Dr.WEB

Desktop Security Suite (для Linux) версия 11

Руководство пользователя

Dr.Web Desktop Security Suite (для Linux)
Версия 11.0
Руководство пользователя
20.05.2019

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Условные обозначения и сокращения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Важное замечание или указание.
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`/home/user`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Команды, которые требуется вести с клавиатуры в командную строку операционной системы (в терминале или эмуляторе терминала), в руководстве предваряются символом приглашения ко вводу `$` или `#`, который указывает, какие полномочия пользователя необходимы для исполнения данной команды. Стандартным для UNIX-систем образом подразумевается, что:

`$` – для исполнения команды достаточно обычных прав пользователя.

`#` – для исполнения команды требуются права суперпользователя (обычно – *root*). Для повышения прав можно использовать команды **su** и **sudo**.

Введение

Благодарим вас за приобретение программного продукта Dr.Web Desktop Security Suite (для Linux). Он позволит вам обеспечить надежную защиту вашего компьютера от компьютерных угроз всех возможных типов, используя наиболее современные технологии обнаружения и обезвреживания угроз.

Данное руководство предназначено для помощи пользователям компьютеров, работающих под управлением операционных систем семейства **GNU/Linux** (далее в документе будет использовано обозначение **Linux**), в установке и использовании Dr.Web Desktop Security Suite (для Linux) версии 11.0.

Если у вас уже установлен Dr.Web Desktop Security Suite (для Linux) предыдущей версии, и вы желаете обновить его до версии 11.0, выполните переход на новую версию (см. раздел Переход на новую версию).

О продукте

Dr.Web Desktop Security Suite (для Linux) создан для защиты компьютеров, работающих под управлением ОС семейства **GNU/Linux**, от вирусов и всех прочих видов вредоносного программного обеспечения, предназначенных для различных платформ.

Основные компоненты программы (антивирусное ядро и вирусные базы) являются не только крайне эффективными и нетребовательными к системным ресурсам, но и кросс-платформенными, что позволяет специалистам компании «Доктор Веб» создавать надежные антивирусные решения, обеспечивающие защиту компьютеров и мобильных устройств, работающих под управлением распространенных операционных систем, от угроз, предназначенных для различных платформ. В настоящее время, наряду с Dr.Web Desktop Security Suite (для Linux), в компании «Доктор Веб» разработаны также антивирусные решения для операционных систем семейства **UNIX** (таких, как **FreeBSD** и **Solaris**), **IBM OS/2**, **Novell NetWare**, **macOS** и **Windows**. Кроме того, разработаны антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением ОС **Andorid**, **Symbian**, **BlackBerry** и **Windows Mobile**.

Компоненты Dr.Web Desktop Security Suite (для Linux) постоянно обновляются, а вирусные базы Dr.Web регулярно дополняются новыми сигнатурами угроз, что обеспечивает актуальный уровень защищенности компьютера, программ и данных пользователей. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре, а также обращение к сервису Dr.Web Cloud, собирающему свежую информацию об актуальных угрозах и способному оградить пользователей от посещения нежелательных веб-сайтов, а также защитить операционные системы от инфицированных файлов.

Основные функции

Основные функции продукта Dr.Web Desktop Security Suite (для Linux):

1. **Поиск и обезвреживание угроз**. Обнаруживаются и обезвреживаются как непосредственно вредоносные программы всех возможных типов (различные вирусы, включая вирусы, инфицирующие почтовые файлы и загрузочные записи дисков, троянские программы, почтовые черви и т.п.), так и нежелательные программы (рекламные программы, программы-шутки, программы автоматического дозвона). Подробнее о видах угроз см. Приложение А. Виды компьютерных угроз.

   Для обнаружения вредоносных и нежелательных программ используются:

   - *Сигнатурный анализ*. Метод проверки, позволяющий обнаружить уже известные угрозы, информация о которых содержится в вирусных базах.
   - *Эвристический анализ*. Набор методов проверки, позволяющих обнаруживать угрозы, которые еще неизвестны.

- *Обращение к сервису Dr.Web Cloud,* собирающему свежую информацию об актуальных угрозах, рассылаемую различными антивирусными продуктами Dr.Web.

Обратите внимание, что эвристический анализатор может ложно реагировать на программное обеспечение, не являющегося вредоносным. Поэтому объекты, содержащие обнаруженные им угрозы, получают специальный статус «подозрительные». Рекомендуется помещать такие файлы в карантин, а также передавать на анализ в антивирусную лабораторию «Доктор Веб». Подробнее об методах обезвреживания см. Приложение Б. Устранение компьютерных угроз.

Проверка файловой системы может запускаться как вручную, по запросу пользователя, так и автоматически – в соответствии с заданным расписанием. Имеется возможность как полной проверки всех объектов файловой системы, доступных пользователю, так и выборочной проверки только указанных объектов (отдельных каталогов или файлов). Кроме того, доступна возможность отдельной проверки загрузочных записей томов и исполняемых файлов, из которых запущены процессы, активные в системе в данный момент. В последнем случае при обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него.

Для операционных систем, имеющих среду графического рабочего стола, реализована интеграция функций проверки файлов как с панелью задач, так и с графическим файловым менеджером. В системах, реализующих мандатную модель доступа к файлам с набором различных уровней доступа, сканирование файлов, недоступных на текущем уровне доступа, может производиться в специальном режиме автономной копии.

Все объекты с угрозами, обнаруженные в файловой системе, регистрируются в постоянно хранимом реестре угроз, за исключением тех угроз, которые были обнаружены в режиме автономной копии.

Утилита управления из командной строки, входящая в состав продукта, позволяет также выполнять проверку на наличие угроз файловых систем удаленных узлов сети, предоставляющих удаленный терминальный доступ через SSH.

> Вы можете использовать удаленное сканирование только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров и прочих «умных» устройств вы можете воспользоваться механизмом обновления прошивки, а для вычислительных машин – выполнив подключение к ним (в том числе – в удаленном терминальном режиме) и произведя соответствующие операции в их файловой системе (удаление или перемещение файлов и т.п.) или запустив антивирусное ПО, установленное на них.

2. **Мониторинг обращений к файлам**. Отслеживаются обращения к файлам с данными и попытки запуска исполняемых файлов. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках инфицирования ими компьютера.

3. **Мониторинг сетевых соединений**. Отслеживаются попытки обращения к серверам в сети Интернет (веб-серверам, почтовым серверам, файловым серверам) для блокировки доступа пользователя к веб-сайтам, отмеченным как нежелательные для посещения, а также для предотвращения получения и отправки сообщений электронной почты, содержащих инфицированные файлы, нежелательные ссылки или классифицированных как спам. Проверка сообщений электронной почты и файлов, загружаемых по сети, на наличие в них вирусов и других угроз, производится «на лету». Для определения нежелательных ссылок используются как поставляемая вместе с Dr.Web Desktop Security Suite (для Linux) автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, так и черные и белые списки, ведущиеся пользователем вручную. Дополнительно продукт обращается к сервису Dr.Web Cloud для проверки, не отмечен ли веб-сайт, к которому пытается обратиться пользователь, как вредоносный, другими антивирусными продуктами Dr.Web.

   В зависимости от поставки, компонент Dr.Web Anti-Spam может отсутствовать в составе продукта. В этом случае спам-проверка сообщений не производится.

   Если какие-либо сообщения электронной почты неправильно распознаются компонентом проверки сообщений электронной почты на спам, рекомендуется пересылать их на специальные почтовые адреса для анализа и повышения качества работы спам-фильтра:

   - письма, ошибочно *оцененные как спам*, отправляйте на адрес vrnonspam@drweb.com;
   - письма, ошибочно *не определенные как спам*, отправляйте на адрес vrspam@drweb.com.

   Каждое сообщение, подлежащие анализу, следует предварительно сохранить в файл (используйте формат `.eml`). Сохраненные файлы прикрепите к сообщению, отправляемому на соответствующий служебный адрес.

4. **Надежная изоляция инфицированных или подозрительных объектов** в специальном хранилище – карантине, чтобы они не могли нанести ущерба системе. При перемещении объектов в карантин они специальным образом переименовываются, и могут быть восстановлены в исходное место (в случае необходимости) только по команде пользователя.
5. **Автоматическое обновление** содержимого вирусных баз Dr.Web и антивирусного ядра для поддержания высокого уровня надежности защиты от вредоносных программ.
6. **Сбор статистики** проверок и вирусных инцидентов; ведение журнала обнаруженных угроз (доступен только через утилиту управления из командной строки).
7. **Обеспечение работы под управлением сервера централизованной защиты** (такого, как Dr.Web Enterprise Server или в рамках сервиса Dr.Web AV-Desk) для применения на защищаемом компьютере единых политик безопасности, принятых в некоторой сети, в состав которой он входит. Это может быть как сеть некоторого предприятия

(корпоративная сеть) или частная сеть VPN, так и сеть, организованная провайдером каких-либо услуг, например, доступа к сети Интернет.

Поскольку для использования информации, хранящейся в облачном сервисе Dr.Web Cloud, необходимо передавать данные об активности пользователя (например, передавать на проверку адреса посещаемых им веб-сайтов), то обращение к Dr.Web Cloud производится только после получения соответствующего разрешения пользователя. При необходимости, использование Dr.Web Cloud можно запретить в любой момент в настройках программы.

Структура программного продукта

Dr.Web Desktop Security Suite (для Linux) состоит из следующих компонентов:

Компонент	Описание
Сканер	Компонент, выполняющий по требованию пользователя или по заданному расписанию проверку объектов файловой системы (файлы, каталоги и загрузочные записи) на наличие в них угроз. Пользователь имеет возможность запускать проверку как из графического режима, так и из командной строки.
Монитор файловой системы SpIDer Guard	Компонент, работающий в резидентном режиме и отслеживающий операции с файлами (такие как создание, открытие, закрытие и запуск файла). Посылает Сканеру запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ. Работает с файловой системой ОС через системный механизм **fanotify** или через специальный модуль ядра (*LKM – Linux Kernel Module*), разработанный компанией «Доктор Веб».
Монитор сетевых соединений SpIDer Gate	Компонент, работающий в резидентом режиме и отслеживающий все сетевые соединения. • Проверяет наличие URL в базах категорий веб-ресурсов и черных списках пользователя; блокирует доступ к веб-сайтам, если ведущие к ним URL зарегистрированы в черном списке пользователя или категориях, отмеченных как нежелательные для посещения. • Блокирует отправку и прием сообщений электронной почты, если они содержат вредоносные объекты или нежелательные ссылки. • Посылает Сканеру на проверку файлы, загружаемые из сети Интернет (с серверов, доступ к которым был разрешен), и блокирует их загрузку, в случае если они содержат угрозы. Дополнительно, при наличии соответствующего разрешения от пользователя, посылает запрашиваемые им URL на проверку в сервис Dr.Web Cloud.

Компонент	Описание
Антивирусное ядро	Центральный компонент антивирусной защиты. Используется Сканером для поиска и распознавания вирусов и вредоносных программ, а также анализа подозрительного поведения.
Dr.Web Anti-Spam	Компонент проверки сообщений электронной почты на наличие признаков спама. Используется компонентом SpIDer Gate. Может отсутствовать, в зависимости от поставки. Если отсутствует, проверка сообщений электронной почты на наличие признаков спама не осуществляется.
Вирусные базы	Автоматически обновляемая база данных, содержащая информацию об известных угрозах, и используемая антивирусным ядром для распознавания и лечения угроз.
База категорий веб-ресурсов	Автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, и используемая SpIDer Gate для блокирования доступа к нежелательным сайтам.
Компонент обновления	Компонент, отвечающий за автоматическую загрузку с серверов обновлений компании «Доктор Веб» обновлений для вирусных баз, антивирусного ядра и базы категорий веб-ресурсов (как автоматически, по расписанию, так и непосредственно по команде пользователя).
Графический интерфейс управления	Компонент, предоставляющий оконный графический интерфейс управления Dr.Web Desktop Security Suite (для Linux). Позволяет пользователю в графическом режиме запускать проверку объектов файловой системы, управлять работой мониторов SpIDer Guard и SpIDer Gate, просматривать содержимое карантина, выполнять запуск получения обновлений, а также настраивать работу Dr.Web Desktop Security Suite (для Linux).
Агент уведомлений	Компонент, работающий в фоновом режиме. Отображает всплывающие уведомления о возникающих событиях и индикатор приложения Dr.Web Desktop Security Suite (для Linux) в области уведомлений, запускает проверки по расписанию. По умолчанию запускается при начале сеанса работы пользователя в среде рабочего стола.
Менеджер лицензий	Компонент, упрощающий работу с лицензиями в графическом режиме. Позволяет активировать лицензию или демонстрационный период, просмотреть данные о текущей лицензии, выполнить ее продление, а также установить и удалить лицензионный ключевой файл.

Кроме перечисленных в таблице, в состав Dr.Web Desktop Security Suite (для Linux) входят также дополнительные сервисные компоненты, работающие в фоновом режиме и не требующие вмешательства пользователя.

Монитор файловой системы SpIDer Guard может использовать два режима работы:

- *FANOTIFY* – работа через системный механизм **fanotify** (поддерживается не всеми ОС семейства **GNU/Linux**).
- *LKM* – работа с использованием загружаемого модуля ядра **Linux**, разработанного компанией «Доктор Веб» (может быть использован в любой ОС семейства **GNU/Linux** с ядром версии 2.6.x и новее).

По умолчанию монитор файловой системы автоматически выбирает подходящий режим работы, исходя из возможностей окружения. В случае если SpIDer Guard не запускается, выполните сборку и установку загружаемого модуля ядра из поставляемых исходных кодов.

Каталоги карантина

Карантин Dr.Web Desktop Security Suite (для Linux) представляет собой систему каталогов, предназначенных для надежной изоляции файлов, содержащих выявленные угрозы, которые в данный момент не могут быть обезврежены по каким-либо причинам. Например, обнаруженная угроза может быть неизлечимой, потому что еще неизвестна Dr.Web Desktop Security Suite (для Linux) (например, она была обнаружена эвристическим анализатором, а в вирусных базах ее сигнатура, а следовательно – и метод лечения, отсутствует), или при попытке ее лечения возникают ошибки. Кроме того, файл может быть перемещен в карантин непосредственно по желанию пользователя, в случае если он выбрал соответствующее действие в списке обнаруженных угроз или указал его как реакцию Сканера или монитора файловой системы SpIDer Guard на угрозы определенного типа.

Когда файл, содержащий угрозу, перемещается в карантин, он специальным образом переименовывается, чтобы предотвратить возможность его идентификации пользователями и программами, и затруднить доступ к нему, минуя инструменты работы с карантином, реализованные в Dr.Web Desktop Security Suite (для Linux). Кроме того, при перемещении файла в карантин, у него всегда сбрасывается бит исполнения для предотвращения его запуска.

Каталоги карантина размещаются:

- *в домашнем каталоге пользователя* (если на данном компьютере имеется несколько учетных записей разных пользователей, то в домашнем каталоге каждого из этих пользователей может быть создан свой собственный каталог карантина).
- *в корневом каталоге каждого логического тома,* смонтированного в файловую систему операционной системы.

Каталоги карантина Dr.Web Desktop Security Suite (для Linux) всегда имеют имя `.com.drweb.quarantine` и создаются по мере необходимости, в тот момент, когда к какой-либо угрозе применяется действие *«Переместить в карантин»* (*«Изолировать»*), т.е. до тех пор, пока угроз не обнаружено, каталоги карантина не создаются. При этом

всегда создается только тот каталог карантина, который требуется для изоляции файла. Для определения, в какой из каталогов требуется изолировать файл, используется имя владельца файла. Если при движении к корню файловой системы / от каталога, содержащего файл, достигается домашний каталог владельца, файл изолируется в каталог карантина, находящийся в нем. В противном случае файл будет изолирован в каталог карантина, созданный в корне тома, содержащего файл (корневой каталог тома необязательно совпадет с корнем файловой системы). Таким образом, любой инфицированный файл, помещаемый в карантин, всегда остается на том томе, на котором он был обнаружен. Это обеспечивает корректную работу карантина при наличии в системе съемных накопителей и других томов, которые могут монтироваться в файловую систему операционной системы периодически и в различные точки.

Пользователь может управлять содержимым карантина как в графическом режиме работы, так и из командной строки. При этом всегда обрабатывается консолидированный карантин, объединяющий в себе все каталоги с изолированными объектами, доступные в данный момент. С точки зрения пользователя, просматривающего содержимое консолидированного карантина, каталог, располагающийся в его домашнем каталоге, называется *Пользовательским* карантином, а все остальные каталоги считаются *Системным* карантином.

Работа с карантином возможна даже тогда, когда отсутствует активная лицензия, но в этом случае становится невозможным лечение изолированных объектов.

Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз Dr.Web Desktop Security Suite (для Linux) (точнее, пользователь, от имени которого он запущен) должен обладать следующими полномочиями:

Действие	**Требуемые полномочия**
Вывод всех обнаруженных угроз	Без ограничений. Специальных полномочий не требуется.
Вывод содержимого контейнера (архива, почтового файла и т.п.) (Отображение только элементов, которые содержат ошибку или угрозу)	Без ограничений. Специальных полномочий не требуется.

Действие	Требуемые полномочия
Перемещение в карантин	Без ограничений. Пользователь может отправлять в карантин все инфицированные файлы, независимо от наличия у него прав на чтение и запись для перемещаемого файла.
Удаление угроз	Пользователь должен иметь права на запись в удаляемый файл. Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления выполняется перемещение контейнера в карантин.
Лечение файлов	Без ограничений. После выполнения лечения остается вылеченный файл с исходными правами доступа и владельцем. Файл может быть удален, если удаление является методом лечения обнаруженной в нем угрозы.
Восстановление файла из карантина	Пользователь должен иметь разрешение на чтение восстанавливаемого файла и иметь разрешение выполнять запись в каталог восстановления.
Удаление файла из карантина	Пользователь должен иметь разрешение на запись в исходный файл, который был перемещен в карантин.

Для временного повышения прав Dr.Web Desktop Security Suite (для Linux), запущенного в графическом режиме, вы можете воспользоваться соответствующей кнопкой, имеющейся на окне Dr.Web Desktop Security Suite (для Linux) (она доступна и отображается только в тех случаях, когда повышение прав может потребоваться для успешного выполнения некоторой операции). Для запуска Dr.Web Desktop Security Suite (для Linux) в графическом режиме или утилиты управления из командной строки с правами суперпользователя вы можете воспользоваться командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

Сканер не может работать с файлами, размер которых больше 4 Гбайт (при попытке проверки таких файлов будет выдаваться ошибка *«Файл слишком большой»*).

Режимы защиты

Dr.Web Desktop Security Suite (для Linux) может работать как автономно, так и в составе корпоративной или частной *антивирусной сети,* управляемой каким-либо *сервером централизованной защиты.* Такой режим работы называется *режимом централизованной защиты.* Использование этого режима не требует установки дополнительного программного обеспечения, переустановки или удаления Dr.Web Desktop Security Suite (для Linux).

- *В одиночном режиме (standalone mode)* защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационный и лицензионный ключевой файлы находятся на локальных дисках, а Dr.Web Desktop Security Suite (для Linux) полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании «Доктор Веб».
- *В режиме централизованной защиты (central protection mode)* защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web Desktop Security Suite (для Linux) могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты, принятой в антивирусной сети. В этом режиме на компьютере используется особый лицензионный ключевой файл, полученный с выбранного сервера централизованной защиты, к которому подключен Dr.Web Desktop Security Suite (для Linux). Лицензионный или демонстрационный ключевой файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы Dr.Web Desktop Security Suite (для Linux), включая статистику вирусных инцидентов. Обновление вирусных баз также выполняется с сервера централизованной защиты.
- *В мобильном режиме (mobile mode)* Dr.Web Desktop Security Suite (для Linux) получает обновления вирусных баз с серверов обновлений компании «Доктор Веб», но использует локально хранящиеся настройки и особый лицензионный ключевой файл, полученные от сервера централизованной защиты.

В случае работы Dr.Web Desktop Security Suite (для Linux) под управлением сервера централизованной защиты (в том числе и в мобильном режиме) блокируются следующие возможности:

1. Возможность удаления лицензионного ключевого файла в Менеджере лицензий.
2. Возможность запуска обновлений вручную и настройки параметров обновления.
3. Возможность настройки параметров проверки объектов файловой системы Сканером.

Возможность настройки монитора файловой системы SplDer Guard, а также его включения и выключения при работе Dr.Web Desktop Security Suite (для Linux) под управлением сервера централизованной защиты зависит от разрешений, заданных на сервере.

В режиме централизованной защиты недоступна проверка файлов по заданному расписанию.

Если на сервере централизованной защиты включен запрет на запуск проверки файлов пользователем, то страница запуска сканирования и кнопка **Сканер** на окне Dr.Web Desktop Security Suite (для Linux) будут недоступны.

Принципы централизованной защиты

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см. иллюстрацию ниже).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз *локальными антивирусными компонентами* (в данном случае – Dr.Web Desktop Security Suite (для Linux)), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

Рисунок 1. Логическая структура антивирусной сети.

Обновление и конфигурация локальных компонентов производится через *сервер централизованной защиты*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и сервером централизованной защиты может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

Все необходимые обновления загружаются на сервер централизованной защиты с серверов обновлений компании «Доктор Веб».

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется сервером централизованной защиты по указанию администраторов антивирусной сети. Администраторы управляют конфигурацией сервера централизованной защиты и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также, при необходимости, задают настройки работы конкретных локальных антивирусных компонентов.

Локальные антивирусные компоненты несовместимы с антивирусным программным обеспечением как других компаний, так и антивирусными решениями Dr.Web, не поддерживающими режим централизованной защиты (например Dr.Web Desktop Security Suite (для Linux) версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Подключение к антивирусной сети

Dr.Web Desktop Security Suite (для Linux) может быть подключен к антивирусной сети следующими способами:

- На вкладке **Режим** страницы настроек окна Dr.Web Desktop Security Suite (для Linux).
- При помощи команды `esconnect` утилиты управления из командной строки **drweb-ctl**.

Отключение от антивирусной сети

Dr.Web Desktop Security Suite (для Linux) может быть отключен от антивирусной сети следующими способами:

- На вкладке **Режим** страницы настроек окна Dr.Web Desktop Security Suite (для Linux).
- При помощи команды `esdisconnect` утилиты управления из командной строки **drweb-ctl**.

Проверка работоспособности

Имеется стандартный тест, позволяющий проверить работоспособность антивирусных программ, использующих сигнатурные методы обнаружения угроз. Для этого применяется специальный тест *EICAR* (*European Institute for Computer Anti-Virus Research*), разработанный одноименной организацией. Этот тест разработан для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении вируса.

Программа, используемая для теста *EICAR,* не является вредоносной, но специально определяется большинством антивирусных программ как вирус. Антивирусные продукты Dr.Web называют этот «вирус» следующим образом: **EICAR Test File (NOT a Virus!)**. Примерно так его называют и другие антивирусные программы. Тестовая программа **EICAR** представляет собой последовательность из 68 байт, образующую тело исполняемого COM-файла для ОС **MS DOS**/**MS Windows**, в результате исполнения которого на экран терминала или в эмулятор консоли выводится текстовое сообщение:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Тело тестовой программы состоит только из текстовых символов, которые формируют следующую строку:

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

Если вы создадите файл, содержащий приведенную выше строку, то в результате получится программа, которая и будет описанным «вирусом».

В случае корректной работы Dr.Web Desktop Security Suite (для Linux), этот файл должен обнаруживаться при проверке объектов файловой системы любым доступным способом, с уведомлением об обнаружении угрозы **EICAR Test File (NOT a Virus!)**.

Пример команды для проверки работоспособности продукта при помощи тестовой программы **EICAR** из командной строки:

```
$ tail /opt/drweb.com/share/doc/drweb-common/readme.eicar | grep X5O > testfile && drweb-ctl scan testfile && rm testfile
```

Данная команда выделяет из файла `/opt/drweb.com/share/doc/drweb-common/readme.eicar` (поставляется вместе с продуктом) строку, представляющую собой тело тестовой программы **EICAR**, записывает ее в файл `testfile` в текущий каталог, выполняет проверку полученного файла, после чего удаляет созданный файл.

Для успешного проведения вышеуказанного теста вы должны иметь права записи в текущий каталог. Кроме того, убедитесь, что в нем отсутствует файл с именем `testfile` (при необходимости измените имя файла в команде).

В случае успешного обнаружения тестового «вируса» на экран будет выдано следующее сообщение:

```
<путь к текущему каталогу>/testfile - infected with EICAR Test File (NOT a Virus!)
```

Если при проверке будет получено сообщение об ошибке, обратитесь к описанию известных ошибок.

Если в системе работает монитор файловой системы SpIDer Guard, при обнаружении угрозы файл может быть тут же удален или перемещен в карантин (в зависимости от настроек компонента). В этом случае после сообщения об обнаружении угрозы команда **rm** сообщит об отсутствии файла. Эта ситуация не является ошибкой, а сигнализирует о корректной работе монитора.

Системные требования

Использование Dr.Web Desktop Security Suite (для Linux) возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
Платформа	Поддерживаются процессоры следующих архитектур и систем команд: • **Байкал-Т1** (*MIPS*). • **Эльбрус** (*Эльбрус-4С, Эльбрус-8С, Эльбрус-8СВ*).
Оперативная память (RAM)	Не менее 500 МБ свободной оперативной памяти (рекомендуется 1 ГБ и более).
Место на жестком диске	Не менее 512 МБ свободного дискового пространства на томе, на котором размещаются каталоги Dr.Web Desktop Security Suite (для Linux).
Операционная система	**Linux** на основе ядра с версией 2.6.37 или новее, использующая **PAM** и библиотеку **glibc** версии 2.13 или новее. Перечень протестированных дистрибутивов **Linux** перечислен ниже. В случае использования 64-битной версии операционной системы, должна быть обязательно включена поддержка исполнения 32-битных приложений (для этого, возможно, потребуются дополнительные библиотеки, см. ниже). Для корректной работы компонента SpIDer Gate ядро ОС должно быть собрано со включением следующих опций: • *CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;* • *CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;* • *CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.* Конкретный набор требуемых опций из указанного перечня может зависеть от используемого дистрибутива ОС **GNU/Linux**.
Прочее	Наличие сетевого подключения:

Компонент	Требование
	• Подключение к сети Интернет для загрузки обновлений, а также для обращения к Dr.Web Cloud (при наличии соответствующего разрешения от пользователя). • При работе в режиме централизованной защиты достаточно только подключения к используемому серверу в рамках локальной сети, доступ в Интернет не требуется.

Dr.Web Desktop Security Suite (для Linux) несовместим с другими антивирусными программами. Так как установка двух антивирусов на один компьютер может привести к ошибкам в системе и потере важных данных, перед установкой Dr.Web Desktop Security Suite (для Linux) следует удалить с компьютера другие антивирусные программы.

Работоспособность программного продукта протестирована на следующих дистрибутивах **Linux**:

Название дистрибутива Linux	Версии	Платформы
Astra Linux Special Edition (Ленинград)	8.1	Эльбрус-4C, Эльбрус-8C, Эльбрус-8CB
Astra Linux Special Edition (Севастополь)	6.1.1	MIPS
Эльбрус	–	Эльбрус-4C, Эльбрус-8C, Эльбрус-8CB

Прочие дистрибутивы **Linux**, соответствующие описанным требованиям, не проходили тестирование на совместимость с Dr.Web Desktop Security Suite (для Linux), но могут быть совместимы. При возникновении проблем с совместимостью с вашим дистрибутивом, обратитесь в техническую поддержку.

Требуемые дополнительные компоненты и пакеты

- Для ОС **CentOS**, **Debian**, **Fedora**, **Red Hat Enterprise Linux**, **Ubuntu** на платформе *x86_64* требуется пакет поддержки исполнения 32-битных приложений (**libc6-i386** или **glibc.i686**, в зависимости от ОС).
- Для работы Dr.Web Desktop Security Suite (для Linux) в графическом режиме, а также для запуска программ установки и удаления продукта для графического режима требуется наличие графической подсистемы **X Window System** и любого менеджера окон. Кроме того, для корректного отображения индикатора в графическом окружении **Ubuntu Unity**

может потребоваться наличие дополнительной библиотеки (по умолчанию требуется библиотека **libappindicator1**).

- Для работы в графическом режиме программ установки и удаления продукта, рассчитанных на режим командной строки, необходимо наличие в системе любого эмулятора терминала (например, **xterm** или **xvt**).
- Для повышения привилегий программ установки и удаления необходимо наличие любой из утилит повышения прав: **su**, **sudo**, **gksu**, **gksudo**, **kdesu**, **kdesudo**. Для корректной работы продукта также необходимо, чтобы в системе использовался механизм аутентификации **PAM**.

Для удобной работы с Dr.Web Desktop Security Suite (для Linux) из командной строки рекомендуется включить автодополнение команд в используемой командной оболочке, если оно не включено.

В случае возникновения проблем с установкой требуемых дополнительных пакетов и компонентов обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

Совместимость с компонентами операционных систем

- Монитор SpIDer Guard по умолчанию использует системный механизм **fanotify**, а для в тех ОС, в которых механизм **fanotify** не реализован или недоступен по иным причинам – специальный *загружаемый модуль ядра (LKM-модуль)*, поставляемый в собранном виде. В составе продукта поставляются LKM-модули всех систем **GNU/Linux**, указанных выше. В случае необходимости вы имеете возможность собрать модуль ядра самостоятельно из поставляемых исходных кодов для любой ОС, использующей ядро **GNU/Linux** версии 2.6.x и новее.

Работа SpIDer Guardчерез модуль ядра **GNU/Linux** (LKM-модуль) не поддерживается для ОС, запущенных в среде гипервизора **Xen**. Попытка загрузки модуля ядра, используемого SpIDer Guard, при работе ОС в среде **Xen** может привести к критической ошибке ядра (т.н. ошибка «*Kernel panic*»).

Работа SpIDer Guard в усиленном («параноидальном») режиме с предварительной блокировкой доступа к еще не проверенным файлам возможна только через **fanotify** и при условии, что ядро ОС собрано с активной опцией `CONFIG_FANOTIFY_ACCESS_PERMISSIONS`.

- Монитор SpIDer Gate может конфликтовать с другими брандмауэрами, установленными в вашей ОС:
  - Конфликт с **Shorewall** и **SuseFirewall2** (в ОС **SUSE Linux Enterprise Server**). В случае конфликта с этими брандмауэрами наблюдается сообщение об ошибке SpIDer Gate с

кодом `x109`. Способ устранения конфликта описан в разделе «Описание известных ошибок».

- Конфликт с **FirewallD** (в ОС **Fedora**, **CentOS**, **Red Hat Enterprise Linux**). В случае конфликта с этим брандмауэром наблюдается сообщение об ошибке SplDer Gate с кодом `x102`. Способ устранения конфликта описан в разделе «Описание известных ошибок».

- В случае если в состав ОС включен **NetFilter** версии *младше 1.4.15*, в работе SplDer Gate возможно возникновение следующей проблемы, связанной с внутренней ошибкой в реализации **NetFilter**: при выключении SplDer Gate нарушается работа сети. Рекомендуется обновить ОС до версии, включающей **NetFilter** версии 1.4.15 или новее. Руководство по устранению указанной проблемы приведено в разделе «Описание известных ошибок».
- В штатном режиме работы монитор SplDer Gate совместим со всеми пользовательскими приложениями, использующими сеть, включая веб-браузеры и почтовые клиенты. Для корректной проверки защищенных соединений необходимо добавить сертификат Dr.Web Desktop Security Suite (для Linux) к перечню доверенных сертификатов тех приложений, которые используют защищенные соединения (например, веб-браузеров и почтовых клиентов).
- После внесения изменений в работу монитора SplDer Gate (включение ранее отключенного монитора, изменение режима проверки защищенных соединений) необходимо *перезапускать почтовые клиенты*, использующие протокол IMAP для получения сообщений электронной почты с почтового сервера.

Совместимость с подсистемами безопасности

При настройках по умолчанию Dr.Web Desktop Security Suite (для Linux) не совместим с подсистемой улучшения безопасности **SELinux**. Кроме того, по умолчанию Dr.Web Desktop Security Suite (для Linux) работает в режиме ограниченной функциональности в системах **GNU/Linux**, использующих мандатные модели доступа (например, в системах, оснащенных подсистемой мандатного доступа **PARSEC**, основанной на присвоении пользователям и файлам различных уровней привилегий, называемых мандатными уровнями).

В случае необходимости установки Dr.Web Desktop Security Suite (для Linux) в системы с **SELinux**, а также в системы, использующие мандатные модели доступа, необходимо выполнить дополнительные настройки подсистем безопасности для снятия ограничений в функционировании Dr.Web Desktop Security Suite (для Linux). Подробнее см. в разделе Настройка систем безопасности.

Лицензирование

Права пользователя на использование копии Dr.Web Desktop Security Suite (для Linux) подтверждаются и регулируются лицензией, приобретенной пользователем у компании «Доктор Веб» или ее партнеров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением (см. https://license.drweb.com/agreement/), условия которого принимаются пользователем при установке программного продукта на свой компьютер. В лицензии фиксируется информация о пользователе и продавце, а также параметры использования приобретенной копии продукта, в частности:

- Перечень компонентов, которые разрешено использовать данному пользователю.
- Период, в течение которого разрешено использование Dr.Web Desktop Security Suite (для Linux).
- Другие ограничения (в частности, количество компьютеров, на которых разрешено использовать приобретенную копию Dr.Web Desktop Security Suite (для Linux)).

С целью ознакомления с продуктом имеется возможность активировать *демонстрационный период*. Если условия активации демонстрационного периода не нарушены, пользователь получает право на полноценное использование установленной копии Dr.Web Desktop Security Suite (для Linux) в течение всего этого периода.

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а на локальном компьютере пользователя с лицензией связывается специальный файл, регулирующий работу компонентов Dr.Web Desktop Security Suite (для Linux) в соответствии с параметрами лицензии. Он называется *лицензионным* ключевым файлом. При активации демонстрационного периода также автоматически формируется специальный ключевой файл, называемый *демонстрационным*.

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода (в том числе, если срок действия ранее приобретенной лицензии или демонстрационного периода истек), антивирусные функции компонентов Dr.Web Desktop Security Suite (для Linux) блокируются. Кроме того, недоступен сервис получения обновлений вирусных баз Dr.Web с серверов обновлений компании «Доктор Веб». Однако имеется возможность активировать Dr.Web Desktop Security Suite (для Linux), подключив его к серверу централизованной защиты антивирусной сети предприятия или антивирусной сети, организованной Интернет-провайдером. В этом случае управление антивирусными функциями и обновлениями копии продукта, установленной на компьютере, возлагается на сервер централизованной защиты.

Приобретение и регистрация лицензий

При приобретении лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов обновлений компании «Доктор Веб», а также получать стандартную техническую поддержку компании «Доктор Веб» и ее партнеров.

Приобрести любой антивирусный продукт Dr.Web или серийный номер для него вы можете у наших партнеров (см. список партнеров по адресу https://partners.drweb.com/) или через Интернет-магазин https://estore.drweb.com/. Дополнительную информацию о сроках и типах лицензирования можно найти на официальном сайте компании «Доктор Веб» https://www.drweb.com/.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем Dr.Web Desktop Security Suite (для Linux) и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки. Приобретенная лицензия может быть активирована любым из указанных ниже способов:

- При помощи мастера регистрации, входящего в состав Менеджера лицензий.
- Непосредственно на сайте компании «Доктор Веб» по адресу https://products.drweb.com/register/.

При активации или продлении лицензии необходимо указать серийный номер. Этот номер может поставляться вместе с продуктом или по электронной почте, при покупке или продлении лицензии онлайн.

В случае продления лицензии требуется также указать серийный номер или лицензионный ключевой файл предыдущей лицензии, в противном случае срок действия новой лицензии будет сокращен на 150 дней.

Если имеется комплект лицензий, выданных для использования Dr.Web Desktop Security Suite (для Linux) на нескольких компьютерах, то при регистрации имеется возможность указать, что Dr.Web Desktop Security Suite (для Linux) будет использоваться только на одном компьютере. В этом случае все лицензии из комплекта будут объединены в одну, и срок ее действия будет автоматически увеличен.

Запрос демонстрационного периода

Пользователям продуктов Dr.Web доступно два типа демонстрационного периода:

- Сроком на 3 месяца.
- Сроком на 1 месяц.

Чтобы получить демонстрационный период сроком на 3 месяца, необходимо пройти процедуру регистрации на официальном сайте компании «Доктор Веб» и указать свои персональные данные. В этом случае вы получите по электронной почте серийный номер для активации вашей копии Dr.Web Desktop Security Suite (для Linux). Демонстрационный период сроком на 1 месяц можно получить непосредственно в окне мастера регистрации Менеджера лицензий, не указывая персональных данных.

Окно мастера регистрации Менеджера лицензий появляется на экране при первом запуске Dr.Web Desktop Security Suite (для Linux) (как правило, он автоматически запускается сразу после окончания установки). Также вы можете в любой момент запустить процесс регистрации или запроса демонстрационного периода из окна Менеджера лицензий, нажав кнопку **Получить новую лицензию** на странице просмотра информации о текущей лицензии.

Для активации при помощи серийного номера, а также для запроса демонстрационного периода требуется подключение к сети Интернет.

Демонстрационный период использования Dr.Web Desktop Security Suite (для Linux) может быть выдан повторно для того же компьютера только по истечении определенного периода времени.

В случае активации лицензии или демонстрационного периода при помощи Менеджера лицензий, ключевой файл (лицензионный или демонстрационный) будет сформирован на локальном компьютере и установлен в надлежащее место автоматически. При получении ключевого файла по электронной почте в результате регистрации на сайте, вам необходимо выполнить его установку вручную.

При отсутствии возможности воспользоваться мастером регистрации (например, из-за отсутствия графической оболочки ОС), вы можете воспользоваться командой управления лицензией утилиты командной строки **drweb-ctl**, которая позволяет автоматически получить демонстрационный ключевой файл или лицензионный ключевой файл для серийного номера зарегистрированной лицензии (в том числе – и для серийного номера демонстрационного периода, полученного на адрес электронной почты). Описание утилиты **drweb-ctl** приведено в Руководстве Пользователя.

Полная версия Руководства пользователя Dr.Web Desktop Security Suite (для Linux) доступна:

- На сайте компании «Доктор Веб» по адресу https://download.drweb.com/doc/ (требуется подключение к сети Интернет).
- В виде документа PDF в каталоге `/opt/drweb.com/share/doc` (суффикс в имени файла указывает на язык руководства).

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты лицензионного ключевого файла при наличии активной лицензии. При повторной регистрации необходимо указать те же персональные данные, которые вы ввели при первой регистрации лицензии. Допускается использовать другой адрес электронной почты – в таком случае лицензионный ключевой файл будет выслан по новому адресу.

Количество запросов на получение лицензионного ключевого файла ограничено – регистрация лицензии с одним и тем же серийным номером допускается *не более 25 раз*. Если это число превышено, лицензионный 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 лицензии). Лицензионный ключевой файл будет выслан службой технической поддержки по электронной почте.

Ключевой файл

Ключевой файл – это специальный файл, который хранится на локальном компьютере и соответствует приобретенной лицензии или активированному демонстрационному периоду для программного продукта Dr.Web Desktop Security Suite (для Linux). В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.

Ключевой файл имеет расширение `.key` и является действительным при одновременном выполнении следующих условий:

- Срок действия лицензии или демонстрационного периода, которым он соответствует, не истек.
- Разрешение, определяемое лицензией или активным демонстрационным периодом, распространяется на все используемые модули.
- Целостность файла не нарушена.

При нарушении любого из этих условий ключевой файл становится недействительным.

При работе Dr.Web Desktop Security Suite (для Linux) ключевой файл по умолчанию должен находиться в каталоге `/etc/opt/drweb.com` и называться `drweb32.key`.

Компоненты Dr.Web Desktop Security Suite (для Linux) регулярно проверяют наличие и корректность ключевого файла. Его содержимое защищено от редактирования при помощи механизма электронной цифровой подписи, поэтому редактирование делает ключевой файл недействительным. Не рекомендуется открывать ключевой файл в текстовых редакторах во избежание случайной порчи его содержимого.

При отсутствии действительного ключевого файла (лицензионного или демонстрационного), а также по истечении срока его действия, антивирусные функции всех компонентов блокируются до установки действующего ключевого файла.

Рекомендуется сохранять имеющийся лицензионный ключевой файл до истечения срока его действия. В этом случае при переустановке продукта или переносе его на другой компьютер повторная регистрация серийного номера лицензии не потребуется, и вы сможете использовать лицензионный ключевой файл, полученный при первом прохождении процедуры регистрации.

По электронной почте ключевые файлы Dr.Web обычно передаются запакованными в zip-архивы. Архив, содержащий ключевой файл для активации продукта, обычно имеет имя `agent.zip` (обратите внимание, что если в письме содержится *несколько* архивов, то нужно использовать именно архив `agent.zip`). В мастере регистрации можно указывать путь непосредственно к архиву, не выполняя его предварительной распаковки. Также перед установкой ключевого файла вы можете распаковать архив любым удобным для вас способом и извлечь из него ключевой файл, сохранив его в любой доступный каталог (например – в домашний каталог или на съемный носитель USB flash).

Установка ключевого файла

В случае если уже имеется ключевой файл, соответствующий действующей лицензии на этот продукт (например, он был получен от продавца по электронной почте после регистрации или Dr.Web Desktop Security Suite (для Linux) переносится на другой компьютер), имеется возможность активировать Dr.Web Desktop Security Suite (для Linux), просто указав путь к имеющемуся ключевому файлу. Это можно сделать следующим образом:

- В Менеджере лицензий, перейдя на первом шаге мастера регистрации по ссылке **Другие виды активации** и указав путь к имеющемуся ключевому файлу или содержащему его zip-архиву.
- Вручную, для этого:
  1. Распакуйте ключевой файл, если он был вами получен в архиве.

2. Скопируйте его в каталог `/etc/opt/drweb.com` и, при необходимости, переименуйте в `drweb32.key`.
3. Выполните команду:

   ```
   # drweb-ctl reload
   ```

   для применения внесенных изменений.

Вы можете также воспользоваться командой:

```
# drweb-ctl cfset Root.KeyPath <путь к ключевому файлу>
```

Обратите внимание, что в последнем случае ключевой файл не будет скопирован в каталог `/etc/opt/drweb.com`, а останется в своем исходном каталоге.

> ⚠ Если ключевой файл не скопирован в каталог `/etc/opt/drweb.com`, пользователь сам несет ответственность за его сохранность. Такой способ установки ключевого файла не рекомендуется из-за возможности его случайного удаления (например, если он был размещен в каталоге, подвергающемся автоматической очистке системой). Помните, что в случае утраты вы можете запросить ключевой файл повторно, но количество запросов на его получение ограничено.

Файл настроек подключения

Файл настроек подключения представляет собой специальный файл, хранящий внутри себя параметры подключения Dr.Web Desktop Security Suite (для Linux) к серверу централизованной защиты. Этот файл может быть предоставлен администратором антивирусной сети или Интернет-провайдером (если он обеспечивает поддержку услуги централизованной антивирусной защиты).

Вы можете использовать этот файл для активации Dr.Web Desktop Security Suite (для Linux) через подключение его к серверу централизованной защиты (в этом случае вы не сможете использовать Dr.Web Desktop Security Suite (для Linux) в автономном режиме, не приобретя дополнительно лицензию).

Активация через подключение к серверу централизованной защиты

В случае если провайдер или администратор сети предприятия предоставил файл настроек подключения к серверу централизованной защиты, вы можете активировать Dr.Web Desktop Security Suite (для Linux), просто указав путь к имеющемуся файлу настроек подключения. Это можно сделать следующим образом:

- В окне настроек программы на вкладке **Режим** установите флажок **Включить режим централизованной защиты**, выберите в появившемся окне пункт выпадающего списка

Загрузить из файла, укажите путь к имеющемуся файлу настроек подключения и нажмите **Подключить**.

Установка и удаление Dr.Web Desktop Security Suite (для Linux)

В этом разделе описываются процедуры установки и удаления программного комплекса Dr.Web Desktop Security Suite (для Linux) версии 11.0, а также процедура получения текущих обновлений и процедура перехода на новую версию, если на вашем компьютере уже установлен Dr.Web Desktop Security Suite (для Linux) предыдущей версии.

Кроме этого, в этом разделе описана процедура выборочной установки и удаления компонентов продукта (например, для устранения ошибок, возникших в процессе эксплуатации Dr.Web Desktop Security Suite (для Linux)) и настройка расширенных подсистем безопасности (таких, как **SELinux**), что может потребоваться при установке или в процессе эксплуатации продукта.

Для осуществления этих операций необходимы права суперпользователя (пользователя *root*). Для получения прав суперпользователя при установке и удалении продукта воспользуйтесь командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

Не гарантируется совместимость Dr.Web Desktop Security Suite (для Linux) с антивирусными программами других производителей. Так как установка двух антивирусов на один компьютер может привести к *ошибкам в работе операционной системы и потере важных данных*, перед установкой Dr.Web Desktop Security Suite (для Linux) *настоятельно рекомендуется* удалить с компьютера антивирусные программы других производителей.

