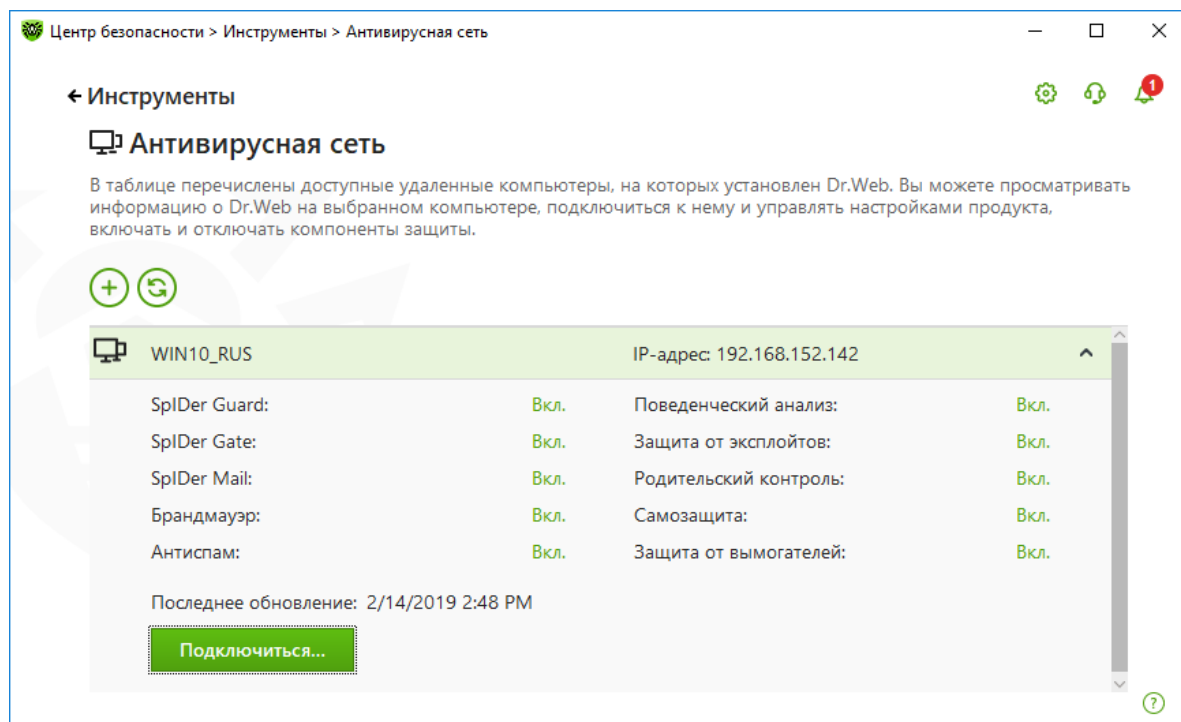
Если необходимый компьютер не отображается в сети, попробуйте добавить его вручную.

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.

Для доступа к удаленному антивирусу выберите компьютер в списке и нажмите кнопку **Подключиться**.




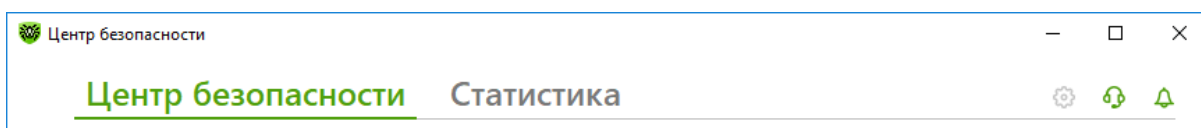
Введите пароль, заданный в настройках удаленного антивируса. В области уведомлений Windows появится значок удаленного **SpIDer Agent'a**, а также будет показано уведомление об успешном подключении.

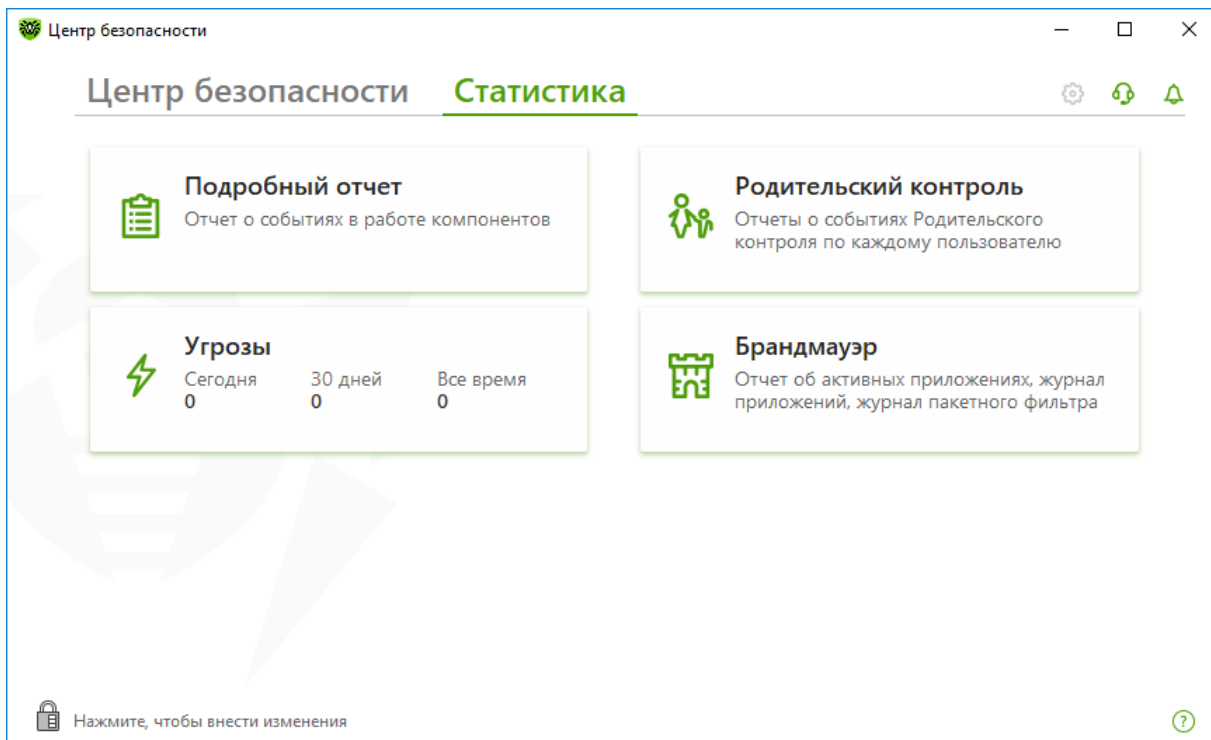
Вы можете установить только одно соединение с удаленным продуктом Dr.Web. При наличии установленного соединения кнопка **Подключиться** недоступна.

Вы можете просматривать статистику, включать и отключать модули, а также изменять их настройки. Компоненты **Антивирусная сеть**, **Карантин** и **Сканер** недоступны. Также вам доступен пункт **Отсоединиться**, при выборе которого завершается установленное соединение с удаленным антивирусом.

8.15. Просмотр статистики работы

Пользователь может в любой момент ознакомиться со статистикой работы системы защиты. Чтобы получить доступ к статистике работы интересующего компонента, щелкнув на значок  в трее, выберите пункт **Центр безопасности** и перейдите на закладку **Статистика**.