Если на вашем компьютере *уже имеется* другой антивирусный продукт Dr.Web, установленный из универсального пакета (`.run`), и вы желаете установить еще один антивирусный продукт Dr.Web (например, у вас из универсального пакета установлен продукт Dr.Web для файловых серверов UNIX, и вы хотите в дополнение к нему установить продукт Dr.Web Desktop Security Suite (для Linux)), необходимо предварительно убедиться, что версия уже установленного продукта *совпадает* с версией того продукта, который вы планируете установить. Если версия продукта, который вы собираетесь установить, новее, чем версия продукта, который уже установлен на вашем компьютере, *перед началом* установки дополнительного продукта следует обновить уже установленный продукт до версии продукта, который вы хотите установить дополнительно.

Установка Dr.Web Desktop Security Suite (для Linux)

Вы можете установить Dr.Web Desktop Security Suite (для Linux) одним из двух способов:

1. Загрузив с сайта компании «Доктор Веб» установочный файл, содержащий универсальный пакет для UNIX-систем, снабженный программами установки в графическом режиме и режиме командной строки (при начале установки будет запущена одна из них, в зависимости от возможностей окружения).
2. Выполнив установку продукта в виде набора нативных пакетов (для этого потребуется подключиться к соответствующему репозиторию пакетов компании «Доктор Веб»).

После установки Dr.Web Desktop Security Suite (для Linux) любым из указанных в данном руководстве способов, в начале работы, вам потребуется активировать лицензию или установить ключевой файл. Кроме того, вы можете подключить Dr.Web Desktop Security Suite (для Linux) к серверу централизованной защиты. До тех пор пока вы этого не сделаете, *функции антивирусной защиты будут отключены*.

Если в системе запущен почтовый клиент (такой, как **Mozilla Thunderbird**), использующий для получения сообщений электронной почты протокол IMAP, его необходимо перезапустить после завершения установки антивируса для обеспечения проверки входящих писем.

Продукт, установленный любым из рассмотренных в этом разделе способов, вы можете впоследствии удалить или обновить при наличии исправлений для входящих в него компонентов или выходе новой версии продукта. При необходимости выполните также настройку подсистем безопасности **Linux** для корректной работы установленного продукта. При возникновении проблем с функционированием отдельных компонентов вы можете выполнить их выборочную установку и удаление, не удаляя установленный продукт целиком.

Установка универсального пакета

Программный комплекс Dr.Web Desktop Security Suite (для Linux) распространяется в виде инсталляционного файла с именем `drweb-<версия>-av-linux-<платформа>.run`, где *<платформа>* – строка, указывающая тип платформы, для которой предназначен продукт (`x86` для 32-битных платформ и `amd64` для 64-битных платформ). Например:

```
drweb-11.0.7-av-linux-amd64.run
```

Обратите внимание, что далее в данном разделе руководства имя установочного файла, соответствующее формату, указанному выше, указывается как *<имя_файла>*`.run`.

Чтобы установить компоненты программного комплекса Dr.Web Desktop Security Suite (для Linux):

1. Загрузите инсталляционный файл с официального сайта компании «Доктор Веб».
2. Сохраните его на жесткий диск компьютера в любой удобный и доступный каталог (например, `/home/<username>`, где *<username>* – имя текущего пользователя).
3. Перейдите в каталог с сохраненным файлом и разрешите его исполнение, например, командой:

   ```
   # chmod +x <имя_файла>.run
   ```

4. Запустите его на исполнение командой:

   ```
   # ./<имя_файла>.run
   ```

   или воспользуйтесь стандартным файловым менеджером вашей графической оболочки как для изменения свойств файла, так и для его запуска.

   

   В случае установки Dr.Web Desktop Security Suite (для Linux) в среде ОС **Astra Linux SE** версии 1.6, работающей в режиме *ЗПС*, может произойти отказ в запуске программы установки из-за отсутствия открытого ключа компании «Доктор Веб» в списке доверенных ключей. В этом случае необходимо выполнить предварительную настройку режима ЗПС (см. Настройка запуска в режиме ЗПС (Astra Linux SE, версия 1.6)), после чего запустить программу установки повторно.

   Сначала будет проверена целостность архива, затем файлы, содержащиеся в архиве, будут распакованы во временный каталог и автоматически запустится программа установки. Если запуск был осуществлен не с правами суперпользователя, то программа установки автоматически попытается повысить свои права, запросив пароль (используется **sudo**). Если попытка повышения прав окончится неудачей, установка будет завершена.

   

   Если в части файловой системы, содержащей временный каталог, не имеется достаточного количества свободного места для распаковки дистрибутива, процесс установки будет завершен после выдачи соответствующего сообщения. В этом случае следует повторить распаковку, изменив значение системной переменной окружения `TMPDIR` таким образом, чтобы она указывала на каталог, имеющий достаточное количество свободного места. Также вы можете воспользоваться ключом распаковки в указанный каталог `--target` (см. в разделе Выборочные установка и удаление компонентов).

   В зависимости от возможностей текущего окружения, в котором произведен запуск дистрибутива, запустится одна из программ установки, входящих в состав дистрибутива:

   - Программа установки для графического режима.
   - Программа установки для режима командной строки.

При этом программа установки для режима командной строки запустится автоматически, если невозможно запустить программу установки для графического режима.

5. Следуйте инструкциям программы установки.

Имеется возможность запустить программу установки в полностью автоматическом режиме, выполнив команду:

```
# ./<имя_файла>.run -- --non-interactive
```

В этом случае программа установки будет запущена в полностью автоматическом режиме, без показа интерфейса пользователя (включая диалоги программы установки для режима командной строки).

Обратите внимание, что:

- Использование этой опции означает, что вы *соглашаетесь* с условиями Лицензионного соглашения Dr.Web. Ознакомиться с текстом Лицензионного соглашения после установки продукта вы можете, прочитав файл `/opt/drweb.com/share/doc/LICENSE`. Расширение файла указывает язык, на котором написан текст Лицензионного соглашения. Файл `LICENSE` без расширения хранит текст Лицензионного соглашения Dr.Web на английском языке. В случае если вы *не согласны* с условиями Лицензионного соглашения, вам следует удалить продукт после установки.
- Запуск программы установки в полностью автоматическом режиме требует наличия прав суперпользователя. Для повышения прав вы можете использовать команды **su** и **sudo**.

Если ваш дистрибутив **Linux** оснащен подсистемой безопасности **SELinux**, то возможно возникновение ситуации, когда работа программы установки будет прервана подсистемой безопасности. В этом случае вам необходимо временно перевести **SELinux** в *разрешающий (Permissive)* режим, для чего выполните команду

```
# setenforce 0
```

После этого перезапустите программу установки. Также в этом случае по окончании процесса установки необходимо выполнить настройку политик безопасности **SELinux** для того, чтобы в дальнейшем антивирусные компоненты работали корректно.

Все установочные файлы, извлеченные из архива, будут автоматически удалены по окончании установки.

Рекомендуется сохранить загруженный файл *<имя_файла>*`.run`, из которого производилась установка, для нужд возможной переустановки продукта или его компонентов в последующем, без обновления версии продукта.

После завершения установки, в графической оболочке рабочего стола, в меню **Приложения**, появится группа **Dr.Web**, содержащая два пункта:

- **Dr.Web Desktop Security Suite (для Linux)** для запуска Dr.Web Desktop Security Suite (для Linux) в графическом режиме.
- **Удалить компоненты Dr.Web** для его удаления.

Значок индикатора состояния программы появится в области уведомления рабочего стола автоматически после повторного входа пользователя в систему.

> Для корректной работы Dr.Web Desktop Security Suite (для Linux) дополнительно может потребоваться установить пакеты, перечисленные в разделе Системные требования (например, библиотеку поддержки исполнения 32-битных приложений для 64-битной платформы, а также библиотеку **libappindicator1** для корректного отображения индикатора состояния программы в области уведомлений рабочего стола).

Установка в графическом режиме

Если программа установки в начале своей работы обнаружит наличие на компьютере ряда проблем, которые могут в дальнейшем привести к полной или частичной неработоспособности Dr.Web Desktop Security Suite (для Linux), на экране появится соответствующее окно с перечислением обнаруженных проблем. Вы можете прервать установку, нажав кнопку **Выход**, чтобы устранить выявленные проблемы до начала установки. В этом случае, после решения выявленных проблем (установки требуемых дополнительных библиотек, временного отключения **SELinux** и т.д.), программу установки потребуется запустить повторно. Если вы не хотите прерывать установку Dr.Web Desktop Security Suite (для Linux), нажмите кнопку **Продолжить**. В этом случае программа установки продолжит свою работу и покажет окно мастера установки. Однако вам потребуется устранить выявленные проблемы позднее, по окончании процесса установки, или при обнаружении ошибок в работе Dr.Web Desktop Security Suite (для Linux).

После запуска программы установки, работающей в графическом режиме, на экране появится окно мастера установки.

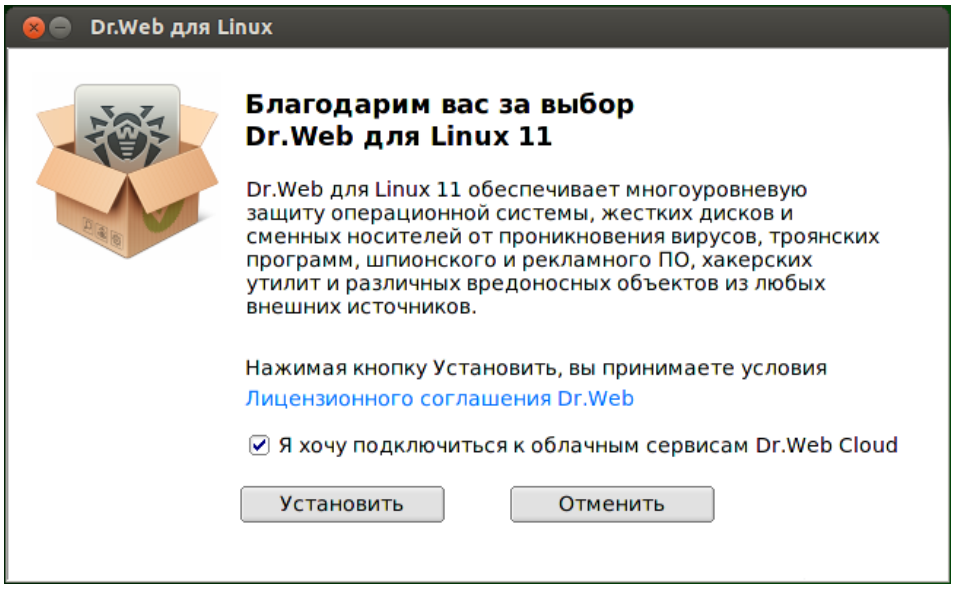

Рисунок 2. Страница приветствия мастера установки

Для установки Dr.Web Desktop Security Suite (для Linux) на свой компьютер необходимо последовательно выполнить следующие действия:

1. Ознакомьтесь с условиями Лицензионного соглашения компании «Доктор Веб». Для этого перейдите по соответствующей ссылке на стартовой странице мастера установки. После этого откроется страница, позволяющая ознакомиться с текстом Лицензионного соглашения и сведениями об авторских правах на компоненты, которые будут установлены на ваш компьютер.

   При необходимости, если в вашей системе установлен и настроен принтер, вы можете распечатать текст Лицензионного соглашения и сведения об авторских правах. Для этого откройте нужную вкладку на странице и нажмите **Печать**.

   Чтобы закрыть страницу ознакомления с Лицензионным соглашением и авторскими правами нажмите **ОК**.
2. Перед началом установки вы можете согласиться с тем, что после установки Dr.Web Desktop Security Suite (для Linux) автоматически подключится к облачному сервису Dr.Web Cloud. Для этого установите соответствующий флажок (по умолчанию он установлен в момент запуска мастера установки). Если вы не хотите разрешать Dr.Web Desktop Security Suite (для Linux) использовать облачный сервис Dr.Web Cloud, снимите отметку флажка. В случае необходимости, вы в любой момент сможете разрешить или запретить Dr.Web Desktop Security Suite (для Linux) использовать сервис Dr.Web Cloud в настройках программы.
3. Для начала установки нажмите кнопку **Установить**. Тем самым вы одновременно подтверждаете, что принимаете условия Лицензионного соглашения компании «Доктор Веб». Если вы решили отказаться от установки Dr.Web Desktop Security Suite (для Linux) на свой компьютер, нажмите кнопку **Отменить** для отказа от установки и завершения работы мастера установки.

4. После начала установки откроется страница мастера, содержащая индикатор, показывающий прогресс процесса установки. Если вы хотите ознакомиться с записями, попадающими в журнал установки в процессе установки, нажмите кнопку **Подробнее**.
5. После успешного окончания процесса копирования файлов программы и внесения необходимых изменений в системные настройки, откроется финальная страница мастера, отображающая результат установки.
6. Чтобы закрыть окно мастера установки, нажмите **OK**. Если данная операция поддерживается возможностями окружения, на финальном шаге появится страница с предложением запустить Dr.Web Desktop Security Suite (для Linux) в графическом режиме. Для запуска установите флажок **Запустить Dr.Web Desktop Security Suite (для Linux) сейчас** и нажмите **OK**.

Если установка была прервана из-за ошибки, финальная страница мастера будет содержать соответствующее сообщение. В этом случае закройте мастер установки, нажав **OK**. После этого устраните проблемы, вызвавшие ошибку установки, и повторите установку заново.

Установка в режиме командной строки

После запуска программы установки, работающей с режиме командной строки, на экране появится текст приглашения к установке.

1. Для начала установки ответьте *Yes* или *Y* на запрос «Вы хотите продолжить?». Чтобы отказаться от установки, введите *No* или *N*. В этом случае работа программы установки будет завершена.
2. Далее вам необходимо ознакомиться с текстом Лицензионного соглашения компании «Доктор Веб», который будет выведен на экран. Для перелистывания текста лицензионного соглашения пользуйтесь клавишами ENTER (перелистывание текста на одну строчку вниз) и ПРОБЕЛ (перелистывание текста вниз на экран). Обратите внимание, что перелистывание текста Лицензионного соглашения назад (вверх) не предусмотрено.
3. После прочтения Лицензионного соглашения вам будет предложено принять его условия. Введите *Yes* или *Y*, если вы принимаете условия, и *No* или *N*, если вы не согласны с условиями Лицензионного соглашения. В случае отказа от принятия условий Лицензионного соглашения работа программы установки будет автоматически завершена.
4. После принятия условий Лицензионного соглашения автоматически будет запущен процесс установки на компьютер компонентов Dr.Web Desktop Security Suite (для Linux). При этом на экран будет выводиться информация о ходе установки (журнал установки), включающая в себя перечень устанавливаемых компонентов.
5. По окончании процесса установки программа установки автоматически завершит свою работу. В случае возникновения ошибки на экран будет выведено соответствующее сообщение с описанием ошибки, после чего работа программы установки также будет завершена.

6. Для начала работы с установленным Dr.Web Desktop Security Suite (для Linux) воспользуйтесь любым удобным для вас способом запуска.

Если установка была прервана из-за ошибки, следует устранить проблемы, вызвавшие ошибку установки, и повторить процесс установки заново.

Установка из репозитория

Нативные пакеты продукта Dr.Web Desktop Security Suite (для Linux) находятся в официальном репозитории Dr.Web https://repo.drweb.com. После добавления репозитория Dr.Web в список репозиториев, используемых менеджером пакетов вашей операционной системы, вы сможете устанавливать его в виде нативных пакетов для операционной системы так же, как и любые другие программы из репозиториев вашей операционной системы. Необходимые зависимости будут разрешаться автоматически. Кроме того, в этом случае поддерживается процедура обнаружения пакетным менеджером ОС обновлений всех компонентов Dr.Web, установленных из подключенного репозитория и предложение установки всех обнаруженных обновлений.

Для доступа к репозиторию Dr.Web требуется подключение к сети Интернет.

Все нижеприведенные команды для подключения репозиториев, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами суперпользователя (пользователя *root*). Для получения соответствующих прав используйте команду смены пользователя **su** или команду выполнения от имени другого пользователя **sudo**.

Debian, Mint, Ubuntu (apt)

В связи с тем, что антивирусное ядро Dr.Web Desktop Security Suite (для Linux) использует 32-битную архитектуру *x86*, в 64-битных системах **Debian**, **Mint**, **Ubuntu** (для платформы *x86-64*, *x64*, *amd64*) может потребоваться разрешить установку пакетов для платформы *x86*, выполнив команду:

```
# dpkg --add-architecture i386
```

1. Репозиторий для этих ОС защищен цифровой подписью «Доктор Веб». Для доступа к репозиторию импортируйте и добавьте в хранилище пакетного менеджера ключ цифровой подписи, выполнив команду:

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 10100609
```

2. Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.list`:

```
deb https://repo.drweb.com/drweb/debian 11.0 non-free
```

Вы можете выполнить пункты 1 и 2, загрузив из репозитория и установив специальный DEB-пакет.
Ссылка на загрузку пакета: https://repo.drweb.com/drweb-repo11.deb.

3. Для установки Dr.Web Desktop Security Suite (для Linux) из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-workstations
```

Установка также может осуществляться с помощью альтернативных менеджеров (например **Synaptic** или **aptitude**). Кроме того, альтернативные менеджеры, такие как **aptitude**, рекомендуется использовать для разрешения конфликта пакетов, если он возникнет.

ALT Linux, PCLinuxOS (apt-rpm)

1. Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.list`:

```
rpm https://repo.drweb.com/drweb/altlinux 11.0/<arch> drweb
```

где <*arch*> – обозначение используемой архитектуры пакетов:

- Для **32-разрядной** версии: `i386`
- Для **64-разрядной** версии: `x86_64`

2. Для установки Dr.Web Desktop Security Suite (для Linux) из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-workstations
```

Установка также может осуществляться с помощью альтернативных менеджеров (например **Synaptic** или **aptitude**).

Mageia, OpenMandriva Lx (urpmi)

1. Подключите репозиторий с помощью команды:

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/mandriva/11.0/<arch>/
```

где <*arch*> – обозначение используемой архитектуры пакетов:

- Для **32-разрядной** версии: `i386`
- Для **64-разрядной** версии: `x86_64`

2. Для установки Dr.Web Desktop Security Suite (для Linux) из репозитория выполните команду:

```
# urpmi drweb-workstations
```

Установка также может осуществляться с помощью альтернативных менеджеров (например **rpmdrake**).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

1. Добавьте файл `drweb.repo` со следующим содержимым в каталог `/etc/yum.repos.d`:

```
[drweb]
name=DrWeb - 11.0
baseurl=https://repo.drweb.com/drweb/el5/11.0/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Если планируется записать вышеуказанное содержимое в файл при помощи команды типа **echo** с перенаправлением вывода, символ `$` следует экранировать: `\$`.

Вы можете выполнить пункт 1, загрузив из репозитория и установив специальный RPM-пакет.
Ссылка на загрузку пакета: https://repo.drweb.com/drweb-repo11.rpm.

2. Для установки Dr.Web Desktop Security Suite (для Linux) из репозитория выполните команду:

```
# yum install drweb-workstations
```

В ОС **Fedora**, начиная с версии 22, рекомендуется вместо менеджера **yum** использовать менеджер **dnf**, например:

```
# dnf install drweb-workstations
```

Установка также может осуществляться с помощью альтернативных менеджеров (например **PackageKit** или **Yumex**).

SUSE Linux (zypper)

1. Чтобы подключить репозиторий, запустите следующую команду:

```
# zypper ar -t YUM 'https://repo.drweb.com/drweb/el5/11.0/$basearch/' drweb
```

2. Для установки Dr.Web Desktop Security Suite (для Linux) из репозитория выполните команды:

```
# zypper refresh
# zypper install drweb-workstations
```

Установка также может осуществляться с помощью альтернативных менеджеров (например **YaST**).

Обновление Dr.Web Desktop Security Suite (для Linux)

Предусмотрено два режима обновления продукта Dr.Web Desktop Security Suite (для Linux):

1. Получение обновлений пакетов и компонентов, выпущенных в рамках эксплуатации текущей версии продукта (как правило, такие обновления содержат исправления ошибок и мелкие улучшения в функционировании компонентов);
2. Переход на новую версию продукта. Этот способ обновления используется, если компания «Доктор Веб» выпустила новую версию используемого вами продукта, отличающуюся новыми возможностями.

Получение текущих обновлений

После установки продукта любым из способов, описанных в соответствующем разделе, происходит автоматическое подключение менеджера пакетов к репозиторию пакетов Dr.Web:

- Если установка производилась из универсального пакета (файл `.run`), а в системе используются пакеты в формате DEB (например, ОС **Debian**, **Mint**, **Ubuntu**), для работы с пакетами Dr.Web используется отдельная версия менеджера пакетов **zypper**, автоматически установленная в рамках установки продукта.

  Чтобы получить и установить обновленные пакеты Dr.Web этим менеджером, перейдите в каталог <*opt_dir*>`/bin` (для **GNU/Linux** – `/opt/drweb.com/bin`), и выполните следующие команды:

  ```
  # ./zypper refresh
  # ./zypper update
  ```

- Во всех остальных случаях используйте команды обновления пакетного менеджера, используемого в вашей ОС, например:
  - В **Red Hat Enterprise Linux** и **CentOS** используйте команду **yum**
  - В **Fedora** используйте команду **yum** или **dnf**
  - В **SUSE Linux** используйте команду **zypper**
  - В **Mageia**, **OpenMandriva Lx** используйте команду **urpmi**
  - В **Alt Linux**, **PCLinuxOS**, **Debian**, **Mint**, **Ubuntu** используйте команду **apt-get**.

Также вы можете использовать и альтернативные менеджеры пакетов, разработанные для вашей операционной системы. При необходимости обратитесь к справочному руководству по используемому вами менеджеру пакетов.

В случае выпуска новой версии продукта, пакеты, содержащие его компоненты, помещаются в раздел репозитория Dr.Web, соответствующий новой версии продукта. В

этом случае для обновления необходимо переключить менеджер пакетов на новый раздел репозитория Dr.Web (см. Переход на новую версию).

Переход на новую версию

Предварительные замечания

Поддерживается процедура обновления предыдущих версий продукта до версии 11.0. Переход на новую версию Dr.Web Desktop Security Suite (для Linux) следует выполнять тем же способом, каким был установлена версия Dr.Web Desktop Security Suite (для Linux), подлежащая обновлению:

- Если версия продукта, подлежащая обновлению, была установлена из репозитория, то переход на новую версию следует выполнять обновлением из репозитория.
- Если версия продукта, подлежащая обновлению, была установлена из универсального пакета, то переход на новую версию следует производить установкой универсального пакета, содержащего новую версию продукта.

Чтобы уточнить способ, которым была установлена версия продукта, подлежащая обновлению, проверьте присутствие в каталоге исполняемых файлов Dr.Web Desktop Security Suite (для Linux) сценария программы удаления `remove.sh`. Если этот файл присутствует, текущая версия продукта была установлена из универсального пакета, а в противном случае – из репозитория.

В случае если вы не имеете возможности обновить продукт тем же способом, каким он был установлен изначально, вам следует предварительно удалить текущую версию продукта, а потом выполнить установку новой версии продукта доступным для вас способом. Способы установки и удаления предыдущих версий продукта Dr.Web Desktop Security Suite (для Linux) аналогичны способам установки и удаления, рассмотренным в данном руководстве для версии 11.0. Для дополнительной информации обратитесь к Руководству пользователя установленной у вас версии Dr.Web Desktop Security Suite (для Linux).

Обратите внимание, что переход с Dr.Web Desktop Security Suite (для Linux) версии 6.0.2 и меньше на версию 11.0 возможен *только* путем предварительного удаления старой версии продукта с последующей установкой продукта версии 11.0.

Если версия продукта, подлежащая обновлению, работает под управлением сервера централизованной защиты, то перед началом обновления рекомендуется сохранить адрес сервера централизованной защиты, к которому подключен продукт. Например, для получения адреса сервера централизованной защиты, к которому подключен Dr.Web Desktop Security Suite (для Linux) с версией новее 6.0.2, вы можете воспользоваться командой:

```
$ drweb-ctl appinfo
```

из присутствующей в выводе команды строчки вида

```
ESAgent; <PID>; RUNNING 1; Connected <адрес>, on-line
```

сохраните часть *<адрес>* (может выглядеть как строка вида `tcp://<IP-адрес>:<порт>`, например: `tcp://10.20.30.40:1234`). Кроме того, рекомендуется сохранить файл публичного ключа сервера.

В случае возникновения затруднений с получением параметров текущего подключения обратитесь к Руководству администратора по установленной версии продукта, а также к администратору вашей антивирусной сети.

Обновление с версии 9.0 и новее

Обновление установкой универсального пакета

Выполните установку Dr.Web Desktop Security Suite (для Linux) версии 11.0 из универсального пакета. В процессе установки, в случае если это необходимо, вам будет предложено автоматически удалить имеющиеся компоненты старой версии продукта.

Обновление из репозитория

Для обновления текущей версии Dr.Web Desktop Security Suite (для Linux), установленной из репозитория компании «Доктор Веб», в зависимости от типа используемых пакетов, вам необходимо выполнить следующие действия:

- **В случае использования пакетов RPM (yum)**:
  1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 11.0).

> Имя репозитория, хранящего пакеты версии 11.0, см. в разделе Установка из репозитория. Для уточнения способа смены репозиториев обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

2. Установите новую версию продукта из репозитория, выполнив команду:

```
# yum update
```

или, если используется менеджер **dnf** (как, например, в ОС **Fedora** версии 22 и старше):

```
# dnf update
```

Если в процессе обновления пакетов возникнет ошибка, то выполните удаление и последующую установку продукта. При необходимости см. разделы Удаление продукта, установленного из репозитория и Установка из репозитория (пункты, соответствующие используемой вами ОС и менеджеру пакетов).

- **В случае использования пакетов DEB (apt-get)**:
  1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 11.0).
  2. Обновите пакеты продукта, выполнив команды:

```
# apt-get update
# apt-get dist-upgrade
```

Обратите внимание, что в ОС **Ubuntu** 14.04 (64-битная версия) применение команды **apt-get** `dist-upgrade` для обновления дистрибутива может завершиться неудачей. В этом случае используйте менеджер пакетов **aptitude** (для обновления дистрибутива используйте команду **aptitude** `dist-upgrade`).

Перенос ключевого файла

При любом способе обновления Dr.Web Desktop Security Suite (для Linux), имеющийся у вас лицензионный ключевой файл будет автоматически установлен в надлежащее место для использования новой версией продукта.

В случае возникновения проблем с автоматической установкой лицензионного ключевого файла, вы можете выполнить его установку вручную. Dr.Web Desktop Security Suite (для Linux), начиная с версии 9.0, хранит ключевой файл в каталоге `/etc/opt/drweb.com`. В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки компании «Доктор Веб».

Повторное подключение к серверу централизованной защиты

Если это возможно, то после обновления (если обновляемый продукт был подключен к серверу централизованной защиты) подключение будет восстановлено автоматически. В случае если подключение не восстановилось автоматически, для подключения обновленной версии Dr.Web Desktop Security Suite (для Linux) к антивирусной сети воспользуйтесь любым из следующих способами (обратите внимание, что вам придется указать предварительно сохраненные адрес и файл публичного ключа сервера):

- Установите флажок на вкладке **Режим** окна настроек Dr.Web Desktop Security Suite (для Linux).
- Используйте команду

```
$ drweb-ctl esconnect <адрес> --Key <путь к файлу публичного ключа сервера>
```

В случае возникновения затруднений с подключением обратитесь к администратору вашей антивирусной сети.

Особенности процесса обновления

- При обновлении продукта из репозитория при работающем Dr.Web Desktop Security Suite (для Linux) обновляемой версии, после завершения установки пакетов новой версии Dr.Web Desktop Security Suite (для Linux), процессы старой версии Dr.Web Desktop Security Suite (для Linux) останутся запущенными до выхода пользователя из системы, в том числе – в области уведомлений рабочего стола (если вы работаете в графическом режиме) может быть доступен значок индикатора старой версии продукта.
- При обновлении Dr.Web Desktop Security Suite (для Linux) настройки SpIDer Gate могут быть сброшены в значения по умолчанию.
- Если в системе запущен почтовый клиент (такой, как **Mozilla Thunderbird**), использующий для получения сообщений электронной почты протокол IMAP, его необходимо перезапустить после завершения обновления для обеспечения проверки входящих писем.

Обновление с версии 6.0.2 и более ранней

Переход с Dr.Web Desktop Security Suite (для Linux) версии 6.0.2 и более ранней на версию 11.0 возможен только путем предварительного удаления старой версии продукта с последующей установкой продукта версии 11.0. Для получения дополнительной информации о способах удаления старой версии продукта обратитесь к Руководству пользователя установленной у вас версии Dr.Web Desktop Security Suite (для Linux).

Перенос ключевого файла

Имеющийся у вас лицензионный ключевой файл старой версии продукта не будет автоматически установлен для использования новой версией, но вы можете выполнить его установку вручную. Dr.Web Desktop Security Suite (для Linux) версии 6.0.2 и ранее хранит ключевой файл в каталоге `/home/<user>/.drweb` (каталог имеет атрибут «скрытый»). В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки компании «Доктор Веб».

Dr.Web Desktop Security Suite (для Linux) версии 11.0 не поддерживает карантин Dr.Web Desktop Security Suite (для Linux) версий, предшествующих версии 9.0. При наличии в карантине этой версии продукта изолированных файлов, вы можете извлечь их оттуда или окончательно удалить вручную. Dr.Web Desktop Security Suite (для Linux) версии 6.0.2 (и ранее) использует в качестве карантина следующие каталоги:

- `/var/drweb/infected` – системный карантин;
- `/home/<user>/.drweb/quarantine` – карантин пользователя (где *<user>* – имя пользователя).

Для упрощения обработки карантина рекомендуется произвести ревизию его содержимого непосредственно из ранней версии Dr.Web Desktop Security Suite (для Linux) перед началом перехода на новую версию.

Удаление Dr.Web Desktop Security Suite (для Linux)

В зависимости от способа установки, вы можете удалить Dr.Web Desktop Security Suite (для Linux) одним из двух способов:

1. Запустив программу удаления универсального пакета (для графического режима или режима командной строки, в зависимости от возможностей окружения).
2. Удалив пакеты продукта, установленные из репозитория компании «Доктор Веб», используя системный менеджер пакетов.

Удаление универсального пакета

Удаление продукта Dr.Web Desktop Security Suite (для Linux), установленного из универсального пакета, можно выполнить как через меню приложений окружения графического рабочего стола, так и при помощи командной строки.

Обратите внимание, что программа удаления удалит не только Dr.Web Desktop Security Suite (для Linux), но и *все другие* продукты Dr.Web, установленные на вашем компьютере.

Если на вашем компьютере, кроме Dr.Web Desktop Security Suite (для Linux), установлены и другие продукты Dr.Web, для удаления только Dr.Web Desktop Security Suite (для Linux) вместо запуска программы автоматического удаления воспользуйтесь процедурой выборочной установки и удаления компонентов.

Удаление продукта через меню приложений

Для этого выберите в меню приложений группу **Dr.Web**, в которой выберите пункт меню **Удалить компоненты Dr.Web**. Далее будет запущена программа удаления для графического режима.

Удаление продукта из командной строки

Запуск программы удаления осуществляется сценарием `remove.sh`, расположенным в каталоге `/opt/drweb.com/bin`. Таким образом, чтобы запустить удаление продукта, необходимо выполнить следующую команду:

```
# /opt/drweb.com/bin/remove.sh
```

Далее запустится программа удаления (использующая графический режим или режим командной строки, в зависимости от возможностей текущего окружения).

Чтобы непосредственно запустить программу удаления для режима командной строки, используйте следующую команду:

```
# /opt/drweb.com/bin/uninst.sh
```

Процедура удаления Dr.Web Desktop Security Suite (для Linux) рассмотрена в соответствующих разделах:

- Удаление в графическом режиме.
- Удаление в режиме командной строки.

Имеется возможность запустить программу удаления в полностью автоматическом режиме, выполнив команду:

```
# /opt/drweb.com/bin/remove.sh --non-interactive
```

В этом случае программа удаления будет запущена в полностью автоматическом режиме, без показа интерфейса пользователя (включая диалоги программы удаления для режима командной строки). Обратите внимание, что запуск программы удаления в полностью автоматическом режиме требует наличия прав суперпользователя. Для повышения прав вы можете использовать команды **su** и **sudo**.

Удаление в графическом режиме

После запуска программы удаления для графического режима, на экране появится окно мастера удаления.

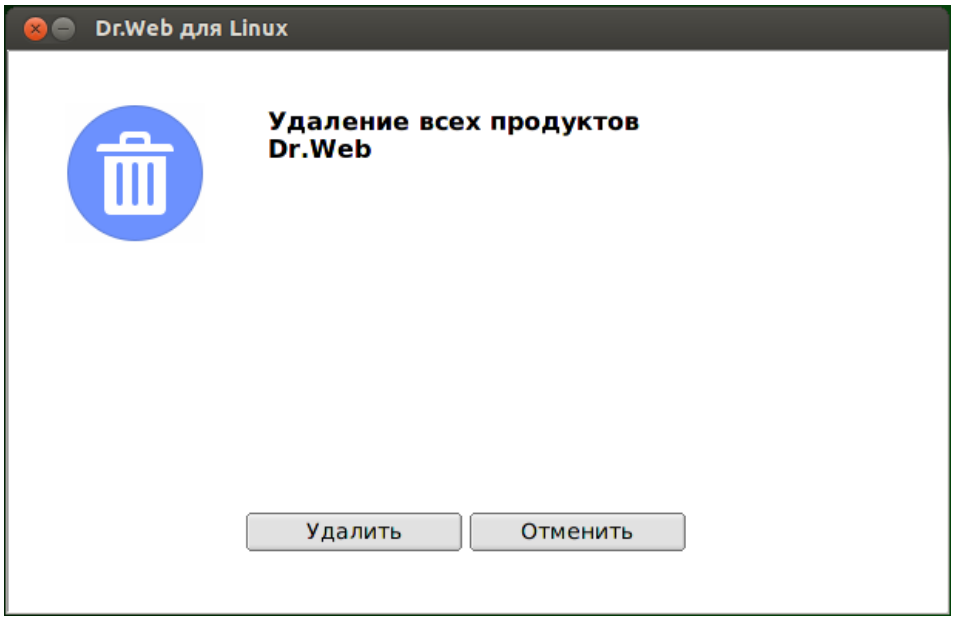

Рисунок 3. Страница приветствия мастера удаления

1. Для удаления Dr.Web Desktop Security Suite (для Linux) нажмите кнопку **Удалить**. Чтобы прекратить работу мастера удаления и отказаться от удаления Dr.Web Desktop Security Suite (для Linux), нажмите кнопку **Отменить**.
2. После начала процесса удаления откроется страница мастера, отражающая ход процесса удаления и содержащая соответствующий индикатор прогресса. Для просмотра сообщений журнала удаления нажмите кнопку **Подробнее**.
3. После успешного окончания процесса удаления файлов Dr.Web Desktop Security Suite (для Linux) и внесения необходимых изменений в системные настройки, откроется финальная страница мастера с сообщением об успешном удалении.
4. Для закрытия окна мастера удаления нажмите **ОК**.

Удаление в режиме командной строки

После запуска программы удаления, работающей в режиме командной строки, на экране появится текст приглашения к удалению.

1. Для начала удаления ответьте *Yes* или *Y* на запрос «Вы хотите продолжить?». Чтобы отказаться от удаления Dr.Web Desktop Security Suite (для Linux), введите *No* или *N*. В этом случае работа программы удаления будет завершена.

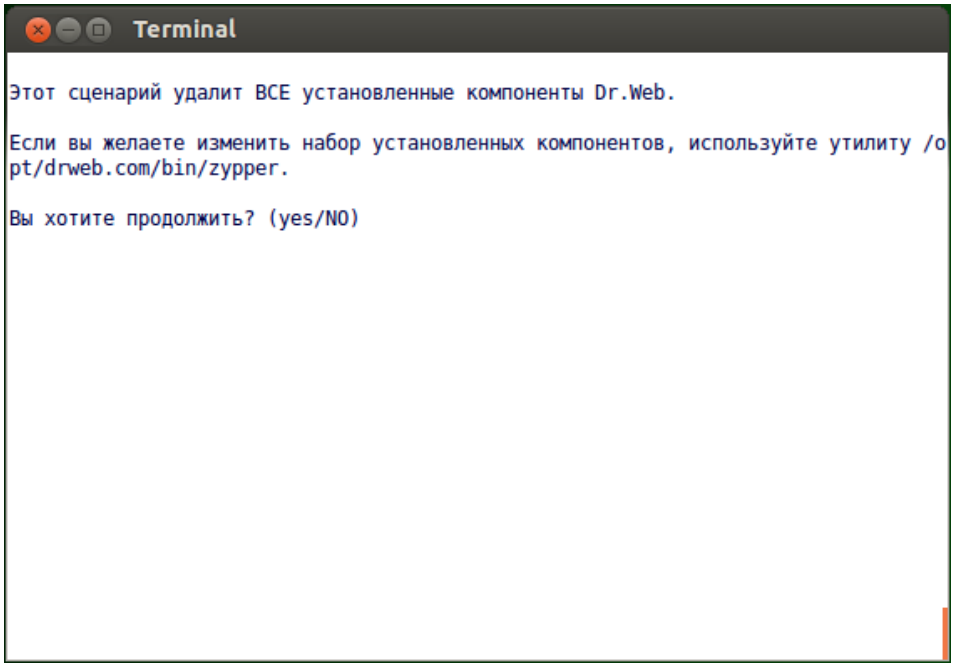

Рисунок 4. Приглашение к удалению

2. После запуска удаления отмеченных ранее пакетов на экран будут выдаваться записи, фиксируемые в журнал удаления и отражающие ход процесса удаления.
3. По окончании процесса программа удаления завершит свою работу автоматически.

Удаление продукта, установленного из репозитория

Все нижеприведенные команды для удаления пакетов должны быть выполнены с правами суперпользователя. Для этого используйте команду смены пользователя **su** или команду выполнения от имени другого пользователя **sudo**.

Debian, Mint, Ubuntu (apt)

Для удаления корневого метапакета продукта Dr.Web Desktop Security Suite (для Linux) выполните команду:

```
# apt-get remove drweb-workstations
```

Для удаления всех установленных пакетов Dr.Web выполните команду (в некоторых системах символ '*' требуется экранировать: '*'):

```
# apt-get remove drweb*
```

Для автоматического удаления из системы всех более не используемых пакетов можно дополнительно воспользоваться командой:

```
# apt-get autoremove
```

Обратите внимание на следующие особенности удаления с использованием **apt-get**:

1. Первая команда удалит только корневой метапакет `drweb-workstations`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Вторая команда удалит из системы все пакеты, название которых начинается на "`drweb`" (стандартное наименование для пакетов программных продуктов Dr.Web). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта Dr.Web Desktop Security Suite (для Linux).
3. Третья команда удалит из системы все пакеты, которые были автоматически установлены для удовлетворения зависимостей других пакетов, но более не требуемые (например, ввиду удаления исходного пакета). Обратите внимание, что эта команда удалит из системы все более не требуемые пакеты, а не только пакеты продукта Dr.Web Desktop Security Suite (для Linux).

Удаление пакетов продукта также может осуществляться с помощью альтернативных менеджеров (например, **Synaptic** или **aptitude**).

ALT Linux, PCLinuxOS (apt-rpm)

Удаление Dr.Web Desktop Security Suite (для Linux) в данном случае выполняется так же, как и в **Debian**, **Ubuntu** (см. выше).

Удаление пакетов продукта также может осуществляться с помощью альтернативных менеджеров (например, **Synaptic** или **aptitude**).

Mageia, OpenMandriva Lx (urpme)

Для удаления Dr.Web Desktop Security Suite (для Linux) выполните команду:

```
# urpme drweb-workstations
```

Для автоматического удаления из системы всех более не используемых пакетов можно дополнительно воспользоваться командой:

```
# urpme --auto-orphans drweb-workstations
```

Обратите внимание на следующие особенности удаления с использованием **urpme**:

1. Первая команда удалит только корневой метапакет `drweb-workstations`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Вторая команда удалит из системы корневой метапакет `drweb-workstations`, а также все пакеты, которые были автоматически установлены для удовлетворения зависимостей других пакетов, но более не требуемые (например, ввиду удаления исходного пакета). Обратите внимание, что эта команда удалит из системы все более не требуемые пакеты, а не только пакеты продукта Dr.Web Desktop Security Suite (для Linux).

Удаление пакетов продукта также может осуществляться с помощью альтернативных менеджеров (например, **rpmdrake**).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

Для удаления всех установленных пакетов Dr.Web выполните команду (в некоторых системах символ '`*`' требуется экранировать: '`\*`'):

```
# yum remove drweb*
```

В ОС **Fedora**, начиная с версии 22, рекомендуется вместо менеджера **yum** использовать менеджер **dnf**, например:

```
# dnf remove drweb*
```

Обратите внимание на следующие особенности удаления с использованием **yum** (**dnf**):

Указанная команда удалит из системы все пакеты, название которых начинается на "drweb" (стандартное наименование для пакетов программных продуктов Dr.Web). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта Dr.Web Desktop Security Suite (для Linux).

Удаление пакетов продукта также может осуществляться с помощью альтернативных менеджеров (например, **PackageKit** или **Yumex**).

SUSE Linux (zypper)

Для удаления Dr.Web Desktop Security Suite (для Linux) выполните команду:

```
# zypper remove drweb-workstations
```

Для удаления всех установленных пакетов Dr.Web выполните команду (в некоторых системах символ '*' требуется экранировать: '*'):

```
# zypper remove drweb*
```

Обратите внимание на следующие особенности удаления с использованием **zypper**:

1. Первая команда удалит только корневой метапакет drweb-workstations, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Вторая команда удалит из системы все пакеты, название которых начинается на "drweb" (стандартное наименование для пакетов программных продуктов Dr.Web). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта Dr.Web Desktop Security Suite (для Linux).

Удаление пакетов продукта также может осуществляться с помощью альтернативных менеджеров (например, **YaST**).

Дополнительно

Расположение файлов продукта

Файлы программного комплекса Dr.Web Desktop Security Suite (для Linux) после установки размещаются в каталогах `/opt`, `/etc` и `/var` дерева файловой системы.

Структура используемых каталогов:

Каталог	Содержимое
`/opt/drweb.com`	Исполняемые файлы компонентов продукта и основные библиотеки, необходимые для работы Dr.Web Desktop Security Suite (для Linux).
`/etc/opt/drweb.com`	Файлы настроек компонентов (по умолчанию) и лицензионный ключевой файл для работы Dr.Web Desktop Security Suite (для Linux) в одиночном режиме («Standalone mode»).
`/var/opt/drweb.com`	Вирусные базы, антивирусное ядро, а также временные файлы и дополнительные библиотеки, необходимые для работы Dr.Web Desktop Security Suite (для Linux).

Выборочные установка и удаление компонентов

В случае необходимости вы можете выполнить выборочную установку и удаление отдельных компонентов продукта, установив или удалив соответствующие пакеты. Выборочную установку и удаление следует производить тем же способом, каким был установлен продукт.

Для переустановки некоторого компонента вы можете сначала удалить его, а потом установить заново.

1. Установка и удаление компонентов продукта, установленного из репозитория

Если ваш продукт был установлен из репозитория, для установки и удаления отдельного компонента воспользуйтесь соответствующей командой менеджера пакетов, используемого в вашей ОС. Например:

1. Чтобы удалить компонент SplDer Gate (пакет `drweb-gated`) из состава продукта, установленного в ОС **CentOS**, используйте команду:

```
# yum remove drweb-gated
```

2. Чтобы добавить компонент SplDer Gate (пакет `drweb-gated`) в состав продукта, установленного в ОС **Ubuntu Linux**, используйте команду:

```
# apt-get install drweb-gated
```

В связи с тем, что антивирусное ядро Dr.Web Desktop Security Suite (для Linux) использует 32-битную архитектуру *x86*, в 64-битных системах **Debian**, **Mint**, **Ubuntu** (для платформы *x86-64*, *x64*, *amd64*) может потребоваться разрешить установку пакетов для платформы *x86*, выполнив команду:

```
# dpkg --add-architecture i386
```

При необходимости воспользуйтесь справкой по менеджеру пакетов, используемому в вашей ОС.

2. Установка и удаление компонентов продукта, установленного из универсального пакета

Если продукт был установлен из универсального пакета, и вы желаете дополнительно установить или переустановить пакет некоторого компонента, вам понадобится установочный файл (с расширением `.run`), из которого был установлен продукт. В случае если вы не сохранили этот файл, загрузите его с сайта компании «Доктор Веб».

Распаковка инсталляционного файла

При запуске run-файла вы можете воспользоваться следующими параметрами командной строки:

`--noexec` – вместо запуска процесса установки просто распаковать установочные файлы продукта. Файлы будут распакованы в каталог, указанный в системной переменной `TMPDIR` (обычно это каталог `/tmp`).

`--keep` – не удалять установочные файлы продукта и журнал установки по окончании установки.

`--target` <*каталог*> – распаковать установочные файлы продукта в указанный каталог <*каталог*>.

С полным перечнем параметров командной строки, которые могут быть использованы для инсталляционного файла, можно ознакомиться, выполнив команду:

```
$ ./<имя_файла>.run --help
```

Для выборочной установки компонентов продукта следует обратиться к каталогу, содержащему распакованные установочные файлы продукта. Если этот каталог отсутствует, выполните команду:

```
$ ./<имя_файла>.run --noexec --target <каталог>
```

В результате в каталоге <*каталог*> появится вложенный каталог <*имя_файла*>, содержащий распакованные установочные файлы продукта.

Выборочная установка компонентов

Установочный run-файл содержит пакеты всех компонентов, из которых состоит программный комплекс Dr.Web Desktop Security Suite (для Linux) (в формате RPM), а также вспомогательные файлы. Файлы пакетов каждого компонента имеют вид:

```
<имя_компонента>_<версия>~linux_<платформа>.rpm
```

где <*версия*> – это строка, включающая в себя версию и дату выпуска пакета, а <*платформа*> – строка, указывающая тип платформы, для которой предназначен продукт. Имена всех пакетов, содержащих компоненты программного комплекса Dr.Web Desktop Security Suite (для Linux), начинаются с префикса «drweb».

Для установки пакетов в состав инсталляционного комплекта включен менеджер пакетов. Для выборочной установки следует использовать служебный сценарий `installpkg.sh`. Для этого необходимо предварительно распаковать содержимое инсталляционного пакета в некоторый каталог.

Для установки пакетов необходимы права суперпользователя (пользователя *root*). Для получения прав суперпользователя воспользуйтесь командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

Чтобы выполнить установку пакета компонента, необходимо перейти в каталог, содержащий распакованный инсталляционный комплект, и выполнить в консоли (или в эмуляторе консоли – терминале для графического режима) команду:

```
# ./scripts/installpkg.sh <имя_пакета>
```

Например:

```
# ./scripts/installpkg.sh drweb-gated
```

Если требуется запустить программу установки программного комплекса целиком, следует запустить сценарий автоматической установки, выполнив команду:

```
$ ./install.sh
```

Кроме этого, вы можете установить все пакеты продукта (в том числе, чтобы установить недостающие компоненты, или компоненты, удаленные по ошибке), запустив установку корневого мета-пакета продукта:

```
# ./scripts/installpkg.sh drweb-workstations
```

Выборочное удаление компонентов

Для выборочного удаления пакета некоторого компонента используйте соответствующую команду удаления менеджера пакетов вашей операционной системы, если в вашей ОС используется формат пакетов RPM:

- В **Red Hat Enterprise Linux** и **CentOS** используйте команду **yum** `remove` <*имя_пакета*>
- В **Fedora** используйте команду **yum** `remove` <*имя_пакета*> или **dnf** `remove` <*имя_пакета*>
- В **SUSE Linux** используйте команду **zypper** `remove` <*имя_пакета*>
- В **Mageia**, **OpenMandriva Lx** используйте команду **urpme** <*имя_пакета*>
- В **Alt Linux** и **PCLinuxOS** используйте команду **apt-get** `remove` <*имя_пакета*>.

Например (для **Red Hat Enterprise Linux**):

```
# yum remove drweb-gated
```

Если ваша ОС использует пакеты формата DEB, для выборочного удаления следует воспользоваться менеджером пакетов **zypper**, автоматически установленным в рамках установки продукта. Для этого перейдите в каталог `/opt/drweb.com/bin`, и выполните следующую команду:

```
# ./zypper rm <имя_пакета>
```

Например:

```
# ./zypper rm drweb-gated
```

Если требуется запустить программу удаления программного комплекса целиком, следует запустить сценарий автоматического удаления, выполнив команду:

```
# ./uninst.sh
```

Для переустановки некоторого компонента вы можете сначала удалить его, а потом установить, запустив выборочную или полную установку из инсталляционного комплекта.

Настройка систем безопасности

Наличие в составе ОС подсистемы обеспечения дополнительной безопасности **SELinux**, а также использование систем мандатного управления доступом (в отличие от классической дискреционной модели UNIX), таких как **PARSEC**, приводит к проблемам в функционировании продукта Dr.Web Desktop Security Suite (для Linux) при настройках по умолчанию. Для обеспечения корректной работы Dr.Web Desktop Security Suite (для Linux) в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web Desktop Security Suite (для Linux).

В этом разделе рассматриваются настройки, обеспечивающие корректную работу Dr.Web Desktop Security Suite (для Linux) в следующих случаях:

- Настройка политик безопасности **SELinux**.
- Настройка разрешений для системы мандатного доступа **PARSEC** (ОС **Astra Linux SE**).
- Настройка запуска в режиме ЗПС (замкнутой программной среды) (ОС **Astra Linux SE**, версия 1.6).

Настройка разрешений системы мандатного доступа **PARSEC** для Dr.Web Desktop Security Suite (для Linux) позволит обходить компонентам антивируса ограничения установленных политик безопасности и получать доступ к файлам разных уровней привилегий.

Обратите внимание, что даже если вы не настроите разрешения системы мандатного доступа **PARSEC** для Dr.Web Desktop Security Suite (для Linux), то вы все равно сможете запускать проверку файлов, используя графический интерфейс Dr.Web Desktop Security Suite (для Linux) в режиме автономной копии. Для этого используйте команду **drweb-gui** с параметром `--Autonomous`. Также вы можете запускать проверку файлов непосредственно из командной строки. Для этого используйте команду **drweb-ctl** с этим же параметром (`--Autonomous`). При этом будет возможна проверка файлов, для доступа к которым необходим уровень привилегий не выше уровня, с которым работает пользователь, запустивший сеанс проверки. Данный режим имеет следующие особенности:

- Для запуска в режиме автономной копии необходимо наличие действующего ключевого файла, работа под управлением сервера централизованной защиты не поддерживается (имеется возможность установить ключевой файл, экспортированный с сервера централизованной защиты). При этом, даже если продукт подключен к серверу централизованной защиты, автономная копия *не сообщает* серверу централизованной защиты об угрозах, обнаруженных при запуске в режиме автономной копии.
- Все вспомогательные компоненты, обслуживающие работу автономной копии, будут запущены от имени текущего пользователя и будут работать со специально сформированным файлом конфигурации.

- Все временные файлы и сокеты UNIX, используемые для взаимодействия компонентов между собой, будут создаваться только в каталоге с уникальным именем, созданным запущенной автономной копии в каталоге временных файлов (указанном в системной переменной окружения `TMPDIR`).
- Автономно запущенная копия графического интерфейса управления *не запускает* мониторы SplDer Guard и SplDer Gate, работают только функции проверки файлов, и управления карантином, поддерживаемые Сканером.
- Пути к файлам вирусных баз, антивирусного ядра и исполняемым файлам сервисных компонентов заданы по умолчанию, либо берутся из специальных переменных окружения.
- Число одновременно работающих автономных копий не ограничено.
- При завершении работы автономно запущенной копии также завершает работу и комплект обслуживающих её сервисных компонентов.

Настройка политик безопасности SELinux

Если используемый вами дистрибутив **Linux** оснащен подсистемой безопасности **SELinux** (*Security-Enhanced Linux – Linux с улучшенной безопасностью*), то для того, чтобы служебные компоненты продукта (такие как сканирующее ядро) работали корректно после установки компонентов приложения, вам, возможно, потребуется внести изменения в политики безопасности, используемые **SELinux**.

1) Проблемы при установке универсального пакета

При включенном **SELinux** установка продукта в виде универсального пакета из установочного файла (`.run`) может окончиться неудачей, поскольку будет заблокирована попытка создания в системе специального пользователя *drweb*, с полномочиями которого работают модули Dr.Web Desktop Security Suite (для Linux).

В случае если попытка установки продукта из установочного файла (`.run`) была прервана из-за невозможности создания пользователя *drweb*, проверьте режим работы **SELinux**, для чего выполните команду **getenforce**. Эта команда выводит на экран текущий режим зашиты:

- *Permissive* – защита активна, но используется разрешающая стратегия: действия, нарушающие политики безопасности, не запрещаются, а только фиксируются в журнале аудита.
- *Enforced* – защита активна, используется запрещающая стратегия: действия, нарушающие политики безопасности, регистрируются в журнале аудита и блокируются.
- *Disabled* – **SELinux** установлен, но неактивен.

Если **SELinux** работает в режиме *Enforced*, следует временно (на период установки продукта) перевести ее в режим *Permissive*. Для этого выполните команду

```
# setenforce 0
```

которая временно (до первой перезагрузки системы) переведет **SELinux** в режим *Permissive*.

Какой бы режим защиты вы ни установили при помощи команды **setenforce**, после перезагрузки операционной системы **SELinux** вернется в режим защиты, заданный в ее настройках (обычно файл настроек **SELinux** находится в каталоге `/etc/selinux`).

После успешной установки продукта из установочного файла, но до его запуска и активации верните режим *Enforced,* для чего выполните команду:

```
# setenforce 1
```

2) Проблемы функционирования продукта

В некоторых случаях при работающем **SELinux** отдельные вспомогательные компоненты Dr.Web Desktop Security Suite (для Linux) (такие, как **drweb-se** и **drweb-filecheck**, используемые Сканером и SpIDer Guard) не смогут запуститься, вследствие чего сканирование объектов и мониторинг файловой системы станут невозможны. Признаком того, что эти вспомогательные модули не могут быть запущены, является появление сообщений об ошибках *119* и *120* на главном окне Dr.Web Desktop Security Suite (для Linux) и в системном журнале **syslog** (обычно расположен в каталоге `/var/log/`).

Ошибки 119 и 120 также могут сигнализировать о том, что вы пытаетесь запустить Dr.Web Desktop Security Suite (для Linux) в 64-битной версии операционной системы при отсутствии библиотеки поддержки исполнения 32-битных приложений (см. раздел Системные требования).

В случае срабатывания системы безопасности **SELinux** информация об отказах фиксируется также в системном журнале аудита. В общем случае, при использовании в системе демона **audit**, журнал аудита располагается в файле `/var/log/audit/audit.log`. В противном случае сообщения о запрете операции записываются в общий файл журнала `/var/log/messages` или `/var/log/syslog`.

Если установлено, что вспомогательные модули не функционируют из-за того, что они блокируются **SELinux**, необходимо скомпилировать для них специальные политики безопасности.

В некоторых дистрибутивах **Linux** указанные ниже утилиты могут быть по умолчанию не установлены. В этом случае вам, возможно, потребуется дополнительно установить содержащие их пакеты.

Создание политик безопасности SELinux:

1. Создайте новый файл с исходным кодом политики **SELinux** (файл с расширением `.te`). Данный файл определяет ограничения, относящиеся к описываемому модулю. Исходный файл политики может быть создан двумя способами:

   1) С помощью утилиты **audit2allow**. Это наиболее простой способ, поскольку данная утилита генерирует разрешающие правила на основе сообщений об отказе в доступе в файлах системных журналов. Возможно задать автоматический поиск сообщений в файлах журналов или указать путь к файлу журнала вручную.

      Обратите внимание, что этот способ можно использовать только в том случае, когда в системном журнале аудита уже зарегистрированы инциденты нарушения политик безопасности **SELinux** компонентами Dr.Web Desktop Security Suite (для Linux). В случае если это не так, следует или дождаться таких инцидентов в процессе работы продукта Dr.Web Desktop Security Suite (для Linux), или создать разрешающие политики принудительно, воспользовавшись утилитой **policygentool** (см. ниже).

Утилита **audit2allow** находится в пакете `policycoreutils-python` или `policycoreutils-devel` (для ОС **RedHat Enterprise Linux**, **CentOS**, **Fedora**, в зависимости от версии) или в пакете `python-sepolgen` (для ОС **Debian**, **Ubuntu**).

Пример использования **audit2allow**:

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

В данном примере утилита **audit2allow** производит поиск в файле `audit.log` сообщений об отказе в доступе для модуля **drweb-se**.

В результате работы утилиты создаются два файла: исходный файл политики `drweb-se.te` и готовый к установке модуль политики `drweb-se.pp`.

Если подходящих инцидентов в системном журнале не обнаружено, утилита вернет сообщение об ошибке.

В большинстве случаев вам не потребуется вносить изменения в файл политики, созданный утилитой **audit2allow**. Поэтому рекомендуется сразу переходить к пункту 4 для установки полученного модуля политики `drweb-se.pp`. Обратите внимание, что по умолчанию утилита **audit2allow** в качестве результата своей работы выводит

на экран готовый вызов команды **semodule**. Скопировав его в командную строку и выполнив, вы выполните пункт 4. Перейдите к пункту 2, только если вы хотите внести изменения в политики, автоматически сформированные для компонентов Dr.Web Desktop Security Suite (для Linux).

2) С помощью утилиты **policygentool**. Для этого укажите в качестве параметров имя модуля, работу с которым вы хотите настроить, и полный путь к его исполняемому файлу.

Обратите внимание, что утилита **policygentool**, входящая в состав пакета `selinux-policy` для ОС **RedHat Enterprise Linux** и **CentOS Linux**, может работать некорректно. В таком случае воспользуйтесь утилитой **audit2allow**.

Пример создания политик при помощи **policygentool**:

- Для **drweb-se**:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- Для **drweb-filecheck**:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-
filecheck.real
```

Вам будет предложено указать несколько общих характеристик домена, после чего для каждого модуля будут созданы три файла, определяющих политику:

<module_name>.te, <module_name>.fc и *<module_name>.if*.

2. При необходимости отредактируйте сгенерированный исходный файл политики *<module_name>.te,* а затем, используя утилиту **checkmodule**, создайте бинарное представление (файл с расширением `.mod`) исходного файла локальной политики.

Обратите внимание, что для успешной работы этой команды в системе должен быть установлен пакет `checkpolicy`.

Пример использования:

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. Создайте устанавливаемый модуль политики (файл с расширением `.pp`) с помощью утилиты **semodule_package**.

Пример:

```
# semodule_package -o drweb-se.pp -m drweb-se.mod
```

4. Для установки созданного модуля политики воспользуйтесь утилитой **semodule**.

Пример:

```
# semodule -i drweb-se.pp
```

Для получения дополнительной информации о принципах работы и настройки **SELinux** обратитесь к документации по используемому вами дистрибутиву **Linux**.

Настройка разрешений PARSEC (Astra Linux SE)

В системах, оснащенных подсистемой безопасности **PARSEC** (система управления мандатным доступом) из-за разности уровней привилегий, необходимых для доступа к файлам, по умолчанию SpIDer Guard не может перехватывать события о доступе к файлам с более высокими уровнями привилегий, нежели уровень привилегий, на котором запущен SpIDer Guard. Кроме того, в случае если пользователь работает на отличном от нуля уровне привилегий, интерфейс пользователя Dr.Web Desktop Security Suite (для Linux) не может взаимодействовать со SpIDer Guard и сервисными компонентами антивируса, работающими на других уровнях привилегий, в том числе может отсутствовать доступ к консолидированному карантину.

В случае если в ОС используется **PARSEC** и имеются учетные записи пользователей, работающих на уровнях привилегий, отличных от нулевого, необходимо выполнить специальную настройку продукта, чтобы обеспечить взаимодействие его компонентов, запускаемых на различных уровнях привилегий.

> Для осуществления этих операций необходимы права суперпользователя (пользователя *root*). Для получения прав суперпользователя воспользуйтесь командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

1. Настройка взаимодействия компонентов, запущенных на разных уровнях привилегий

Для ОС Astra Linux SE версии 1.6:

Внесите изменения в системный файл `/etc/parsec/privsock.conf`, наделив демон управления конфигурацией Dr.Web Desktop Security Suite (для Linux) (**drweb-configd**) правом на использование механизма *privsock*. **drweb-configd** – сервисный компонент продукта, обеспечивающий взаимодействие всех антивирусных компонентов между собой. Механизм *privsock* предназначен для обеспечения функционирования системных сетевых сервисов, не осуществляющих обработку информации с использованием мандатного контекста, но взаимодействующих с процессами, работающими в мандатном контексте субъекта доступа. Для этого выполните следующее:

1. В любом текстовом редакторе откройте файл `/etc/parsec/privsock.conf`. Добавьте в этот файл указанные строки:

```
/opt/drweb.com/bin/drweb-configd
/opt/drweb.com/bin/drweb-configd.real
```

2. Сохраните файл и перезагрузите систему.

Для ОС Astra Linux SE версии 1.5 и менее:

Внесите изменения в сценарий запуска демона управления конфигурацией Dr.Web Desktop Security Suite (для Linux) (**drweb-configd**). Для этого выполните следующее:

1. Совершите вход в систему с использованием учетной записи, обладающей нулевым уровнем привилегий.
2. В любом текстовом редакторе откройте файл сценария `/etc/init.d/drweb-configd`.
3. Найдите в этом файле определение функции `start_daemon()`, в которой замените строку

   ```
   "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
   ```

   на строку

   ```
   execaps -c 0x100 -- "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
   ```

4. В некоторых ОС (например, **Astra Linux SE** 1.3) может потребоваться указать дополнительно зависимость запуска компонента от подсистемы **PARSEC**. В этом случае также необходимо модифицировать в этом файле строку:

   ```
   # Required-Start: $local_fs $network
   ```

   Измените данную строку следующим образом:

   ```
   # Required-Start: $local_fs $network parsec
   ```

5. Сохраните файл и перезапустите систему.

2. Настройка SpIDer Guard для перехвата событий доступа к файлам

Для предоставления файловому монитору SpIDer Guard возможности обнаруживать доступ к файлам, имеющим любой уровень привилегий доступа, необходимо перевести SpIDer Guard в режим работы *LKM* (будет использован специальный загружаемый модуль ядра **Linux**, поставляемый совместно с Dr.Web Desktop Security Suite (для Linux)).

Чтобы перевести SpIDer Guard в режим работы *LKM*, выполните следующую команду:

```
# drweb-ctl cfset LinuxSpider.Mode LKM
```

Для получения дополнительной информации используйте команду:

```
$ man drweb-spider
```

Настройка запуска в режиме ЗПС (Astra Linux SE, версия 1.6)

В ОС **Astra Linux SE** поддерживается особый режим *замкнутой программной среды* (ЗПС), в котором запускаются только приложения, исполняемые файлы которых подписаны цифровой подписью разработчика, чей открытый ключ добавлен в перечень ключей, которым доверяет ОС.

По умолчанию компоненты Dr.Web Desktop Security Suite (для Linux), поставляемые для исполнения в среде **Astra Linux SE**, подписаны цифровой подписью компании «Доктор Веб», а открытый ключ для этой цифровой подписи автоматически добавляется в перечень доверенных при установке программы, в связи с чем продукт должен корректно запускаться при активизации режима ЗПС в ОС **Astra Linux SE** версии 1.5 и более старой.

Однако, в связи с тем, что в версии 1.6 ОС **Astra Linux SE** механизм подписи был изменен, для обеспечения запуска Dr.Web Desktop Security Suite (для Linux) в режиме ЗПС в ОС версии 1.6 необходимо выполнить предварительные настройки системы.

Настройка Astra Linux SE версии 1.6 для запуска Dr.Web Desktop Security Suite (для Linux) в режиме ЗПС

1. Установите пакет `astra-digsig-oldkeys` с установочного диска ОС, если он еще не установлен;
2. Поместите открытый ключ компании «Доктор Веб» в каталог `/etc/digsig/keys/legacy/keys` (в случае отсутствия каталога его необходимо создать).
3. Выполните команду:

```
# update-initramfs -k all -u
```

4. Перезагрузите систему.

Работа с Dr.Web Desktop Security Suite (для Linux)

Работа пользователя с Dr.Web Desktop Security Suite (для Linux) может производиться как в графическом режиме, при помощи компонента, предоставляющего графический интерфейс управления, так и из командной строки (включая работу через эмуляторы терминала в графического режиме).

- Для запуска графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) необходимо выбрать пункт **Dr.Web Desktop Security Suite (для Linux)** в системном меню **Приложения**, или выполнить в командной строке операционной системы команду:

  ```
  $ drweb-gui
  ```

  После этого, если окружение графического рабочего стола доступно, будет запущен графический интерфейс управления Dr.Web Desktop Security Suite (для Linux). Для запуска проверки при старте графического интерфейса или для запуска его в режиме автономной копии, можно воспользоваться вызовом данной команды с аргументами.
- Управление работой Dr.Web Desktop Security Suite (для Linux) из командной строки рассмотрено в разделе Работа из командной строки.
- Для графических сред рабочего стола также поддерживается запуск проверки файлов из панели задач (такой как **Unity Launcher** в ОС **Ubuntu**) и из графического файлового менеджера (такого как **Nautilus**). Кроме того, в области уведомлений рабочего стола, отображается индикатор состояния, используемый для показа всплывающих уведомлений и доступа к контекстному меню приложения. Индикатор отображается агентом уведомлений, который, как и другие сервисные компоненты приложения, запускается автоматически и не требует ручного вмешательства в свою работу. Подробнее см. в разделе Интеграция со средой рабочего стола.

После установки Dr.Web Desktop Security Suite (для Linux) любым из указанных в данном руководстве способов, в начале работы, вам потребуется активировать лицензию, либо установить ключевой файл, если он у вас уже имеется, или подключить Dr.Web Desktop Security Suite (для Linux) к серверу централизованной защиты (см. раздел Лицензирование). До тех пор, пока вы этого не сделаете, *функции антивирусной защиты будут отключены.*

Обратите внимание, что почтовый протокол IMAP, который в большинстве случаев используется почтовыми клиентами (такими, как **Mozilla Thunderbird**) для получения сообщений электронной почты с почтового сервера, является сеансовым. Поэтому после внесения изменений в работу монитора SpIDer Gate (включение ранее отключенного монитора, изменение режима проверки защищенных соединений) необходимо обязательно перезапустить почтовый клиент для того, чтобы монитор SpIDer Gate смог проверять входящие сообщения после изменения режима своей работы.

Работа в графическом режиме

За работу Dr.Web Desktop Security Suite (для Linux) в окружении рабочего стола отвечает два компонента:

- Агент уведомлений – компонент, запускаемый автоматически при начале сеанса работы пользователя в окружении рабочего стола. Этот компонент показывает всплывающие уведомления о событиях в работе продукта, а также предоставляет индикатор состояния Dr.Web Desktop Security Suite (для Linux) в области системных уведомлений и основное меню для взаимодействия с продуктом.
- Графический интерфейс – компонент, работающий в окружении графического рабочего стола и предоставляющий оконный интерфейс для управления работой Dr.Web Desktop Security Suite (для Linux).

Агент уведомлений

Агент уведомлений Dr.Web Desktop Security Suite (для Linux) предназначен для:

1. Отображения индикатора состояния Dr.Web Desktop Security Suite (для Linux).
2. Управления мониторами и обновлением, запуска графического интерфейса управления.
3. Показа всплывающих уведомлений о событиях.
4. Запуска проверок по заданному расписанию.

Графический интерфейс управления

Графический интерфейс управления Dr.Web Desktop Security Suite (для Linux) позволяет решать следующие задачи:

1. Просмотр состояния работы Dr.Web Desktop Security Suite (для Linux), включая актуальность имеющихся вирусных баз и срока действия лицензии.
2. Запуск и остановка монитора файловой системы SplDer Guard.
3. Запуск и остановка монитора сетевых соединений SplDer Gate.
4. Запуск проверки файлов по требованию, в том числе:
   - *Быстрая проверка* системных файлов и наиболее уязвимых системных объектов.
   - *Полная проверка* всех файлов системы.
   - *Выборочная проверка* только указанных файлов и каталогов или специализированных объектов (загрузочных записей дисков, активных процессов).

   Выбор файлов для проверки выполняется как указанием целевых каталогов или файлов перед запуском проверки, так и их перетаскиванием («*drag and drop*») мышью из окна файлового менеджера на главную страницу (см. ниже) или на страницу **Сканер** окна Dr.Web Desktop Security Suite (для Linux).

5. Обзор всех угроз, обнаруженных Dr.Web Desktop Security Suite (для Linux) во время текущего сеанса работы в графическом режиме, включая обзор нейтрализованных и пропущенных угроз, а также объектов, перемещенных в карантин.
6. Обзор объектов, перемещенных в карантин, с возможностью их окончательного удаления или восстановления.
7. Настройка параметров работы компонентов Dr.Web Desktop Security Suite (для Linux), включая следующие параметры:
   - Действия, которые Сканеру и SplDer Guard следует автоматически применять к обнаруженным угрозам (в зависимости от их типа).
   - Перечень каталогов и файлов, которые не должны проверяться Сканером и не должны контролироваться монитором файловой системы SplDer Guard.
   - Черные и белые списки веб-сайтов и нежелательных категорий веб-ресурсов, используемые монитором SplDer Gate, а также параметры проверки файлов, загруженных из сети Интернет или полученных по электронной почте.
   - Расписание плановых проверок файловой системы, включая периодичность и тип производимой проверки, а также перечень объектов, подлежащих выборочной проверке согласно заданному расписанию.
   - Режим работы (подключение к серверу централизованной защиты и отключение от него).
   - Параметры мониторинга сетевой активности, включая анализ зашифрованного трафика.
   - Разрешение на использование сервиса Dr.Web Cloud.
8. Управление лицензиями (выполняется через Менеджер лицензий).

Для корректной работы Dr.Web Desktop Security Suite (для Linux) необходимо, чтобы предварительно были запущены его сервисные компоненты, в противном случае он завершит свою работу непосредственно после запуска, выдав соответствующее предупреждение. В штатном режиме все необходимые сервисные компоненты запускаются автоматически и не требуют вмешательства пользователя.

Внешний вид графического интерфейса управления

Вид главного окна графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) представлен на рисунке ниже.

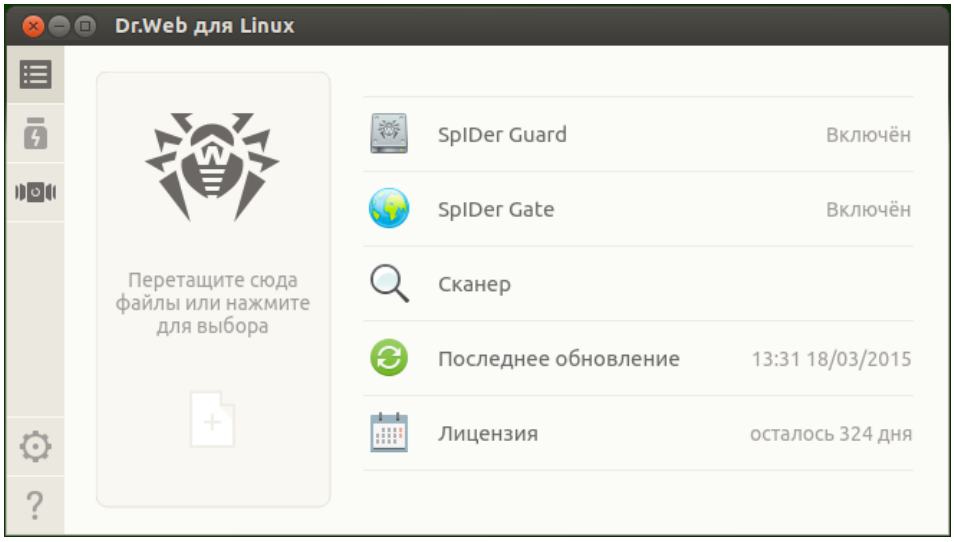

Рисунок 5. Графический интерфейс управления Dr.Web Desktop Security Suite (для Linux)

В левой части окна расположена навигационная панель, кнопки которой позволяют выполнить следующие действия.

Кнопка	Описание
1. Постоянно доступные	
	Открывает главную страницу, на которой имеется возможность: • Включить или выключить монитор файловой системы SpIDer Guard. • Включить или выключить монитор сетевых соединений SpIDer Gate. • Запустить проверку объектов файловой системы (файлов, загрузочных записей) и запущенных процессов. • Просмотреть состояние актуальности вирусных баз и выполнить их обновление при необходимости. • Запустить Менеджер лицензий для просмотра состояния текущей лицензии и регистрации новой, при необходимости.
	Открывает страницу работы с карантином, позволяющую просмотреть файлы, помещенные в карантин, а также выполнить их удаление или восстановление из карантина.
	Открывает окно настройки работы Dr.Web Desktop Security Suite (для Linux), в частности:

Кнопка	Описание
	• Сканера объектов файловой системы. • Монитора файловой системы SpIDer Guard. • Монитора сетевых соединений SpIDer Gate. • Запуска проверок по расписанию. Кроме того, здесь может быть настроена работа в режиме централизованной защиты.
	Предоставляет доступ к справочным материалам и вспомогательным ресурсам компании «Доктор Веб»: • Информация о продукте. • Руководство пользователя. • Форум Dr.Web. • Техническая поддержка. • Персональный кабинет пользователя **Мой Dr.Web**. Все ссылки открываются в браузере, установленном в системе.
2. Появляющиеся в зависимости от условий	
	Открывает страницу списка задач проверки файлов, в котором имеются незавершенные (выполняющиеся) задачи проверки. *Присутствует на навигационной панели только в случае если хотя бы одна проверка выполняется.*
  	Открывает страницу списка результатов законченных проверок. Окрашивается в зависимости от результата: 1) Зеленая – все проверки закончились успешно, все найденные угрозы, если найдены, обезврежены. 2) Красная – имеются необезвреженные угрозы. 3) Желтая – какая-либо из проверок завершилась вследствие ошибки. *Присутствует на навигационной панели только в случае если запускалась хотя бы одна проверка.*
	Открывает страницу просмотра угроз, обнаруженных при проверке файлов сканером или монитором файловой системы SpIDer Guard. *Присутствует на навигационной панели только в случае если имеются обнаруженные угрозы.*
	Присутствует на навигационной панели только в случае если открыта и активна страница запуска сканирования.

Кнопка	Описание
	При переходе на любую другую страницу главного окна, а также при запуске сканирования страница запуска сканирования будет автоматически закрыта, а кнопка убрана с навигационной панели.
	Присутствует на навигационной панели только в случае если открыта и активна страница управления SpIDer Guard. *При переходе на любую другую страницу главного окна, страница управления SpIDer Guard будет автоматически закрыта, а кнопка убрана с навигационной панели.*
	Присутствует на навигационной панели только в случае если открыта и активна страница управления SpIDer Gate. *При переходе на любую другую страницу главного окна, страница управления SpIDer Gate будет автоматически закрыта, а кнопка убрана с навигационной панели.*
	Присутствует на навигационной панели только в случае если открыта и активна страница управления обновлениями. *При переходе на любую другую страницу главного окна, страница управления обновлениями будет автоматически закрыта, а кнопка убрана с навигационной панели.*
	Присутствует на навигационной панели только в случае если открыта и активна страница Менеджера лицензий. *При переходе на любую другую страницу главного окна, страница Менеджера лицензий будет автоматически закрыта, а кнопка убрана с навигационной панели.*

Главная страница

На главной странице окна графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) расположена целевая область («мишень») для перетаскивания файлов и каталогов, подлежащих проверке. Она отмечена надписью **Перетащите сюда файлы или нажмите для выбора**. При перетаскивании и отпускании файлов и каталогов из окна файлового менеджера на главную страница окна Dr.Web Desktop Security Suite (для Linux) запускается их выборочная проверка (если Сканер уже выполняет какую-либо проверку, то задача проверки указанных файлов ставится в очередь).

Также на главной странице окна расположены следующие кнопки:

- **SpIDer Guard** – отображает текущее состояние, в котором находится монитор файловой системы SpIDer Guard. При нажатии открывает страницу управления, на которой можно запустить или остановить SpIDer Guard, а также просмотреть статистику его работы

- **SplDer Gate** – отображает текущее состояние, в котором находится монитор сетевых соединений SplDer Gate. При нажатии открывает страницу управления, на которой можно запустить или остановить SplDer Gate, а также просмотреть статистику его работы.
- **Сканер** – позволяет открыть страницу запуска проверки файлов, каталогов и других объектов файловой системы (например, загрузочные записи).
- **Последнее обновление** – отображает текущее состояние обновления вирусных баз. При нажатии открывает страницу управления обновлением, на которой можно запустить процесс обновления по требованию.
- **Лицензия** – отображает состояние текущей лицензии. При нажатии открывает страницу Менеджера лицензий, на которой можно ознакомиться с более детальной информацией о текущей лицензии, а также выполнить процедуру приобретения и регистрации новой лицензии, если это требуется.

Интеграция со средой рабочего стола

Dr.Web Desktop Security Suite (для Linux) поддерживает четыре способа интеграции с графическим окружением рабочего стола:

- Отображение в области уведомлений рабочего стола пиктограммы приложения, играющей роль индикатора состояния, позволяющего вызвать контекстное меню приложения;
- Вызов контекстного меню с основными командами проверки файлов при нажатии правой кнопки мыши на пиктограмме приложения в панели задач;
- Запуск проверки файлов и каталогов при помощи команды контекстного меню в графическом файловом менеджере;
- Запуск проверки файлов и каталогов при перетаскивании их мышью на главную страницу окна Dr.Web Desktop Security Suite (для Linux).

Индикатор приложения в области уведомлений

После входа пользователя в систему, в области уведомлений рабочего стола (если она поддерживается используемой графической средой) агент уведомлений отображает индикатор, имеющий вид пиктограммы с логотипом Dr.Web Desktop Security Suite (для Linux). Индикатор используется для отображения статуса приложения, а также доступа к контекстному меню Dr.Web Desktop Security Suite (для Linux). При наличии каких-либо проблем в работе продукта (например, устарели вирусные базы или заканчивается срок действия лицензии) в индикаторе поверх логотипа Dr.Web Desktop Security Suite (для Linux) отображается символ восклицательного знака:  .

Кроме индикатора состояния, агент уведомлений также отображает всплывающие уведомления, информирующих пользователя о важных событиях в работе Dr.Web Desktop Security Suite (для Linux), таких, как:

- Обнаружена угроза (в том числе – резидентными мониторами SpIDer Guard и SpIDer Gate).
- Заканчивается срок действия лицензии.

При нажатии кнопки мыши на пиктограмму индикатора на экране отображается контекстное меню Dr.Web Desktop Security Suite (для Linux).

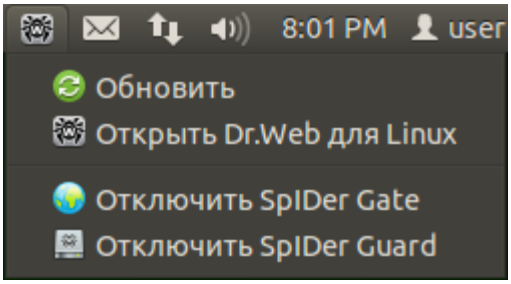

Рисунок 6. Контекстное меню индикатора Dr.Web Desktop Security Suite (для Linux)

При выборе пункта меню **Открыть Dr.Web Desktop Security Suite (для Linux)** на экране появляется окно графического интерфейса управления Dr.Web Desktop Security Suite (для Linux), т.е. происходит его запуск. Выбор пунктов меню **Включить SpIDer Gate**/**Отключить SpIDer Gate** и **Включить SpIDer Guard**/**Отключить SpIDer Guard** позволяет запустить или завершить работу соответствующего монитора. Обратите внимание, что для выключения работы любого монитора вам будет необходимо пройти аутентификацию, указав логин и пароль пользователя, обладающего административными правами (см. Управление правами приложения). Выбор пункта **Обновить** принудительно запускает процедуру получения обновлений.

Если индикатор указывает на наличие проблем в функционировании Dr.Web Desktop Security Suite (для Linux), то в меню пиктограмма соответствующего пункта, вызвавшего проблему, также снабжается символом восклицательного знака, например:  .

Проблемы в работе индикатора приложения

1. Если индикатор отображается с символом критической ошибки  , а выпадающее меню содержит только неактивный пункт **Запуск**, это означает, что Dr.Web Desktop Security Suite (для Linux) не может запуститься из-за того, что некоторые сервисные компоненты недоступны. Если это состояние продолжается длительное время, то попробуйте устранить эту ошибку самостоятельно, или обратитесь в техническую поддержку.
2. Если после входа пользователя в систему индикатор не отобразился в области уведомлений рабочего стола, попробуйте устранить эту ошибку самостоятельно, или обратитесь в техническую поддержку.

В некоторых окружениях рабочего стола внешний вид и поведение индикатора могут отличаться от описанного, например, могут не отображаться пиктограммы в выпадающем меню.

Контекстное меню пиктограммы панели задач

Если окружение рабочего стола поддерживает использование панели задач, например, такой как **Unity Launcher** в ОС **Ubuntu**, то при запуске графического интерфейса Dr.Web Desktop Security Suite (для Linux), на панели задач появится кнопка с пиктограммой приложения. Для этого рекомендуется запускать приложение через выбор пункта **Dr.Web Desktop Security Suite (для Linux)** в меню **Приложения**. Нажатие правой кнопки мыши на кнопку с пиктограммой запущенного приложения откроет на экране контекстное меню, примерный вид которого показан на рисунке ниже (меню для **Unity Launcher** в ОС **Ubuntu** 12.04).

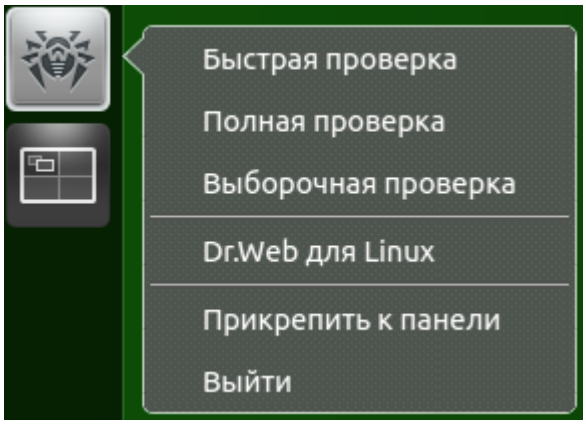

Рисунок 7. Контекстное меню Dr.Web Desktop Security Suite (для Linux) в панели задач

- Выбор пунктов меню **Быстрая проверка**, **Полная проверка** и **Выборочная проверка** позволяет запустить соответствующую задачу проверки (для **Выборочная проверка** – открыть страницу выбора объектов, подлежащих проверке).
- Выбор пункта меню **Dr.Web Desktop Security Suite (для Linux)** запускает графический интерфейс (если не запущен), а пункта **Выйти** – завершает работу графического интерфейса (если он запущен в данный момент).
- Выбор пункта меню **Прикрепить к панели** позволяет закрепить кнопку приложения на панели задач для быстрого доступа к запуску графического интерфейса и основных задач проверки.

Если в очереди задач имеются выполняемые задачи проверки файловой системы, поверх кнопки с пиктограммой приложения в панели задач отображается индикатор суммарного выполнения активных задач проверки.

В различных окружениях рабочего стола внешний вид панели задач, контекстного меню и поведение пунктов меню, отличных от **Быстрая проверка**, **Полная проверка** и **Выборочная проверка**, могут отличаться от описанного.

Проблемы в работе пиктограммы панели задач

Если пиктограмма запущенного графического интерфейса отображается на панели задач, но выпадающее меню не содержит пунктов запуска задач проверки, попробуйте осуществить запуск графического приложения через выбор пункта **Dr.Web Desktop Security Suite (для Linux)** меню **Приложения** (вместо запуска через исполнение команды **drweb-gui** в эмуляторе терминала или выбора пункта **Открыть Dr.Web Desktop Security Suite (для Linux)** в меню индикатора приложения в области уведомлений).

Проверка файлов и каталогов через контекстное меню файлового менеджера

Dr.Web Desktop Security Suite (для Linux) позволяет выполнять проверку файлов и каталогов непосредственно из окна обзора файлов и каталогов графического файлового менеджера (такого, как **Nautilus**). Для проверки файлов и каталогов необходимо:

1. Выделить их в окне файлового менеджера и нажать правую кнопку мыши.
2. В открывшемся контекстном меню выбрать пункт **Открыть в другой программе**.
3. В появившемся списке установленных приложений найти **Dr.Web Desktop Security Suite (для Linux)**.

Как правило, после первого использования Dr.Web Desktop Security Suite (для Linux) в качестве приложения для открытия файлов, эта ассоциация будет запомнена файловым менеджером и в дальнейшем в контекстном меню будет доступен пункт **Открыть в Dr.Web Desktop Security Suite (для Linux)**.

В различных графических файловых менеджерах указанное название пункта контекстного меню для выбора приложения, также как и способ выбора приложения из списка установленных в системе, могут отличаться от описанного.

Проблемы с использованием контекстного меню файлового менеджера

Некоторые графические среды для ОС **GNU/Linux** могут автоматически настроить ассоциацию файлов или каталогов (по MIME-типу этих объектов) с **Dr.Web Desktop Security Suite (для Linux)**, выбранным в файловом менеджере для проверки при помощи пункта контекстного меню **Открыть в другой программе**. В этом случае в дальнейшем для таких файлов и каталогов двойной щелчок левой кнопкой мыши будет приводить к запуску **Dr.Web Desktop Security Suite (для Linux)**. Для исправления этой ситуации

отмените настроенную ассоциацию между файлами и **Dr.Web Desktop Security Suite (для Linux)**.

Перетаскивание файлов и каталогов на окно графического интерфейса управления

Dr.Web Desktop Security Suite (для Linux) позволяет выполнять проверку файлов и каталогов путем перетаскивания их курсором мыши из окна обзора файлов и каталогов графического файлового менеджера на окно запущенного графического интерфейса управления Dr.Web Desktop Security Suite (для Linux). Чтобы началась проверка файлов и каталогов, перетащенных мышью на окно приложения, необходимо, чтобы окно интерфейса было открыто на главной странице или на странице выбора типа проверки. Признаком того, что на данную страницу окна интерфейса управления Dr.Web Desktop Security Suite (для Linux) можно перетаскивать файлы и каталоги для проверки, служит наличие на странице «мишени», содержащей надпись **Перетащите сюда файлы или нажмите для выбора**.

Запуск и завершение работы

Запуск графического интерфейса управления Dr.Web Desktop Security Suite (для Linux)

Для запуска графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) необходимо:

- Выбрать в системном меню **Приложения** пункт **Dr.Web Desktop Security Suite (для Linux)**.

или

- Нажать правой кнопкой мыши на индикатор Dr.Web Desktop Security Suite (для Linux) в области уведомлений рабочего стола и выбрать в выпадающем меню пункт **Открыть Dr.Web Desktop Security Suite (для Linux)**.

Вы также можете запустить графический интерфейс управления Dr.Web Desktop Security Suite (для Linux) из командной строки. Это возможно только в том случае, если графическое окружение доступно при работе с командной строкой, например – из окна эмулятора терминала.

Завершение работы графического интерфейса управления Dr.Web Desktop Security Suite (для Linux)

Для завершения работы графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) необходимо закрыть его окно, используя стандартную кнопку закрытия, расположенную в заголовке окна.

Обратите внимание, что при завершении работы графического интерфейса Dr.Web Desktop Security Suite (для Linux) сервисные компоненты, включая агент уведомлений и мониторы SpIDer Guard и SpIDer Gate (если они не были отключены пользователем) продолжают свою работу.

В штатном режиме все необходимые сервисные компоненты не требуют вмешательства пользователя в свою работу.

Поиск и обезвреживание угроз

Поиск и обезвреживание угроз осуществляется как Сканером (по требованию пользователя или по заданному расписанию), так и в процессе работы мониторов файловой системы SpIDer Guard и сетевых соединений SpIDer Gate.

- Включение и выключение SpIDer Guard и SpIDer Gate осуществляется как из меню в области уведомлений, так и на соответствующих страницах управления их работой (см. Мониторинг файловой системы и Мониторинг сетевых соединений).
- Обзор текущих задач на проверку Сканером объектов файловой системы и управление ими осуществляется на странице управления списком проверок.
- Все угрозы, обнаруженные Сканером или монитором файловой системы SpIDer Guard, отображаются в виде списка на странице просмотра обнаруженных угроз.
- Управление угрозами, помещенными в карантин, осуществляется на странице работы с карантином.
- Настройка реакции Dr.Web Desktop Security Suite (для Linux) на обнаруженные угрозы осуществляется в окне настроек. Там же имеется возможность включить и настроить расписание периодических проверок, а также настроить проверку зашифрованных соединений.

Если Dr.Web Desktop Security Suite (для Linux) работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то страница **Сканер** окна Dr.Web Desktop Security Suite (для Linux) будет недоступна. Кроме того, в этом случае агент уведомлений и графический интерфейс управления не будут запускать проверки по расписанию.