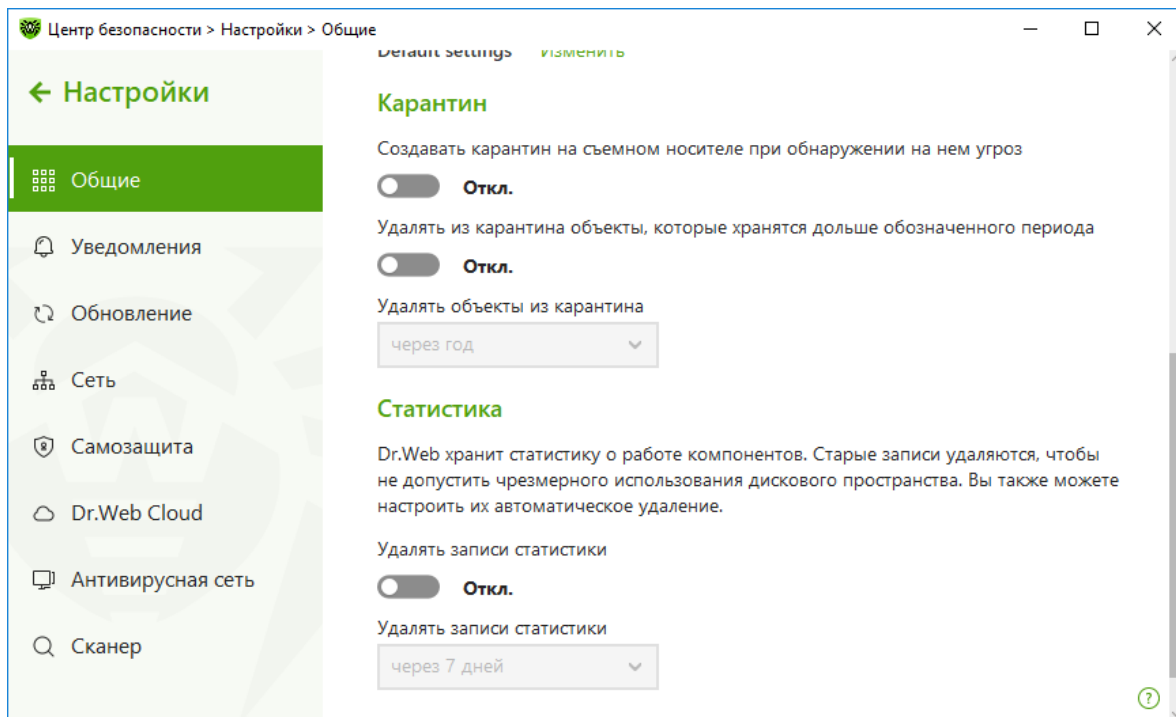


Просмотреть статистику работы конкретного компонента можно с помощью использования фильтров.

8.16. Карантин

Карантин антивируса Dr.Web служит для изоляции подозрительных файлов.

Для управления настройками карантина кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . В окне **Центр безопасности**, нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Общие** и далее **Дополнительные настройки**.



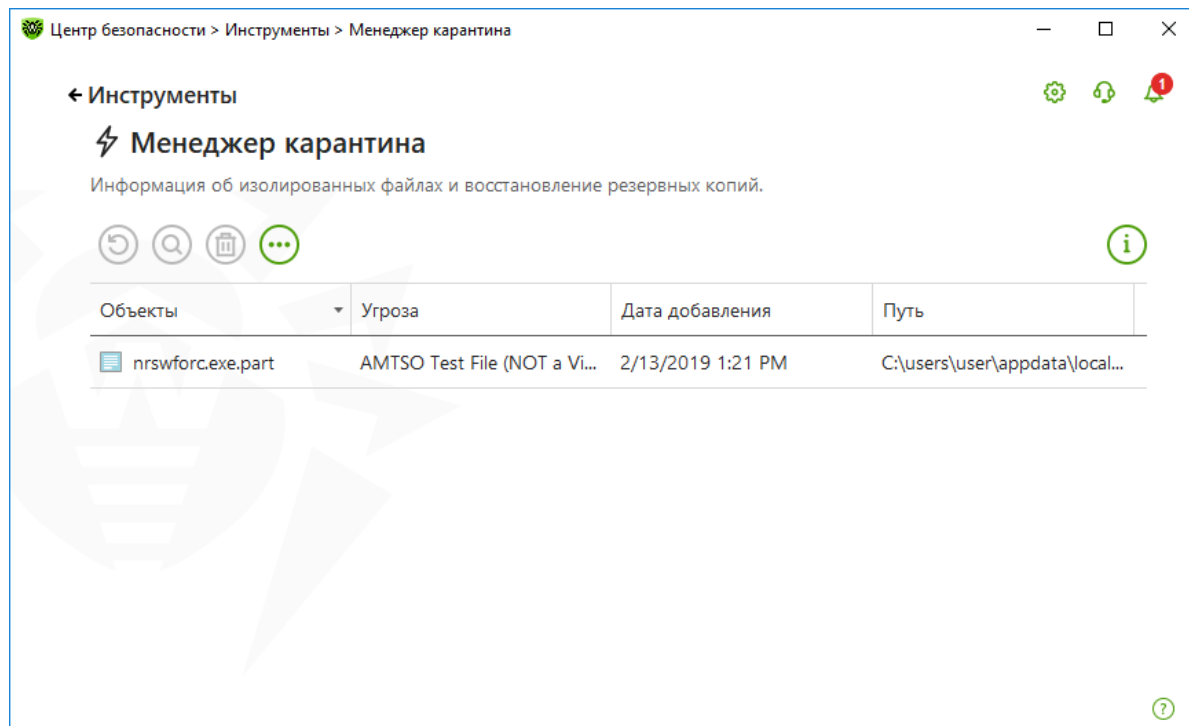
Папка карантина создается отдельно на каждом логическом диске, где были обнаружены подозрительные файлы. Папка карантина под названием Dr.Web Quarantine создается в корне диска и является скрытой. Пользователь не имеет прав доступа к файлам папки карантина.

В настройках **Менеджера карантина** вы можете включить опцию, которая определяет режим изоляции зараженных объектов, обнаруженных на съемных носителях.

При включении этой опции подобные угрозы помещаются в папку на том же носителе и в отличие от файлов карантина, размещаемых на жестком диске, не шифруются. При этом папка карантина создается только в том случае, если возможна запись на носитель. Если данная опция не выбрана — папка карантина создается на локальном диске.

Использование отдельных папок и отказ от шифрования на съемных носителях позволяет предотвратить возможную потерю данных.


Для просмотра и редактирования содержимого карантина выберите в меню значка Agent пункт **Центр безопасности**. В открывшемся окне выберите **Инструменты** и далее **Менеджер карантина** — откроется окно, содержащее табличные данные о текущем состоянии карантина.



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

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

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**.

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

Для одновременной работы с несколькими файлами установите флажки рядом с названиями объектов, а затем выберите необходимое действие.

В контекстном меню объектов доступны следующие кнопки управления:

- **Восстановить** — переместить один или несколько объектов под заданным именем в нужную папку;
- **Перепроверить** — проверить объект, перемещенный в карантин, повторно.
- **Удалить** — удалить один или несколько объектов из карантина и из системы.


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

При переполнении диска осуществляется автоматическая очистка карантина — в первую очередь удаляются резервные копии файлов карантина, а при нехватке дискового пространства удаляются файлы карантина с истекшим сроком хранения.

При переполнении карантина и невозможности его автоматической очистки перемещение

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

файлов в карантин будет завершаться с ошибкой.

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

8.17. Включение и отключение самозащиты





Самозащита Dr.Web (Dr.Web SelfPROtect) применяется для защиты компонентов и каталогов самого антивируса как от несанкционированного воздействия извне (вирусные атаки), так и от случайных действий пользователя, которые могут навредить работе антивируса.