Проверка объектов по требованию

Типы выполняемых проверок

По требованию пользователя Сканер может выполнять следующие типы проверок:

- *Быстрая проверка* – проверка только жестко определенного набора критических системных объектов, подверженных наибольшему риску (загрузочные записи дисков, системные файлы и т.п.).
- *Полная проверка* – проверка всех объектов локальной файловой системы, доступных пользователю, от имени которого запущен Dr.Web Desktop Security Suite (для Linux).
- *Выборочная проверка* – проверка объектов файловой системы, или некоторых объектов специального типа, непосредственно указанных пользователем.

Если Dr.Web Desktop Security Suite (для Linux) работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то эта страница окна Dr.Web Desktop Security Suite (для Linux) будет недоступна.

При проверке объектов увеличивается нагрузка на процессор, что, в случае использования мобильных устройств, может привести к быстрой разрядке аккумулятора. Поэтому на портативных компьютерах рекомендуется проводить проверку системы при питании от сети.

Запуск проверки

Запустить процесс проверки объектов файловой системы вы можете, нажав кнопку **Сканер** на главной странице окна.

При этом откроется страница выбора типа проверки. Чтобы инициировать *Быструю* или *Полную* проверку, следует нажать соответствующую кнопку. После этого проверка начнется автоматически.

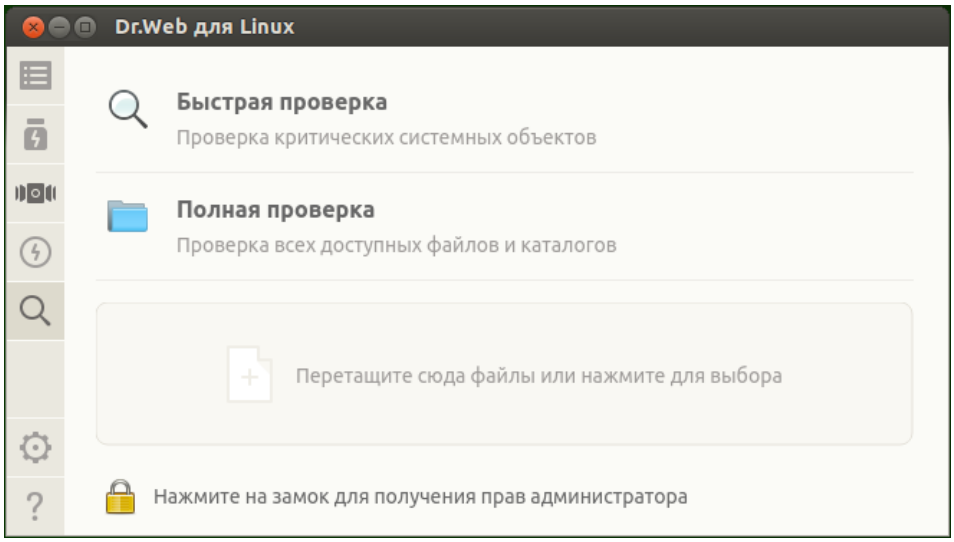

Рисунок 8. Страница выбора типа проверки

Проверка объектов всегда выполняется Сканером с текущими правами приложения. Если приложение не обладает повышенными правами, то при проверке будут пропущены все файлы и каталоги, недоступные пользователю, запустившему Dr.Web Desktop Security Suite (для Linux). Чтобы обеспечить проверку всех требуемых файлов, владельцем которых вы не являетесь, следует перед началом проверки повысить права приложения, если они не повышены. См. Управление правами приложения.

Если требуется *Выборочная проверка* только требуемых файлов и каталогов, то это можно сделать любым из способов, указанных ниже:

- **Перетаскивание курсором**.

  Файлы и каталоги, подлежащие проверке, можно перетащить мышью из окна файлового менеджера на открытую страницу выбора типа проверки (в зону, отмеченную надписью **Перетащите сюда файлы или нажмите для выбора**). Также можно перетащить их на главную страницу окна Dr.Web Desktop Security Suite (для Linux).

  При наведении перемещаемых файлов и/или каталогов курсором мыши на окно, на нем отображается мишень, содержащая надпись **Поместите файлы сюда**. Для начала проверки выбранных файлов достаточно «бросить» их на страницу, отпустив кнопку мыши. После этого проверка начнется автоматически.

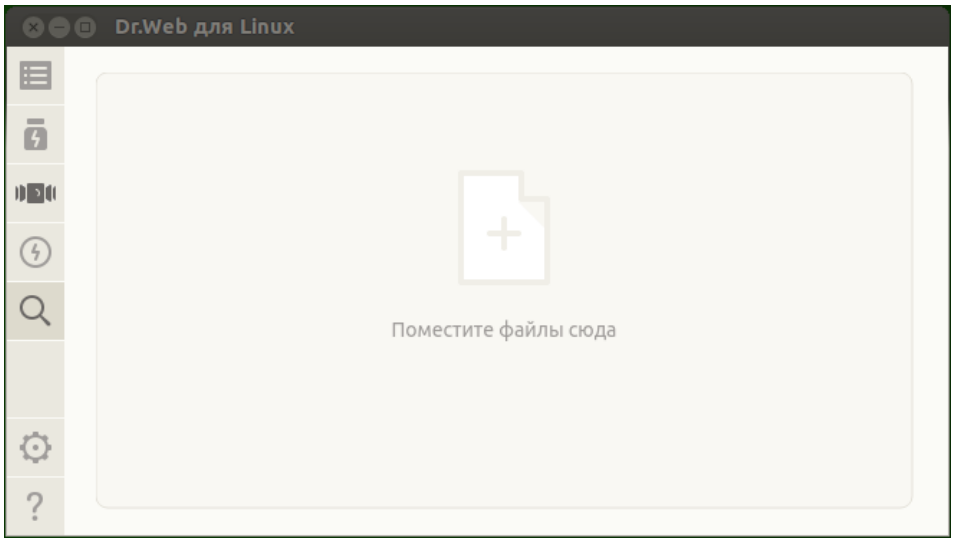

Рисунок 9. Мишень для файлов, подлежащих проверке

- **Формирование списка объектов для выборочной проверки**.

  Для формирования списка объектов для выборочной проверки необходимо щелкнуть мышью по мишени для выбора файлов. В этом случае на экране откроется список объектов для выборочной проверки.

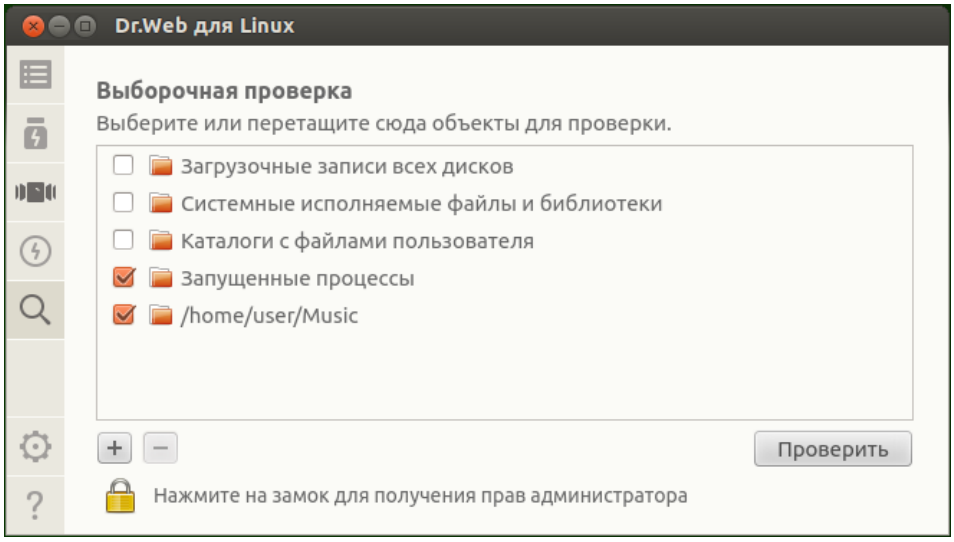

Рисунок 10. Список объектов для выборочной проверки

В списке также имеется четыре специальных пункта, задающие предопределенные группы объектов:

- *Загрузочные записи всех дисков*. При выборе этого пункта автоматически выделяются для проверки все загрузочные записи всех доступных в системе дисков.
- *Системные исполняемые файлы и библиотеки*. При выборе этого пункта автоматически выбираются для проверки все каталоги, содержащие системные исполняемые файлы (`/bin`, `/sbin` и т.д.).
- *Каталоги с файлами пользователя*. При выборе этого пункта автоматически выбираются для проверки каталоги, содержащие файлы пользователя и текущего

сеанса работы (домашний каталог `/home/<username>` (~), `/tmp`, `/var/mail`, `/var/tmp`).

- *Запущенные процессы*. При выборе этого пункта автоматически проверяются исполняемые файлы, из которых были запущены процессы, активные в системе в данный момент. При этом, если в исполняемом файле обнаруживается угроза, то все процессы, запущенные из этого файла, принудительно завершаются, а к файлу применяются меры по нейтрализации угрозы.

Добавление и удаление объектов из списка выборочной проверки

При необходимости вы можете добавить в список выборочной проверки собственные пути для проверки. Для этого перетащите требуемые объекты мышью (пути, ведущие к указанным объектам, автоматически будут добавлены в список выборочной проверки), или нажмите кнопку `+`, расположенную под списком. В этом случае откроется стандартное окно выбора файлов и каталогов. Выберите требуемый объект (файл или каталог) и нажмите кнопку **Открыть**.

> Файлы и каталоги с установленным атрибутом «скрытый» по умолчанию не отображаются в окне выбора файлов и каталогов. Чтобы отобразить их, нажмите кнопку  на панели инструментов окна выбора файлов и каталогов.

Кнопка `–`, расположенная под списком, удаляет из списка все выделенные пути (путь считается выделенным, если выделена строка списка, содержащая путь). Для выделения более одного пути используйте выделение элементов списка с нажатой клавишей SHIFT или CTRL. Обратите внимание, что нельзя удалить из списка первые четыре предопределенных пункта.

Запуск выборочной проверки из списка

Чтобы начать выборочную проверку, отметьте флажками в списке все объекты, подлежащие проверке, и нажмите кнопку **Проверить**. После этого запустится проверка.

После запуска созданная задача проверки помещается в очередь, которая содержит все проверки, выполнявшиеся Сканером в текущем сеансе работы, как завершенные, так и выполняющиеся в данный момент или еще только ожидающие своего выполнения. Просмотр списка задач проверки и управление им осуществляется на странице просмотра списка задач проверки.

Проверка объектов по расписанию

Dr.Web Desktop Security Suite (для Linux) может выполнять автоматический запуск периодических проверок заданного перечня объектов файловой системы по указанному расписанию.

Если Dr.Web Desktop Security Suite (для Linux) работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то эта возможность Dr.Web Desktop Security Suite (для Linux) будет недоступна.

Типы выполняемых проверок

По расписанию можно выполнять следующие типы проверок:

- *Быстрая проверка* – проверка только жестко определенного набора критических системных объектов, подверженных наибольшему риску (загрузочные записи дисков, системные файлы и т.п.).
- *Полная проверка* – проверка всех объектов локальной файловой системы, доступных пользователю, от имени которого запущен Dr.Web Desktop Security Suite (для Linux).
- *Выборочная проверка* – проверка объектов файловой системы, или некоторых объектов специального типа, непосредственно указанных пользователем.

Запуск проверки

Проверки запускаются автоматически, согласно заданному расписанию. Запуск проверки осуществляется:

1. Самим графическим интерфейсом, если он запущен в момент начала проверки.
2. Агентом уведомлений, если в момент начала проверки графический интерфейс недоступен.

При начале проверки по расписанию автоматически запускается графический интерфейс управления (если он еще не запущен), созданная задача проверки помещается в очередь, которая содержит все проверки, выполнявшиеся Сканером в текущем сеансе работы, как завершенные, так и выполняющиеся в данный момент или еще только ожидающие своего выполнения. Просмотр списка задач проверки и управление им осуществляется на странице просмотра списка задач проверки.

Управление списком проверок

Перечень созданных и выполняющихся Сканером задач проверки объектов файловой системы и их результатов доступен на специальной странице окна Dr.Web Desktop Security Suite (для Linux). При наличии в очереди Сканера хотя бы одной задачи, на навигационной панели окна появляется специальная кнопка, нажатие которой открывает страницы обзора списка задач проверки. В зависимости от состояния задач проверки, эта кнопка имеет следующий вид:

	В списке задач имеются незавершенные проверки (используется анимация).
	Все проверки, имеющиеся в списке, завершены или были остановлены пользователем, угроз не найдено, или все найденные угрозы обезврежены.
	Все проверки, имеющиеся в списке, завершены или были остановлены пользователем, имеются необезвреженные угрозы.
	Все проверки, имеющиеся в списке, завершены или были остановлены пользователем. Имеются проверки, завершившиеся из-за ошибки.

Задачи в списке упорядочены по мере их создания сверху вниз (от самой последней к первой).

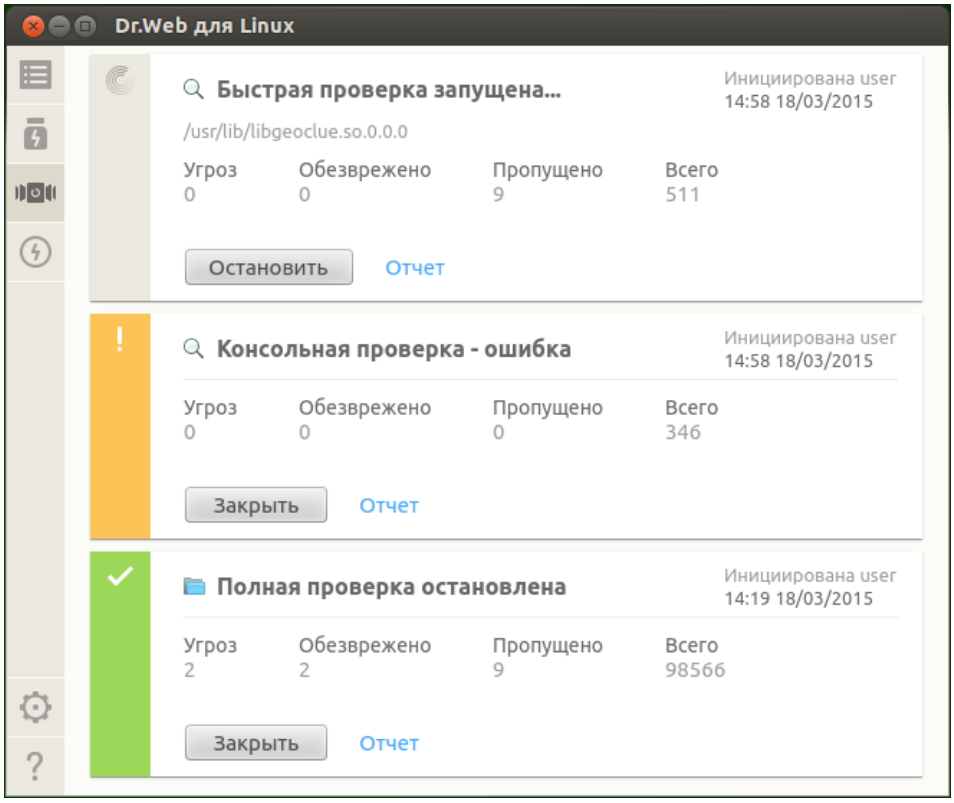

Рисунок 11. Страница просмотра списка проверок

Для каждой задачи выводится следующая информация:

- Тип проверки.
- Имя пользователя, инициировавшего проверку (если имя пользователя неизвестно, выводится его системный идентификатор – *UID*).
- Дата создания задачи и ее окончания, если она уже завершена.
- Количество обнаруженных угроз, обезвреженных угроз, пропущенных файлов и общее количество проверенных объектов.

Состояние, в котором находится задача, указывается при помощи цветовой метки, присвоенной задаче в списке. Используются следующие цвета:

	Проверка еще не завершена или дожидается своей очереди.
	Проверка завершена или остановлена пользователем, угроз не найдено, или все найденные угрозы обезврежены.
	Проверка остановлена из-за возникшей ошибки.
	Проверка завершена или остановлена пользователем, имеются необезвреженные угрозы.

Обратите внимание, что в списке отображаются все проверки, выполняемые Сканером в текущем сеансе работы, а не только те, которые были непосредственно инициированы пользователем в окне Dr.Web Desktop Security Suite (для Linux). Это могут быть проверки следующих дополнительных типов:

- *Консольная проверка* – проверка, инициированная пользователем или какой-либо другой внешней программой через командную строку.
- *Централизованная проверка* – проверка, инициированная сервером централизованной защиты.
- *Проверка по расписанию* – проверка, запущенная автоматически в соответствии с расписанием, заданным в настройках приложения.

На области описания задачи может располагаться одна из следующих кнопок:

- **Отменить** – отменить проверку, дожидающуюся своей очереди. Доступна, если задача ожидает выполнения. После нажатия задача завершается. Информация о задаче остается в списке.
- **Остановить** – остановить начатую проверку без возможности ее возобновления. Доступна, если задача выполняется. После нажатия задача завершается, а в списке остается информация о задаче, содержащая результаты проверки, полученные к моменту остановки.
- **Закрыть** – закрыть информацию о завершенной задаче и удалить ее из списка. Доступна, если задача завершена и не имеется необезвреженных угроз.

- **Обезвредить** – выполнить обезвреживание угроз. Доступна, если задача проверки завершена и имеются необезвреженные угрозы.
- **Подробнее** – перейти к просмотру списка угроз. Доступна, если по результатам обезвреживания некоторые угрозы остались необезвреженными.

Щелчок по ссылке **Отчет** открывает на экране окно отчета, содержащего подробную информацию о проверке, включающую в себя как общую информацию о задаче, так и перечень обнаруженных угроз, если они были обнаружены в ходе этой проверки.

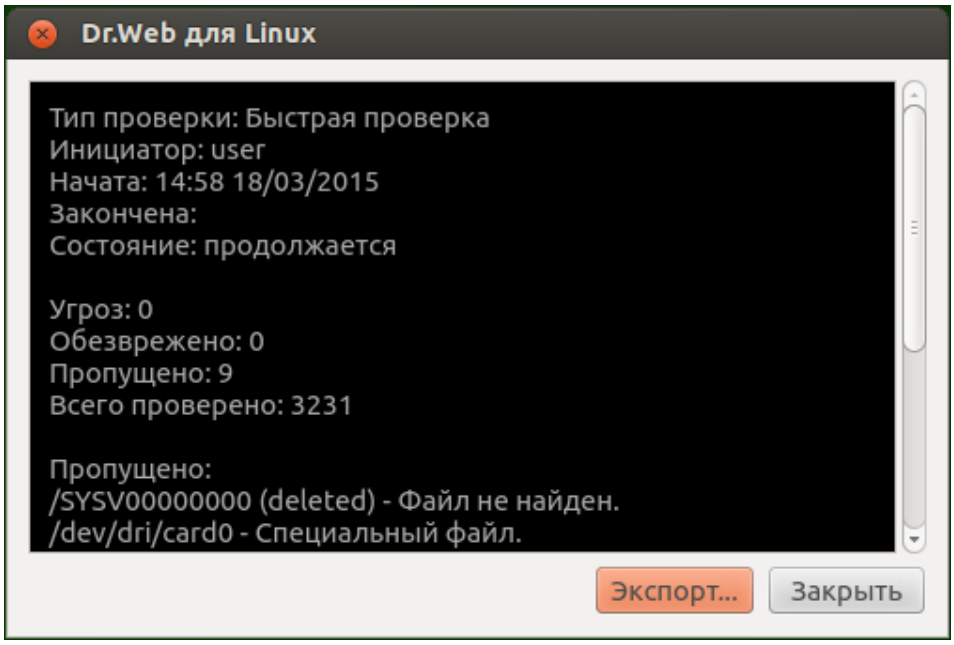

Рисунок 12. Детальная информация о проверке

В файловой системе UNIX-подобных операционных систем, к которым относятся и ОС **GNU/Linux**, могут встречаться специальные объекты, которые выглядят как файлы, и имеют имя, но по своей природе не являющиеся файлами, содержащими данные (например, это символические ссылки, сокеты, именованные каналы и файлы устройств). В противоположность к *обычным* (*регулярным*) файлам такие объекты носят название *специальных файлов*. Специальные файлы *всегда* пропускаются Dr.Web Desktop Security Suite (для Linux) при проверке.

Щелчок по ссылке с названием обнаруженной угрозы откроет в установленном в системе веб-браузере страницу с информацией об угрозе (производится переход на сайт компании «Доктор Веб», требуется наличие подключения к сети Интернет).

Нажмите кнопку **Экспорт**, если вы хотите сохранить отчет о проверке в текстовый файл. Чтобы закрыть окно подробной информации о проверке, нажмите кнопку **Закрыть**.

К угрозам, обнаруженным Сканером в процессе любой проверки, запущенной через окно Dr.Web Desktop Security Suite (для Linux) (включая проверку по расписанию), применяются действия по их обезвреживанию в соответствии с настройками, указанными на вкладке **Сканер**.

Настройки обезвреживания угроз, заданные на вкладке **Сканер**, не используются для *Централизованной* и *Консольной* проверок.

Общий список всех обнаруженных угроз доступен на странице Просмотра обнаруженных угроз.

Мониторинг файловой системы

Функция постоянного контроля над объектами файловой системы реализуется монитором файловой системы SpIDer Guard.

Графический интерфейс управления Dr.Web Desktop Security Suite (для Linux) позволяет управлять работой SpIDer Guard, а именно:

- Запускать и останавливать монитор файловой системы.
- Просматривать статистику работы компонента и перечень обнаруженных угроз.
- Настраивать следующие параметры работы монитора файловой системы:
  - Реакция на обнаружение угроз.
  - Перечень исключений из проверки.

Управление работой монитора файловой системы

Запуск и остановка монитора файловой системы SpIDer Guard, а также просмотр статистики его работы производятся со специальной страницы окна Dr.Web Desktop Security Suite (для Linux). Чтобы перейти на страницу управления мониторингом, нажмите кнопку **SpIDer Guard** на главной странице.

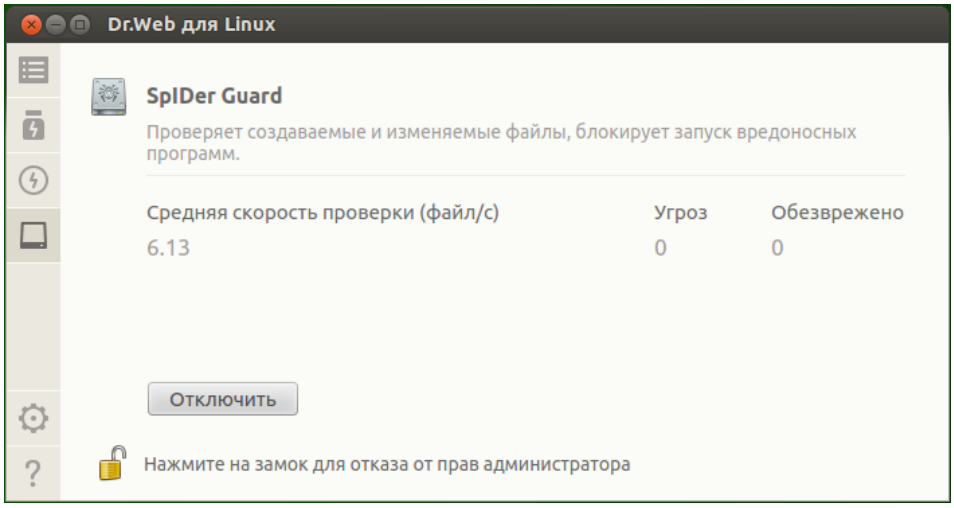

Рисунок 13. Страница управления работой SpIDer Guard

На странице управления мониторингом файловой системы выводится следующая информация:

- Состояние монитора файловой системы SpIDer Guard (включен или отключен), а также, возможно, сведения о произошедшей в процессе его работы ошибке.
- Статистика мониторинга файловой системы:
  - Средняя скорость проверки файлов.
  - Количество обнаруженных и обезвреженных угроз.

Чтобы включить мониторинг, если он отключен, нажмите кнопку **Включить**. Чтобы отключить мониторинг, если он включен, нажмите кнопку **Отключить**.

Для выключения мониторинга файловой системы необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Возможность включения и выключения монитора файловой системы SpIDer Guard при работе Dr.Web Desktop Security Suite (для Linux) под управлением сервера централизованной защиты может быть заблокирована, если это запрещено сервером.

Состояние SpIDer Guard (включен или отключен) иллюстрируется индикатором:

	Монитор файловой системы SpIDer Guard включен и защищает файловую систему.
	Монитор файловой системы SpIDer Guard не защищает файловую систему, потому что отключен пользователем или в силу произошедшей ошибки.

Для закрытия страницы управления мониторингом файловой системы достаточно перейти к любой другой странице при помощи кнопок навигационной панели.

Перечень угроз, обнаруженных SpIDer Guard в текущем сеансе работы Dr.Web Desktop Security Suite (для Linux), отображается на странице просмотра обнаруженных угроз (эта страница доступна только в том случае, если имеются обнаруженные угрозы).

Настройка работы монитора файловой системы

Настройка работы монитора файловой системы SpIDer Guard производится в окне настроек:

- На вкладке **SpIDer Guard** – реакция на обнаруженные угрозы.
- На вкладке **Исключения** – исключение объектов из наблюдения.

Включение усиленного режима мониторинга файлов монитором SplDer Guard описано в разделе <%TARGETTITLE%>.

Проблемы в работе SplDer Guard

В случае возникновения ошибок функционирования SplDer Guard, на странице управления отображается сообщение о возникшей ошибке. Для устранения ошибки воспользуйтесь описанием известных ошибок, приведенным в Приложении Г.

Мониторинг сетевых соединений

Функция постоянного контроля установленных сетевых соединений реализуется монитором SplDer Gate. Он позволяет предотвращать доступ к сайтам, внесенным в черные списки пользователя, а также относящихся к категориям сайтов, указанных как нежелательные для посещения. Кроме этого, SplDer Gate выполняет проверку:

- отправляемых и принимаемых сообщений электронной почты (в том числе – на наличие признаков спама);
- файлов, загружаемых из Интернет.

В случае обнаружения угроз в проверенном объекте, SplDer Gate блокирует его прием или передачу, а угрозы, обнаруженные в сообщении электронной почты, помещаются в архив, защищенный паролем.

Графический интерфейс управления Dr.Web Desktop Security Suite (для Linux) позволяет управлять работой SplDer Gate, а именно:

- Запускать и останавливать мониторинг сетевых соединений.
- Просматривать количество проверенных и заблокированных объектов и попыток доступа к сайтам.
- Настраивать следующие параметры работы мониторинга сетевых соединений:
  - Выбирать тип проверяемого трафика (веб-трафик, исходящие сообщения электронной почты, входящие сообщения электронной почты).
  - Перечень категорий сайтов, доступ к которым запрещается.
  - Персональные черные и белые списки сайтов пользователя.
  - Параметры проверки файлов, загружаемых из сети Интернет или передаваемых по электронной почте.

Даже если прием и передача файлов и сообщений электронной почты не контролируются SplDer Gate, угрозы, содержащиеся в них, могут быть обнаружены работающим монитором файловой системы SplDer Guard в момент их сохранения почтовым клиентом в виде файлов в локальную файловую систему.

Управление работой монитора сетевых соединений

Запуск и остановка монитора сетевых соединений SpIDer Gate, а также просмотр статистики его работы производятся со специальной страницы окна Dr.Web Desktop Security Suite (для Linux). Чтобы перейти на страницу управления мониторингом сетевых соединений, нажмите кнопку **SpIDer Gate** на главной странице.

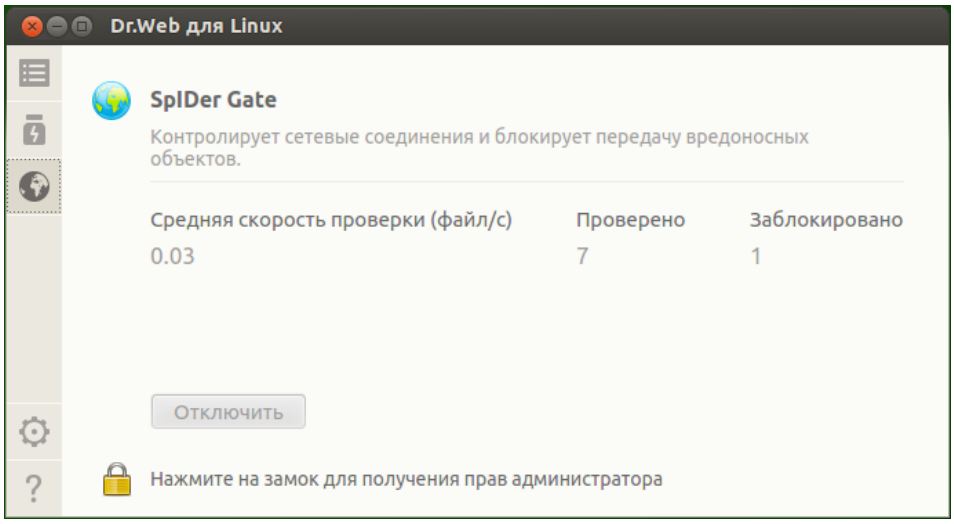

Рисунок 14. Страница управления работой SpIDer Gate

На странице управления мониторингом сетевых соединений выводится следующая информация:

- Состояние монитора сетевых соединений SpIDer Gate (включен или отключен), а также, возможно, сведения о произошедшей в процессе его работы ошибке.
- Статистика мониторинга:
  - Средняя скорость проверки сообщений электронной почты и файлов, загружаемых из Интернет.
  - Количество проверенных объектов (сообщений электронной почты, файлов, загруженных из Интернет, а также URL).
  - Количество заблокированных обращений к сайтам и объектов, содержащих угрозы.

Чтобы включить мониторинг, если он отключен, нажмите кнопку **Включить**. Чтобы отключить мониторинг, если он включен, нажмите кнопку **Отключить**.

Для выключения мониторинга сетевых соединений необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Возможность включения и выключения монитора сетевых соединений SpIDer Gate при работе Dr.Web Desktop Security Suite (для Linux) под управлением сервера централизованной защиты может быть заблокирована, если это запрещено сервером.

Состояние монитора сетевых соединений SpIDer Gate (включен или отключен) иллюстрируется индикатором:

	SpIDer Gate включен и контролирует сетевые соединения (прием и передачу электронной почты, а также доступ к сети Интернет).
	SpIDer Gate не контролирует сетевые соединения (доступ к сайтам не ограничивается, сообщения электронной почты при их приеме и передаче, а также загружаемые из сети файлы не проверяются), потому что отключен пользователем или в силу произошедшей ошибки.

Если в системе запущен почтовый клиент (такой, как **Mozilla Thunderbird**), использующий для получения сообщений электронной почты протокол IMAP, его необходимо перезапустить после включения монитора SpIDer Gate для обеспечения проверки входящих писем.

Для закрытия страницы управления мониторингом сетевых соединений достаточно перейти к любой другой странице при помощи кнопок навигационной панели.

Настройка работы монитора сетевых соединений

Настройка работы монитора сетевых соединений SpIDer Gate производится в окне настроек:

- на вкладке **SpIDer Gate** – указание перечня блокируемых категорий сайтов и реакция на обнаруженные угрозы.
- на вкладке **Исключения** – управление черными и белыми списками сайтов, а также исключение из наблюдения сетевой активности приложений.
- на вкладке **Сеть** – управление проверкой защищенных сетевых соединений (SSL/TLS).

Проблемы в работе монитора сетевых соединений

В случае возникновения ошибок функционирования монитора сетевых соединений, на странице управления отображается сообщение о возникшей ошибке. Для устранения

ошибки воспользуйтесь описанием известных ошибок, приведенным в разделе Приложение Г. Описание известных ошибок.

В зависимости от поставки, компонент Dr.Web Anti-Spam может отсутствовать в составе продукта. В этом случае спам-проверка сообщений не производится.

Если какие-либо сообщения электронной почты неправильно распознаются компонентом Dr.Web Anti-Spam, рекомендуется пересылать их на специальные почтовые адреса для анализа и повышения качества работы спам-фильтра:

- письма, ошибочно *оцененные как спам*, отправляйте на адрес vrnonspam@drweb.com;
- письма, ошибочно *не определенные как спам*, отправляйте на адрес vrspam@drweb.com.

Каждое сообщение, подлежащие анализу, следует предварительно сохранить в файл (используйте формат `.eml`). Сохраненные файлы прикрепите к сообщению, отправляемому на соответствующий служебный адрес.

Просмотр обнаруженных угроз

Список угроз, обнаруженных Сканером и монитором файловой системы SpIDer Guard во время текущего сеанса работы Dr.Web Desktop Security Suite (для Linux), отображается на специальной странице окна, которая доступна только в том случае, если была обнаружена хотя бы одна угроза.

В случае если были обнаружены угрозы, то, чтобы открыть страницу со списком угроз, нажмите кнопку  на навигационной панели.

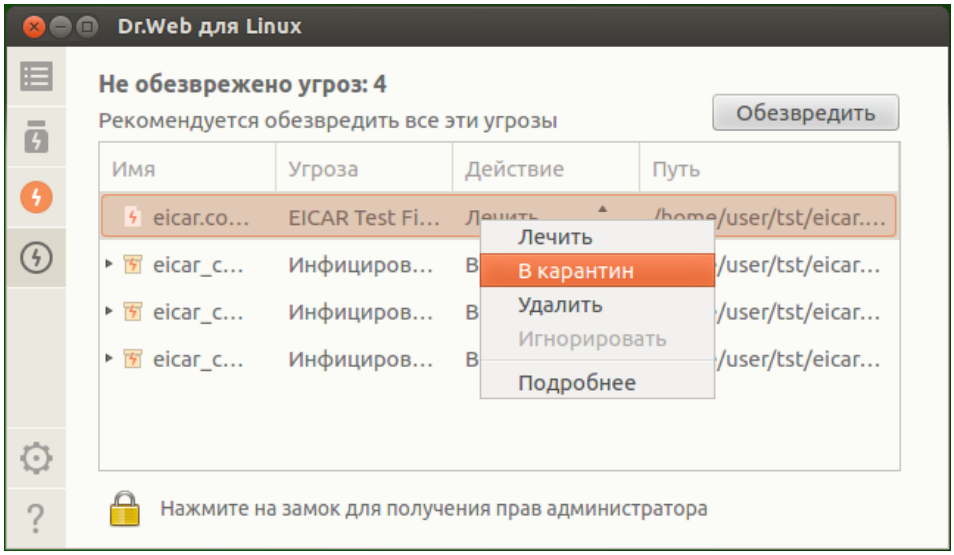

Рисунок 15. Страница обзора угроз

В списке для каждой обнаруженной угрозы выводится следующая информация:

- Имя объекта, содержащего угрозу.
- Имя угрозы, содержащейся в объекте (по классификации «Доктор Веб»).
- Действие, которое будет применено к объекту для нейтрализации угрозы (или уже было применено, если угроза нейтрализована).
- Путь к объекту файловой системы, в котором эта угроза была обнаружена.

Уже обезвреженные угрозы в списке представлены в списке неактивными строками.

Обезвреживание обнаруженных угроз

Если в списке имеются необезвреженные угрозы, на странице, непосредственно над списком, доступна кнопка **Обезвредить**, при нажатии на которую ко всем угрозам, представленным в списке, будут применены действия по их обезвреживанию, указанные в поле *Действие* у каждой необезвреженной угрозы. Если угроза обезвреживается успешно, ее строка в таблице становится неактивной. Если попытка обезвреживания оказывается неудачной, то строка, содержащая сведения об угрозе, остается активной, текст в строке окрашивается в красный цвет, а в поле *Действие* выводится информация об ошибке.

По умолчанию в списке в качестве действий выбираются действия, заданные в качестве реакций на угрозу в настройках компонента, обнаружившего угрозу. Действия, которые по умолчанию выбираются для угроз, обнаруживаемых Сканером и монитором файловой системы SplDer Guard, могут быть изменены на соответствующих вкладках окна настроек.

Если требуется применить к угрозе действие, отличное от представленного в списке, щелкните по полю *Действие* в строке угрозы и выберите требуемое действие в появившемся контекстном меню.

Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления выполняется перемещение контейнера в карантин.

Имеется возможность выделения набора угроз в списке. Для этого нужно выделять их мышью, удерживая нажатой клавишу CTRL или SHIFT:

- При удержании CTRL угрозы будут добавляться в список выделения по одной.
- При удержании клавиши SHIFT угрозы выделяются непрерывным списком.

После выбора угроз, для применения к ним некоторого действия, нажмите правую кнопку мыши в области списка и выберите требуемое действие в появившемся выпадающем меню. Действие, выбранное в меню, будет применено ко всем выделенным угрозам.

Обратите внимание, что:

- Если угроза была обнаружена в составном объекте (архив, сообщение электронной почты и т.п.), то выбранное действие применяется не ко вложенному инфицированному объекту, а ко всему контейнеру целиком.
- Действие *Лечить* может быть применено не ко всем типам угроз.

В случае необходимости, для успешного применения действий к угрозам, повысьте права приложения.

Просмотр информации об угрозах

Для получения детальной информации о любой обнаруженной угрозе нажмите правую кнопку мыши в строке информации об угрозе и выберите в появившемся контекстном меню пункт **Подробнее**. После этого на экране появится окно, содержащее подробную информацию об угрозе и содержащем ее объекте. Если требуется получить подробную информацию сразу о нескольких угрозах, выделите в списке мышью, удерживая нажатой клавишу CTRL, перед вызовом контекстного меню.

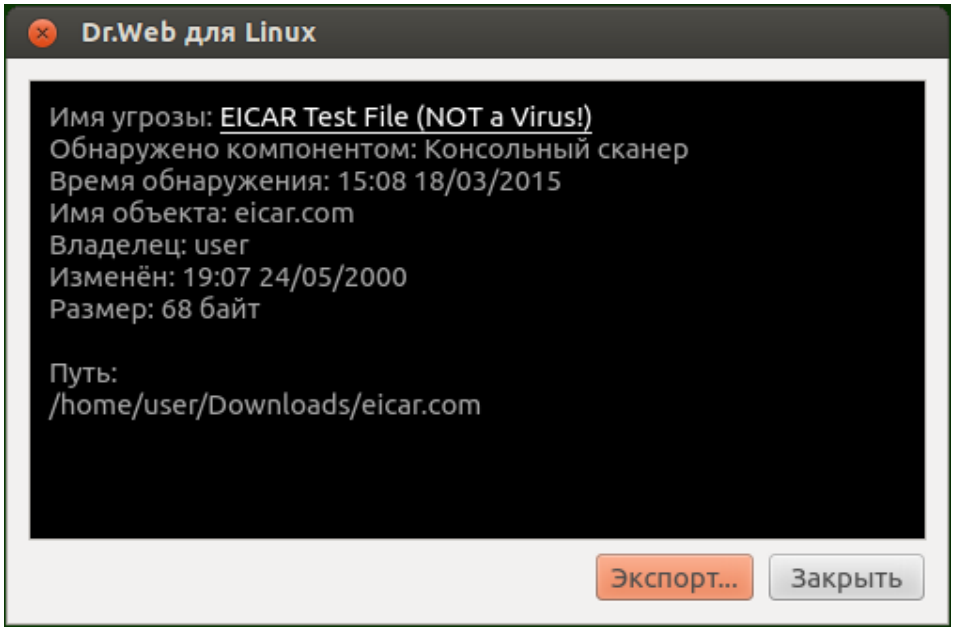

Рисунок 16. Информация об угрозе

В этом окне отображается следующая информация:

- Имя угрозы (по классификации «Доктор Веб»).
- Название компонента Dr.Web Desktop Security Suite (для Linux), обнаружившего угрозу.
- Дата и время обнаружения угрозы.
- Информация об объекте файловой системы, в котором эта угроза была обнаружена: имя, пользователь-владелец объекта, дата последнего изменения и путь к объекту в файловой системе.

- Последнее действие, которое применялось к угрозе, и его результат (если в настройках компонента, обнаружившего угрозу, задано автоматическое применение действий, например, для Сканера оно может быть задано на соответствующей вкладке окна настроек).

Щелчок по ссылке с именем угрозы откроет в установленном в системе веб-браузере веб-страницу с описанием угрозы (происходит переход на сайт компании «Доктор Веб», требуется подключение к сети Интернет).

Нажмите кнопку **Экспорт**, если вы хотите сохранить информацию, показанную в окне, в текстовый файл (по нажатию кнопки откроется окно выбора файла для сохранения информации). Чтобы закрыть окно подробной информации об угрозе и содержащем ее объекте, нажмите кнопку **Закрыть**.

Управление карантином

Список объектов, изолированных Dr.Web Desktop Security Suite (для Linux) в карантин, отображается на специальной странице. Чтобы ее открыть, нажмите кнопку  на навигационной панели.

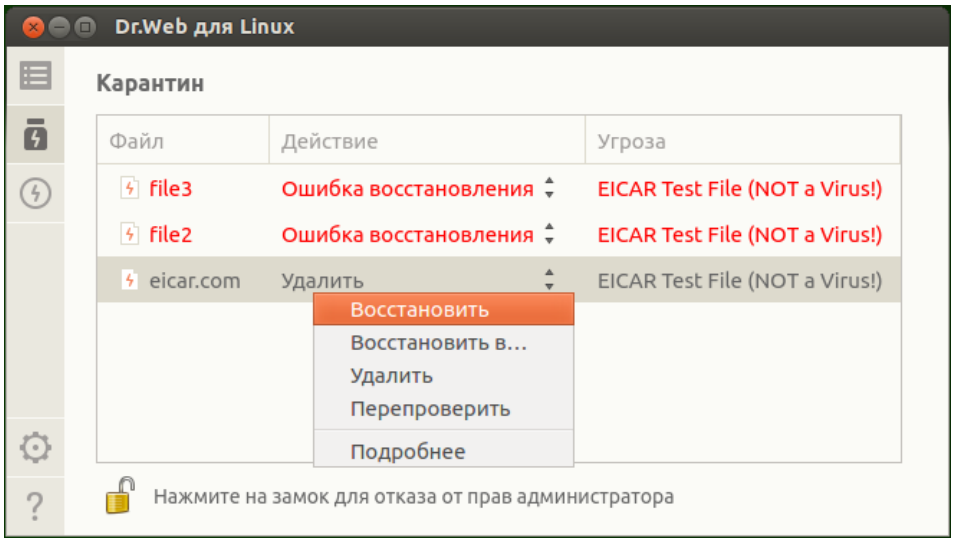

Рисунок 17. Страница управления карантином

Если карантин не пуст, в списке для каждой обнаруженной угрозы выводится следующая информация:

- Имя объекта, содержащего угрозу.
- Действие, которое следует применить к объекту в карантине.
- Имя угрозы, содержащейся в объекте (по классификации «Доктор Веб»).

Применение действий к изолированным объектам

Для выполнения какого-либо действия с изолированным в карантин объектом, следует щелкнуть правой кнопкой мыши в строке, содержащей информацию об объекте, и выбрать требуемое действие в появившемся контекстном меню. Если требуется совершить некоторое действие с несколькими изолированными объектами, их следует перед вызовом контекстного меню выделить в списке. Выделение осуществляется мышью при нажатой клавише CTRL или SHIFT:

- При удержании CTRL изолированные объекты будут добавляться в список выделения по одному.
- При удержании клавиши SHIFT изолированные объекты выделяются непрерывным списком.

В меню доступны следующие действия:

- **Восстановить** – восстановление выделенных объектов в их исходные места в файловой системе.
- **Восстановить в** – восстановление выделенных объектов в выбранное место в файловой системе (откроется окно выбора каталога для восстановления).
- **Удалить** – необратимое удаление выделенных объектов.
- **Перепроверить** – выполнить повторную проверку выделенных объектов и их излечение, если это возможно.

В случае если выбранное действие применяется к выделенному объекту успешно, его строка исчезает из таблицы. В случае если попытка оказывается неудачной, строка, содержащая сведения об изолированном объекте, остается активной, текст в строке окрашивается в красный цвет, а в поле *Действие* выводится информация об ошибке.

Для успешного применения действий к изолированным объектам может потребоваться повышение прав приложения. Например, повышение прав необходимо, чтобы применять действия к объектам, помещенным в карантин любым из пользователей.

Просмотр информации об изолированных объектах

Для получения детальной информации о любом изолированном объекте необходимо нажать правую кнопку мыши в строке информации об этом объекте и выбрать в появившемся контекстном меню пункт **Подробнее**. После этого на экране появится окно, содержащее подробную информацию об объекте. Если требуется получить подробную информацию сразу о нескольких изолированных объектах, их следует перед вызовом контекстного меню выделить в списке мышью, удерживая нажатой клавишу CTRL.