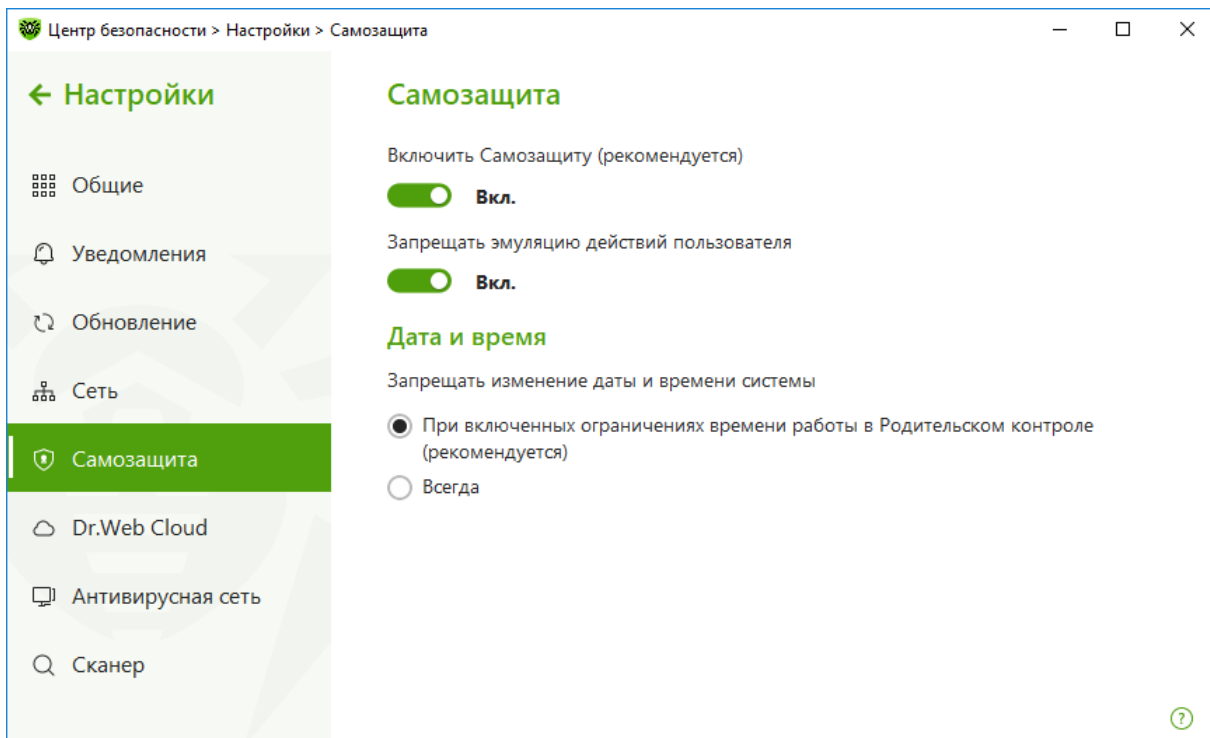
Dr.Web SelfPROtect служит для защиты модулей, процессов, а также веток реестра, которые использует Dr.Web для Windows в своей работе, от воздействия извне. Под внешним воздействием в данном случае могут пониматься как неосторожные действия пользователя, которые могут привести к неработоспособности или неправильной работе антивируса, так и деятельность анти-антивирусных вредоносных программ, в арсенал которых могут входить такие действия, как завершение процессов антивируса, модификация или удаление файлов антивируса, а также модификация или удаление веток реестра Windows, которые использует Dr.Web.

По умолчанию **Самозащита** всегда включена, и не рекомендуется отключать ее. Исключение составляют немногие ситуации. После завершения нужного действия не забудьте снова включить **Самозащиту**.

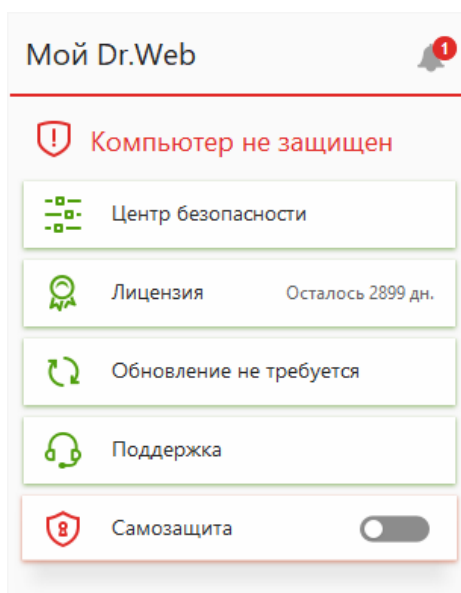
Модуль самозащиты **Dr.Web SelfPROtect** выполнен в виде драйвера уровня ядра системы `dwprot.sys`, и его невозможно выгрузить до перезагрузки системы.

Пользователь может временно приостановить работу модуля самозащиты, но для этого он должен ввести случайное число (либо пароль — в том случае, если он ранее был задан), которое показывается в специальном окне при попытке отключения **Dr.Web SelfPROtect**. Таким образом, вредоносная программа или пользователь без явного намерения не смогут прекратить работу модуля самозащиты.

Для отключения самозащиты кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора). Значок изменит вид на . В окне **Центр безопасности**, нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Общие** и далее **Самозащита**. Нажмите на переключатель.




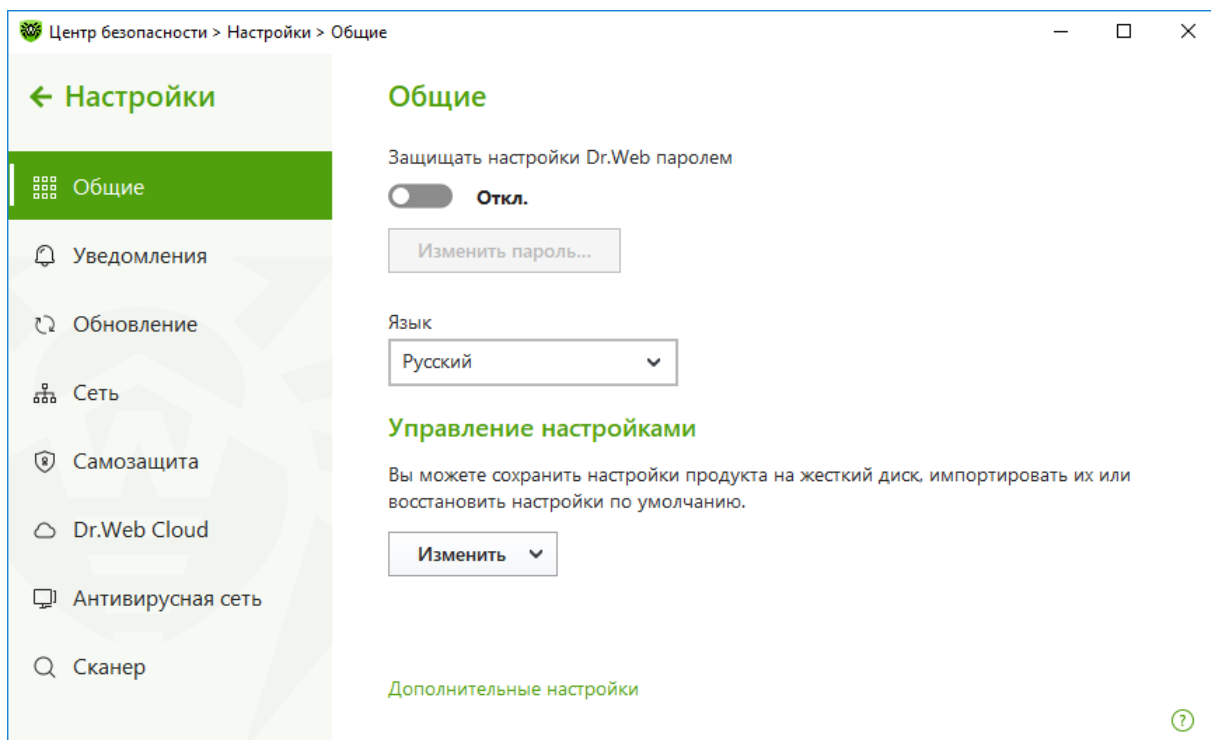
Меню агента изменит вид на следующий:



8.18. Установка пароля доступа к настройкам антивирусной защиты

Установка пароля позволит гарантировать невозможность отключения защиты, в том числе в случае взлома.