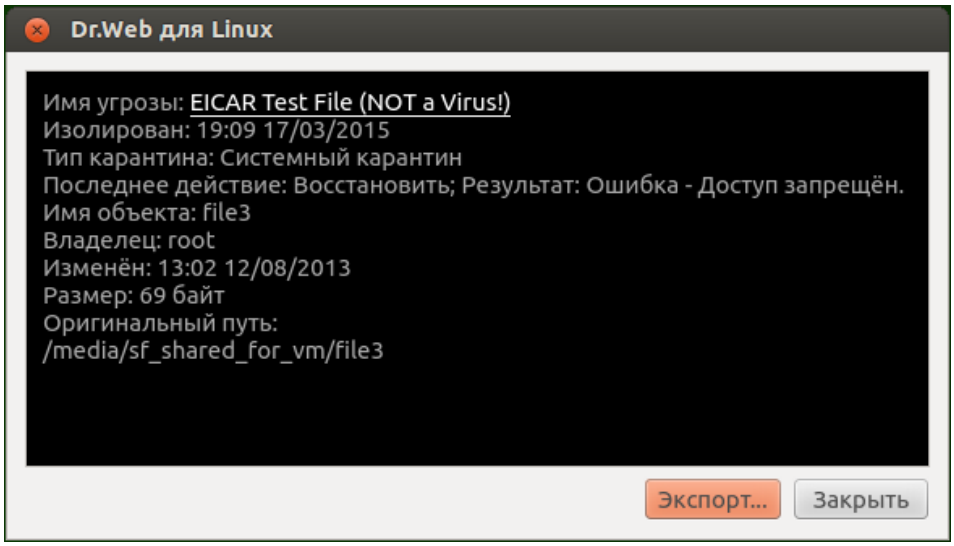

Рисунок 18. Информация об изолированном объекте

В этом окне отображается следующая информация:

- Имя угрозы (по классификации «Доктор Веб»).
- Дата и время изоляции объекта в карантин.
- Тип карантина, в который изолирован объект.
- Наименование и результат последнего действия, которое применялось к объекту.
- Информация об изолированном объекте файловой системы: имя, пользователь-владелец объекта, дата последнего изменения и путь к объекту в файловой системе.

Щелчок по ссылке с именем угрозы откроет в установленном в системе веб-браузере веб-страницу с описанием угрозы (происходит переход на сайт компании «Доктор Веб», требуется подключение к сети Интернет).

Нажмите кнопку **Экспорт**, если вы хотите сохранить информацию, показанную в окне, в текстовый файл (по нажатию кнопки откроется окно выбора файла для сохранения информации). Чтобы закрыть окно подробной информации об угрозе и содержащем ее объекте, нажмите кнопку **Закрыть**.

Обновление антивирусной защиты

Периодическое обновление вирусных баз, антивирусного ядра и баз категорий веб-ресурсов производится Компонентом обновления автоматически. Просмотр состояния обновлений и принудительный запуск обновления по требованию производятся со специальной страницы окна Dr.Web Desktop Security Suite (для Linux). Чтобы перейти на страницу управления обновлением, нажмите кнопку **Последнее обновление** на главной странице.

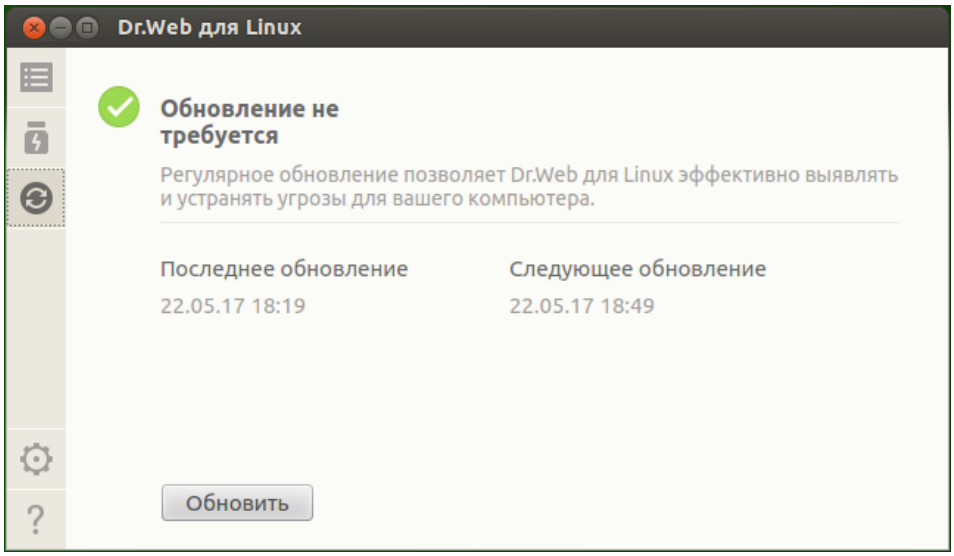

Рисунок 19. Страница управления обновлением

На странице управления обновлением выводится следующая информация:

- Актуальность вирусных баз, антивирусного ядра и баз категорий веб-ресурсов.
- Информация о последнем произведенном обновлении и время следующего планового обновления.

Чтобы выполнить принудительное обновление, нажмите кнопку **Обновить**. Для закрытия страницы управления обновлением достаточно перейти к любой другой странице при помощи кнопок навигационной панели.

> Если Dr.Web Desktop Security Suite (для Linux) работает в режиме централизованной защиты, эта страница будет заблокирована.

Настройка обновлений

Настройка обновлений Dr.Web Desktop Security Suite (для Linux) производится на окне настроек, на вкладке **Основные**.

Проблемы в работе компонента обновлений

В случае возникновения ошибок функционирования Компонента обновления, на странице управления обновлением отображается сообщение о возникшей ошибке. Для устранения ошибки воспользуйтесь описанием известных ошибок, приведенным в Приложении Г.

Менеджер лицензий

Менеджер лицензий позволяет просмотреть в графическом режиме информацию о текущей лицензии, которая выдана пользователю Dr.Web Desktop Security Suite (для Linux).

Данные лицензии, выданной пользователю, хранятся в лицензионном ключевом файле, обеспечивающем работу Dr.Web Desktop Security Suite (для Linux) на компьютере пользователя. В случае отсутствия на компьютере лицензионного или демонстрационного ключевого файла все антивирусные функции Dr.Web Desktop Security Suite (для Linux) (проверка и мониторинг объектов файловой системы, обновление вирусных баз) будут заблокированы.

Запуск Менеджера лицензий

Менеджер лицензий интегрирован в окно Dr.Web Desktop Security Suite (для Linux). Чтобы открыть страницу Менеджера лицензий, нажмите кнопку **Лицензия** на главной странице окна.

Если на компьютере уже установлен ключевой файл, связанный с некоторой лицензией на использование Dr.Web Desktop Security Suite (для Linux), выданной пользователю, или с активным демонстрационным периодом, то на начальной странице Менеджера лицензий отображаются данные о лицензии, такие, как ее номер, имя владельца, а также срок действия, извлеченные из ключевого файла.

Вид страницы просмотра данных о лицензии представлен на рисунке ниже.

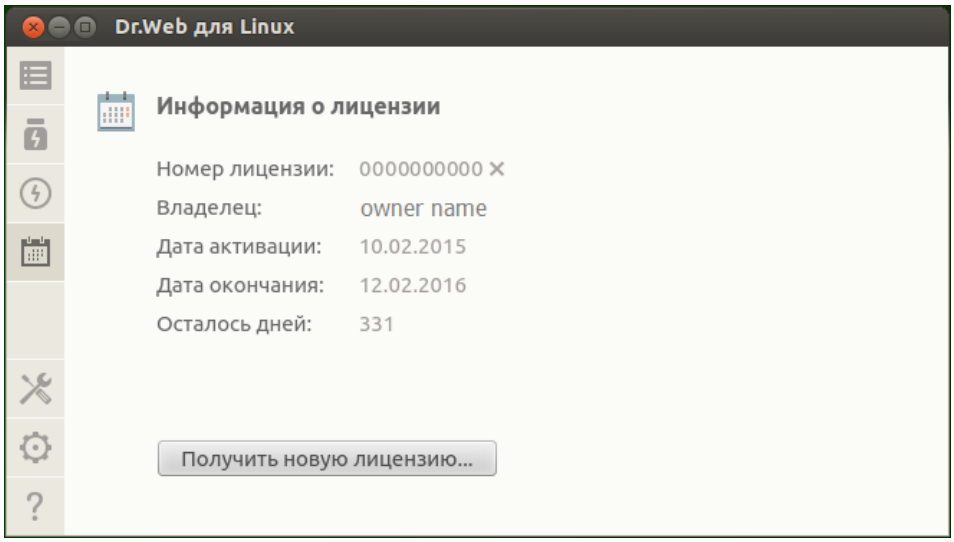

Рисунок 20. Информация о лицензии

Нажатие на символ ✕ справа от номера лицензии позволяет удалить ключевой файл.

Вы можете закрыть Менеджер лицензий, перейдя к любой другой странице при помощи кнопок навигационной панели.

Активация лицензии

Для того чтобы при помощи Менеджера лицензий активировать лицензию (в том числе – приобрести новую лицензию или продлить текущую) или демонстрационный период, и

получить на компьютер соответствующий ключевой файл, обеспечивающий работу Dr.Web Desktop Security Suite (для Linux), нажмите кнопку **Получить новую лицензию**. После этого на экране появится мастер регистрации. Обратите внимание, что мастер регистрации также отображается автоматически при первом запуске Dr.Web Desktop Security Suite (для Linux) после его инсталляции.

На первом этапе активации необходимо выбрать способ активации. Доступно три способа:

1. Активация лицензии или демонстрационного периода по имеющемуся серийному номеру.
2. Получение демонстрационного периода.
3. Установка ключевого файла, полученного ранее.

> Для регистрации серийного номера и для получения демонстрационного периода требуется наличие подключения к сети Интернет.

1. Активация лицензии или демонстрационного периода при помощи серийного номера

Для активации лицензии или демонстрационного периода при помощи имеющегося у вас серийного номера, введите символы имеющегося у вас серийного номера в поле ввода и нажмите кнопку **Активировать**.

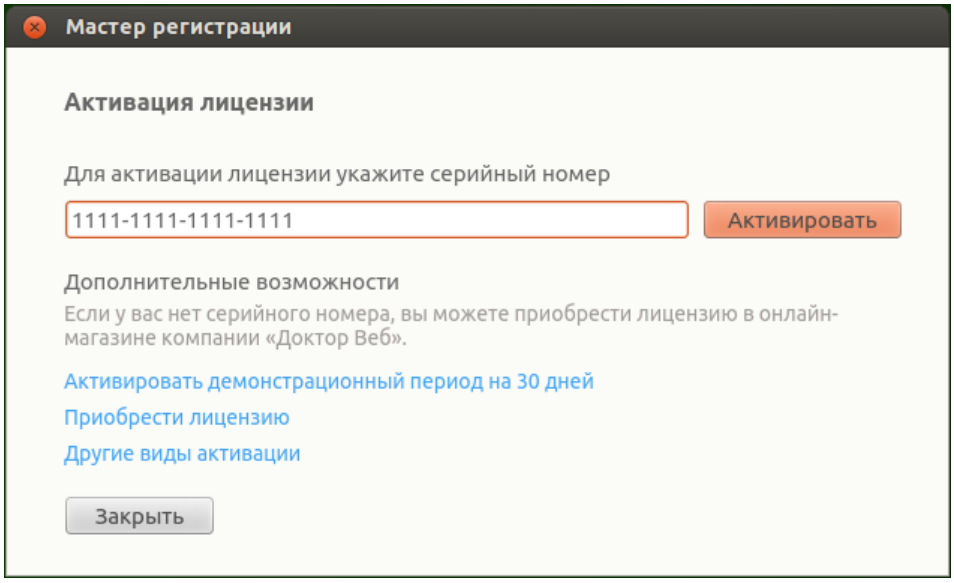

Рисунок 21. Регистрация при помощи серийного номера

Если у вас нет серийного номера или действующего ключевого файла, то вы можете приобрести лицензию в онлайн-магазине компании «Доктор Веб», перейдя по ссылке **Приобрести лицензию**.

О дополнительных способах приобретения лицензии на продукты Dr.Web см. в разделе Лицензирование.

После нажатия кнопки **Активировать** будет произведено подключение к серверу регистрации компании «Доктор Веб».

Если указанный вами серийный номер был получен на сайте компании «Доктор Веб» для активации демонстрационного периода сроком на 3 месяца, то дополнительных шагов для активации не потребуется.

Если указанный на первом шаге серийный номер входит в комплект из двух серийных номеров, то далее вам нужно выбрать, на каком количестве компьютеров вы планируете использовать продукт. Если вы выберете вариант **На двух компьютерах**, то второй серийный номер из этого комплекта вы сможете активировать на еще одном компьютере и получить второй лицензионный ключевой файл. При этом для обоих компьютеров выданные лицензии будут действительны в течение одинакового срока (например, на год). Если же вы выберете вариант **На одном компьютере**, то вам необходимо будет указать второй серийный номер из комплекта. В дальнейшем вы уже не сможете зарегистрировать этот серийный номер на другом компьютере (также как и использовать на нем копию лицензионного ключевого файла, полученного вами в результате активации объединенной лицензии), но для текущего компьютера срок действия лицензии будет увеличен вдвое (например, до двух лет, если лицензия была выдана сроком на год).

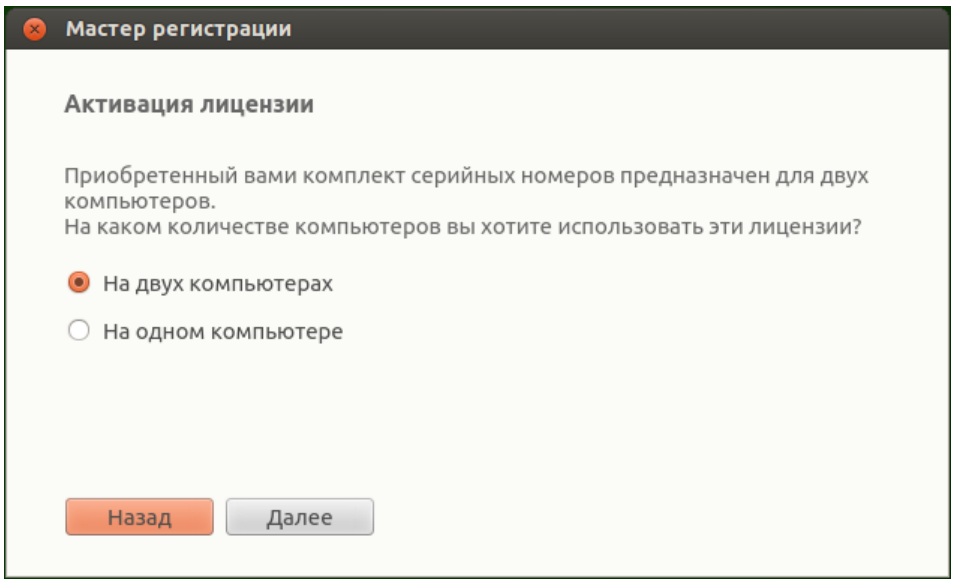

Рисунок 22. Выбор количества компьютеров

После выбора количества компьютеров, для которого может быть активирована лицензия, нажмите кнопку **Далее**, и, если вы выбрали вариант **На одном компьютере**,

укажите на появившейся странице мастера второй серийный номер из комплекта, после чего еще раз нажмите **Далее**.

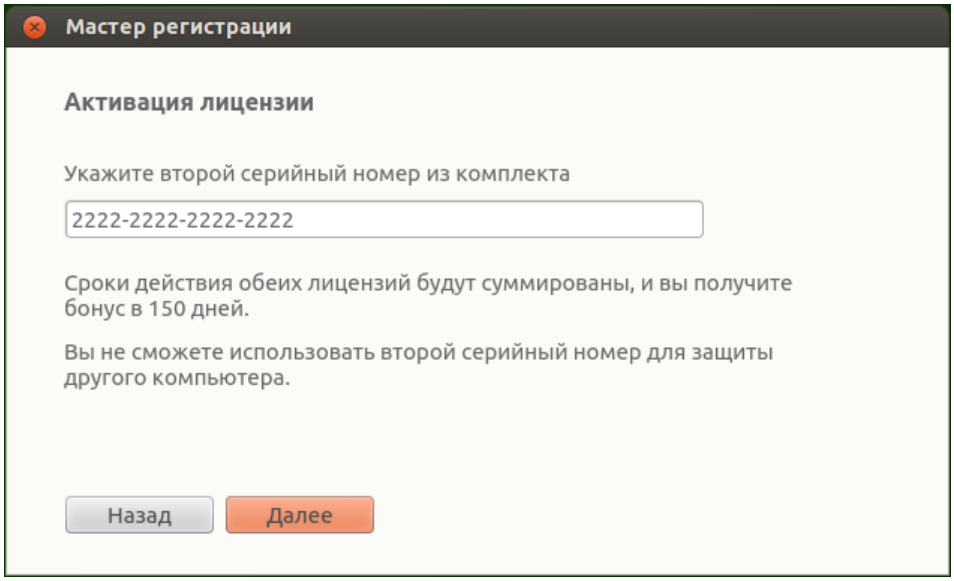

Рисунок 23. Указание второго серийного номера из комплекта

Далее вам будет предложено получить бонус в 150 дней к сроку действия активируемой лицензии. Для этого будет необходимо указать информацию о предыдущей приобретенной вами лицензии, если она у вас имеется. Если вы хотите получить бонус, то выберите пункт **Указать предыдущую лицензию**, а если вы не хотите получать бонус, или вы не имеете предыдущей лицензии, выберите пункт **У меня нет предыдущей лицензии**, после чего нажмите **Далее**.

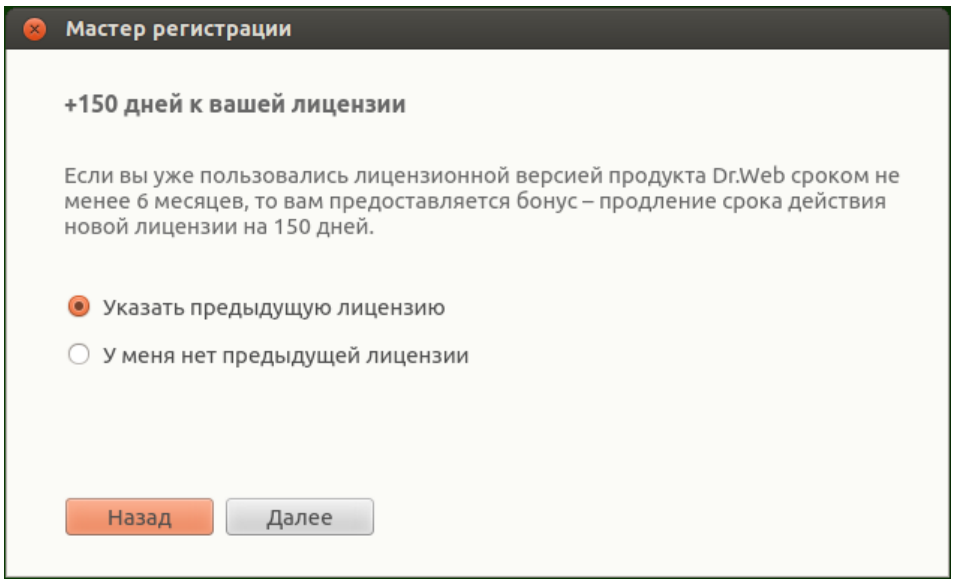

Рисунок 24. Получение бонуса

Если на первом шаге вы указали специальный *серийный номер продления,* то, вместо предложения получения бонуса вам будет предложено указать предыдущую лицензию, чтобы не потерять 150 дней из срока действия активируемой лицензии. Если в этом

случае вы выберете пункт **У меня нет предыдущей лицензии**, то вы уменьшите срок действия новой лицензии на 150 дней.

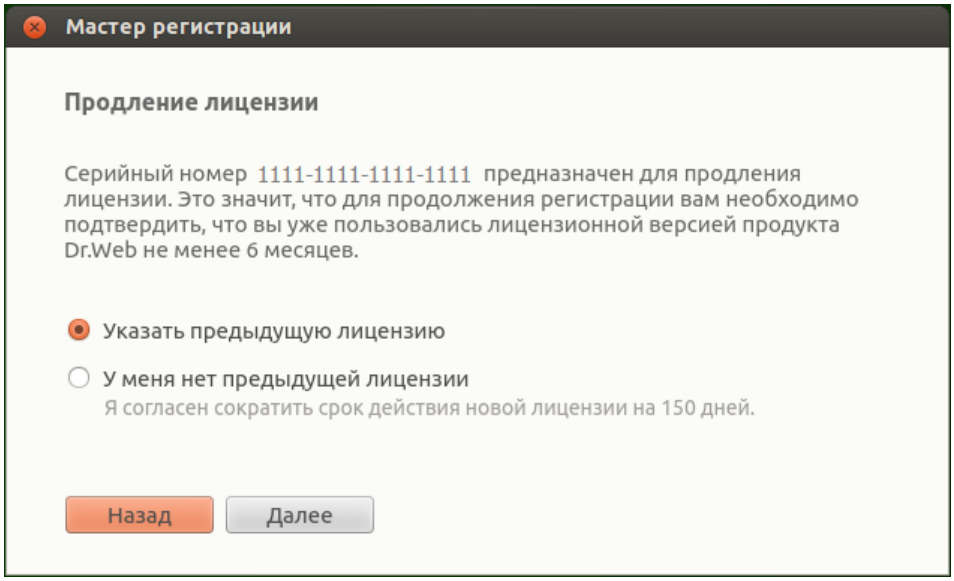

Рисунок 25. Продление лицензии

Если вы выбрали пункт **Указать предыдущую лицензию**, то в появившемся окне вам следует указать серийный номер предыдущей лицензии, или указать путь к связанному с ней ключевому файлу.

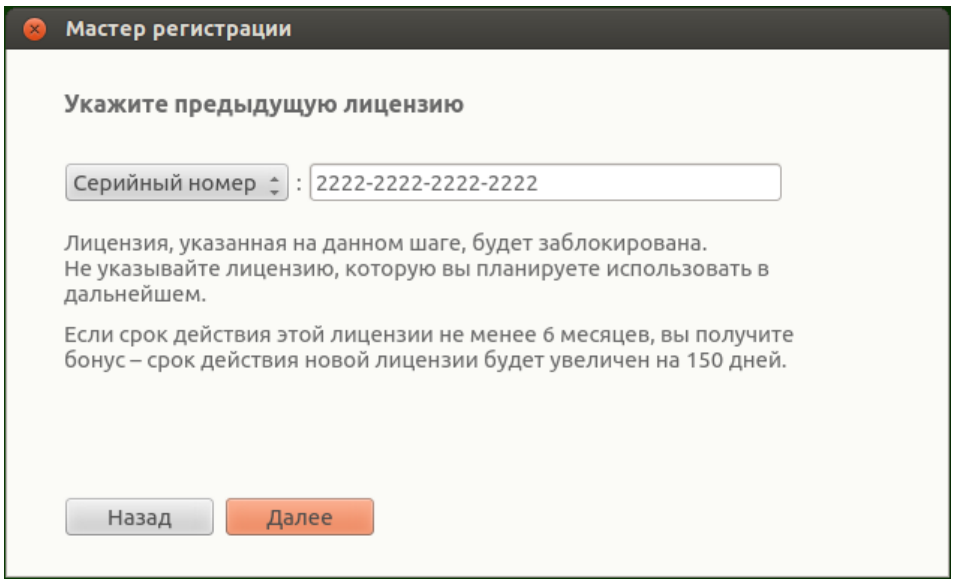

Рисунок 26. Указание предыдущей лицензии

Если вы укажете на этом шаге лицензию, срок действия которой еще не истек, то срок действия активируемой лицензии будет дополнительно продлен и на остаток срока действия старой лицензии. В случае активации комплекта из двух серийных номеров, порядок обработки бонуса зависит от того, какой вариант использования был выбран на предыдущем шаге мастера регистрации:

- **На двух компьютерах**, *и это первый компьютер*. Для получения бонуса для первого компьютера, вы должны использовать на данном шаге предыдущую

лицензию, выданную для этого компьютера, если она имеется. *Второй серийный номер из комплекта здесь указывать нельзя*.

- **На двух компьютерах**, *и это второй компьютер*. Для получения бонуса для второго компьютера, вы должны использовать на данном шаге предыдущую лицензию, выданную для этого компьютера, если она имеется. *Первый серийный номер из комплекта здесь указывать нельзя*.
- **На одном компьютере**. В этом случае не только удваивается срок действия активируемой лицензии, но к нему также автоматически прибавляется бонус (первый серийный номер дает бонус для второго номера). Кроме этого, если вы на данном шаге дополнительно укажете предыдущую лицензию, выданную для этого компьютера, если она имеется, то к удвоенному сроку действия активируемой лицензии также прибавится бонус и остаток срока действия указанной лицензии, если он имеется.

Для указания на предыдущую лицензию можно ввести ее серийный номер в соответствующее поле или указать связанный с ней ключевой файл. Тип указания информации о предыдущей лицензии выбирается из выпадающего списка, расположенного слева от поля ввода. Для указания ключевого файла вы можете:

- Ввести путь к нему непосредственно в строку ввода.
- Воспользоваться стандартным окном выбора файлов графической оболочки, нажав кнопку **Обзор**.
- Перетащить его мышью на страницу мастера из окна файлового менеджера.

Вместо ключевого файла вы можете указать файл zip-архива, содержащего ключевой файл, распаковки архива при этом не требуется.

Для продолжения активации нажмите кнопку **Далее**.

На следующем шаге требуется указать корректную регистрационную информацию, которая включает следующие данные:

- Регистрационное имя.
- Регион (страна) нахождения, выбирается из списка.
- Корректный адрес электронной почты.

Все поля регистрационной формы являются обязательными для заполнения.

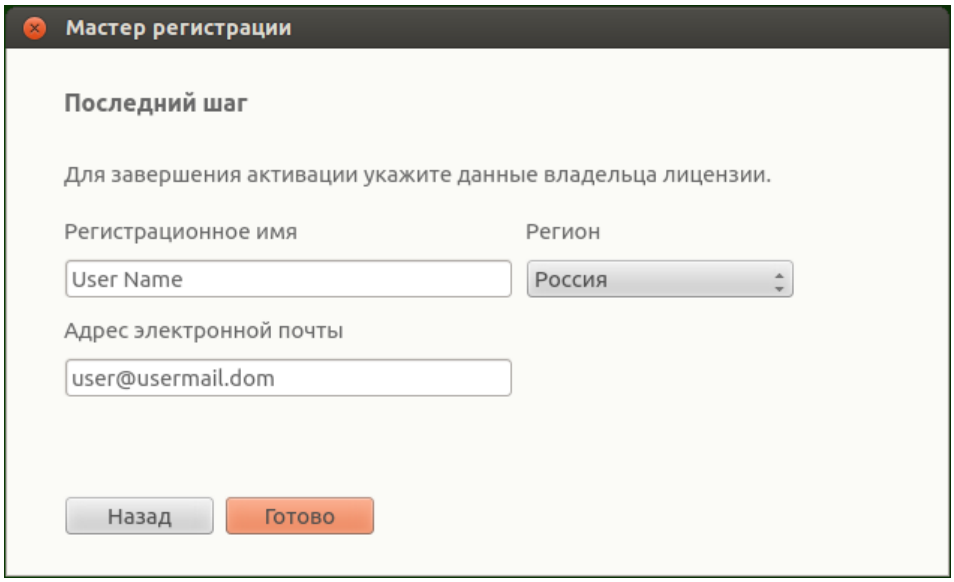

Рисунок 27. Регистрационная информация пользователя

После заполнения всех полей формы нажмите кнопку **Готово** для подключения к серверу и получения лицензионного ключевого файла. При необходимости вы сможете перенести полученный лицензионный ключевой файл на любой компьютер при условии, что вы перестанете использовать его на этом компьютере.

2. Получение демонстрационного периода

Если требуется получить демонстрационный период для работы Dr.Web Desktop Security Suite (для Linux) в течение 30 дней, перейдите на первом шаге активации по ссылке **Активировать демонстрационный период на 30 дней**.

При получении демонстрационного периода сроком на 1 месяц через Менеджер лицензий вам не требуется указывать свои персональные данные. Однако вы можете зарегистрироваться на официальном сайте компании «Доктор Веб» и получить серийный номер, предоставляющий демонстрационный период сроком на 3 месяца.

Демонстрационный период для одного и того же компьютера может быть выдан повторно только по истечении определенного периода времени. Подробнее см. в разделе Лицензирование.

3. Установка имеющегося ключевого файла

Если вы уже имеете действующую лицензию и связанный с ней ключевой файл (возможно, полученный от компании «Доктор Веб» или ее партнеров по электронной почте), то вы можете активировать Dr.Web Desktop Security Suite (для Linux), установив этот ключевой файл. Для этого на первом шаге активации щелкните по ссылке **Другие виды активации**, после чего укажите в появившемся поле ввода путь к имеющемуся у вас ключевому файлу.

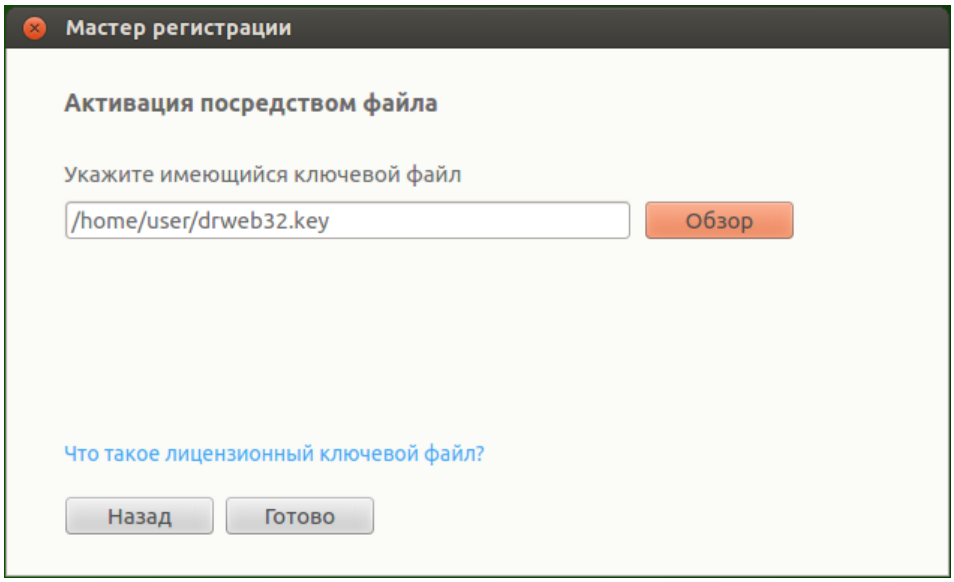

Рисунок 28. Активация посредством ключевого файла

Для указания ключевого файла вы можете:

- Ввести путь к нему непосредственно в строку ввода.
- Воспользоваться стандартным окном выбора файлов графической оболочки, нажав кнопку **Обзор**.
- Перетащить его мышью на страницу мастера из окна файлового менеджера.

Вместо ключевого файла вы можете указать файл zip-архива, содержащего ключевой файл, распаковки архива при этом не требуется.

После указания пути к ключевому файлу (или содержащему его архиву) нажмите кнопку **Готово** для автоматической установки ключевого файла. Ключевой файл будет при необходимости распакован и скопирован в каталог служебных файлов Dr.Web Desktop Security Suite (для Linux). Подключения к сети Интернет в данном случае не требуется.

В случае успешного завершения процесса активации (любым из описанных выше способов) на экране будет показана финальная страница мастера регистрации с сообщением об успешной активации лицензии или демонстрационного периода. Нажмите кнопку **ОК** для закрытия мастера регистрации и возвращения на главную страницу окна Dr.Web Desktop Security Suite (для Linux).

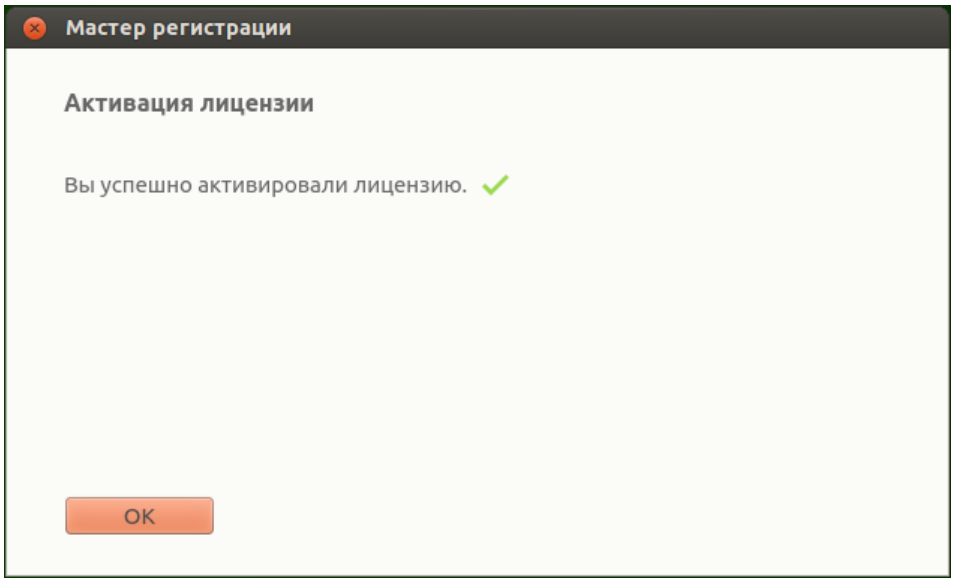

Рисунок 29. Сообщение об успешной активации

В случае если на каком-либо из этапов регистрации возникнет ошибка, появится страница с соответствующим сообщением и кратким описанием ошибки. Пример такой страницы показан ниже.

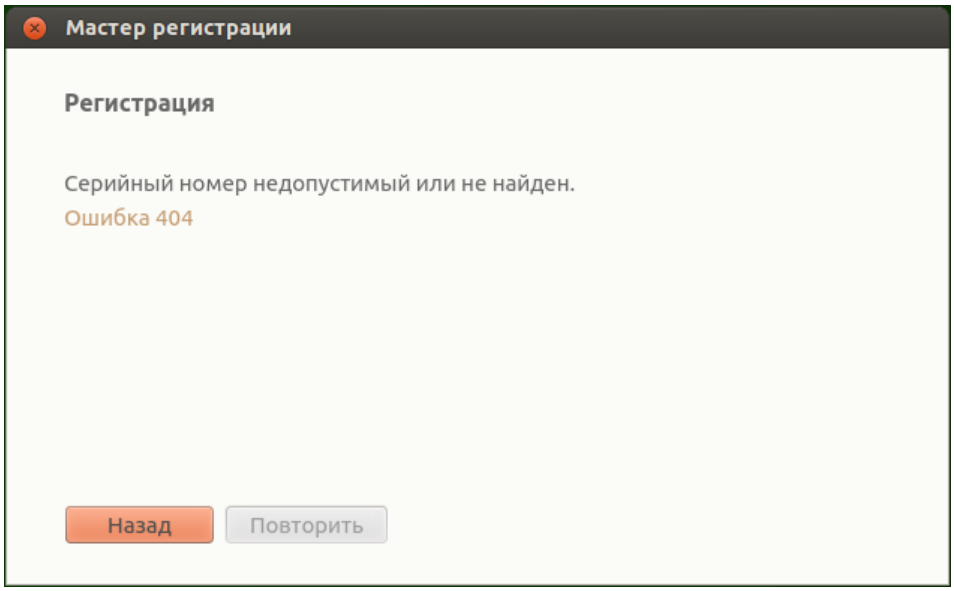

Рисунок 30. Сообщение об ошибке

В этом случае вы имеете возможность вернуться на предыдущий шаг регистрации, чтобы внести исправления (например, исправить серийный номер или указать правильный путь к файлу). Для этого нажмите кнопку **Назад**.

В случае если ошибка связана с временной неполадкой, например, временным сбоем в сети, то вы можете попытаться повторить этот шаг, нажав кнопку **Повторить**. В случае необходимости вы можете нажать кнопку **Закрыть**, чтобы прервать регистрацию и закрыть мастер регистрации. В этом случае вам придется позднее повторить процедуру регистрации заново. Если мастер регистрации не сможет установить соединение с

сервером регистрации компании «Доктор Веб» для проверки введенного серийного номера, будет показана страница с соответствующим сообщением об ошибке.

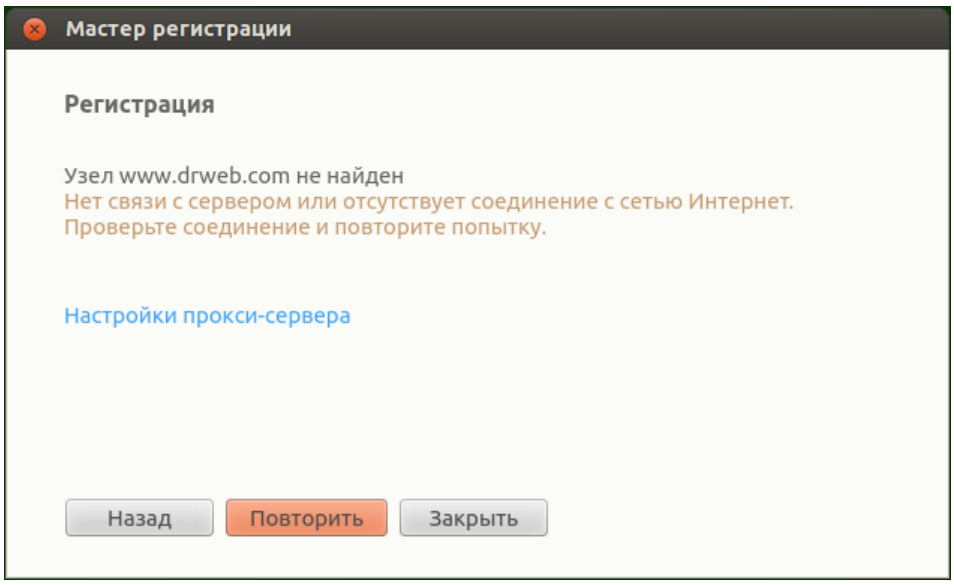

Рисунок 31. Ошибка подключения к серверу регистрации

Если ошибка связана с тем, что у вас отсутствует возможность прямого подключения к сети Интернет, но возможно установление соединения через прокси-сервер, то переход по ссылке **Настройки прокси-сервера** открывает на экране окно настроек использования прокси-сервера:

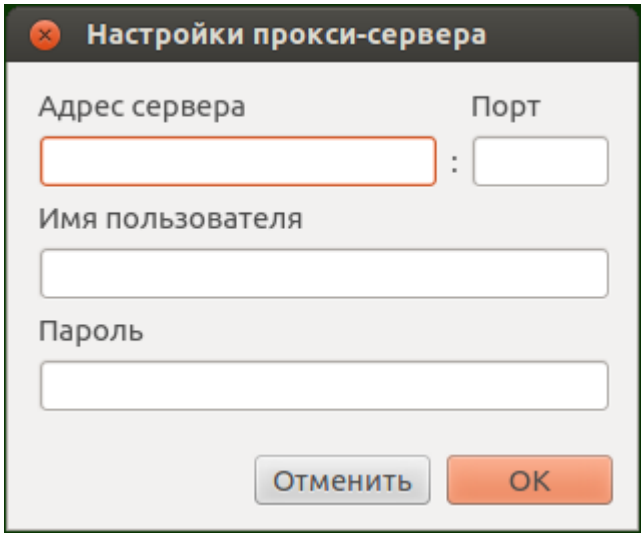

Рисунок 32. Настройки прокси-сервера

В данном окне следует указать параметры доступа к прокси-серверу и нажать кнопку **OK**. Далее следует повторить попытку подключения к серверу регистрации компании «Доктор Веб», нажав кнопку **Повторить**.

При активации новой лицензии и формировании нового ключевого файла, предыдущий ключевой файл, который использовался Dr.Web Desktop Security Suite (для Linux), автоматически сохраняется в виде файла резервной копии в каталоге `/etc/opt/drweb.com`. В случае необходимости вы можете вернуться к его использованию, выполнив процедуру установки ключевого файла.

Удаление лицензионного ключевого файла

В случае необходимости (например, вы решили больше не использовать Dr.Web Desktop Security Suite (для Linux) на этом компьютере, а перенести его на другой компьютер) можно удалить установленный на компьютере лицензионный ключевой файл, управляющий работой Dr.Web Desktop Security Suite (для Linux). Для этого откройте страницу информации о лицензии (начальная страница Менеджера лицензий) и кликните мышью по символу ✕ справа от номера текущей лицензии.

После этого вам необходимо в появившемся окне подтвердить удаление лицензионного ключевого файла с данного компьютера. Для этого нажмите кнопку **Да**. Если вы решили отказаться от удаления с данного компьютера лицензионного ключевого файла, нажмите кнопку **Нет**.

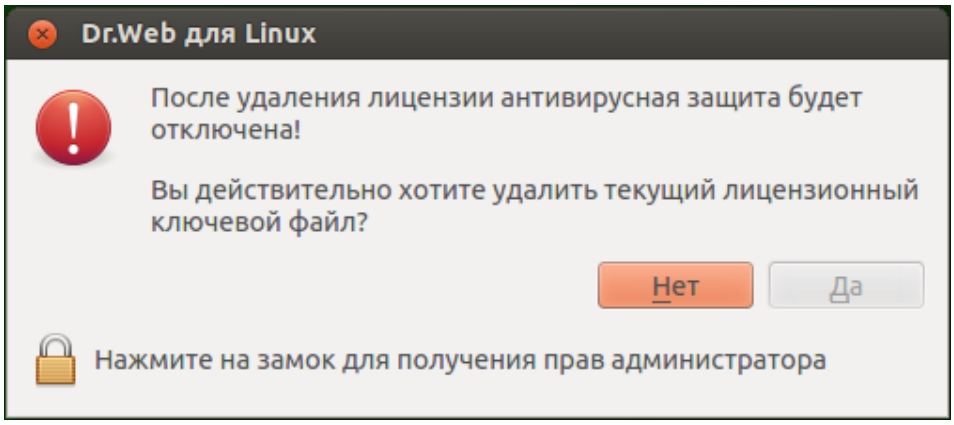

Рисунок 33. Окно подтверждения удаления лицензионного ключевого файла

Для удаления лицензионного ключевого файла приложение должно обладать повышенными правами. Если в момент попытки удаления права приложения не повышены, кнопка **Да** будет недоступна. При необходимости вы можете повысить права приложения, и в случае успешного их повышения кнопка **Да** станет доступной.

Удаление с компьютера лицензионного ключевого файла не влияет на срок действия лицензии. Если срок действия лицензии еще не истек, то вы сможете получить новый ключевой файл для этой лицензии на оставшийся срок.

После удаления лицензионного ключевого файла и до момента активации новой лицензии или демонстрационного периода все антивирусные функции Dr.Web Desktop Security Suite (для Linux) (проверка файлов, обновление вирусных баз, антивирусного ядра и баз категорий веб-ресурсов, мониторинг файловой системы) будут заблокированы.

Управление правами приложения

Некоторые действия в окне Dr.Web Desktop Security Suite (для Linux) можно выполнить только в том случае, если приложение имеет повышенные права (*права администратора*), соответствующие правам специального пользователя системы – *суперпользователя* (пользователя *root*). В частности, обладания повышенными правами требуют следующие функции:

1. Управление объектами, помещенными в системный карантин (т.е. в каталог карантина, не принадлежащий пользователю, запустившему Dr.Web Desktop Security Suite (для Linux)).
2. Проверка файлов и каталогов, принадлежащих другим пользователям (в частности – суперпользователю).
3. Выключение монитора файловой системы SpIDer Guard.
4. Выключение монитора сетевых соединений SpIDer Gate.
5. Удаление лицензионного ключевого файла, подключение и отключение от сервера централизованной защиты.

> Даже если приложение было запущено из учетной записи суперпользователя (например, с использованием команд **su** или **sudo**), оно по умолчанию *не будет* обладать повышенными правами.

На всех страницах окна Dr.Web Desktop Security Suite (для Linux), функциональность которых зависит от наличия у приложения повышенных прав, расположена специальная кнопка с изображением замка. Состояние замка показывает, обладает ли в данный момент окно Dr.Web Desktop Security Suite (для Linux) повышенными правами:

	Приложение не обладает повышенными правами. Нажатие замка приведет к попытке повышения прав приложения до прав суперпользователя.
	Права приложения повышены до прав суперпользователя. Нажатие замка приведет к понижению прав приложения, т.е. отказа от прав суперпользователя и возврат к исходным правам обычного пользователя.

В случае попытки повышения прав, после нажатия на изображение замка появляется окно аутентификации пользователя.

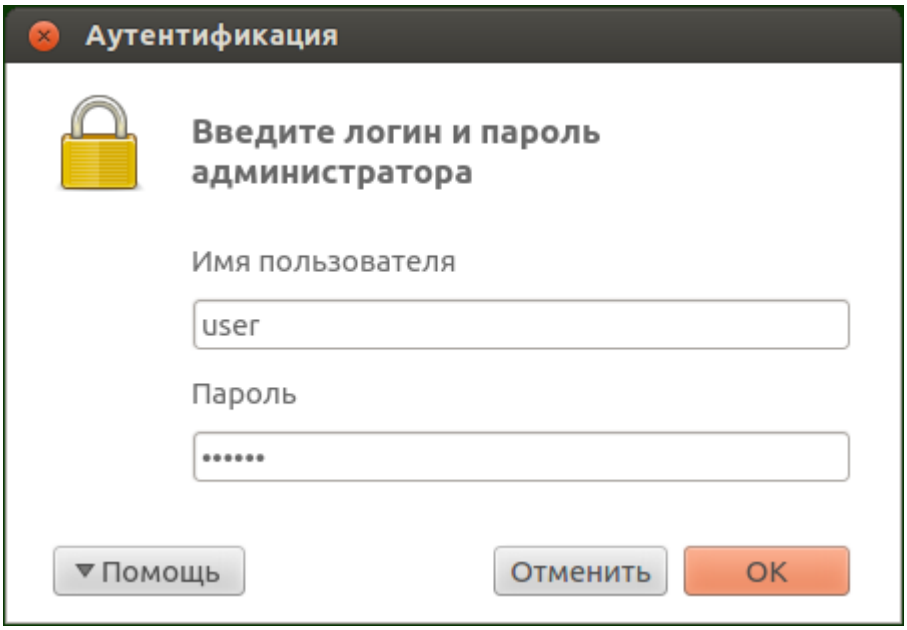

Рисунок 34. Окно аутентификации

Для получения приложением прав суперпользователя требуется пройти аутентификацию, указав имя (логин) и пароль любого пользователя, включенного в группу пользователей, указанную в настройках Dr.Web Desktop Security Suite (для Linux) как *группа администраторов*, или логин и пароль суперпользователя (учетная запись *root*), и нажать кнопку **OK**. Чтобы отказаться от повышения прав, следует закрыть окно, нажав кнопку **Отменить**. Нажатие кнопки **Справка** отображает на окне краткую подсказку по аутентификации, или скрывает ее.

По умолчанию при установке Dr.Web Desktop Security Suite (для Linux) в качестве «группы администраторов» в настройках автоматически фиксируется имя системной группы пользователей, обладающих возможностью получения прав суперпользователя (например, группа *sudo*). Если имя такой системной группы определить не удалось, то для повышения прав приложения в окне аутентификации можно использовать логин и пароль суперпользователя (*root*).

При понижении прав приложения до прав обычного пользователя ввода пароля не требуется.

Справочные материалы

Для доступа к справочным материалам используйте кнопку ? на навигационной панели окна Dr.Web Desktop Security Suite (для Linux).

При нажатии на эту кнопку на экране появляется выпадающее меню, содержащее следующие пункты:

- **Справка** – открытие краткого Руководства пользователя Dr.Web Desktop Security Suite (для Linux).
- **Форум Dr.Web** – открытие в браузере страницы форума пользователей продуктов компании «Доктор Веб» (требуется подключение к сети Интернет).
- **Техническая поддержка** – открытие в браузере страницы службы технической поддержки компании «Доктор Веб» (требуется подключение к сети Интернет).
- **Мой Dr.Web** – открытие в браузере персональной страницы пользователя продуктов компании «Доктор Веб» (требуется подключение к сети Интернет).
- **О программе** – открытие окна с краткой информацией об Dr.Web Desktop Security Suite (для Linux) и его версии.

Кроме того, когда на любой странице главного окна Dr.Web Desktop Security Suite (для Linux) отображается сообщение о произошедшей ошибке, вы можете щелкнуть по ссылке **Подробнее** для получения более полной информации об ошибке и указаний по решению возникшей проблемы.

Настройка работы

Настройка параметров работы приложения, таких, как:

- Периодичность выполнения обновлений.
- Реакции Dr.Web Desktop Security Suite (для Linux) на обнаруженные угрозы при проверках по требованию Сканером и при обнаружении их монитором файловой системы SplDer Guard.
- Перечень объектов, исключаемых Сканером и SplDer Guard из проверки.
- Параметры контроля сетевых соединений.
- Расписание периодических проверок объектов Сканером.
- Режим защиты (автономный, централизованный).
- Использование сервиса Dr.Web Cloud.

выполняется в окне настроек Dr.Web Desktop Security Suite (для Linux).

Для доступа к окну настроек нажмите кнопку  на навигационной панели.

На окне настроек доступны следующие вкладки:

- Основные – позволяет настроить использование уведомлений, а также периодичность автоматических обновлений.

- Сканер – позволяет настроить реакцию Dr.Web Desktop Security Suite (для Linux) на угрозы, обнаруживаемые Сканером в процессе проверки по требованию и по расписанию.
- SplDer Guard – позволяет настроить реакцию Dr.Web Desktop Security Suite (для Linux) на угрозы, обнаруживаемые монитором файловой системы SplDer Guard.
- SplDer Gate – позволяет настроить параметры контроля сетевых соединений монитором SplDer Gate.
- Исключения – позволяет настроить список объектов, которые следует исключать из проверки по требованию и по расписанию, а также из перечня объектов, наблюдаемых SplDer Guard и контролируемых SplDer Gate.
- Планировщик – позволяет настроить периодический запуск проверок по заданному расписанию.
- Сеть – позволяет включить или отключить для SplDer Gate режим проверки защищенных сетевых соединений (основанных на SSL/TLS, таких как HTTPS), сохранить в файл сертификат Dr.Web, используемый для перехвата защищенных сетевых соединений.
- Режим – позволяет выбрать режим защиты (автономный, централизованный), в котором работает Dr.Web Desktop Security Suite (для Linux).
- Dr.Web Cloud – позволяет разрешить или запретить Dr.Web Desktop Security Suite (для Linux) использовать сервис Dr.Web Cloud.

Для получения справки нажмите кнопку  на соответствующей странице окна настроек.

Все изменения, вносимые в настройки, представленные на этих вкладках, применяются немедленно.

Если Dr.Web Desktop Security Suite (для Linux) работает в режиме централизованной защиты, то некоторые настройки могут быть заблокированы и недоступны для изменения.

Основные настройки

На вкладке **Основные** вы можете настроить основные параметры работы приложения.

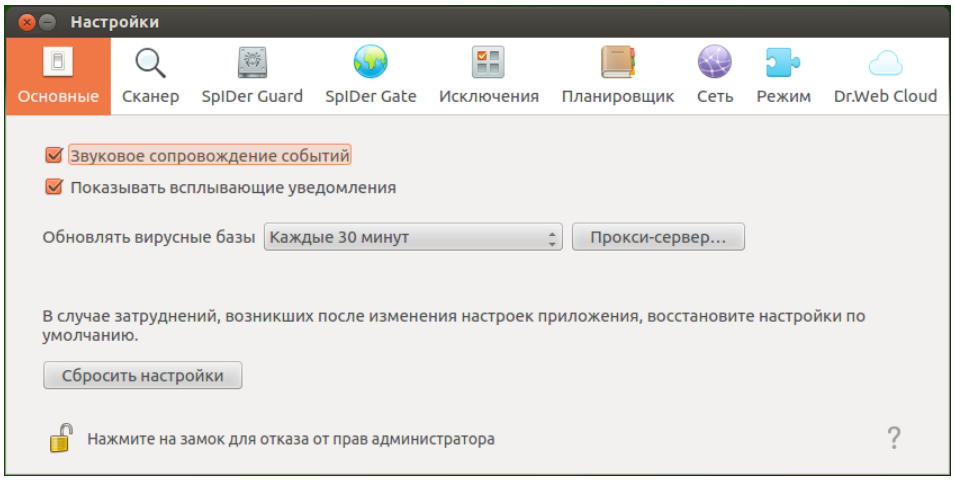

Рисунок 35. Вкладка основных настроек

Элемент управления	Действие
Флажок **Звуковое сопровождение событий**	Установка этого флажка предписывает Dr.Web Desktop Security Suite (для Linux) проигрывать звуковые уведомления при возникновении таких событий, как: • Обнаружена угроза (как Сканером так и SplDer Guard) • Ошибка проверки объекта • и т.п.
Флажок **Показывать всплывающие уведомления**	Установка этого флажка предписывает Dr.Web Desktop Security Suite (для Linux) при работе в режиме графического рабочего стола отображать на экране всплывающие уведомления при возникновении таких событий, как: • Обнаружена угроза • Ошибка проверки • и т.п.
Выпадающий список **Загружать обновления**	Позволяет выбрать периодичность автоматического обновления вирусных баз, баз категорий веб-ресурсов и антивирусного ядра Компонентом обновления.
Кнопка **Прокси-сервер**	Открывает окно настройки использования прокси-сервера Компонентом обновления для получения обновлений (использование прокси-сервера может понадобиться в том случае если обращение к внешним серверам запрещено политиками безопасности сети).
Кнопка **Сбросить настройки**	Позволяет сбросить настройки в значения по умолчанию.

Для управления параметрами получения обновлений и сброса настроек в значения по умолчанию необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Настройки прокси-сервера, используемого для получения обновлений

В окне настройки использования прокси-сервера Компонентом обновления для получения обновлений вы можете настроить следующие параметры:

- Использовать или нет прокси-сервер для получения обновлений.
- Адрес прокси-сервера, который следует использовать для получения обновлений.
- Порт для подключения к прокси-серверу.
- Имя пользователя и пароль, используемые для аутентификации на прокси-сервере.

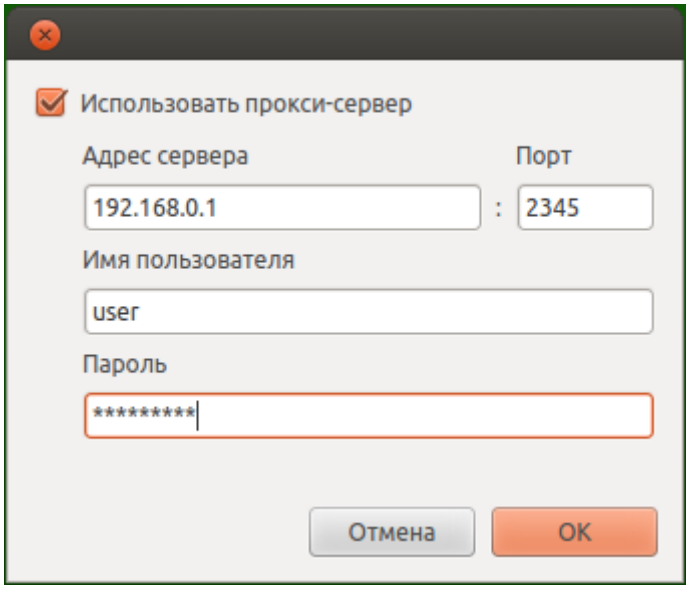

Рисунок 36. Настройки прокси-сервера

В качестве адреса можно использовать как IP-адрес, так и FQDN узла, на котором работает прокси-сервер. Адрес и порт требуется указывать обязательно. Поскольку обновление производится по протоколу HTTP, необходимо использовать прокси-сервер HTTP. Имя пользователя и пароль обязательно указывать только в том случае, если прокси-сервер HTTP требует авторизации.

Чтобы закрыть окно с применением всех внесенных изменений, нажмите **OK**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

Настройки проверки файлов

На вкладке **Сканер** вы можете настроить действия, которые Dr.Web Desktop Security Suite (для Linux) должен применять к угрозам в случае обнаружения их Сканером в процессе проверки файлов по требованию пользователя или по расписанию.

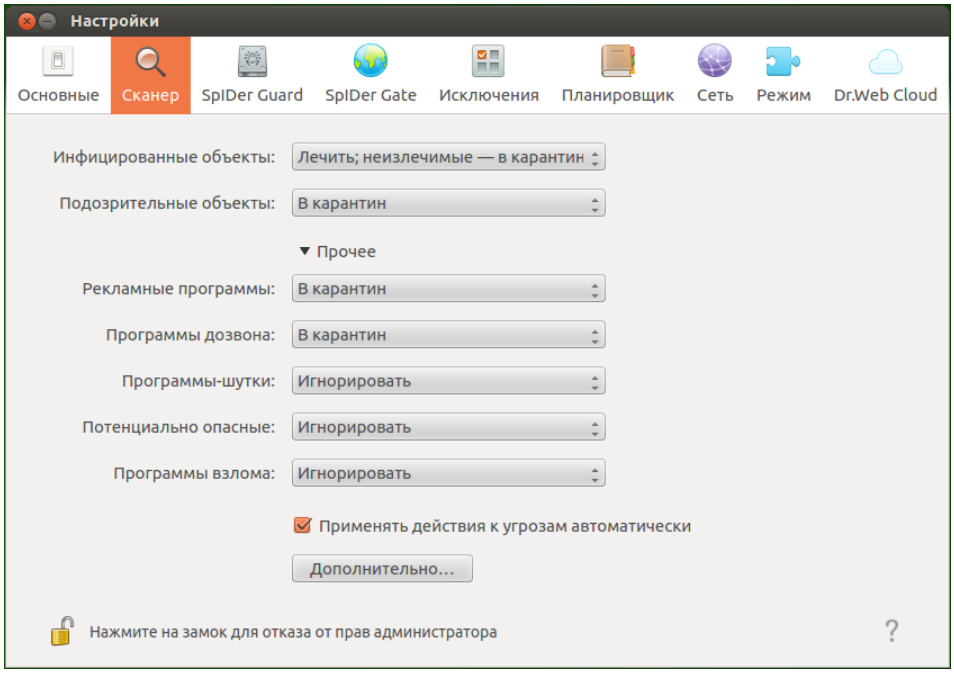

Рисунок 37. Вкладка настроек проверки файлов Сканером

В выпадающих списках следует выбрать действие, которое Dr.Web Desktop Security Suite (для Linux) должен применить к объекту в случае обнаружения в нем угрозы определенного типа.

> Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления выполняется перемещение контейнера в карантин.

Установка флажка **Применять действия к угрозам автоматически** предписывает Dr.Web Desktop Security Suite (для Linux) применять указанное действие к объекту, содержащему угрозу сразу в момент ее обнаружения Сканером в ходе проверки по требованию или по расписанию (пользователь будет проинформирован о нейтрализации угрозы, а информация об ней будет доступна в списке угроз). В случае если флажок сброшен, угроза, обнаруженная Сканером, будет только добавлена в список обнаруженных угроз, в котором пользователю придется самостоятельно выбрать, какое действие к ней следует применить.

Нажатие кнопки **Дополнительно** открывает окно дополнительных настроек проверки файлов.

Замечания:

- Настройка исключения файлов и каталогов из проверки Сканером производится на вкладке **Исключения**.
- Реакции на обнаружение угроз, включая автоматическое применение действий, заданные для Сканера, не влияют на поведение монитора SplDer Guard. Его реакции на угрозы задаются на соответствующей странице.

> Для изменения реакции Сканера на угрозы и для доступа к расширенным настройкам необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.
>
> ---
>
> Возможность настройки Сканера при работе Dr.Web Desktop Security Suite (для Linux) под управлением сервера централизованной защиты может быть заблокирована, если это запрещено сервером.

Дополнительные настройки проверки файлов

В окне дополнительных настроек проверки вы можете настроить следующие параметры работы Сканера:

- Включить и отключить проверку содержимого контейнеров:
  - Архивов.
  - Почтовых файлов.
- Задать ограничение на время проверки одного файла.

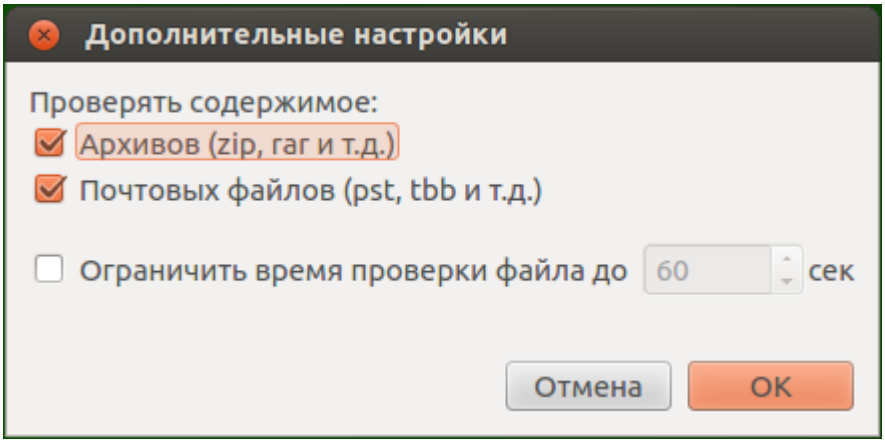

Рисунок 38. Дополнительные настройки проверки файлов

> Если флажки проверки содержимого контейнеров не включены, то это означает, что файлы-контейнеры все равно проверяются Сканером, но без отдельной проверки вложенных в них файлов.

Чтобы закрыть окно с применением всех внесенных изменений, нажмите **ОК**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

Настройки мониторинга файловой системы

На вкладке **SpIDer Guard** вы можете настроить действия, которые Dr.Web Desktop Security Suite (для Linux) должен применять к угрозам в случае обнаружения их монитором файловой системы SpIDer Guard.

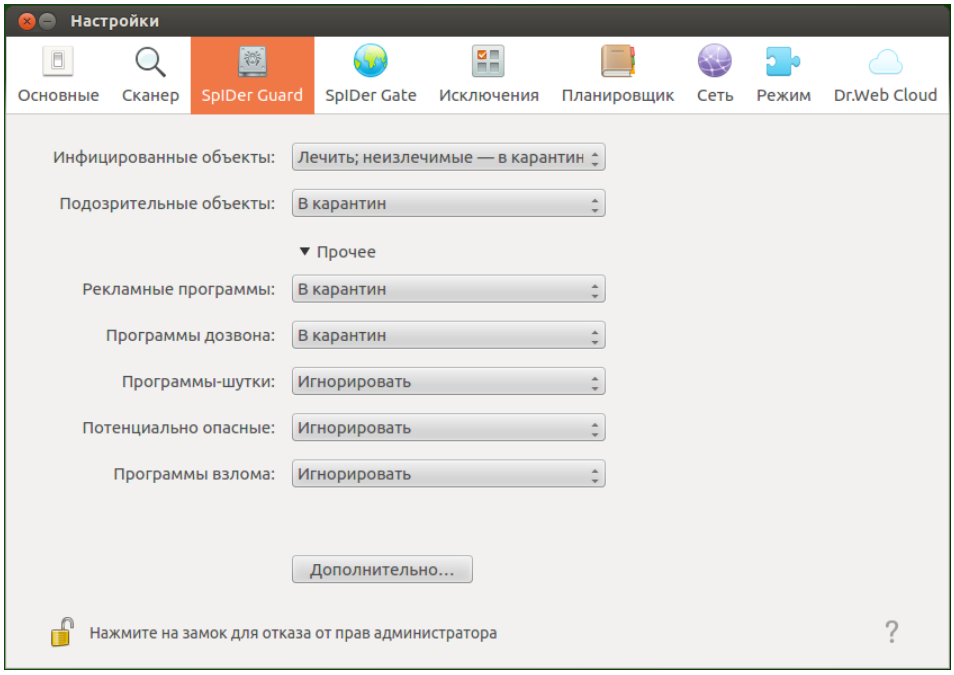

Рисунок 39. Вкладка настроек мониторинга файловой системы

Эта вкладка, включая окно дополнительных настроек, аналогична вкладке настройки проверки файлов (вкладка **Сканер**).

Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления выполняется перемещение контейнера в карантин.

Замечания:

- Настройка исключения файлов и каталогов из наблюдения монитором SpIDer Guard производится на вкладке **Исключения**.
- Включение усиленного режима мониторинга файлов монитором SpIDer Guard описано в разделе <%TARGETTITLE%>.
- Реакции на обнаружение угроз, заданные для монитора SpIDer Guard, не влияют на поведение Сканера. Его реакции на угрозы задаются на соответствующей странице.

Для изменения настроек монитора файловой системы SpIDer Guard необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Возможность настройки SpIDer Guard при работе Dr.Web Desktop Security Suite (для Linux) под управлением сервера централизованной защиты может быть заблокирована, если это запрещено сервером.

Настройки мониторинга сетевых соединений

На вкладке **SpIDer Gate** вы можете настроить политики безопасности, которые монитор сетевых соединений SpIDer Gate будет использовать при проверке отправляемых и получаемых сообщений электронной почты, а также при контроле обращений к Интернет.

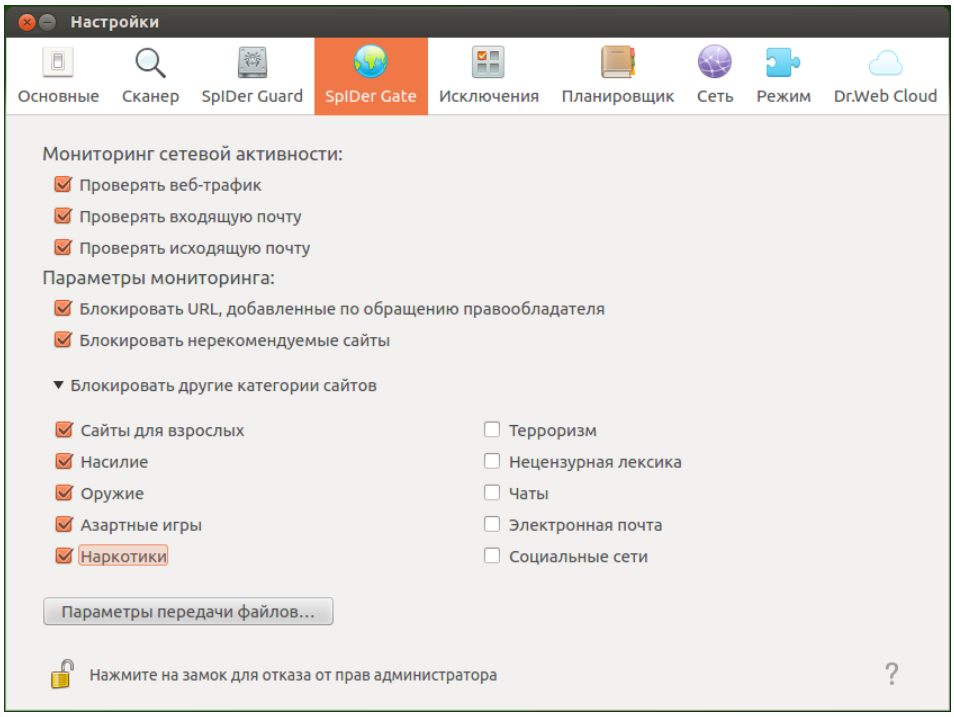

Рисунок 40. Вкладка настроек контроля доступа к сети

Устанавливая и сбрасывая переключатели в разделе **Мониторинг сетевой активности**, вы можете определить, какие типы сетевой активности контролирует монитор, если он включен.

При проверке электронной почты SpIDer Gate проверяет сообщения не только на наличие угроз, но и на наличие признаков спама. Если компонент Dr.Web Anti-Spam отсутствует в составе продукта, проверка сообщений электронной почты на наличие признаков спама не производится.

Переключатели в разделе **Параметры мониторинга** определяют, доступ к веб-сайтам каких категорий блокируется (это относится не только к попыткам доступа к этим сайтам через браузер, но и к блокировке сообщений электронной почты, содержащих ссылки на такие веб-сайты). Устанавливая или снимая соответствующие переключатели, вы можете запретить или разрешить доступ к веб-сайтам следующих категорий:

Категория	**Описание**
URL, добавленные по обращению правообладателя	Сайты, содержащие материалы, нарушающие законодательство об авторских правах (по мнению правообладателя материалов, размещенных на сайте). Это различные «пиратские» сайты, каталоги файловых ссылок, файлообменные ресурсы и т.п.
Нерекомендуемые сайты	Сайты, содержащие сомнительное содержимое, заподозренные в фишинге, краже паролей и т.п.
Сайты для взрослых	Сайты, содержащие материалы, предназначенные только для взрослых (эротического и порнографического характера)
Насилие	Сайты, содержащие описание и демонстрацию сцен насилия (включая войны, сцены террористических актов и т.п.)
Оружие	Сайты, посвященные описанию и изготовлению оружия и взрывчатых веществ
Азартные игры	Сайты, посвященные азартным играм и играм на деньги, в т.ч. онлайн-казино
Наркотики	Сайты, посвященные наркотическим веществам, в т.ч. описанию их изготовления или опыта их употребления
Нецензурная лексика	Сайты, содержащие нецензурную лексику
Чаты	Сайты чатов
Терроризм	Сайты, посвященные терроризму
Электронная почта	Сайты бесплатных почтовых служб
Социальные сети	Сайты социальных сетей

База категорий веб-ресурсов поставляется в составе Dr.Web Desktop Security Suite (для Linux) и автоматически обновляется совместно с вирусными базами. Пользователь не имеет возможности редактировать содержимое базы категорий веб-ресурсов.

Один и тот же веб-сайт может быть отнесен сразу к нескольким различным категориям. Монитор сетевых соединений SplDer Gate будет блокировать доступ к веб-сайту, если он попадает хотя бы в одну из категорий, включенных для запрета доступа. Щелчок по надписи **Блокировать другие категории сайтов** позволяет показать перечень доступных категорий в сжатом или расширенном виде.

При необходимости заблокировать доступ к некоторому веб-сайту, не относящемуся ни к одной из указанных категорий, его следует включить в пользовательский черный список. Если наоборот, требуется принудительно разрешить доступ к некоторому сайту, не смотря на то, что он относится к какой-либо из нежелательных категорий, его следует включить в пользовательский белый список. Кроме того, если нужно, вы можете настроить список приложений, чьи сетевые соединения не контролируются монитором SplDer Gate.

Настройка черных и белых списков веб-сайтов, а также приложений, исключаемых из наблюдения монитором SplDer Gate, производится на вкладке **Исключения**.

Существует особая категория веб-сайтов – *Источники распространения вирусов*. Доступ к сайтам этой категории запрещается в любом случае, даже если они включены в пользовательский белый список.

Управление параметрами проверки файлов

Для управления параметрами, которые монитор SplDer Gate будет применять при проверке файлов, загруженных из Интернет, или передаваемых в сообщениях электронной почты, нажмите кнопку **Параметры передачи файлов**.

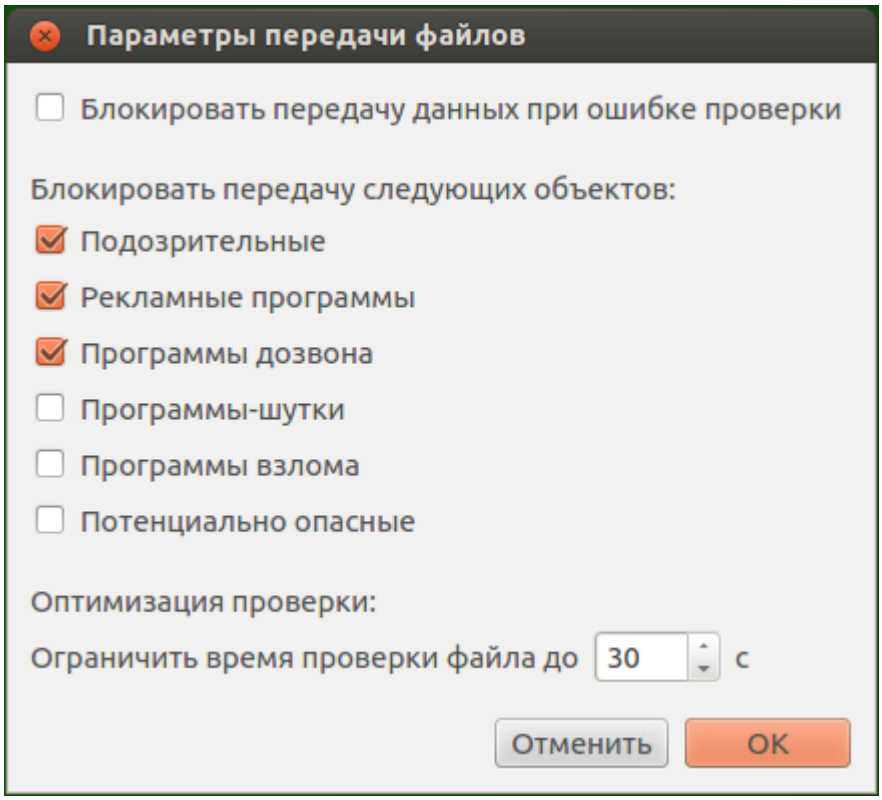

Рисунок 41. Окно управления настройками проверки файлов

В появившемся окне вы можете указать, какие категории вредоносных объектов следует блокировать при попытке их передачи (в том числе – в виде вложений в сообщения электронной почты). Если некоторый переключатель включен, то файлы, содержащие угрозу соответствующего типа, будут отвергаться при попытке их загрузки на компьютер или передачи посредством электронной почты. Если переключатель отключен, то файлы, содержащие угрозы этого типа, будут загружаться из Интернет и передаваться по электронной почте. Кроме этого вы можете также установить максимальный интервал времени, отводимый на проверку загружаемых файлов (и сообщений электронной почты). Если включен переключатель **Блокировать передачу данных при ошибке проверки**, то файлы или сообщения электронной почты, которые не удалось проверить из-за возникновения ошибки, будут блокироваться при загрузке. Для разрешения загрузки непроверенных файлов и сообщений электронной почты переключатель можно отключить (не рекомендуется).

Если загружаемый файл или передаваемое сообщение электронной почты не удалось проверить из-за того, что истек интервал времени, отведенный на его проверку, то такой файл или сообщение *не будут* считаться непроверенными и не будут блокироваться, даже если переключатель **Блокировать передачу данных при ошибке проверки** включен.

Чтобы закрыть окно с применением всех внесенных изменений, нажмите **ОК**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

Для изменения настроек монитора сетевых соединений SplDer Gate необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Настройка исключений

На вкладке **Исключения** доступны кнопки, позволяющие настроить следующие исключения:

- **Файлы и каталоги** – открывает окно перечисления путей к объектам файловой системы, исключаемых из проверки Сканером и монитором файловой системы SplDer Guard.
- **Веб-сайты** – открывает окно управления черными и белыми списками веб-сайтов, доступ к которым будет регулироваться независимо от политик блокировки, заданных для монитора сетевых соединений SplDer Gate.
- **Приложения** – открывает окно перечисления приложений, сетевые соединения которых не будут контролироваться монитором сетевых соединений SplDer Gate.

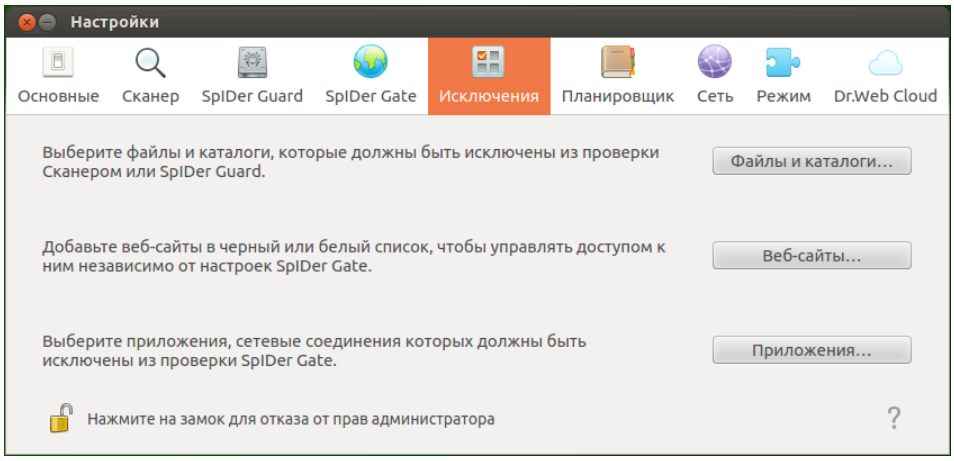

Рисунок 42. Вкладка настройки исключений

Для добавления и удаления объектов из перечня исключений необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Исключение файлов и каталогов

Управление исключением файлов и каталогов из проверки осуществляется в окне **Файлы и каталоги**. Для открытия окна нажмите кнопку **Файлы и каталоги** на вкладке **Исключения**.

В данном окне вы можете указать перечень путей к объектам, которые следует исключать из проверки Сканером по требованию пользователя и/или по расписанию, и от наблюдения их монитором файловой системы SplDer Guard.

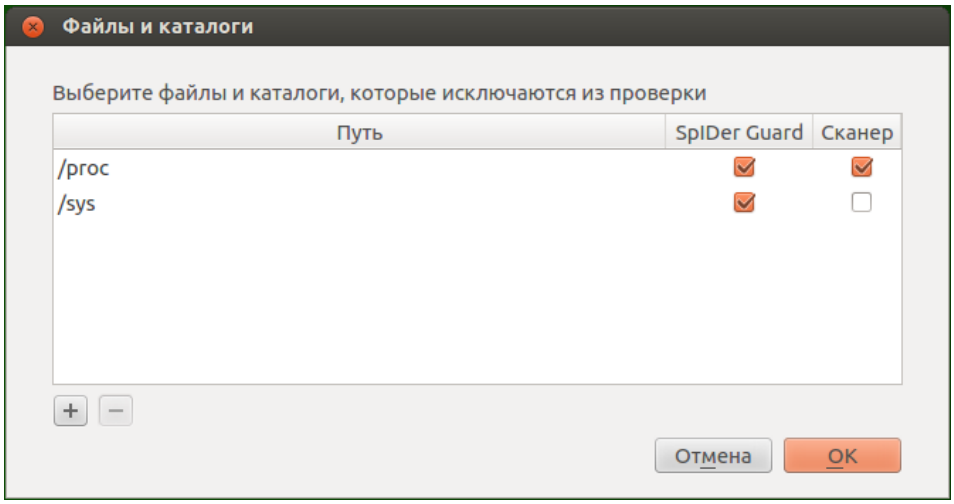

Рисунок 43. Настройка исключений файлов и каталогов

Один и тот же объект вы можете добавить в список исключений как для проверки Сканером (по запросу и/или по расписанию), так и для наблюдения монитором файловой системы SplDer Guard. Отметка, для какого компонента объект из списка добавлен в исключения, изображается флажком в соответствующем столбце таблицы.

Добавление и удаление объектов из списков исключений

- Чтобы добавить объект, присутствующий в списке, в перечень исключаемых объектов для Сканера или для SplDer Guard, необходимо установить соответствующий флажок в строке объекта. Чтобы исключить объект, представленный в списке, из перечня объектов исключаемых из проверки Сканером или SplDer Guard, необходимо сбросить соответствующий флажок в строке объекта.
- Чтобы добавить в список новый объект, следует нажать кнопку `+`, расположенную под списком объектов, и выбрать объект в появившемся окне выбора каталогов и файлов. Кроме этого, вы можете добавить объекты в этот список, перетащив их мышью из окна файлового менеджера.
- Чтобы удалить объект из списка, следует выделить его строчку в списке и нажать кнопку `–`, расположенную под списком.

Чтобы закрыть окно с применением всех внесенных изменений, нажмите **OK**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

Исключение сетевых соединений приложений

Управление исключением сетевых соединений приложений из наблюдения монитором сетевых соединений SplDer Gate осуществляется в окне **Приложения**. Для открытия окна нажмите кнопку **Приложения** на вкладке **Исключения**.

В данном окне вы можете указать перечень путей к исполняемым файлам приложений, чьи сетевые соединения не должны контролироваться монитором сетевых соединений SplDer Gate.

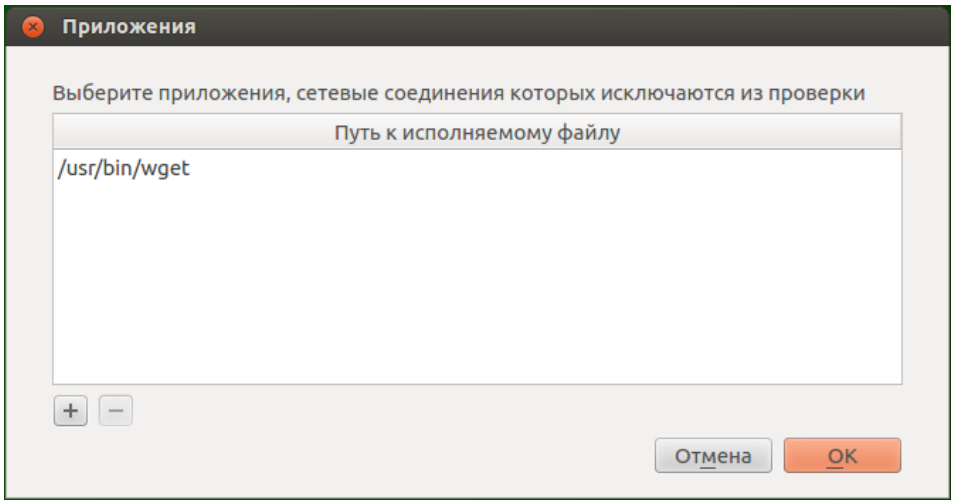

Рисунок 44. Настройка исключений сетевых соединений приложений

Добавление и удаление приложений из списка исключений

- Чтобы добавить в список новое приложение, следует нажать кнопку `+`, расположенную под списком приложений, и выбрать исполняемый файл приложения в появившемся окне выбора каталогов и файлов. Кроме этого, вы можете добавить приложения в этот список, перетащив их исполняемые файлы мышью из окна файлового менеджера.
- Чтобы удалить приложение из списка, следует выделить его строчку в списке и нажать кнопку `−`, расположенную под списком.

Чтобы закрыть окно с применением всех внесенных изменений, нажмите **ОК**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

Черный и белый списки веб-сайтов

Управление черными и белыми списками веб-сайтов осуществляется в окне **Управление списками**. Для открытия окна нажмите кнопку **Веб-сайты** на вкладке **Исключения**.

В данном окне вы можете указать перечень веб-сайтов, доступ к которым будет всегда разрешен, или наоборот, всегда запрещен монитором сетевых соединений SpIDer Gate.

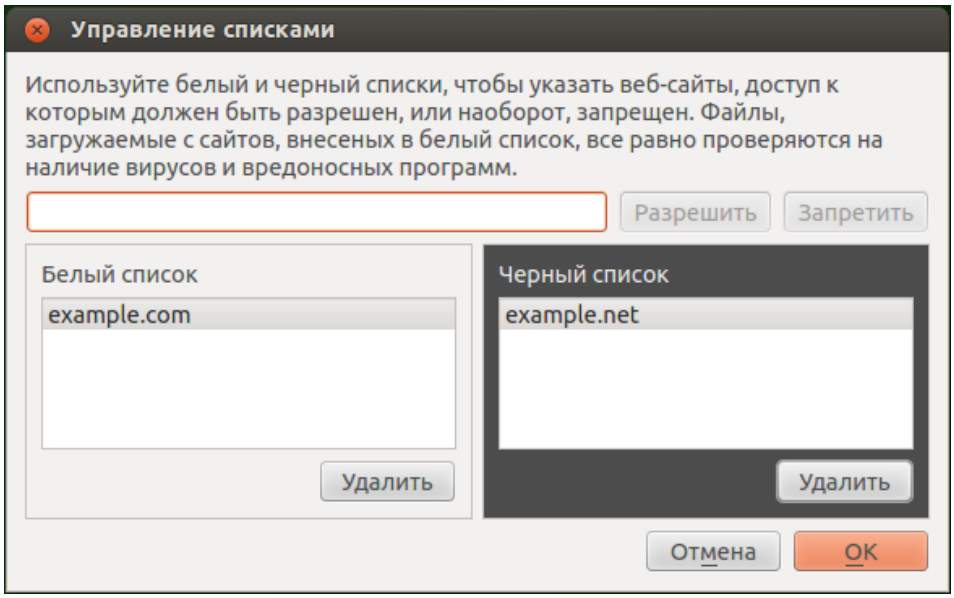

Рисунок 45. Окно управления черным и белым списками

Существует особая категория веб-сайтов – *Источники распространения вирусов*. Доступ к сайтам этой категории запрещается в любом случае, даже если они включены в пользовательский белый список.

Добавление и удаление веб-сайтов из черного и белого списка

- Для добавления веб-сайта в черный или белый список введите его домен в поле ввода и нажмите соответствующую кнопку:
  - **Разрешить**, чтобы добавить введенный адрес в *белый* список.
  - **Запретить**, чтобы добавить введенный адрес в *черный* список.
- Добавление некоторого доменного адреса в белый или черный список разрешает, или, соответственно, запрещает доступ ко всем ресурсам, расположенным на данном домене.
- Для удаления веб-сайта из белого или черного списка выделите его в соответствующем списке и нажмите кнопку **Удалить**.

Чтобы закрыть окно с применением всех внесенных изменений, нажмите **ОК**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

Настройка проверки по расписанию

На вкладке **Планировщик** вы можете включить автоматический запуск проверок по расписанию, задать расписание запуска и выбрать тип проверки.

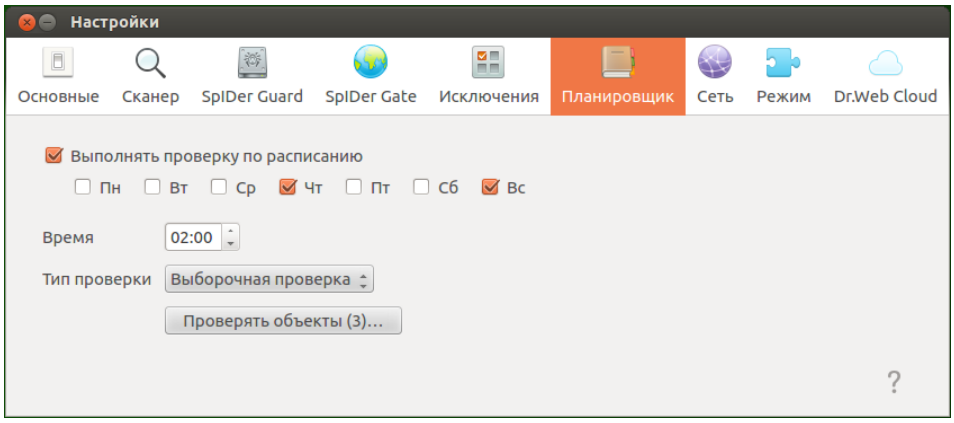

Рисунок 46. Вкладка настройки расписания

Для включения автоматической проверки по расписанию установите флажок **Выполнять проверку по расписанию**. В этом случае Dr.Web Desktop Security Suite (для Linux) сформирует расписание периодического запуска проверки выбранного типа.

Проверки по заданному расписанию будут запускаться с указанной периодичностью агентом уведомлений, либо непосредственно графическим интерфейсом управления, если он запущен в момент начала проверки. Проверки по расписанию не запускаются, если Dr.Web Desktop Security Suite (для Linux) работает под управлением сервера централизованной защиты, или если отсутствует действующая лицензия.

Для проверок, запускаемых по расписанию, как и для проверок по требованию, действуют настройки проверки, заданные на вкладке **Сканер**.

Настройка проверки по расписанию

Включив проверку по расписанию, вы можете настроить следующие параметры:

- Выбрать дни недели, в которые следует запускать проверку (включив соответствующие флажки).
- Установить время (часы и минуты) начала проверки.
- Задать тип проверки (*Быстрая проверка, Полная проверка* или *Выборочная проверка*).
- Если вы выбрали тип проверки *Выборочная проверка*, то вам также нужно указать перечень объектов, подлежащих проверке. Для этого нажмите кнопку **Проверять объекты** (в скобках указывается количество объектов, выбранных для проверки по расписанию).

  После этого на экране откроется окно выбора объектов для выборочной проверки объектов по расписанию, аналогичное окну выбора объектов для выборочной проверки по требованию. Вы можете добавить объекты в список, как используя кнопку `+`, так и перетаскивая их в список мышью из окна файлового менеджера.

Для отключения автоматической проверки объектов по расписанию сбросьте флажок **Выполнять проверку по расписанию**. Соответствующая задача для агента уведомлений будет автоматически удалена.

Настройка защиты от угроз, передаваемых через сеть

На вкладке **Сеть** вы можете включить для монитора сетевых соединений SplDer Gate режим проверки трафика, передаваемого через защищенные сетевые соединения, использующие протоколы на основе SSL и TLS.

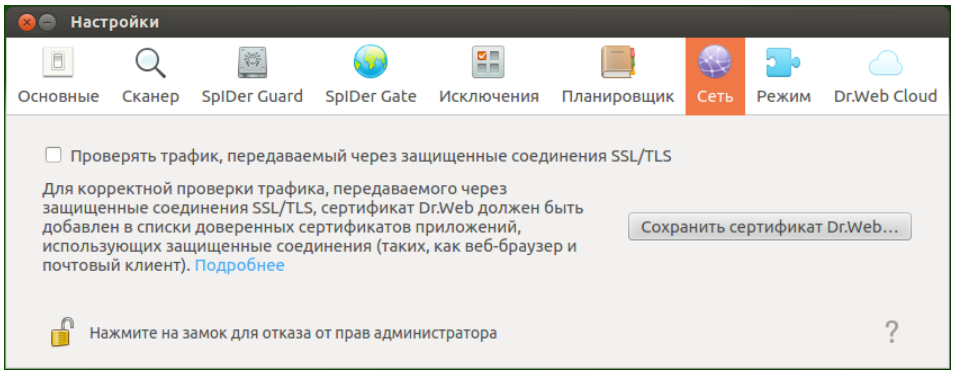

Рисунок 47. Вкладка настройки защиты от угроз, передаваемых через сеть

Настройка проверки защищенных сетевых соединений

Для разрешения монитору SplDer Gate проверять трафик, передаваемый через защищенные сетевые соединения, использующие протоколы на основе SSL и TLS, установите флажок **Проверять трафик, передаваемый через защищенные соединения SSL/TLS**. Чтобы отключить проверку защищенного трафика, снимите флажок.