Для установки пароля доступа в **Центре безопасности** нажмите значок  (значок изменит вид на ) и, нажав на ставший зеленым значок  в правом верхнем углу окна, выберите в меню **Настройки** пункт **Общие** и далее на кнопку **Изменить пароль**.



Введите пароль.

Внимание! Не рекомендуется устанавливать пароль, совпадающий с паролем доступа к компьютеру или устройству, — в случае взлома компьютера это облегчит действия злоумышленника по нейтрализации защиты.

8.19. Получение услуг службы технической поддержки

В случае возникновения неразрешимой ситуации, какой-либо проблемы при работе антивируса или обнаружении недетектированного или ложно детектированного как вирус объекта, обратитесь в службу технической поддержки компании «Доктор Веб».

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, настоятельно рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу <http://download.drweb.ru/doc>,
- прочитать раздел часто задаваемых вопросов по адресу <http://support.drweb.ru>,
- посетить форумы Dr.Web по адресу <http://forum.drweb.com>.

Чтобы отправить запрос в техподдержку, перейдите по ссылке **Поддержка** в верхнем меню официального сайта компании «Доктор Веб» (www.drweb.ru). Попасть напрямую в данный раздел можно по ссылке <https://support.drweb.ru>.

ЗАЩИТИ СОЗДАННОЕ

ОТПРАВИТЬ ЗАПРОС САМОПОДДЕРЖКА РЕСУРСЫ ЛИЦЕНЗИРОВАНИЕ ФОРУМ ОНЛАЙН-УСЛУГИ БЕСПЛАТНО

Круглосуточная служба поддержки

Самоподдержка

Позвоните нам

Бесплатно в России
8-800-333-7932

Частые вопросы Форум Бот для Telegram

skype Позвонить

Задать вопрос в поддержку

[Правила обращения в службу поддержки](#)

Выберите тему:

СЛУЖБА ПОДДЕРЖКИ ПРОДАЖ

- Регистрация серийного номера / получение ключевого файла
- Покупка/продление/дозакупка
- Отзывы и предложения

[Войти через аккаунт на сайте](#) (?)
[Войти через «Мой Dr.Web»](#) (?)

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

- Работа программы Dr.Web
- Обнаружение/удаление вируса

ДАЛЕЕ

- ✓ [Поддержка партнеров](#)
- ✓ [Поддержка участников КОД Dr.Web](#)
- ✓ [Запрос на расшифровку Trojan Encoder/Cryptolocker](#)
- ✓ [Заявка на расследование ВК/И](#)

На начальной странице пользователю предлагается выбрать тему обращения.

На следующем этапе укажите серийный номер или иной идентификатор, позволяющий идентифицировать используемый продукт.

Круглосуточная служба поддержки

Тема запроса: Работа программы Dr.Web

Чтобы значительно ускорить обработку вашего запроса,

<p>укажите вашу лицензию Dr.Web ЭЛЕКТРОННЫЕ ЛИЦЕНЗИИ И КОРОБКИ DR.WEB</p> <p>Ваш серийный номер</p> <p>XXXX XXXX XXXX XXXX Восстановить серийный номер?</p> <p>Регистрационный e-mail</p> <p><input type="text"/></p> <p>Забыли адрес? Зарегистрируйте серийный номер еще раз — письмо с ключом будет выслано на этот адрес.</p>	<p>или номер заказа ВАШ ЗАКАЗ ALLSOFT</p> <p><input type="text"/></p>
<p>ПОДПИСКИ НА УСЛУГУ «АНТИВИРУС DR.WEB»</p> <p>ID подписки (?)</p> <p><input type="text"/></p> <p>или ваш Поставщик</p> <p><input type="text"/></p> <p>Если вы пользуетесь веб-цппом, просто войдите через Веб-ЦПП. Восстановить доступ?</p>	<p>ВАШ ЗАКАЗ GOOGLE PLAY</p> <p>GPA: XXXX XXXX XXXX XXXX <input type="text"/></p> <p>Адрес</p> <p><input type="text"/> @gmail.com</p> <p><input type="checkbox"/> Life license</p>

Вы также можете попробовать найти ответ в ресурсах [самоподдержки](#).

[Далее](#)

[Назад](#) | [Начать заново](#)

Если лицензия позволяет использование нескольких решений, выберите то, которого будет касаться запрос.

Круглосуточная служба поддержки

Тема запроса: Работа программы Dr.Web

Выберите продукт Dr.Web

<p>Для дома</p>	<p>Для бизнеса</p>
<p>ЗАЩИТА ДОМАШНЕГО ПК/МАС</p> <p><input checked="" type="radio"/> Windows</p> <p><input type="radio"/> macOS</p> <p><input type="radio"/> Linux</p>	<p>ЗАЩИТА МОБ. УСТРОЙСТВА</p> <p><input type="radio"/> Android (кроме <i>Light</i> (?))</p> <p><input type="radio"/> BlackBerry</p>

[Далее](#)

[Назад](#) | [Начать заново](#)

Заполните поля для непосредственного создания запроса на открывшейся странице.

КОНТАКТНЫЕ ДАННЫЕ

Тема запроса: Работа программы Dr.Web

Ваши Ф. И. О. *

E-mail *

На этот адрес будет отправлен ответ

Ваш вопрос *

! УТИЛИТА СБОРА ИНФОРМАЦИИ О РАБОТЕ DR.WEB

Присоединить файл

Обзор... Файл не выбран.

Код с картинки *



Я даю согласие ООО «Доктор Веб» (правообладателю ПО Dr.Web) на обработку моих персональных данных

Отправить

[Назад](#) | [Начать заново](#)

В соответствующие поля введите следующие данные:

- **Ф. И. О.** Для обращения сотрудников службы поддержки к клиенту. Это поле может быть заполнено автоматически, при условии что на первом шаге указан серийный номер или ключевой файл.
- **Организация.** Название организации, владеющей лицензией (присутствует только в разделах для корпоративных клиентов).
- **Должность.** Можно указать должность сотрудника, обращающегося за поддержкой (присутствует только в разделах для корпоративных клиентов).
- **Провайдер.** Требуется указать провайдера, клиентом которого является пользователь (присутствует только при выборе варианта *Вопрос об услуге «Антивирус Dr.Web»*).
- **Контактный e-mail.** Для получения пользователем уведомлений о ходе рассмотрения запроса. Также заполняется автоматически при условиях, указанных в описании поля Ф. И. О.
- **Номер контактного телефона.** Как вариант контакта для быстрой связи при необходимости.
- **Код, отображенный на картинке.** Предназначено для противодействия отправлению

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

запросов автоматическими средствами.

- **Ваш вопрос.** В этом поле предельно конкретно и подробно опишите суть возникшей проблемы. Это и есть текст вашего обращения в службу поддержки.

Также есть возможность с помощью кнопки **Обзор** приложить к запросу какие-либо файлы. Это может быть отчет о работе антивируса, файлы, иллюстрирующие проблему (подозрительные объекты, скриншоты и т. д.).