Для управления проверкой защищенного трафика необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Если в системе запущен почтовый клиент (такой, как **Mozilla Thunderbird**), его необходимо перезапустить после включения режима **Проверять трафик, передаваемый через защищенные соединения SSL/TLS**.

Для обеспечения правильной работы механизма проверки трафика, передаваемого через защищенные сетевые соединения, экспортируйте в файл специальный сертификат Dr.Web. В дальнейшем экспортированный сертификат необходимо вручную добавить в перечни доверенных сертификатов приложений, использующих защищенные соединения. В первую очередь это веб-браузеры и почтовые клиенты. Если в перечень доверенных сертификатов веб-браузера не добавить сертификат Dr.Web, будет нарушена корректность отображения данных, получаемых с сайтов, доступ к которым осуществляется по безопасному протоколу HTTPS (например – сайтов систем онлайн-банкинга, а также веб-интерфейсов почтовых

сервисов). Если сертификат Dr.Web не добавить в перечень доверенных сертификатов почтового клиента, будет невозможной авторизация на почтовых серверах, использующих для передачи почты защищенные протоколы (такие, как SMTPS).

Чтобы экспортировать сертификат Dr.Web в файл, нажмите кнопку **Сохранить сертификат Dr.Web**, а далее в появившемся окне сохранения файла укажите место для его сохранения. По умолчанию файл получает имя `SpIDer Gate Trusted Root Certificate.pem`, которое вы можете изменить при необходимости.

Далее сохраненный файл сертификата Dr.Web следует вручную добавлять в списки доверенных сертификатов тех приложений, в работе которых будут замечены неполадки при установлении защищенных соединений. Добавление сертификата в список для некоторого приложения достаточно выполнить только один раз. В дальнейшем, при сбросе и повторной установке флажка **Проверять трафик, передаваемый через защищенные соединения SSL/TLS** на странице настроек **Сеть** вам не придется заново сохранять и добавлять сертификат Dr.Web в список доверенных сертификатов.

Добавление сертификата Dr.Web в списки доверенных сертификатов приложений

Веб-браузер Mozilla Firefox

1) Выберите пункт **Настройки** в главном меню, затем (на появившейся странице настроек) пункт **Дополнительные**, а на открывшейся странице – раздел **Сертификаты**.
2) Нажмите **Просмотр сертификатов**, в появившемся окне выберите вкладку **Центры сертификации** и нажмите кнопку **Импортировать**.
3) В появившемся окне выбора файлов укажите к файлу сертификата Dr.Web (по умолчанию это файл `SpIDer Gate Trusted Root Certificate.pem`) и нажмите **Открыть**.
4) Далее, в появившемся окне, при помощи флажков укажите требуемую степень доверия к сертификату. Рекомендуется установить все три флажка (для идентификации веб-сайтов, для идентификации пользователей электронной почты, для идентификации программного обеспечения). После этого нажмите **OK**.
5) В списке доверенных сертификатов появится раздел *DrWeb,* содержащий в качестве сертификата добавленный сертификат (*SpIDer Gate Trusted Root Certificate* по умолчанию).
6) Закройте окно просмотра списка сертификатов, нажав **OK**, после чего закройте страницу настроек браузера (закрыв соответствующую вкладку на панели вкладок браузера).

Почтовый клиент Mozilla Thunderbird

1) Выберите пункт **Настройки** в главном меню, затем в появившемся окне настроек выберите раздел **Дополнительные**, а на открывшейся странице – вкладку **Сертификаты**.
2) Нажмите **Просмотр сертификатов**, в появившемся окне выберите вкладку **Центры сертификации** и нажмите **Импортировать**.
3) В появившемся окне выбора файлов укажите к файлу сертификата Dr.Web (по умолчанию это файл `SpIDer Gate Trusted Root Certificate.pem`) и нажмите **Открыть**.
4) Далее, в появившемся окне, при помощи флажков укажите требуемую степень доверия к сертификату. Рекомендуется установить все три флажка (для идентификации веб-сайтов, для идентификации пользователей электронной почты, для идентификации программного обеспечения). После этого нажмите **ОК**.
5) В списке доверенных сертификатов появится раздел *DrWeb*, содержащий в качестве сертификата добавленный сертификат (*SpIDer Gate Trusted Root Certificate* по умолчанию).
6) Закройте окно просмотра списка сертификатов, нажав **ОК**, после чего закройте окно настроек почтового клиента, нажав **Закрыть**.
7) Перезапустите почтовый клиент.

Настройка режима защиты

На вкладке **Режим** вы можете подключить Dr.Web Desktop Security Suite (для Linux) к серверу централизованной защиты (переведя его в режим централизованной защиты) или отключиться от сервера централизованной защиты (в этом случае Dr.Web Desktop Security Suite (для Linux) будет работать в одиночном режиме).

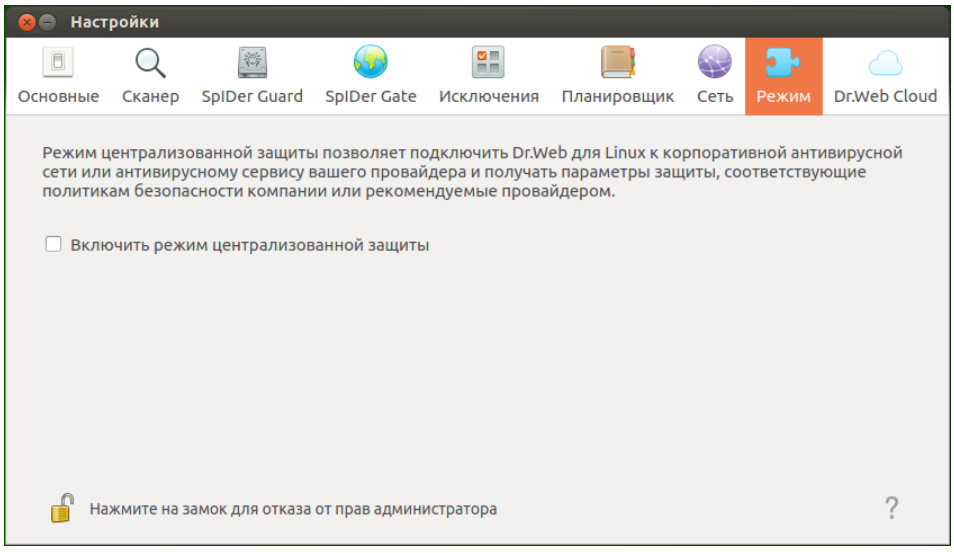

Рисунок 48. Вкладка управления режимом работы

Чтобы подключить Dr.Web Desktop Security Suite (для Linux) к серверу централизованной защиты или отключиться от него, используйте соответствующий флажок.

> Для подключения Dr.Web Desktop Security Suite (для Linux) к серверу централизованной защиты или отключения от него необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Подключение к серверу централизованной защиты

При попытке подключения к серверу централизованной защиты на экране появится окно, в котором требуется указать параметры подключения к серверу.

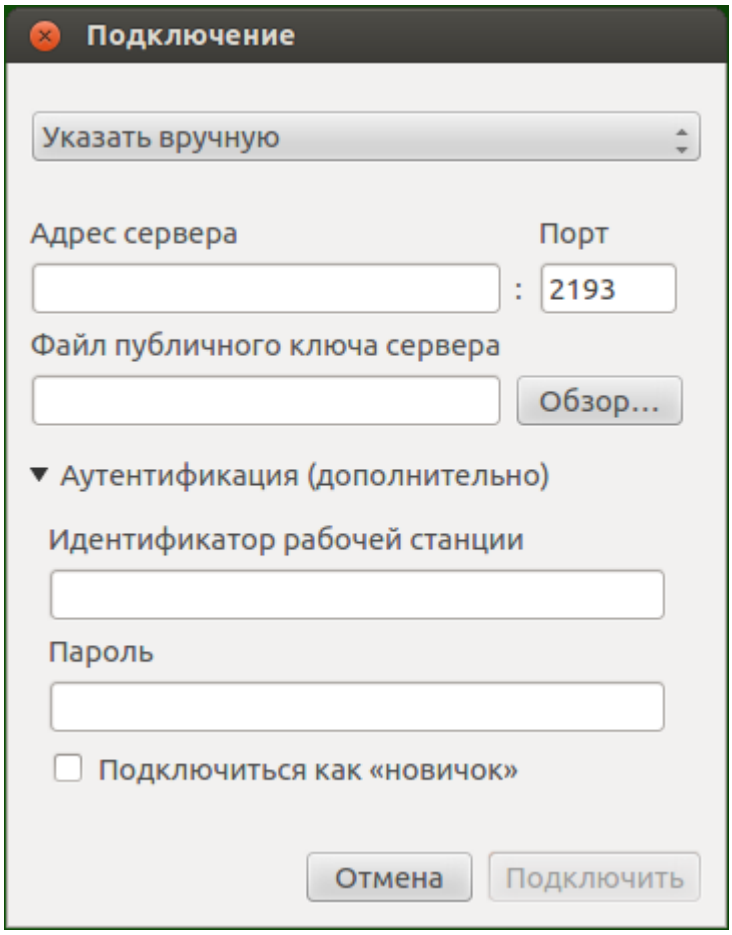

Рисунок 49. Окно подключения к серверу централизованной защиты

В выпадающем списке, расположенном в верхней части окна, выберите способ подключения к серверу. Доступно три способа:

- *Загрузить из файла.*
- *Указать вручную.*
- *Определить автоматически.*

В случае выбора варианта *Загрузить из файла* достаточно указать в соответствующем поле окна путь к файлу настроек подключения к серверу, предоставленному вам администратором антивирусной сети. При выборе варианта *Указать вручную* следует указать адрес и порт для подключения к серверу централизованной защиты. Кроме того, для способов подключения *Указать вручную* и *Определить автоматически* вы можете также указать путь к файлу публичного ключа сервера, если он у вас имеется (обычно этот файл предоставляется администратором антивирусной сети или провайдером).

Дополнительно, в разделе **Аутентификация**, вы можете указать идентификатор рабочей станции и пароль для аутентификации на сервере, если они вам известны. Если эти поля заполнены, то подключение к серверу будет успешным только при указании правильной пары идентификатор/пароль. Если эти поля оставить пустыми, то подключение к серверу будет успешным только в случае его одобрения на сервере (автоматически или администратором антивирусной сети, в зависимости от настроек сервера).

Кроме того, вы можете установить флажок **Подключиться как «новичок»**. Если опция «новичок» разрешена на сервере, то после одобрения подключения он автоматически сгенерирует уникальную пару идентификатор/пароль, которая в дальнейшем будет использоваться для подключения вашего компьютера к этому серверу. Обратите внимание, что при подключении как «новичок», новая учетная запись для вашего компьютера будет сгенерирована сервером централизованной защиты даже в том случае, если ранее он уже имел учетную запись на этом сервере.

Параметры подключения следует задавать в строгом соответствии с инструкциями, предоставленными администратором антивирусной сети или провайдером.

Для подключения к серверу после указания всех параметров нажмите кнопку **Подключить** и дождитесь окончания процесса подключения. Чтобы закрыть окно без подключения к серверу, нажмите кнопку **Отменить**.

После того, как вы подключили Dr.Web Desktop Security Suite (для Linux) к серверу централизованной защиты, он будет работать под управлением сервера до тех пор, пока вы его не переведете в одиночный режим. Подключение к серверу будет происходить автоматически каждый раз при запуске операционной системы. Подробнее см. раздел Режимы защиты.

Если на сервере централизованной защиты включен запрет на запуск проверки файлов пользователем, то страница запуска сканирования и кнопка **Сканер** на окне Dr.Web Desktop Security Suite (для Linux) будут недоступны. Кроме того, в этом случае Сканер не будет выполнять проверку файлов по заданному расписанию.

Настройка использования Dr.Web Cloud

На вкладке **Dr.Web Cloud** вы можете разрешить или запретить Dr.Web Desktop Security Suite (для Linux) использовать сервис Dr.Web Cloud.

Подключение к Dr.Web Cloud позволяет Dr.Web Desktop Security Suite (для Linux) использовать свежую информацию об угрозах, обновляемую на серверах компании «Доктор Веб» в режиме реального времени. В зависимости от настроек обновления, информация об угрозах, используемая компонентами антивирусной защиты, может устаревать. Использование облачных сервисов позволяет гарантировано оградить пользователей вашего компьютера от сайтов с нежелательным содержимым, а также от инфицированных файлов.

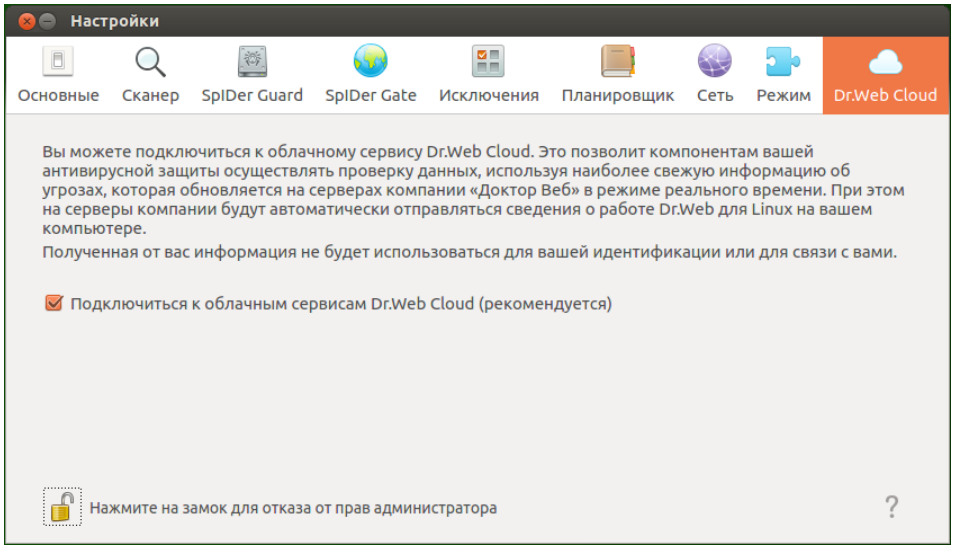

Рисунок 50. Вкладка управления использованием Dr.Web Cloud

Чтобы разрешить или наоборот, запретить Dr.Web Desktop Security Suite (для Linux) использовать сервис Dr.Web Cloud, используйте соответствующий флажок.

Для обращения к сервису Dr.Web Cloud необходимо наличие соединение с сетью Интернет.

Для разрешения или запрещения Dr.Web Desktop Security Suite (для Linux) использовать сервис Dr.Web Cloud необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Дополнительно

Аргументы командной строки

Для запуска графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) из командной строки операционной системы используется следующая команда:

```
$ drweb-gui [<путь>[ <путь> ...] | <параметры>]
```

где <*путь*> – путь, подлежащий проверке. Может быть указан список путей, разделенных пробелами.

Команда допускает также использование следующих параметров (<*параметры*>):

- `--help (-h)` – Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы графического интерфейса управления.
- `--version (-v)` – Вывод на экран информации о версии графического интерфейса управления.
- `--Autonomous (-a)` – Запустить графический интерфейс управления Dr.Web Desktop Security Suite (для Linux) в режиме автономной копии.
- `--FullScan` – Запустить полную проверку при старте графического интерфейса управления Dr.Web Desktop Security Suite (для Linux).
- `--ExpressScan` – Запустить быструю проверку при старте графического интерфейса управления Dr.Web Desktop Security Suite (для Linux).
- `--CustomScan` – Запустить выборочную проверку при старте графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) (открыть страницу выбора объектов, подлежащих проверке).

Пример:

```
$ drweb-gui /home/user/
```

Данная команда запустит графический интерфейс управления Dr.Web Desktop Security Suite (для Linux), после чего Сканер начнет проверять файлы по указанному пути (соответствующая задача проверки будет отображаться в списке текущих проверок).

Запуск автономной копии

Dr.Web Desktop Security Suite (для Linux) поддерживает работу в особом режиме – режиме *автономной копии*.

Если запустить графический интерфейс управления Dr.Web Desktop Security Suite (для Linux) в режиме автономной копии, то он будет работать с отдельным комплектом сервисных компонентов (работающим в фоне *демоном управления конфигурацией Dr.Web Desktop*

Security Suite (для Linux) (**drweb-configd**), Сканером и используемым им антивирусным ядром), запущенным специально для поддержки работоспособности запущенного экземпляра программы.

Особенности функционирования графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) в режиме автономной копии:

- Для запуска графического интерфейса управления Dr.Web Desktop Security Suite (для Linux) в режиме автономной копии необходимо наличие действующего ключевого файла, работа под управлением сервера централизованной защиты не поддерживается (имеется возможность установить ключевой файл, экспортированный с сервера централизованной защиты). При этом, даже если продукт подключен к серверу централизованной защиты, автономная копия *не сообщает* серверу централизованной защиты об угрозах, обнаруженных при запуске в режиме автономной копии.
- Все вспомогательные компоненты, обслуживающие работу автономной копии графического интерфейса, будут запущены от имени текущего пользователя и будут работать со специально сформированным файлом конфигурации.
- Все временные файлы и сокеты UNIX, используемые для взаимодействия компонентов между собой, будут создаваться только в каталоге с уникальным именем, созданным запущенной автономной копии в каталоге временных файлов (указанном в системной переменной окружения `TMPDIR`).
- Автономно запущенная копия графического интерфейса управления *не запускает* мониторы SplDer Guard и SplDer Gate, работают только функции проверки файлов, и управления карантином, поддерживаемые Сканером.
- Пути к файлам вирусных баз, антивирусного ядра и исполняемым файлам сервисных компонентов заданы по умолчанию, либо берутся из специальных переменных окружения.
- Число одновременно работающих автономных копий графического интерфейса управления не ограничено.
- При завершении работы автономно запущенной копии графического интерфейса также завершает работу и комплект обслуживающих её сервисных компонентов.

Работа из командной строки

Dr.Web Desktop Security Suite (для Linux) позволяет осуществлять управление своей работой из командной строки операционной системы, для чего в его состав входит специальная утилита **drweb-ctl**.

Имеется возможность выполнять из командной строки следующие действия:

- Запуск проверки файлов, загрузочных записей дисков и исполняемых файлов активных процессов.
- Запуск проверки файлов на удаленных узлах сети (см. примечание ниже).
- Запуск обновления вирусных баз.

- Просмотр и изменение параметров конфигурации Dr.Web Desktop Security Suite (для Linux).
- Просмотр состояния компонентов программного комплекса и статистики обнаруженных угроз.
- Просмотр карантина и управление его содержимым.
- Подключение к серверу централизованной защиты и отключение от него.

Для того, чтобы команды управления Dr.Web Desktop Security Suite (для Linux), вводимые пользователем, имели эффект, должны быть запущены сервисные компоненты Dr.Web Desktop Security Suite (для Linux) (по умолчанию они автоматически запускаются при старте операционной системы).

Обратите внимание, что для выполнения некоторых управляющих команд требуются полномочия суперпользователя. Для получения полномочий суперпользователя используйте команду смены пользователя **su** или команду выполнения от имени другого пользователя **sudo**.

Утилита **drweb-ctl** поддерживает стандартное автодополнение команд управления Dr.Web Desktop Security Suite (для Linux), если функция автодополнения включена в используемой вами командной оболочке. В случае если командная оболочка не поддерживает автодополнение, вы можете настроить ее при необходимости. Для этого обратитесь к справочному руководству по используемому вами дистрибутиву операционной системы.

При завершении работы утилита возвращает код выхода в соответствии с соглашением для POSIX-совместимых систем: 0 (нуль) – если операция выполнена успешно, и не нуль – в противном случае.

Обратите внимание, что ненулевой код выхода утилита возвращает только в том случае, когда произошла внутренняя ошибка (например: утилита не смогла подключиться к некоторому компоненту, запрошенная операция не может быть выполнена и т.п.). Если утилита обнаруживает (и, возможно) нейтрализует некоторую угрозу, она возвращает код выхода 0, так как запрошенная операция (такая как `scan` и т.п.) выполнена успешно. Если необходимо установить перечень обнаруженных угроз и примененных к ним действий, то проанализируйте сообщения, которые утилита выводит на консоль.

Удаленная проверка узлов

Dr.Web Desktop Security Suite (для Linux) позволяет выполнить проверку на наличие угроз файлов, находящихся на удаленных узлах сети. В качестве таких узлов могут выступать не только полноценные вычислительные машины (рабочие станции и серверы), но и роутеры, ТВ-приставки и прочие «умные» устройства, образующие так называемый «Интернет вещей». Для выполнения удаленной проверки необходимо, чтобы удаленный узел предоставлял возможность удаленного терминального доступа через SSH (Secure Shell).

Кроме этого необходимо знать IP-адрес или доменное имя удаленного узла, имя и пароль пользователя, который может совершить удаленный доступ к системе через SSH. Указанный пользователь должен иметь права доступа к проверяемым файлам (как минимум – право на их чтение).

Данная функция может быть использована только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Устранение угроз (то есть изоляция их в карантин, удаление или лечение вредоносных объектов) средствами удаленной проверки невозможны. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров и прочих «умных» устройств можно воспользоваться механизмом обновления их прошивки, а для вычислительных машин – выполнив подключение к ним (в том числе – в удаленном терминальном режиме) и произведя соответствующие операции в их файловой системе (удаление или перемещение файлов и т.п.) или запустив антивирусное ПО, установленное на них.

Удаленная проверка реализуется только через утилиту управления из командной строки **drweb-ctl** (используется команда `remotescan`).

Формат вызова

1. Формат вызова утилиты управления из командной строки

Утилита управления работой Dr.Web Desktop Security Suite (для Linux) имеет следующий формат вызова:

```
$ drweb-ctl [<общие опции> | <команда> [<аргумент>] [<опции команды>]]
```

Где:

- *<общие опции>* – опции, которые могут быть использованы при запуске без указания команды или для любой из команды. Не являются обязательными для запуска.
- *<команда>* – команда, которая должна быть выполнена Dr.Web Desktop Security Suite (для Linux) (например, запустить проверку файлов, вывести содержимое карантина и т.п.).
- *<аргумент>* – аргумент команды. Зависит от указанной команды. У некоторых команд аргументы отсутствуют.
- *<опции команды>* – опции, управляющие работой указанной команды. Зависит от команды. У некоторых команд опции отсутствуют.

2. Общие опции

Доступны следующие общие опции:

Опция	Описание
`-h, --help`	Вывести на экран краткую общую справку и завершить работу. Для вывода справки по любой команде используйте вызов: `$ drweb-ctl <команда> -h`
`-v, --version`	Вывести на экран версию модуля и завершить работу
`-d, --debug`	Предписывает выводить на экран расширенные диагностические сообщения во время выполнения указанной команды. Не имеет смысла без указания команды. Используйте вызов: `$ drweb-ctl <команда> -d`

3. Команды

Команды управления Dr.Web Desktop Security Suite (для Linux) разделены на следующие группы:

- Команды антивирусной проверки.
- Команды управления обновлением и работой в режиме централизованной защиты.
- Команды управления конфигурацией.
- Команды управления угрозами и карантином.
- Информационные команды.

3.1. Команды антивирусной проверки

Доступны следующие команды антивирусной проверки файловой системы:

Команда	Описание
`scan <путь>`	**Назначение:** Инициировать проверку Сканером указанного файла или каталога. **Аргументы:** <*путь*> – путь к файлу или каталогу, который нужно проверить.

Команда	Описание
	Этот аргумент может быть опущен в случае использования опции `--stdin` *или* `--stdin0`. *Для проверки перечня файлов, выбираемых по некоторому условию, рекомендуется использовать утилиту* **find** *(см.* Примеры использования*) и опцию* `--stdin` *или* `--stdin0`. **Опции:** `-a [--Autonomous]` – запустить отдельную копию антивирусного ядра и Сканера для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением. `--stdin` – получить список путей для проверки из стандартного потока ввода (*stdin*). Пути в списке должны быть разделены символом новой строки ('`\n`'). `--stdin0` – получить список путей для проверки из стандартного потока ввода (*stdin*). Пути в списке должны быть разделены нулевым символом NUL ('`\0`'). При использовании опций `--stdin` и `--stdin0` пути в списке не должны содержать шаблонов. Предпочтительное использование опций `--stdin` и `--stdin0` – обработка в команде `scan` списка путей, сформированного внешней программой, например, **find** (см. Примеры использования). `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--PackerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8*

Команда	Описание
	`--ArchiveMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MailMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ContainerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MaxCompressionRatio` <*степень*> – установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее *2*. **Значение по умолчанию:** *3000* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** *On* `--OnKnownVirus` <*действие*> – действие, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза. **Возможные действия:** *REPORT, CURE, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnIncurable` <*действие*> – действие, которое следует выполнить в случае если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnSuspicious` <*действие*> – действие, которое следует выполнить в случае если эвристический анализ обнаружит подозрительный объект. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnAdware` <*действие*> – действие, которое следует выполнить в случае если обнаружена рекламная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*.

Команда	Описание
	Значение по умолчанию: *REPORT* `--OnDialers` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа дозвона. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnJokes` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа-шутка. **Возможные действия**: *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnRiskware` <*действие*> – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnHacktools` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа взлома. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления (*DELETE*) выполняется перемещение контейнера в карантин (*QUARANTINE*).
`bootscan` <*устройство*> `| ALL`	**Назначение:** Инициировать проверку Сканером загрузочной записи на указанных дисковых устройствах. Проверяются как записи MBR, так и записи VBR. **Аргументы:** <*устройство*> – путь к блочному файлу дискового устройства, загрузочная запись на котором подлежит проверке. Может быть указано несколько дисковых устройств через пробел. Обязательный аргумент. Если вместо файла устройства указано `ALL`, будут проверены все загрузочные записи на всех доступных дисковых устройствах. **Опции:** `-a [--Autonomous]` – запустить отдельную копию антивирусного ядра и Сканера для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`

Команда	Описание
	(см. ниже), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением. `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** *On* `--Cure` <*Yes*|*No*> – требуется ли делать попытки лечения обнаруженных угроз. Если указано *No*, то производится только информирование об обнаруженной угрозе. **Значение по умолчанию:** *No* `--ShellTrace` – включить вывод дополнительной отладочной информации при проверке загрузочной записи.
`procscan`	**Назначение:** Инициировать проверку Сканером содержимого исполняемых файлов, содержащих код процессов, запущенных в системе. При обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него. **Аргументы:** Нет. **Опции:** `-a [--Autonomous]` – запустить отдельную копию антивирусного ядра и Сканера для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением. `--Report` <*тип*> – установить тип отчета о проверке.

Команда	Описание
	Возможные значения: • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** *On* `--PackerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--OnKnownVirus` <*действие*> – действие, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза. **Возможные действия:** *REPORT, CURE, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnIncurable` <*действие*> – действие, которое следует выполнить в случае если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnSuspicious` <*действие*> – действие, которое следует выполнить в случае если эвристический анализ обнаружит подозрительный объект. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnAdware` <*действие*> – действие, которое следует выполнить в случае если обнаружена рекламная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnDialers` <действие> – действие, которое следует выполнить в случае если обнаружена программа дозвона. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT*

Команда	Описание
	`--OnJokes` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа-шутка. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnRiskware` <*действие*> – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnHacktools` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа взлома. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT*
`remotescan` <*узел*> <*путь*>	**Назначение:** Инициировать проверку указанного файла или каталога на указанном удаленном узле, подключившись к нему через SSH. Обратите внимание, что угрозы, обнаруженные при удаленном сканировании, не будут нейтрализованы, а также они не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). Вы можете использовать эту команду только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров, ТВ-приставок и прочих «умных» устройств вы можете воспользоваться механизмом обновления прошивки, а для вычислительных машин – выполнив подключение к ним (в том числе – в удаленном терминальном режиме) и произведя соответствующие операции в их файловой системе (удаление или перемещение файлов и т.п.) или запустив антивирусное ПО, установленное на них. **Аргументы:** <*узел*> – IP-адрес или доменное имя узла, к которому необходимо подключиться для проверки.

Команда	Описание
	<*путь*> – путь к файлу или каталогу, который нужно проверить (должен быть абсолютным). **Опции:** `-l [--Login]` <*имя*> – логин (имя пользователя) для авторизации на удаленном узле через SSH. *Если имя пользователя не указано, будет произведена попытка подключиться к удаленному узлу от имени пользователя, запустившего команду.* `-i [--Identity]` <*путь к файлу*> – файл закрытого ключа для аутентификации указанного пользователя через SSH. `-p [--Port]` <*число*> – номер порта на удаленном узле для подключения через SSH. **Значение по умолчанию:** *22* `--Password` <*пароль*> – пароль для аутентификации указанного пользователя через SSH. *Обратите внимание, что пароль передается в открытом виде.* `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--PackerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ArchiveMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MailMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8*

Команда	Описание
	`--ContainerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MaxCompressionRatio` <*степень*> – установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее *2*. **Значение по умолчанию:** *3000* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** `On`
`checkmail` <*путь к файлу*>	**Назначение:** Выполнить проверку почтового сообщения, сохраненного в файл, на наличие угроз, признаков спама, или несоответствия правилам обработки писем. В поток вывода (stdout) консоли будут возвращены результаты проверки письма, а также - какое действие было бы применено к данному письму при его проверке. **Аргументы:** <*путь к файлу*> – путь к файлу сообщения электронной почты, которое нужно проверить. Обязательный аргумент. **Опции:** `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `-r [--Rules]` <*список правил*> – указать набор правил, которые следует применить к письму при его проверке. *Если правила не указаны, будет использован набор правил, применяемых по умолчанию.* `-c [--Connect]` <*IP*>:<*port*> – указать сетевой сокет, который будет использован как адрес, с которого подключился отправитель проверяемого сообщения. `-e [--Helo]` <*имя*> – указать идентификатор клиента, отправившего сообщение (IP-адрес или FQDN узла, как для SMTP-команды HELO/EHLO).

Команда	Описание
	`-f [--From]` <*email*> – указать адрес электронной почты отправителя (как для SMTP-команды MAIL FROM). *Если адрес не указан, будет использован соответствующий адрес из письма.* `-t [--Rcpt]` <*email*> – указать адрес электронной почты получателя (как для SMTP-команды RCPT TO). *Если адрес не указан, будет использован соответствующий адрес из письма.*

Кроме команд, перечисленных в таблице выше, утилита **drweb-ctl** поддерживает дополнительные команды проверки. С их описанием вы можете ознакомиться, обратившись к документации **man** `1 drweb-ctl`.

3.2. Команды управления обновлением и работой в режиме централизованной защиты

Доступны следующие команды управления обновлением и работой в режиме централизованной защиты:

Команда	Описание
`update`	**Назначение:** Инициировать процесс обновления Компонентом обновления вирусных баз и антивирусного ядра с серверов обновлений компании «Доктор Веб» или прервать уже запущенный процесс обновления. *Команда не имеет эффекта, если Dr.Web Desktop Security Suite (для Linux) работает под управлением сервера централизованной защиты.* **Аргументы:** Нет. **Опции:** `--Stop` – прервать уже идущий процесс обновления.
`esconnect` <*сервер*>`[:`<*порт*>`]`	**Назначение:** Подключить Dr.Web Desktop Security Suite (для Linux) к указанному серверу централизованной защиты (например, Dr.Web Enterprise Server). *О режимах работы Dr.Web Desktop Security Suite (для Linux) см. в разделе* Режимы защиты.

Команда	Описание
	Аргументы: • <*сервер*> – IP-адрес или имя узла в сети, на котором располагается сервер централизованной защиты. Обязательный аргумент. • <*порт*> – номер порта, используемого сервером централизованной защиты. Необязательный аргумент, указывается только в случае, если сервер централизованной защиты использует нестандартный порт. **Опции:** `--Key` <*путь*> – путь к файлу публичного ключа сервера централизованной защиты, к которому производится подключение. `--Login` <*ID*> – логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты. `--Password` <*пароль*> – пароль для подключения к серверу централизованной защиты. `--Group` <*ID*> – идентификатор группы на сервере, в которую следует поместить рабочую станцию при подключении. `--Rate` <*ID*> – идентификатор тарифной группы, которую следует применить к рабочей станции при ее включении в группу на сервере централизованной защиты (может быть указана только совместно с опцией `--Group`). `--Compress` <*On*|*Off*> – принудительно инициировать сжатие передаваемых данных (*On*) или запретить его (*Off*). Если опция не указана, использование сжатия определяется сервером. `--Encrypt` <*On*|*Off*> – принудительно инициировать шифрование передаваемых данных (*On*) или запретить его (*Off*). Если опция не указана, использование шифрования определяется сервером. `--Newbie` – подключиться как «новичок» (получить новую учетную запись на сервере). Для выполнения этой команды требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя. При необходимости используйте команды **su** или **sudo**.
`esdisconnect`	**Назначение:** Отключить Dr.Web Desktop Security Suite (для Linux) от сервера централизованной защиты и перевести его в *одиночный (standalone)* режим работы. *Команда не имеет смысла, если Dr.Web Desktop Security Suite (для Linux) находится в одиночном (standalone) режиме.*

Команда	Описание
	Аргументы: Нет. **Опции:** Нет. Для выполнения этой команды требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя. При необходимости используйте команды **su** или **sudo**.

3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
`cfset` *<секция>*`.`*<параметр>* *<значение>*	**Назначение:** Изменить активное значение указанного параметра текущей конфигурации. *Обратите внимание, что знак равенства не используется.* **Аргументы:** • *<секция>* – имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент. • *<параметр>* – имя изменяемого параметра. Обязательный аргумент. • *<значение>* – значение, которое следует присвоить изменяемому параметру. Обязательный аргумент. Для задания значения параметров всегда используется формат *<секция>*.*<параметр>* *<значение>*. *Описание конфигурационного файла доступно в документации* **man**: `drweb.ini(5)`. **Опции:** `-a [--Add]` – не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). Также эту опцию следует использовать для добавления новых групп параметров с тегом.

Команда	Описание
	`-e [--Erase]` – не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). `-r [--Reset]` – сбросить параметр в значение по умолчанию. <*значение*> в этом случае в команде не указывается, а если указано – игнорируется. Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе – список значений) заменяется на указанное значение. Для выполнения этой команды требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя. При необходимости используйте команды **su** или **sudo**.
`cfshow [<`*секция*`>[.<`*параметр*`>]]`	**Назначение:** Вывести на экран параметры текущей конфигурации программного комплекса. Для вывода параметров по умолчанию используется формат <*секция*>.<*параметр*> = <*значение*>. Секции и параметры не установленных компонентов по умолчанию не выводятся. **Аргументы:** • <*секция*> – имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла. • <*параметр*> – имя выводимого параметра. Необязательный аргумент. Если не указан, выводятся все параметры указанной секции, в противном случае выводится только этот параметр. Если указан без имени секции, то выводятся все вхождения этого параметра во все секции конфигурационного файла. **Опции:** `--Uncut` – вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. В противном случае выводятся только те параметры, которые используются имеющимися компонентами. `--Changed` – вывести только те параметры, значения которых отличаются от значений по умолчанию. `--Ini` – вывести значения параметров в формате INI-файла: сначала в отдельной строке выводится имя секции, заключенное в квадратные скобки, после чего параметры, принадлежащие секции,

Команда	Описание
	перечисляются в виде пар <*параметр*> = <*значение*> (по одному в строке). `--Value` – вывести только значение указанного параметра. В этом случае аргумент <*параметр*> обязателен.
`reload`	**Назначение:** Перезапустить сервисные компоненты Dr.Web Desktop Security Suite (для Linux). При этом заново открываются журналы, перечитывается файл конфигурации, и производится попытка перезапустить аварийно завершенные компоненты. **Аргументы:** Нет. **Опции:** Нет.

3.4. Команды управления угрозами и карантином

Доступны следующие команды управления угрозами и карантином:

Команда	Описание
`threats [`<*действие*> <*объект*>`]`	**Назначение:** Выполнить указанное действие с обнаруженными ранее угрозами по их идентификаторам. Тип действия определяется указанной опцией команды. Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. Для каждой угрозы выводится следующая информация: • Идентификатор, присвоенный угрозе (порядковый номер). • Полный путь к инфицированному файлу. • Информация об угрозе (имя, тип по классификации компании «Доктор Веб»). • Информация о файле: размер, пользователь-владелец, дата последнего изменения. • История действий с инфицированным файлом: обнаружение, применявшиеся действия и т.п. **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (CTRL+C прерывает ожидание).

Команда	Описание
	Если эта опция указана совместно с любой из опций-действий, она игнорируется. `--Cure` <*список угроз*> – выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Quarantine` <*список угроз*> – выполнить перемещение в карантин перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Delete` <*список угроз*> – выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Ignore` <*список угроз*> – игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить данную команду ко всем обнаруженным угрозам, вместо <*список угроз*> следует указать `All`. Например, команда: `$ drweb-ctl threats --Quarantine All` перемещает в карантин все обнаруженные объекты с угрозами.
`quarantine [`<*действие*> <*объект*>`]`	**Назначение:** Применить действие к указанному объекту, находящемуся в карантине. Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине, с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в карантин. Для каждого изолированного объекта выводится следующая информация: • Идентификатор, присвоенный изолированному объекту в карантине. • Исходный путь к файлу, перемещенному в карантин. • Дата перемещения файла в карантин. • Информация о файле: размер, пользователь-владелец, дата последнего изменения. • Информация об угрозе (имя, тип по классификации компании «Доктор Веб»). **Аргументы:** Нет. **Опции:** `-a [--Autonomous]` – запустить отдельную копию Сканера для выполнения заданного действия с карантином, завершив ее работу после окончания действия.

Команда	Описание
	Эта опция может быть применена совместно с любой из опций, указанных ниже. `--Delete` <*объект*> – удалить указанный объект из карантина. *Обратите внимание, что удаление из карантина – необратимая операция.* `--Cure` <*объект*> – попытаться вылечить указанный объект в карантине. *Обратите внимание, что, даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина следует воспользоваться командой восстановления* `--Restore`. `--Restore` <*объект*> – восстановить указанный объект из карантина в исходное место. *Обратите внимание, что для выполнения этой команды может потребоваться, чтобы* **drweb-ctl** *была запущена от имени суперпользователя. Восстановить файл из карантина можно даже если он инфицирован.* `--TargetPath` <*путь*> – восстановить объект из карантина в указанное место: как файл с указанным именем, если <*путь*> – это путь к файлу, или в указанный каталог (если <*путь*> – это путь к каталогу). *Обратите внимание, что опция применяется только совместно с командой восстановления* `--Restore`. В качестве <*объект*> используется идентификатор объекта в карантине. Если требуется применить данную команду ко всем объектам, находящимся в карантине, вместо <*объект*> следует указать `All`. Например, команда: `$ drweb-ctl quarantine --Restore All` восстанавливает из карантина все имеющиеся в нем объекты. *Обратите внимание, что для варианта* `--Restore All` *дополнительная опция* `--TargetPath`*, если указана, должна задавать путь к каталогу, а не к файлу.*

3.5. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	**Назначение:** Вывести на экран информацию о работающих модулях Dr.Web Desktop Security Suite (для Linux). Для каждого модуля выводится следующая информация: • Внутреннее имя. • Идентификатор процесса **GNU/Linux** (PID). • Состояние (запущен, остановлен и т.п.). • Код ошибки, если работа компонента завершена вследствие ошибки. • Дополнительная информация (опционально). Для демона управления конфигурацией (**drweb-configd**) в качестве дополнительной информации выводятся: • Перечень установленных компонентов – *Installed*. • Перечень компонентов, запуск которых должен быть обеспечен демоном – *Should run*. **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об изменении состояния модулей и выводить их на экран сразу, как только они будут поступать (CTRL+C прерывает ожидание).
`baseinfo`	**Назначение:** Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз. Выводится следующая информация: • Версия антивирусного ядра. • Дата и время выпуска используемых вирусных баз. • Число доступных вирусных записей. • Момент последнего успешного обновления вирусных баз и антивирусного ядра. • Момент следующего запланированного автоматического обновления. **Аргументы:** Нет. **Опции:** Нет.

Команда	Описание
`certificate`	**Назначение:** Вывести на экран содержимое доверенного сертификата Dr.Web, который используется Dr.Web Desktop Security Suite (для Linux) для доступа к защищенным соединениям с целью их проверки, если эта проверка включена в настройках. Для сохранения сертификата в файл <*cert_name*>`.pem` вы можете использовать команду: `$ drweb-ctl certificate > <cert_name>.pem` **Аргументы:** Нет. **Опции:** Нет.
`license`	**Назначение:** Вывести на экран информацию об активной лицензии, получить демонстрационную лицензию или получить ключевой файл для уже зарегистрированной лицензии (например – на сайте компании). Если не указана ни одна опция, то выводится следующая информация (если используется лицензия для одиночного режима работы): • Номер лицензии. • Дата и время окончания действия лицензии. Если используется лицензия, выданная сервером централизованной защиты (для работы в режиме централизованной защиты или в мобильном режиме), выводится соответствующая информация. **Аргументы:** Нет. **Опции:** `--GetDemo` – запросить демонстрационный ключ сроком на месяц, и получить его, в случае если не нарушены условия получения демонстрационного периода. `--GetRegistered` <*серийный номер*> – получить лицензионный ключевой файл для указанного серийного номера, если не нарушены условия получения нового ключевого файла (например, программа не находится в режиме централизованной защиты, когда лицензией управляет сервер централизованной защиты). *Если серийный номер не является серийным номером демонстрационного периода, то он должен быть предварительно зарегистрирован на сайте компании.* Подробнее о лицензировании продуктов Dr.Web см. в разделе Лицензирование.

Команда	Описание
	Для регистрации серийного номера и для получения демонстрационного периода требуется наличие подключения к сети Интернет.

Примеры использования

Примеры использования утилиты **drweb-ctl**:

1. Проверка объектов

1.1. Простые команды проверки

1. Выполнить проверку каталога `/home` с параметрами по умолчанию:

```
$ drweb-ctl scan /home
```

2. Выполнить проверку списка путей, перечисленных в файле `daily_scan` (по одному пути в строке файла):

```
$ drweb-ctl scan --stdin < daily_scan
```

3. Выполнить проверку загрузочной записи на дисковом устройстве *sda*:

```
$ drweb-ctl bootscan /dev/sda
```

4. Выполнить проверку запущенных процессов:

```
$ drweb-ctl procscan
```

1.2. Проверка файлов, отобранных по критериям

В нижеприведенных примерах для формирования выборки файлов, подлежащих проверке, используется результат работы утилиты **find**. Полученный перечень файлова передается команде **drweb-ctl** `scan` с параметром `--stdin` или `--stdin0`.

1. Выполнить проверку списка файлов, возвращенных утилитой **find**, и разделенных символом NUL ('\0'):

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Проверить все файлы всех каталогов, начиная с корневого, находящихся на одном разделе файловой системы:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Проверить все файлы всех каталогов, начиная с корневого, кроме файлов `/var/log/messages` и `/var/log/syslog`:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |
drweb-ctl scan -stdin
```

4. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователю *root*:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям *root* и *admin*:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям с UID из диапазона 1000 – 1005:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Проверить файлы во всех каталогах, начиная с корневого, но находящихся не более чем на пятом уровне вложенности относительно корневого каталога:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Проверить файлы в корневом каталоге, не заходя во вложенные каталоги:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Проверить файлы во всех каталогах, начиная с корневого, при этом следовать по встречающимся символическим ссылкам:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Проверить файлы во всех каталогах, начиная с корневого, при этом не следовать по встречающимся символическим ссылкам:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Проверить во всех каталогах, начиная с корневого, файлы, созданные не позже, чем 01 мая 2017 года:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. Проверка дополнительных объектов

1. Проверка объектов, расположенном в каталоге `/tmp` на удаленном узле *192.168.0.1*, подключившись к нему через SSH как пользователь *user* с паролем *passw*:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

2. Проверка сообщения электронной почты, сохраненного в файл `email.eml`, с использованием набора правил по умолчанию:

```
$ drweb-ctl checkmail email.eml
```

2. Управление конфигурацией

1. Вывести на экран информацию о текущем составе программного комплекса, включая информацию о запущенных компонентах:

```
$ drweb-ctl appinfo
```

2. Вывести на экран все параметры из секции `[Root]` активной конфигурации:

```
$ drweb-ctl cfshow Root
```

3. Задать значение 'No' для параметра **Start** в секции `[LinuxSpider]` активной конфигурации (это приведет к остановке работы монитора файловой системы SplDer Guard):

```
# drweb-ctl cfset LinuxSpider.Start No
```

Обратите внимание на то, что в данном случае требуются полномочия суперпользователя. Пример вызова этой же команды с использованием **sudo** для временного повышения полномочий:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Выполнить принудительное обновление антивирусных компонентов продукта:

```
$ drweb-ctl update
```

5. Выполнить перезагрузку конфигурации для компонентов установленного программного комплекса Dr.Web:

```
# drweb-ctl reload
```

Обратите внимание на то, что в данном случае требуются полномочия суперпользователя. Пример вызова этой же команды с использованием **sudo** для временного повышения полномочий:

```
$ sudo drweb-ctl reload
```

6. Подключить продукт к серверу централизованной защиты, работающему на узле *192.168.0.1*, при условии, что открытый ключ сервера располагается в файле `/home/user/cskey.pub`:

```
$ drweb-ctl esconnect 192.168.0.1 --Key /home/user/cskey.pub
```

7. Отключить продукт от сервера централизованной защиты:

```
# drweb-ctl esdisconnect
```

Обратите внимание на то, что в данном случае требуются полномочия суперпользователя. Пример вызова этой же команды с использованием **sudo** для временного повышения полномочий:

```
$ sudo drweb-ctl esdisconnect
```

3. Управление угрозами

1. Вывести на экран информацию об обнаруженных угрозах:

```
$ drweb-ctl threats
```

2. Переместить все файлы, содержащие необезвреженные угрозы, в карантин:

```
$ drweb-ctl threats --Quarantine All
```

3. Вывести на экран список файлов, перемещенных в карантин:

```
$ drweb-ctl quarantine
```

4. Восстановить все файлы из карантина:

```
$ drweb-ctl quarantine --Restore All
```

4. Пример работы в режиме автономной копии

1. Проверить файлы и обработать карантин в режиме автономной копии:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=Quarantine
$ drweb-ctl quarantine -a --Delete All
```

Первая команда проверит файлы в каталоге `/home/user` в режиме автономной копии, и файлы, содержащие известные вирусы, будут помещены в карантин. Вторая команда обработает содержимое карантина (так же в режиме автономной копии) и удалит все содержащиеся в нем объекты.