Примечание. Во время ввода вопроса в левом верхнем углу окна может появиться зеленый прямоугольник **Похожие вопросы** — таким образом система предлагает вам поискать решение своей проблемы в FAQ. Нажмите левой кнопкой мыши на прямоугольник, и окно с похожими вопросами (отбор идет по ключевым словам) развернется в центр экрана.

Если проигнорировать предложение — после нажатия кнопки **Отправить** окно с похожими вопросами раскроется автоматически.

В окне похожих вопросов нажмите на подходящий, если он имеется в списке, или нажмите **Заккрыть**.

При нажатии на выбранный вопрос он раскрывается, и вы можете прочесть ответ. Отреагировать на полученные данные можно тремя способами:

- **Ответ помог** — если вы получили необходимую информацию и дальнейшая помощь не требуется.
- **Полезная информация** — если представленный текст был полезен или интересен, но не дал требуемого вам ответа.
- **Неподходящий вопрос** — если информация не имеет прямого отношения к интересующей вас проблеме.

При выборе любого из вариантов они исчезают, и окно похожих вопросов можно закрыть. Если ответ получен — запрос можно не отсылать, если неясные моменты еще остались — нажмите **Отправить**.

Если указанный серийный номер или ключевой файл заблокирован, пользователь будет автоматически перенаправлен на страницу http://support.drweb.ru/key_blocked.

Примечание. Если вы выбрали раздел **Вопрос об услуге «Антивирус Dr.Web»**, то вам будет доступен только этот раздел, при этом не требуется указывать используемый продукт и операционную систему.

Незарегистрированные пользователи могут обратиться в службу поддержки со следующими запросами (без предоставления регистрационных данных):

- Вопрос об услуге «Антивирус Dr.Web»
- Помощь в выборе антивируса, покупка/продление лицензии (в том числе демолицензии)
- Сообщить о ложном срабатывании Родительского контроля Dr.Web
- Бесплатная помощь пострадавшим от Trojan.Winlock (https://support.drweb.ru/new/free_unlocker/?lng=ru)
- Хочу работать в «Доктор Веб»!
- Предложения по улучшению функционала антивируса
- Отзыв о работе компании и ее партнеров

Порядок действий с этими вариантами не отличается от описанных в примере. Для отправки запроса нажмите **Отправить**. Откроется окно с уведомлением об успешном создании запроса

и ссылкой **Перейти к запросу**.

При взятии запроса в обработку и каждом изменении его статуса сотрудником, на указанный пользователем адрес электронной почты приходит информационное письмо с темой **your ticket KEYJ-0213** (где **KEYJ-0213** — уникальный номер запроса, присваиваемый автоматически) и следующим содержанием:

Уважаемый пользователь,

Это напоминание послано Вам о Вашем запросе в службу технической поддержки компании «Доктор Веб». В статусе Вашего запроса произошли изменения, возможно, от Вас требуется дополнительная информация. Чтобы посмотреть статус своего запроса, перейдите, пожалуйста, по ссылке:

<https://support.drweb.ru/process/?ticket=KEYJ-0213>

Если проблема для Вас неактуальна или же Вы не хотите более получать уведомления по этому запросу, пожалуйста, нажмите на кнопку «Закрыть запрос», после чего Ваш запрос не будет обрабатываться.

Спасибо за сотрудничество.

С уважением,

ООО «Доктор Веб»

Служба техподдержки

<http://support.drweb.ru>

Вы всегда можете открыть свой запрос, перейдя по указанной в письме ссылке.

После нажатия **Перейти к запросу** откроется окно, содержимое которого является своеобразным диалогом между пользователем и сотрудником технической поддержки.

Рассмотрим страницу работы с запросом подробнее.

В верхней части указан номер запроса и его актуальный статус. Статус может быть следующим:

- **Новый** — запрос, не взятый в обработку никем из сотрудников.
- **Подтвержденный** — запрос, взятый в обработку сотрудником технической поддержки.
- **Ожидание ответа пользователя** — запрос, в котором ожидается реакция от пользователя. Если проблема решена, пользователь может закрыть запрос или предоставить дополнительную информацию (например, отчеты работы компонентов антивируса), если это требуется. Если пользователь никак не отреагировал в течение 10 рабочих дней, запрос будет автоматически закрыт.
- **Ожидание ответа разработчиков** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется помощь разработчиков. Например, требуется воспроизвести проблемную ситуацию на тестовом стенде или исправить ошибку в компоненте антивируса.
- **Ожидание ответа службы вирусного мониторинга** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется участие работников службы вирусного мониторинга. Например, при ложном срабатывании антивируса.
- **Ожидание ответа отдела по работе с партнерами** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется привлечь сотрудников отдела по работе с партнерами. Например, когда нужна консультация по вопросам, связанным с продажей или продлением лицензий, перевыдачей серийного номера.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

- **Ожидание выпуска обновленного компонента** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется обновление какого-либо компонента антивируса. Например, если в ходе обработки запроса выяснилось, что возникшая проблема исправлена в одном из обновлений и нужно дождаться его выхода.
- **Ожидание ответа техподдержки** — запрос, в котором требуется ответ сотрудника техподдержки. В это состояние запрос переключается после ответа пользователя.
- **Закрытый запрос** — статус присваивается, если пользователь самостоятельно закрывает запрос или автоматически после 10 рабочих дней отсутствия ответа от него. Также запрос может быть закрыт сотрудником при некорректном поведении пользователя. Закрытый запрос может быть вновь открыт сотрудником техподдержки с помощью добавления сообщения.

Ниже расположена таблица, первая колонка которой называется **Дата, время, статус**. Здесь указываются дата и время каждого нового сообщения (если только время — значит, сообщение написано в текущие сутки) и его статус. Статус отображает актуальное состояние запроса на момент размещения этого сообщения. Вторая колонка **Кто** показывает автора каждого из сообщений. Если ответ исходит от пользователя, здесь указано, что он ввел в поле **Ф. И. О.** при создании запроса, если сотрудник техподдержки — то имя сотрудника.

В колонке **Информация** отображаются сообщения участников диалога. Если текст слишком большой, видна только его часть. Чтобы прочитать такое сообщение, воспользуйтесь ссылкой **просмотр**.

Также при работе с запросом можно использовать кнопки:

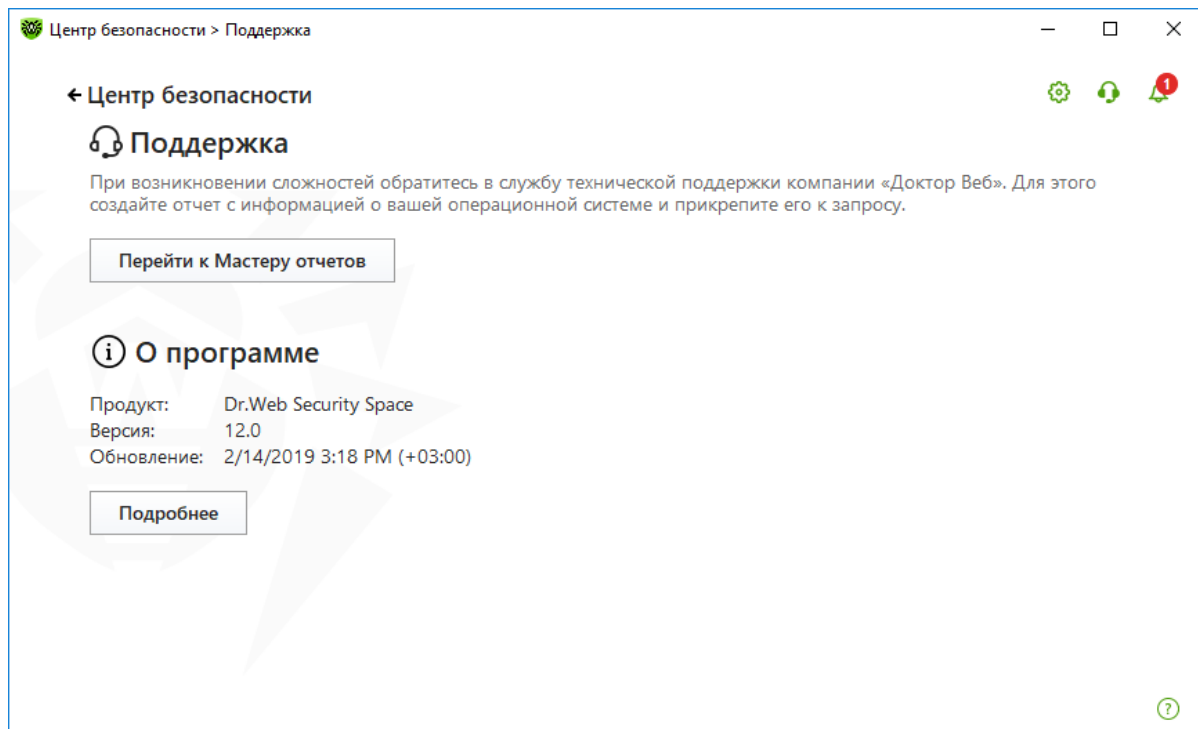
- **Добавить комментарий** — позволяет пользователю ответить на вопросы, заданные сотрудником техподдержки, или разъяснить какие-либо элементы проблемы. Также на странице добавления комментария к ответу можно приложить запрошенные сотрудником данные (например, log-файлы).
- **Обновить** — обновляет текущую страницу. Используется во время интенсивного диалога пользователя с сотрудником.
- **Закрыть запрос** — позволяет пользователю самостоятельно закрыть запрос, когда проблема решена. При этом предлагается оценить по пятибалльной шкале работу сотрудника и указать причину, по которой запрос закрывается.

Отметив флажком оценку работы сотрудника и указав причину закрытия запроса, нажмите на кнопку **Отправить**. После этого откроется страница, информирующая об успешном закрытии запроса. Отсюда пользователь может либо вернуться на главную страницу трекера, либо еще раз просмотреть запрос, воспользовавшись одной из предложенных ссылок.

8.19.1. Сбор информации для службы технической поддержки

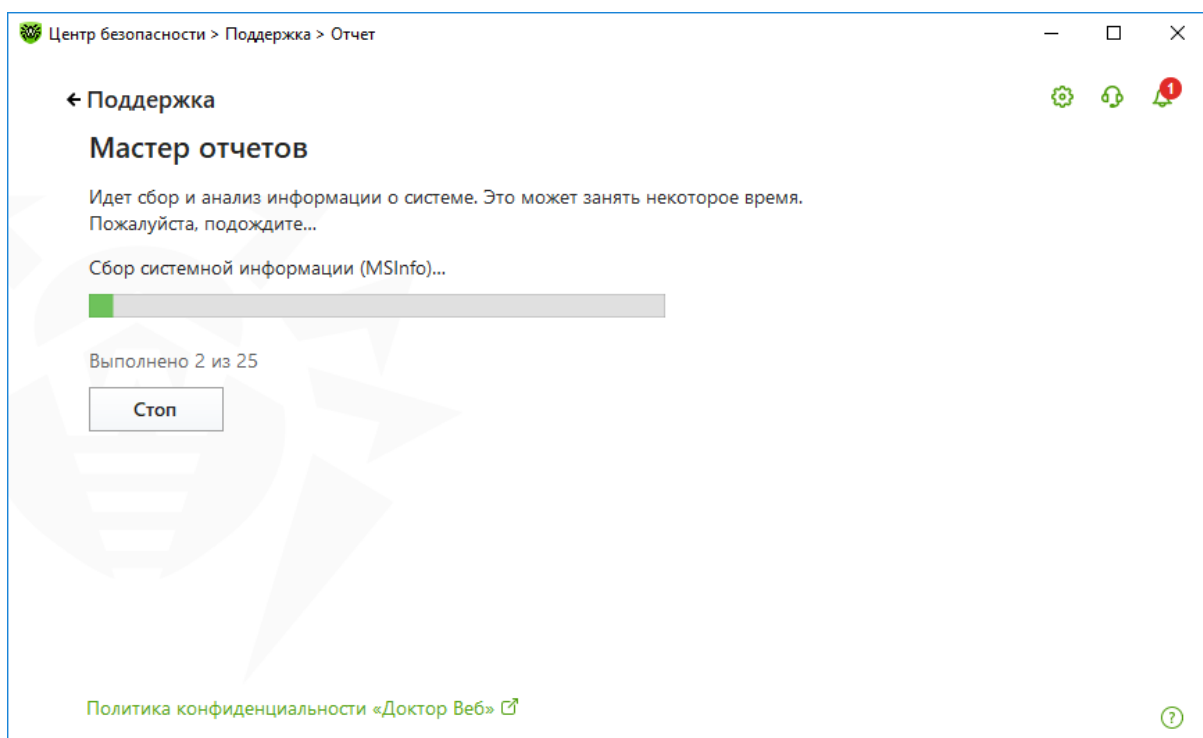
Немаловажным преимуществом продукта является простота сбора необходимой информации для службы технической поддержки. Пользователю не нужно собирать все необходимые файлы и данные — за него это делает сама система.

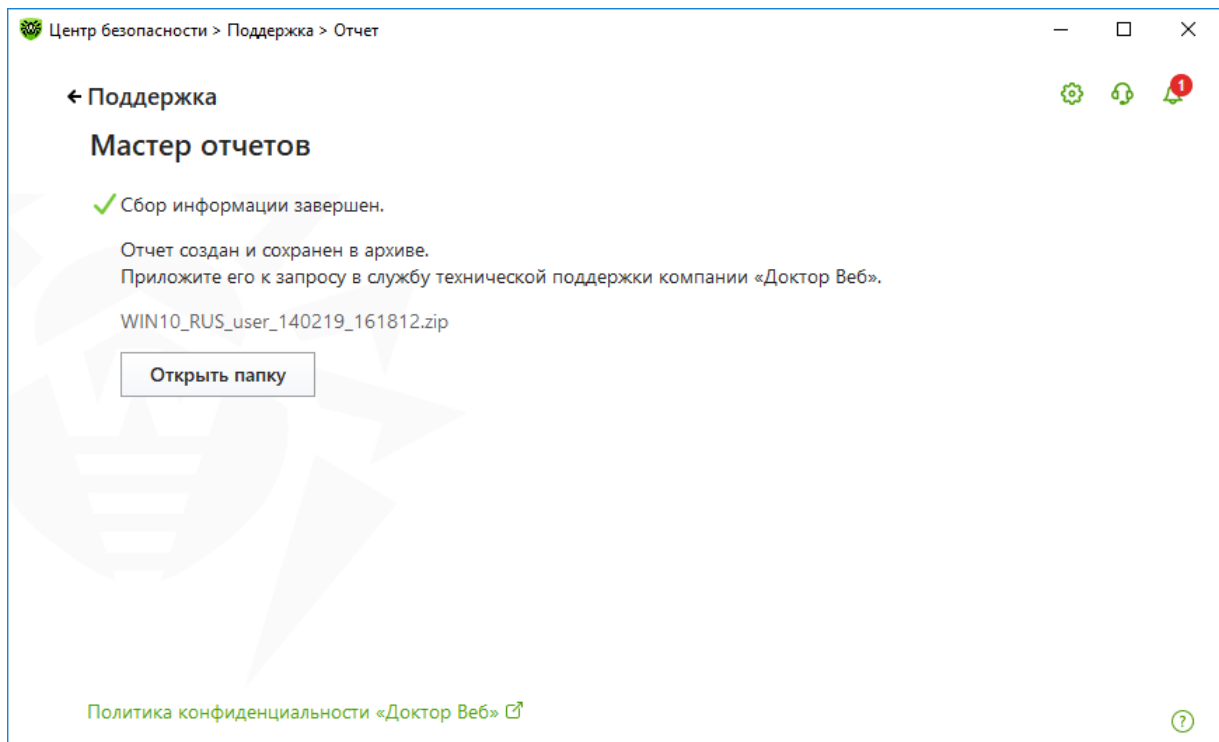
Для сбора информации кликните по значку  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Поддержка** → **Перейти к мастеру отчетов**.



В появившемся окне нажмите кнопку **Создать отчет**.

Антивирус автоматически соберет все данные и создаст в папке по умолчанию архив — передайте его в службу технической поддержки или системному администратору.





Отчет будет сохранен в виде архива в каталоге DoctorWeb, расположенном в папке профиля пользователя %USERPROFILE%.

Отчет может включать в себя следующие:

1. Техническая информация об ОС включает общие сведения о следующем:

- компьютер;
- запущенные процессы;
- запланированные задания;
- службы, драйвера;
- браузер по умолчанию;
- установленные приложения;
- политики ограничений;
- файл HOSTS;
- серверы DNS;
- отчеты программы MSInfo;
- записи системного журнала событий;
- перечень системных каталогов;
- ветви реестра;
- провайдеры Winsock;
- сетевые соединения;
- отчеты отладчика Dr.Watson;
- индекс производительности.

2. Информация о продуктах Dr.Web:

Dr.Web® Security Space. Руководство по быстрой установке и разворачиванию

Информация о работе антивирусных решений Dr.Web всегда доступна в журнале событий операционной системы Windows, в разделе **Журналы приложений и служб — Doctor Web**. Чтобы создать отчет выбранной конфигурации, просто нажмите на кнопку **Сформировать отчет**.

8.20. Отсылка образцов на анализ

Если вы считаете, что Dr.Web не определил объект как вредоносный или же произошло ложное срабатывание (не представляющий опасности объект был детектирован как вирус):

- поместите объект, на который произошло ложное срабатывание, в **Карантин**;
- проведите обновление вирусных баз;
- выберите объект в **Карантине** и произведите повторное сканирование;
- если все еще наблюдается ложное срабатывание, отошлите объект на анализ в **Антивирусную лабораторию «Доктор Веб»**:
 - С главной страницы сайта «Доктор Веб» перейдите на страницу **Послать вирус**: <https://vms.drweb.ru/sendvirus>.

9. Получение документации по продуктам Dr.Web

Наиболее подробная информация об установке и настройке продукта содержится в документации. Чтобы получить документацию, откройте в браузере страницу <http://download.drweb.ru/doc> (с сайта «Доктор Веб» перейти по ссылке **Скачать**, затем выберите в меню пункт **Документация**).

Откроется список продуктов, для которых доступно скачивание и просмотр документации.

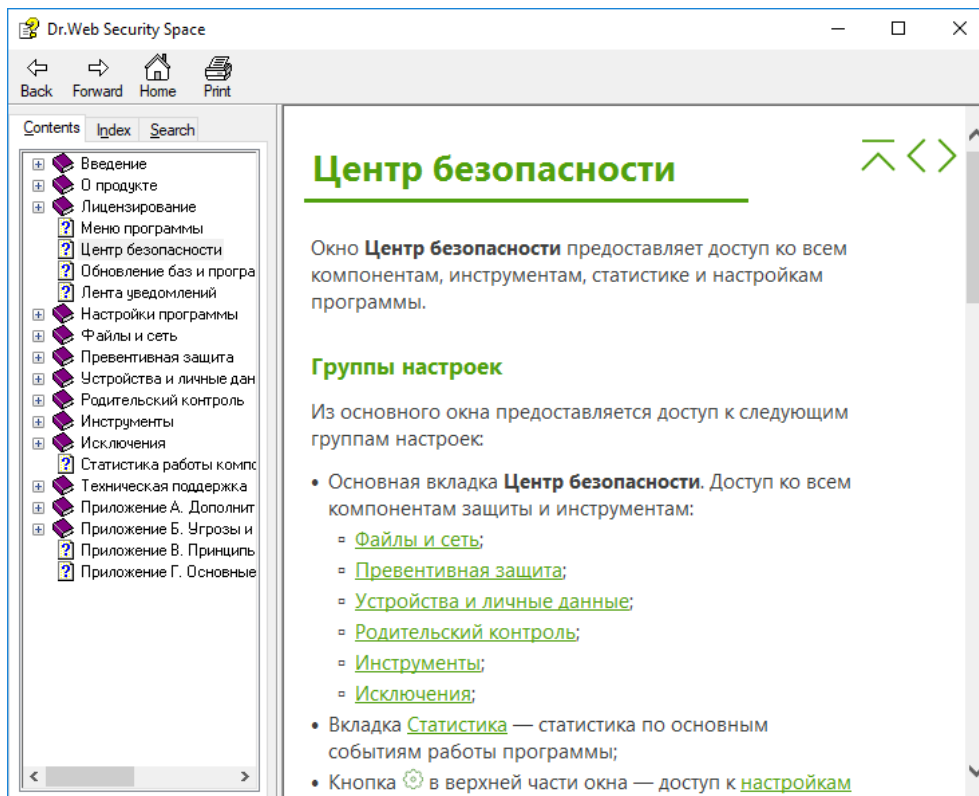
В нашем случае найдите пункт Dr.Web Desktop Security Suite, выберите свою операционную систему. Скачайте документацию в формате pdf либо просмотрите онлайн.

Продукт	Поддерживаемые ОС и платформы	Документация	Онлайн-документация
Dr.Web® Desktop Security Suite	Windows 7/Vista /XP/2000 SP 4 + Rollup 1	Антивирус <input type="text" value="русский"/> <input type="button" value="Скачать"/>	<input type="button" value="Открыть"/>
		Security space <input type="text" value="русский"/> <input type="button" value="Скачать"/>	

10. Работа со справкой о программе

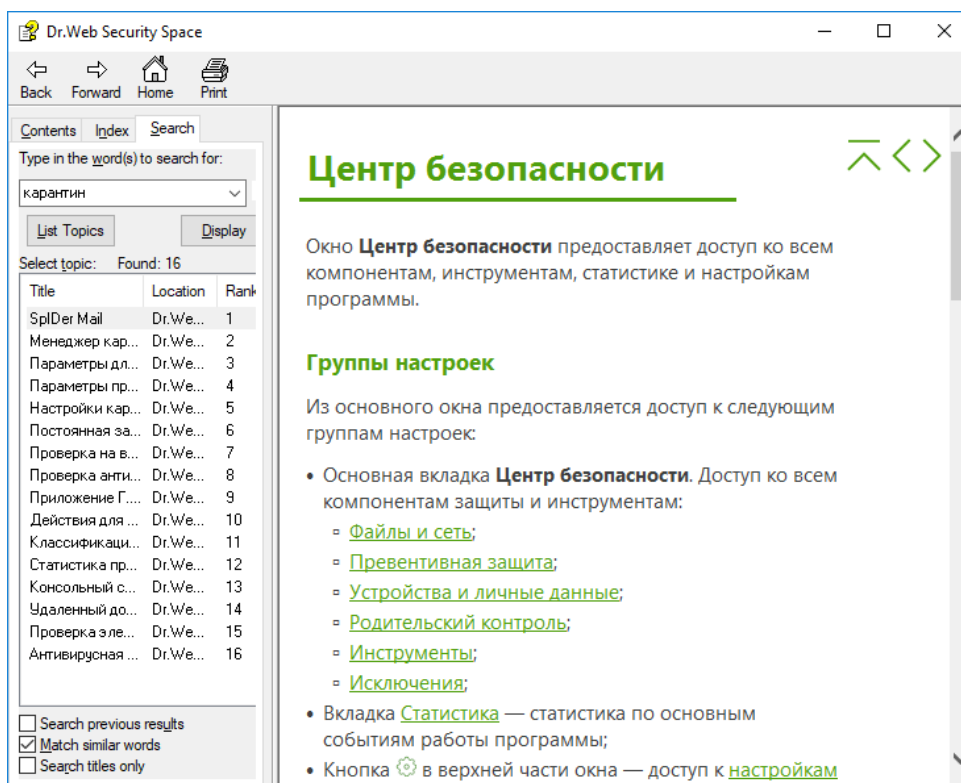
Справка о программе Dr.Web содержит достаточно подробную информацию о каждом компоненте, доступном в настройках программы. В случае возникновения затруднений при работе с программой, до того, как обратиться в службу технической поддержки, рекомендуется ознакомиться со справочными материалами.

Вызовите справку нажатием на значок справки в правом левом углу окна приложения — **Справка** откроется на нужном пункте, соответствующем разделу настроек.



В левой части окна **Справки** имеются две вкладки. Во вкладке **Содержание** расположен иерархический список компонентов справочного материала, каждый пункт раскрывается при нажатии на значок +:

Во вкладке **Поиск** вы можете найти интересующую вас информацию по ключевым словам или фразам. При этом вы можете использовать операторы **И**, **ИЛИ**, **ОКОЛО** (приблизительно) и **НЕ** для уточнения параметров поиска. Результатом станет список разделов **Справки**, касающихся в той или иной степени (ранг) интересующего вас предмета:



Кнопка **Домой** в левом верхнем углу открывает главную страницу «Доктор Веб» в окне **Справки**, кнопка **Печать** позволяет распечатать **Справку** на любом доступном вам принтере.

11. Дополнительная информация

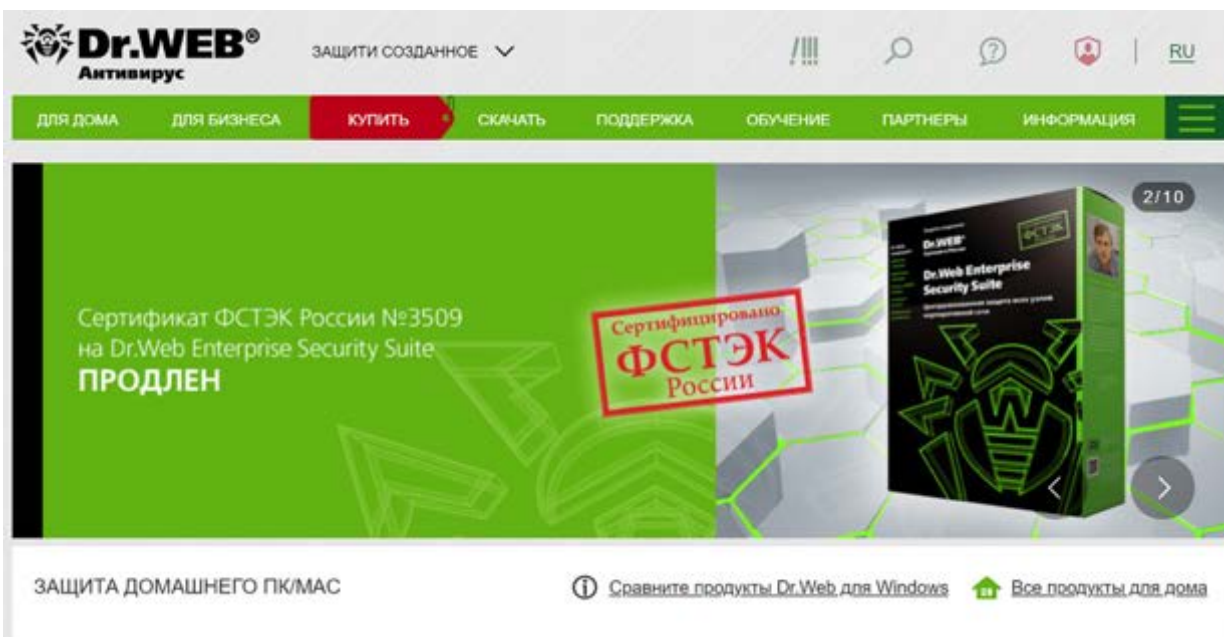
При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу <http://download.drweb.ru>;
- прочитать раздел часто задаваемых вопросов по адресу <http://support.drweb.ru>;
- попытаться найти ответ в базе знаний Dr.Web по адресу <http://wiki.drweb.com>;
- посетить форумы Dr.Web по адресу <http://forum.drweb.com>.

Если после этого все еще не удастся решить проблему, заполните веб-форму вопроса в соответствующей секции раздела <http://support.drweb.ru>.

Найти ближайшее представительство «Доктор Веб» и всю контактную информацию, необходимую пользователю, можно по адресу <http://company.drweb.ru/contacts/moscow>.

Быть в курсе последних новостей позволяет личный кабинет пользователя «Мой Dr.Web». Для того чтобы попасть в него из контекстного меню, выберите пункт **Мой Dr.Web** и перейдите на домашнюю страницу сайта «Доктор Веб» (она откроется в браузере по умолчанию):



Наиболее важными разделами сайта, с которыми рекомендуется ознакомиться, являются:

- ▲ **Скачать** — получение дистрибутивов продуктов Dr.Web, а также просмотр и скачивание документации.
- ▲ **Магазин** — интернет-магазин компании «Доктор Веб», здесь вы можете приобрести лицензию на любой из продуктов компании, а также ознакомиться с информацией о продуктах.
- ▲ **Новости** — рекомендуется подписаться на новости компании, поскольку в ленте новостей периодически появляется важная информация об обновлении линейки продуктов Dr.Web, а также о вирусной активности.

Dr.Web® Security Space. Руководство по быстрой установке и развертыванию

- ^ **Поддержка** — обращение в техническую поддержку (см. п. 6) и прочие полезные ресурсы и сервисы, которые помогут вам улучшить антивирусную защиту и узнать больше о вредоносных программах и средствах борьбы с ними.
- ^ **Обучение и сертификация** — важный раздел, посвященный обучению администрированию продуктов Dr.Web. На странице <https://training.drweb.ru/external/courses/?lng=ru> вы можете зарегистрироваться в **Кабинете заочника**, записаться на понравившиеся курсы или вебинары, а по завершении этих курсов сдать экзамен и стать сертифицированным специалистом по антивирусной защите. Такой сертификат откроет для вас новые карьерные возможности и станет подтверждением полученных знаний.

О компании «Доктор Веб»

ООО «Доктор Веб» — российский разработчик средств информационной безопасности под маркой Dr.Web.

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

Антивирусные продукты Dr.Web разрабатываются с 1992 года, неизменно демонстрируют превосходные результаты детектирования вредоносных программ и 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!

Центральный офис в России

125040 Россия, Москва 3-я улица Ямского поля, вл. 2, корп. 12а

Веб-сайт: www.drweb.ru

Телефон: +7 495 789-45-87

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