Приложения

Приложение А. Виды компьютерных угроз

Под термином *«угроза»* в данной классификации следует понимать любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они также могут нанести вред пользователю.

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Большая часть вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы делят по типу файлов, которые они инфицируют:

- *Файловые вирусы* инфицируют файлы операционной системы (обычно исполняемые файлы и динамические библиотеки) и активизируются при обращении к инфицированному файлу.
- *Макро-вирусы* инфицируют документы, которые используют программы из пакета **Microsoft® Office** (и другие программы, которые используют макросы, написанные, например, на языке **Visual Basic**). *Макросы* – это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в **Microsoft® Word** макросы могут запускаться при открытии, закрытии или сохранении документа).
- *Скрипт-вирусы* пишутся на языках сценариев (скриптов) и в большинстве случаев инфицируют другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях.
- *Загрузочные вирусы* инфицируют загрузочные сектора дисков и разделов, а также главные загрузочные сектора жестких дисков. Они занимают очень мало памяти и

остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- *Шифрованные вирусы* шифруют свой код при каждом новом инфицировании, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры.
- *Полиморфные вирусы* используют помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур.
- *Стелс-вирусы* (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т.д.) и по инфицируемым ими операционным системам.

Компьютерные черви

В последнее время вредоносные программы типа «компьютерный червь» стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через сеть Интернет) и рассылает свои функциональные копии на другие компьютеры. Для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

В компании «Доктор Веб» червей делят по способу (среде) распространения:

- *Сетевые черви* распространяются посредством различных сетевых протоколов и протоколов обмена файлами.
- *Почтовые черви* распространяются посредством почтовых протоколов (POP3, SMTP и т.д.).
- *Чат-черви* распространяются, используя популярные программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т.д.).

Троянские программы

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

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловых сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполнять другие типы угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- *Бэкдоры* – это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы; они прописывают себя в реестре, модифицируя ключи.
- *Руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (*User Mode Rootkits – UMR*), и руткиты, работающие в режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет обнаружение и обезвреживание) (*Kernel Mode Rootkits – KMR*).
- *Клавиатурные перехватчики* (*кейлоггеры*) используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действия является кража

личной информации (например, сетевых паролей, логинов, номеров банковских карт и т.д.).

- *Кликеры* переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак).
- *Прокси-трояны* предоставляют злоумышленнику анонимный выход в сеть Интернет через компьютер жертвы.

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (файерволах, брандмауэрах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут пользоваться администраторы для проверки надежности своих сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например в веб-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

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

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-серверы и т.д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типов компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать в карантин, а также отправлять на анализ специалистам антивирусной лаборатории «Доктор Веб».

Приложение Б. Устранение компьютерных угроз

Все антивирусные продукты, разработанные компанией Dr.Web, применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Методы обнаружения угроз

Сигнатурный анализ

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

Origins Tracing™

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

Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и шифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи *эмулятора* – программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (буфером эмуляции). При этом инструкции не передаются на центральный процессор для реального исполнения.

Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Эвристический анализ

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

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

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

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

Действия с угрозами

В продуктах Dr.Web реализована возможность применять определенные действия к обнаруженным объектам для обезвреживания компьютерных угроз. Пользователь может оставить автоматически применяемые к определенным типам угроз действия, заданные по умолчанию, изменить их или выбирать нужное действия для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий:

- **Ignore** *(Игнорировать, Пропустить)* – Пропустить обнаруженную угрозу, не предпринимая никаких действий;
- **Report** *(Информировать)* – Уведомить о наличии угрозы, но ничего не делать с инфицированным объектом;
- **Cure** *(Лечить)* – Попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое. Обратите внимание, что это действие применимо не ко всем видам угроз;
- **Quarantine** *(Переместить в карантин, Изолировать)* – Переместить инфицированный объект (если он допускает эту операцию) в специальный каталог карантина с целью его изоляции;
- **Delete** *(Удалить)* – Безвозвратно удалить инфицированный объект.

Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления выполняется перемещение контейнера в карантин.

Приложение В. Техническая поддержка

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

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

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

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

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

Приложение Г. Описание известных ошибок

В данном разделе представлены:

- Описание ошибок, определяемых по коду ошибки.
- Описание ошибок, не имеющих кода, но определяемых по симптомам их проявления.

Если описание возникшей у вас ошибки отсутствует в данном разделе, рекомендуется обратиться в техническую поддержку, сообщив код ошибки и описав обстоятельства ее появления.

Рекомендации по идентификации ошибок

- Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).
- Для облегчения идентификации ошибки рекомендуется настроить вывод журнала в отдельный файл и разрешить вывод расширенной отладочной информации. Для этого выполните следующие команды:

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Для возврата настроек ведения журнала по умолчанию выполните следующие команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Ошибки, определяемые по коду

Сообщение об ошибке	*Ошибка связи с монитором*
Код ошибки	x1
Описание	Ошибка связи некоторого компонента с демоном управления конфигурацией Dr.Web ConfigD.

Устранение ошибки:

1. Перезапустите демон управления конфигурацией, выполнив команду

```
# service drweb-configd restart
```

2. Проверьте, что в системе установлен, настроен и корректно функционирует механизм аутентификации **PAM**. Если это не так, установите и настройте его (за подробностями обратитесь к руководствам по администрированию вашего дистрибутива ОС).
3. Если перезапуск демона управления конфигурацией при корректно настроенном **PAM** не помогает, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией.
4. Если демон управления конфигурацией запустить не удается, попробуйте переустановить пакет `drweb-configd`.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Операция уже выполняется*
Код ошибки	`x2`
Описание	Операция, запрошенная пользователем, в данный момент уже выполняется.

Устранение ошибки:

1. Подождите завершения выполняющейся операции и при необходимости повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Операция ожидает выполнения*
Код ошибки	`x3`
Описание	Операция, запрошенная пользователем, в данный момент ожидает выполнения (возможно, производится установление сетевого соединения или осуществляется загрузка и инициализация какого-либо компонента программного комплекса, требующая продолжительного времени).

Устранение ошибки:

1. Подождите начала выполнения операции и при необходимости повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Прервано пользователем*
Код ошибки	`x4`
Описание	Выполнявшееся действие было прервано пользователем (возможно, оно выполнялось слишком долго).

Устранение ошибки:

1. Повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Операция отменена*
Код ошибки	`x5`
Описание	Выполнявшееся действие было отменено (возможно, оно выполнялось слишком долго).

Устранение ошибки:

1. Повторите требуемое действие снова.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Соединение IPC разорвано*
Код ошибки	`x6`
Описание	IPC-соединение с некоторым компонентом программного комплекса разорвано (скорее всего, компонент завершил свою работу из-за простоя или вследствие команды пользователя).

Устранение ошибки:

1. Если выполнявшаяся операция не была завершена, то повторите ее запуск снова. В противном случае разрыв соединения не является ошибкой.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый размер сообщения IPC*
Код ошибки	x7
Описание	В процессе обмена данными между компонентами получено сообщение недопустимого размера.

Устранение ошибки:

1. Перезапустите программный комплекс, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый формат сообщения IPC*
Код ошибки	x8
Описание	В процессе обмена данными между компонентами получено сообщение недопустимого формата.

Устранение ошибки:

1. Перезапустите программный комплекс, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Не готов*
Код ошибки	x9
Описание	Требуемое действие не может быть выполнено, потому что запрошенный компонент или устройство еще не инициализированы.

Устранение ошибки:

1. Повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Компонент не установлен*
Код ошибки	x10

Описание	Некоторая функция программного комплекса Dr.Web Desktop Security Suite (для Linux) недоступна, поскольку реализующий ее компонент не установлен.

Устранение ошибки:

1. Выполните отдельную установку или переустановку пакета, содержащего требуемый компонент:
   - `drweb-filecheck`, если не установлен Сканер.
   - `drweb-spider`, если не установлен SpIDer Guard.
   - `drweb-gated`, если не установлен SpIDer Gate.
   - `drweb-update`, если не установлен Компонент обновления.
2. Если ошибка повторится, или если вы не можете определить, какой компонент отсутствует, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Неожиданное сообщение IPC*
Код ошибки	`x11`
Описание	В процессе обмена данными между компонентами получено недопустимое сообщение.

Устранение ошибки:

1. Перезапустите программный комплекс, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Нарушение протокола IPC*
Код ошибки	`x12`
Описание	В процессе обмена данными между компонентами произошло нарушение протокола обмена данными.

Устранение ошибки:

1. Перезапустите программный комплекс, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Неизвестное состояние подсистемы*
Код ошибки	x13
Описание	Обнаружено, что некоторая подсистема программного комплекса, требуемая для выполнения операции, находится в неизвестном состоянии.

Устранение ошибки:

1. Повторите операцию.
2. При повторении ошибки перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Путь должен быть абсолютным*
Код ошибки	x20
Описание	Требуется абсолютный (т.е. начинающийся от корня файловой системы) путь к файлу или каталогу, а указан относительный путь.

Устранение ошибки:

1. Измените путь к файлу или каталогу таким образом, чтобы он был абсолютным, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недостаточно памяти для завершения операции*
Код ошибки	x21
Описание	Для выполнения требуемой операции не хватает памяти (например, попытка распаковать слишком большой файл).

Устранение ошибки:

1. Попробуйте увеличить объем памяти, доступной процессам программного комплекса (например, изменив лимиты при помощи команды **ulimit**), перезапустить программный комплекс и повторить операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Ошибка ввода-вывода*
Код ошибки	`x22`
Описание	Произошла ошибка ввода/вывода (например, дисковое устройство еще не инициализировано или раздел файловой системы более недоступен).

Устранение ошибки:

1. Проверьте доступность требуемого устройства ввода/вывода или раздела файловой системы. При необходимости выполните его монтирование и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Нет такого файла или каталога*
Код ошибки	`x23`
Описание	Указанный объект файловой системы (файл или каталог) отсутствует, возможно, он был удален.

Устранение ошибки:

1. Проверьте правильность указанного пути. При необходимости исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Доступ запрещён*
Код ошибки	`x24`
Описание	Недостаточно прав для доступа к указанному объекту файловой системы (файлу или каталогу).

Устранение ошибки:

1. Проверьте правильность указанного пути и наличие необходимых прав у компонента. При необходимости доступа к объекту, измените права доступа к нему или повысьте права компонента и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Не каталог*
Код ошибки	`x25`
Описание	Ожидался путь к каталогу, однако указанный объект файловой системы не является каталогом.

Устранение ошибки:

1. Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Файл данных повреждён*
Код ошибки	`x26`
Описание	Данные, к которым производится обращение, повреждены.

Устранение ошибки:

1. Повторите операцию.
2. При повторении ошибки перезапустите программный комплекс, выполнив команду

   ```
   # service drweb-configd restart
   ```

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Файл уже существует*
Код ошибки	`x27`
Описание	При попытке создать файл было обнаружено, что файл с таким именем уже существует.

Устранение ошибки:

1. Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Файловая система только для чтения*

Код ошибки	x28
Описание	При попытке создать или изменить объект файловой системы (каталог, файл или сокет) было обнаружено, что файловая система доступна только для чтения.
Устранение ошибки: 1. Проверьте правильность указанного пути. Исправьте путь так, чтобы он вел на раздел файловой системы, доступный для записи, и повторите операцию.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Ошибка сети*
Код ошибки	x29
Описание	Произошла сетевая ошибка (возможно, внезапно перестал отвечать удаленный узел или не удается установить требуемое соединение).
Устранение ошибки: 1. Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Не дисковое устройство*
Код ошибки	x30
Описание	Производится попытка обращения к устройству ввода/вывода, которое не является дисковым устройством.
Устранение ошибки: 1. Проверьте правильность указанного имени устройства. Исправьте путь так, чтобы он вел к дисковому устройству, и повторите операцию.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Неожиданный конец файла*
Код ошибки	x31
Описание	При чтении данных неожиданно был достигнут конец файла.
Устранение ошибки:	

1. Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к правильному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Файл был изменён*
Код ошибки	`x32`
Описание	При сканировании файла было обнаружено, что он был изменен.

Устранение ошибки:

1. Повторите операцию сканирования.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Специальный файл*
Код ошибки	`x33`
Описание	При доступе к объекту файловой системы было обнаружено, что это не регулярный файл (т.е. это каталог, сокет или иной объект файловой системы).

Устранение ошибки:

1. Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к регулярному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Имя уже используется*
Код ошибки	`x34`
Описание	При попытке создать объект файловой системы (каталог, файл или сокет) было обнаружено, что объект с таким именем уже существует.

Устранение ошибки:

1. Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Хост отключён*

Код ошибки	x35
Описание	Обнаружено, что удаленный узел недоступен по сети.
Устранение ошибки: 1. Проверьте доступность требуемого узла сети. При необходимости исправьте адрес узла сети и повторите операцию.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Достигнут предел использования ресурса*
Код ошибки	x36
Описание	Достигнут предел использования некоторого ресурса.
Устранение ошибки: 1. Проверьте доступность требуемого ресурса. При необходимости увеличьте лимит на использование ресурса и повторите операцию.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Различные точки монтирования*
Код ошибки	x37
Описание	Производится попытка выполнить восстановление файла, требующая его перемещение между каталогами файловой системы, принадлежащим различным точкам монтирования.
Устранение ошибки: 1. Выберите другой путь для восстановления файла и повторите операцию.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Ошибка распаковки*
Код ошибки	x38
Описание	Не удалось распаковать архив (возможно, он защищен паролем или поврежден)
Устранение ошибки:	

1. Убедитесь что файл не поврежден. Если архив защищен паролем, снимите защиту, указав правильный пароль, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Вирусная база повреждена*
Код ошибки	`x40`
Описание	Обнаружено, что повреждены вирусные базы.

Устранение ошибки:

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **`VirusBaseDir`** в секции `[Root]` файла конфигурации).

   Для просмотра и исправления пути воспользуйтесь командами утилиты управления из командной строки:

   - Для просмотра текущего значения параметра введите команду:

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Для установки нового значения параметра введите команду:

     ```
     # drweb-ctl cfset Root.VirusBaseDir <новый путь>
     ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

     ```
     # drweb-ctl cfset Root.VirusBaseDir -r
     ```

2. Обновите вирусные базы любым из указанных ниже способов:

   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Не поддерживаемая версия вирусных баз*
Код ошибки	`x41`
Описание	Обнаружено, имеющиеся вирусные базы предназначены для старой версии программы.

Устранение ошибки:

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в секции [Root] файла конфигурации).

   Для просмотра и исправления пути воспользуйтесь командами утилиты управления из командной строки:

   - Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   - Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <новый путь>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

   ```
   $ drweb-ctl update
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Вирусная база пуста*
Код ошибки	x42
Описание	Обнаружено, что вирусные базы пусты.

Устранение ошибки:

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в секции [Root] файла конфигурации).

   Для просмотра и исправления пути воспользуйтесь командами утилиты управления из командной строки:

   - Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   - Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новый путь>
```

- Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Объект не может быть вылечен*
Код ошибки	x43
Описание	Попытка применить действие «Лечить» к неизлечимому объекту при нейтрализации угрозы.

Устранение ошибки:

1. Выберите действие, допустимое для данного объекта и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Не поддерживаемая комбинация вирусных баз*
Код ошибки	x44
Описание	Обнаружено, что имеющийся набор вирусных баз несовместим.

Устранение ошибки:

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в секции [Root] файла конфигурации).

   Для просмотра и исправления пути воспользуйтесь командами утилиты управления из командной строки:

   - Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

- Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новый путь>
```

- Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Достигнут предел проверки*
Код ошибки	x45
Описание	При сканировании объекта превышены заданные ограничения (например, на величину распакованного файла, на глубину уровней вложенности и т.п.).

Устранение ошибки:

1. Измените ограничения для сканирования объектов (в настройках соответствующего компонента) любым удобным вам способом:
   - Используя страницу настроек этого компонента на окне управления настройками приложения.
   - При помощи команд **drweb-ctl** `cfshow` и **drweb-ctl** `cfset`.
2. После изменения настроек повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Неверные учетные данные пользователя*
Код ошибки	x47
Описание	Попытка пройти аутентификацию с неверными учетными данными пользователя.

Устранение ошибки:

1. Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Пользователь не имеет требуемых прав*
Код ошибки	`x48`
Описание	Попытка пройти авторизацию с учетными данными пользователя, не имеющего требуемых прав.

Устранение ошибки:

1. Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый токен доступа*
Код ошибки	`x49`
Описание	Компонент программного комплекса предъявил некорректный токен авторизации при попытке получения доступа к операции, требующей повышенные права.

Устранение ошибки:

1. Пройдите аутентификацию, указав правильные учетные данные пользователя, имеющего необходимые полномочия, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый аргумент*
Код ошибки	`x60`
Описание	При попытке исполнить некоторую команду был указан недопустимый аргумент.

Устранение ошибки:

1. Повторите требуемое действие снова, указав допустимый аргумент.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимая операция*
Код ошибки	`x61`
Описание	Совершена попытка выполнить недопустимую команду.

Устранение ошибки:

1. Повторите требуемое действие снова, указав допустимую команду.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Требуются полномочия суперпользователя*
Код ошибки	`x62`
Описание	Требуемое действие может быть выполнено только пользователем, обладающим полномочиями суперпользователя.

Устранение ошибки:

1. Повысьте свои права до суперпользователя и повторите требуемое действие снова. Для повышения прав вы можете воспользоваться командами **su** и **sudo**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Не разрешено в режиме централизованной защиты*
Код ошибки	`x63`
Описание	Требуемое действие может быть выполнено только при работе программного комплекса в одиночном (standalone) режиме.

Устранение ошибки:

1. Переведите программный комплекс в одиночный режим и повторите операцию снова.
2. Для перевода программного комплекса в одиночный режим:
   - Сбросьте флажок **Включить режим централизованной защиты** на странице настроек **Режим**.
   - Или выполните команду:

```
# drweb-ctl esdisconnect
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Не поддерживаемая ОС*

Код ошибки	x64
Описание	Операционная система, установленная на узле, не поддерживается программным комплексом.

Устранение ошибки:

1. Установите операционную систему из списка, указанного в системных требованиях.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Функция не реализована*
Код ошибки	x65
Описание	Производятся попытки использования функций некоторого компонента, которые не реализованы в текущей версии.

Устранение ошибки:

1. Выполните сброс настроек программного комплекса в значения по умолчанию, очистив содержимое файла конфигурации `/etc/opt/drweb.com/drweb.ini`. Рекомендуется выполнить предварительное сохранение резервной копии файла. Например:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

2. После очистки файла конфигурации перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Неизвестный параметр*
Код ошибки	x66
Описание	Файл конфигурации содержит параметры, неизвестные или не поддерживаемые в текущей версии программного комплекса.

Устранение ошибки:

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` в любом текстовом редакторе, удалите строку, содержащую недопустимый параметр, сохраните файл и перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите программный комплекс.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Неизвестная секция*
Код ошибки	`x67`
Описание	Файл конфигурации содержит секции, неизвестные или не поддерживаемые в текущей версии программного комплекса.

Устранение ошибки:

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` в любом текстовом редакторе и удалите неизвестную секцию, после чего сохраните файл и перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите программный комплекс.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимое значение параметра*
Код ошибки	`x68`
Описание	Некоторый параметр в файле конфигурации имеет недопустимое для этого параметра значение.

Устранение ошибки:

1. Измените значение параметра любым удобным для вас способом:
   - Используя страницу настроек этого компонента на окне управления настройками приложения.
   - При помощи команд **drweb-ctl** `cfshow` и **drweb-ctl** `cfset`.

   Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту, использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.
2. Также вы можете отредактировать непосредственно файл конфигурации `/etc/opt/drweb.com/drweb.ini`. Для этого откройте его в любом текстовом редакторе, найдите строку, содержащую недопустимое значение параметра, задайте допустимое значение, сохраните файл и перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```
3. Если предыдущие шаги не помогли, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите программный комплекс.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимое состояние*
Код ошибки	`x69`
Описание	Некоторый компонент или весь программный комплекс находятся в недопустимом состоянии для выполнения запрошенной операции.

Устранение ошибки:

1. Повторите требуемое действие через некоторое время.
2. При повторении ошибки перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Разрешено только одно значение*
Код ошибки	`x70`
Описание	Некоторый параметр в файле конфигурации имеет список значений, что недопустимо для этого параметра.

Устранение ошибки:

1. Измените значение параметра любым удобным для вас способом:
   - Используя страницу настроек этого компонента на окне управления настройками приложения.
   - При помощи команд **drweb-ctl** `cfshow` и **drweb-ctl** `cfset`.

   Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту, использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.
2. Также вы можете отредактировать непосредственно файл конфигурации `/etc/opt/drweb.com/drweb.ini`. Для этого откройте его в любом текстовом редакторе, найдите строку, содержащую недопустимое значение параметра, задайте допустимое значение, сохраните файл и перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```
3. Если предыдущие шаги не помогли, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите программный комплекс.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимое имя тега*
Код ошибки	`x71`
Описание	Некоторая секция в файле конфигурации, в имя которой включен уникальный идентификатор-тег, имеет недопустимое значение тега.

Устранение ошибки:

1. Если ошибка произошла при использовании команды

```
# drweb-ctl cfset <секция>.<параметр> <новое значение>
```

то повторите сохранение, задав для тега допустимое значение.

2. Если секция сохранена непосредственно в файл конфигурации `/etc/opt/drweb.com/drweb.ini`, то отредактируйте его. Для этого откройте его в любом текстовом редакторе, найдите заголовок секции, содержащий недопустимое значение тега, задайте для тега допустимое значение, сохраните файл и перезапустите программный комплекс, выполнив команду:

```
# service drweb-configd restart
```

3. Если вышеприведенные шаги не помогут, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   После очистки файла конфигурации перезапустите программный комплекс.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Запись не найдена*
Код ошибки	x80
Описание	При попытке обратиться к информации о найденной угрозе было обнаружено, что информация о ней отсутствует (возможно, угроза уже была обработана другим компонентом программного комплекса).

Устранение ошибки:

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Запись обрабатывается в данный момент*
Код ошибки	x81
Описание	При попытке обратиться к информации о найденной угрозе было обнаружено, что в данный момент времени она уже обрабатывается другим компонентом программного комплекса.

Устранение ошибки:

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Файл уже находится в карантине*
Код ошибки	`x82`
Описание	При попытке перемещения файла с найденной угрозой в карантин было обнаружено, что он уже в карантине (скорее всего, угроза уже была обработана другим компонентом программного комплекса).

Устранение ошибки:

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Не удалось сохранить резервную копию перед обновлением*
Код ошибки	`x89`
Описание	Перед началом загрузки обновлений с сервера обновлений не удалось выполнить сохранение резервной копии обновляемых файлов.

Устранение ошибки:

1. Проверьте правильность пути к каталогу, хранящему резервные копии обновляемых файлов и при необходимости исправьте его (параметр **`BackupDir`** в секции `[Update]` файла конфигурации).

   Для просмотра и исправления пути вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

     ```
     $ drweb-ctl cfshow Update.BackupDir
     ```

   - Для установки нового значения параметра введите команду:

     ```
     # drweb-ctl cfset Update.BackupDir <новый путь>
     ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

     ```
     # drweb-ctl cfset Update.BackupDir -r
     ```

2. Обновите вирусные базы любым из указанных ниже способов:

- Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
- Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
- Выполните команду:

```
$ drweb-ctl update
```

3. Если ошибка повторится, проверьте, что пользователь, от имени которого исполняется Компонент обновления, имеет права на запись в каталог, указанный в параметре **BackupDir**. Имя пользователя указано в параметре **RunAsUser**. При необходимости измените имя пользователя, изменив значение параметра **RunAsUser**, или предоставьте недостающие права в свойствах каталога.
4. Если ошибка повторится, попробуйте переустановить пакет `drweb-update`.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый DRL-файл*
Код ошибки	`x90`
Описание	Обнаружено, что нарушена структура одного из файлов списков серверов обновлений.

Устранение ошибки:

1. Проверьте правильность пути к файлу списка серверов и при необходимости исправьте его (параметры с именем вида ***DrlPath** в секции `[Update]` файла конфигурации. Для этого воспользуйтесь командами утилиты управления из командной строки.
   - Для просмотра текущего значения параметра введите команду (<**DrlPath*> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значение всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

```
$ drweb-ctl cfshow Update[.<*DrlPath>]
```

   - Для установки нового значения параметра введите команду (<**DrlPath*> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlPath> <новый путь>
```

   - Для сброса значения параметра в значение по умолчанию введите команду (<**DrlPath*> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlPath> -r
```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

   ```
   $ drweb-ctl update
   ```

3. Если ошибка повторится, выполните установку или переустановку пакетов `drweb-bases` и `drweb-dws`, после чего выполните обновление.
4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый LST-файл*
Код ошибки	`x91`
Описание	Обнаружено, что нарушена структура файла, содержащего перечень обновляемых вирусных баз.

Устранение ошибки:

1. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

   ```
   $ drweb-ctl update
   ```

2. Если ошибка повторится, попробуйте переустановить пакет `drweb-update`.
3. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый сжатый файл*

Код ошибки	x92
Описание	Обнаружено, что нарушена структура загруженного файла, содержащего обновления.

Устранение ошибки:

1. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Ошибка аутентификации на прокси-сервере*
Код ошибки	x93
Описание	Не удалось подключиться к серверам обновлений через прокси-сервер, заданный в настройках.

Устранение ошибки:

1. Проверьте правильность параметров подключения к прокси-серверу (задаются в параметре с именем **Proxy** в секции [Update] файла конфигурации). При необходимости смените используемый прокси-сервер или откажитесь от использования прокси-сервера.

   Для просмотра и задания параметров подключения перейдите на страницу основных настроек.

   Также вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

     ```
     $ drweb-ctl cfshow Update.Proxy
     ```

   - Для установки нового значения параметра введите команду:

     ```
     # drweb-ctl cfset Update.Proxy <новые параметры>
     ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

     ```
     # drweb-ctl cfset Update.Proxy -r
     ```

2. Обновите вирусные базы любым из указанных ниже способов:

- Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
- Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
- Выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Нет доступных серверов обновлений*
Код ошибки	x94
Описание	Не удалось подключиться ни к одному из серверов обновлений.

Устранение ошибки:

1. Проверьте доступность сети и исправьте при необходимости сетевые настройки.
2. Если доступ к сети возможен только через прокси-сервер, задайте параметры подключения к прокси-серверу (определяются в параметре с именем **Proxy** в секции [Update] файла конфигурации). При необходимости смените используемый прокси-сервер или откажитесь от использования прокси-сервера.

   Для просмотра и задания параметров подключения перейдите на страницу основных настроек.

   Также вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Update.Proxy
   ```

   - Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Update.Proxy <новые параметры>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Update.Proxy -r
   ```

3. Если параметры сетевого подключения (в том числе – используемого прокси-сервера) правильные, а ошибка происходит, убедитесь в том, что вы используете доступный список серверов обновления. Перечень используемых серверов обновления указывается в параметрах вида ***DrlPath** в секции [Update] файла конфигурации. Обратите внимание, что если параметры вида ***CustomDrlPath** указывают на существующий корректный файл списка серверов, то указанные там серверы будут использоваться вместо серверов стандартной зоны обновления (значение, указанное в соответствующем параметре ***DrlPath**, игнорируется).

Для просмотра и задания параметров подключения вы можете воспользоваться командами утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду (<*DrlPath> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значение всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

```
$ drweb-ctl cfshow Update[.<*DrlPath>]
```

Для установки нового значения параметра введите команду (<*DrlPath> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlPath> <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду (<*DrlPath> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlPath> -r
```

4. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый формат ключевого файла*
Код ошибки	x95
Описание	Нарушен формат ключевого файла.

Устранение ошибки:

1. Проверьте наличие ключевого файла и правильности пути к нему. Путь к ключевому файлу задается в параметре **KeyPath** в секции [Root] файла конфигурации.

   Для просмотра параметров лицензии и задания пути к ключевому файлу перейдите на страницу Менеджера лицензий главного окна приложения.

   Также вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.KeyPath
```

- Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.KeyPath <путь к файлу>
```

- Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.KeyPath -r
```

2. Если у вас отсутствует ключевой файл, или используемый ключевой файл поврежден, приобретите и установите его. Описание ключевого файла, способы приобретения и установки описаны в разделе Лицензирование.
3. Для установки имеющегося у вас ключевого файла вы можете воспользоваться Менеджером лицензий.
4. Параметры текущей лицензии вы также можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Срок действия лицензии истек*
Код ошибки	x96
Описание	Срок действия имеющейся у вас лицензии истёк.

Устранение ошибки:

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы можете воспользоваться Менеджером лицензий.
3. Параметры текущей лицензии вы также можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Истек тайм-аут сетевой операции*
Код ошибки	x97
Описание	

Устранение ошибки:

1. Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

2. Если ошибка возникает при получении обновлений, то дополнительно проверьте параметры использования прокси-сервера, при необходимости смените используемый прокси-сервер или откажитесь от его использования.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимая контрольная сумма*
Код ошибки	`x98`
Описание	Обнаружено, что нарушена контрольная сумма загруженного файла, содержащего обновления.

Устранение ошибки:

1. Выполните обновление повторно через некоторое время любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый демонстрационный ключевой файл*
Код ошибки	`x99`
Описание	Используемый демонстрационный ключевой файл недействителен (например, он был получен для другого компьютера).

Устранение ошибки:

1. Запросите новый демонстрационный период для данного компьютера, или приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы можете воспользоваться Менеджером лицензий.
3. Параметры текущей лицензии вы также можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Лицензионный ключевой файл заблокирован*
Код ошибки	`x100`
Описание	Используемая вами лицензия была заблокирована (возможно, нарушены условия лицензионного соглашения на использование программного продукта Dr.Web).

Устранение ошибки:

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы можете воспользоваться Менеджером лицензий.
3. Параметры текущей лицензии вы также можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимая лицензия*
Код ошибки	`x101`
Описание	Используемая вами лицензия предназначена для другого программного продукта или не содержит необходимых разрешений для работы компонентов установленного у вас продукта.

Устранение ошибки:

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы можете воспользоваться Менеджером лицензий.
3. Параметры текущей лицензии вы также можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимая конфигурация*
Код ошибки	`x102`
Описание	Некоторый компонент программного комплекса не может функционировать из-за неправильных настроек конфигурации.

Устранение ошибки:

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Если ошибка вызвана компонентом SpIDer Guard, то скорее всего задан способ работы компонента, который не поддерживается операционной системой. Проверьте установленный режим работы компонента и при необходимости исправьте его, указав значение `AUTO` (параметр **`Mode`** в секции `[LinuxSpider]` файла конфигурации).

   Для просмотра и исправления режима работы вы можете воспользоваться командами утилиты управления из командной строки.

   - Для установки значения `AUTO` введите команду

   ```
   # drweb-ctl cfset LinuxSpider.Mode AUTO
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду

   ```
   # drweb-ctl cfset LinuxSpider.Mode -r
   ```

   Если ошибка повторится, выполните ручную сборку и установку загружаемого модуля ядра для компонента SpIDer Guard.

   

   Обратите внимание, что работа компонента SpIDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список протестированных дистрибутивов **Linux** (см. раздел Системные требования).

3. Если ошибка вызвана компонентом SpIDer Gate, то скорее всего наблюдается конфликт с другим брандмауэром. Например, известно, что SpIDer Gate конфликтует с брандмауэром **FirewallD** в ОС **Fedora**, **CentOS**, **Red Hat Enterprise Linux** (при каждом перезапуске **FirewallD** портит правила маршрутизации трафика, задаваемые SpIDer Gate). Для устранения ошибки перезагрузите программный комплекс, выполнив команду

   ```
   # service drweb-configd restart
   ```

   или

   ```
   # drweb-ctl reload
   ```

   

   Обратите внимание, что если не запретить работу **FirewallD**, указанная ошибка SpIDer Gate может повторяться при каждом перезапуске **FirewallD**, в том числе – при перезапуске ОС. Вы можете устранить данную ошибку, отключив **FirewallD** (обратитесь к руководству **FirewallD** в составе руководства по вашей ОС).

4. Если ошибка вызвана другим компонентом, то попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:
   - При помощи команд **drweb-ctl** `cfshow` и **drweb-ctl** `cfset`.

- Отредактировав вручную файл конфигурации, удалив все параметры из секции компонента.

5. Если предыдущие шаги не помогли, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите программный комплекс, выполнив команду

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый исполняемый файл*
Код ошибки	`x104`
Описание	Не запускается некоторый компонент программного комплекса, потому что неправильно указан путь к его исполняемому файлу или содержимое файла испорчено.

Устранение ошибки:

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Проверьте значение пути к исполняемому файлу компонента в конфигурации программного комплекса (параметр **`ExePath`** в секции компонента), выполнив команду (замените <*секция компонента*> на название соответствующей секции файла конфигурации)

   ```
   $ drweb-ctl cfshow <секция компонента>.ExePath
   ```

3. Попробуйте сбросить путь в значение по умолчанию, выполнив команду (замените <*секция компонента*> на название соответствующей секции файла конфигурации)

   ```
   # drweb-ctl cfset <секция компонента>.ExePath -r
   ```

4. Если предыдущие шаги не помогли, попробуйте переустановить пакет соответствующего компонента.
   - `drweb-filecheck`, если поврежден исполняемый файл компонента Сканер.
   - `drweb-spider`, если поврежден исполняемый файл SpIDer Guard.
   - `drweb-gated`, если поврежден исполняемый файл SpIDer Gate.

- `drweb-update`, если поврежден исполняемый файл Компонента обновления.

5. Если ошибка повторится, или если вы не можете определить, исполняемый файл какого компонента поврежден, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Ядро Virus-Finding Engine недоступно*
Код ошибки	`x105`
Описание	Отсутствует или недоступен файл антивирусного ядра Dr.Web Virus-Finding Engine (требуется для поиска угроз).

Устранение ошибки:

1. Проверьте правильность пути к файлу антивирусного ядра **drweb32.dll** и при необходимости исправьте его (параметр **`CoreEnginePath`** в секции `[Root]` файла конфигурации).

   Для просмотра и исправления пути вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду

   ```
   $ drweb-ctl cfshow Root.CoreEnginePath
   ```

   - Для установки нового значения параметра введите команду

   ```
   # drweb-ctl cfset Root.CoreEnginePath <новый путь>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду

   ```
   # drweb-ctl cfset Root.CoreEnginePath -r
   ```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

   ```
   $ drweb-ctl update
   ```

3. Если путь правильный и ошибка повторится после обновления вирусных баз, переустановите пакет `drweb-bases`.
4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Вирусные базы отсутствуют*
Код ошибки	`x106`
Описание	Обнаружено, что вирусные базы отсутствуют.

Устранение ошибки:

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **`VirusBaseDir`** в секции `[Root]` файла конфигурации).

   Для просмотра и исправления пути вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   - Для установки нового значения параметра введите команду

   ```
   # drweb-ctl cfset Root.VirusBaseDir <новый путь>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```

2. Обновите вирусные базы любым из указанных ниже способов:

   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

   ```
   $ drweb-ctl update
   ```

3. Если ошибка повторится, выполните отдельную установку или переустановку пакета `drweb-bases`, содержащего антивирусное ядро и вирусные базы.
4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Процесс завершен по сигналу*
Код ошибки	`x107`
Описание	Компонент завершил свою работу (возможно, из-за простоя или вследствие команды пользователя).

Устранение ошибки:

1. Если выполнявшаяся операция не была завершена, то повторите ее запуск снова. В противном случае завершение работы не является ошибкой.
2. Если компонент постоянно завершает свою работу, попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:
   - При помощи команд **drweb-ctl** `cfshow` и **drweb-ctl** `cfset`.
   - Отредактировав вручную файл конфигурации (удалив все параметры из секции компонента).
3. Если это не помогло, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Непредвиденное завершение процесса*
Код ошибки	`x108`
Описание	Компонент неожиданно завершил свою работу вследствие сбоя.

Устранение ошибки:

1. Попробуйте повторить выполнявшуюся операцию.
2. Если компонент постоянно аварийно завершает свою работу, попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:
   - При помощи команд **drweb-ctl** `cfshow` и **drweb-ctl** `cfset`.
   - Отредактировав вручную файл конфигурации (удалив все параметры из секции компонента).

3. Если это не помогло, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите программный комплекс, выполнив команду:

   ```
   # service drweb-configd restart
   ```

4. Если ошибка повторится после сброса настроек программного комплекса, попробуйте переустановить пакет компонента.
5. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Обнаружено несовместимое ПО*
Код ошибки	`x109`
Описание	Компонент программного комплекса не может функционировать, поскольку обнаружено программное обеспечение, препятствующие его корректной работе.

Устранение ошибки:

1. Если ошибка вызвана компонентом SpIDer Gate, то скорее всего проблема в том, что в системе присутствует программное обеспечение, формирующее для системного брандмауэра **NetFilter** правила, препятствующие корректной работе SpIDer Gate. Например, это может быть **Shorewall** или **SuseFirewall2** (в ОС **SUSE Linux**). Основная причина конфликта SpIDer Gate с другими приложениями, настраивающими системный брандмауэр **NetFilter**, в том, что они периодически выполняют проверку целостности заданной ими системы правил и перезаписывают ее.

   Настройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе SpIDer Gate. Если не удается настроить конфликтующее приложение таким образом, чтобы оно не мешало работе SpIDer Gate, отключите это приложение с запретом его запуска при последующих загрузках ОС. Приложение **SuseFirewall2** (в ОС **SUSE Linux**) можно попытаться настроить следующим образом:

   1) Откройте файл конфигурации **SuseFirewall2** (по умолчанию это файл `/etc/sysconfig/SuSEfirewall2`).

2) Найдите в файле блок текста:

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

3) Установите значение параметра в `"no"`:

```
FW_LO_NOTRACK="no"
```

4) Перезапустите **SuseFirewall2**, выполнив команду:

```
# rcSuSEfirewall2 restart
```

Обратите внимание, что если в настройках **SuseFirewall2** параметр `FW_LO_NOTRACK` отсутствует, то для устранения конфликта необходимо отключить приложение с запретом его запуска при последующих загрузках ОС (например, это необходимо сделать в ОС **SUSE Linux Enterprise Server** 11).

5) После изменения настроек или отключения конфликтующего приложения перезапустите SplDer Gate (отключите, а затем включите его на соответствующей странице).

2. Если ошибка вызвана другим компонентом, то отключите или перенастройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимая библиотека VadeRetro*
Код ошибки	x110
Описание	Отсутствует, недоступен или испорчен файл антиспам-библиотеки **VadeRetro** (требуется при проверке электронной почты).

Устранение ошибки:

1. Проверьте правильность пути к файлу библиотеки **vaderetro.so** и при необходимости исправьте его (параметр **VaderetroLibPath** в секции `[Root]` файла конфигурации).

   Для просмотра и исправления пути вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду

```
$ drweb-ctl cfshow Root.VaderetroLibPath
```

- Для установки нового значения параметра введите команду

```
# drweb-ctl cfset Root.VaderetroLibPath <новый путь>
```

- Для сброса значения параметра в значение по умолчанию введите команду

```
# drweb-ctl cfset Root.VaderetroLibPath -r
```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

```
$ drweb-ctl update
```

3. Если путь правильный и ошибка повторится после обновления вирусных баз, переустановите пакет `drweb-maild`.
4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Базы категорий веб-ресурсов отсутствуют*
Код ошибки	`x112`
Описание	Обнаружено, что базы категорий веб-ресурсов отсутствуют.

Устранение ошибки:

1. Проверьте правильность пути к каталогу базы данных категорий веб-ресурсов и при необходимости исправьте его (параметр **`DwsDir`** в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду

```
$ drweb-ctl cfshow Root.DwsDir
```

   Для установки нового значения параметра введите команду

```
# drweb-ctl cfset Root.DwsDir <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду

```
# drweb-ctl cfset Root.DwsDir -r
```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите кнопку **Обновить** на странице управления обновлениями главного окна приложения.
   - Выберите пункт **Обновить** в контекстном меню индикатора приложения в области уведомлений рабочего стола.
   - Выполните команду:

```
$ drweb-ctl update
```

3. Если ошибка повторится, выполните отдельную установку или переустановку пакета `drweb-dws`, содержащего базы категорий веб-ресурсов.
4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недоступен модуль ядра Linux для SpIDer Guard*
Код ошибки	`x113`
Описание	SpIDer Guard для работы требуется модуль ядра **Linux**, который отсутствует.

Устранение ошибки:

1. Проверьте установленный режим работы компонента и при необходимости исправьте его, указав значение `AUTO` (параметр **Mode** в секции `[LinuxSpider]` файла конфигурации).

   Для просмотра и исправления режима вы можете воспользоваться командами утилиты управления из командной строки.
   - Для установки значения `AUTO` введите команду

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
```

   - Для сброса значения параметра в значение по умолчанию введите команду

```
# drweb-ctl cfset LinuxSpider.Mode -r
```

2. Если ошибка повторится, выполните ручную сборку и установку загружаемого модуля ядра для компонента SpIDer Guard.

Обратите внимание, что работа компонента SpIDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список протестированных дистрибутивов **Linux** (см. раздел Системные требования).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*SpIDer Gate недоступен*
Код ошибки	`x117`
Описание	Отсутствует компонент SpIDer Gate (требуется для проверки сетевых соединений).

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-gated** и при необходимости исправьте его (параметр **`ExePath`** в секции `[GateD]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow GateD.ExePath
   ```

   - Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset GateD.ExePath <новый путь>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset GateD.ExePath -r
   ```

2. При отсутствии настроек компонента SpIDer Gate в конфигурации, или если ошибка возникает при указании правильного пути, установите или переустановите пакет `drweb-gated`.
3. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Компонент MailD недоступен*
Код ошибки	`x118`

Описание	Отсутствует компонент Dr.Web MailD (требуется для проверки электронной почты).

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-maild** и при необходимости исправьте его (параметр **ExePath** в секции `[MailD]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow MailD.ExePath
   ```

   - Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset MailD.ExePath <новый путь>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset MailD.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web MailD в конфигурации, или если ошибка возникает при указании правильного пути, установите или переустановите пакет `drweb-maild`.
3. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Scanning Engine недоступен*
Код ошибки	`x119`
Описание	Невозможно проверять файлы, поскольку отсутствует или не запускается компонент Dr.Web Scanning Engine (**drweb-se**), используемый для проверки наличия вредоносного содержимого. Невозможна работа компонентов: Сканер, SpIDer Guard, SpIDer Gate (частично).

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-se** и при необходимости исправьте его (параметр **ExePath** в секции `[ScanEngine]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow ScanEngine.ExePath
```

- Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset ScanEngine.ExePath <новый путь>
```

- Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset ScanEngine.ExePath -r
```

2. В случае возникновения ошибки при указании правильного пути:

   - Выполните команду

   ```
   $ drweb-ctl rawscan /
   ```

   если в выводе на экран присутствует строка `Error: No valid license provided`, то это означает, что отсутствует действующий ключевой файл. Зарегистрируйте продукт и получите лицензию. Если лицензия вами получена, то проверьте наличие ключевого файла и установите его при необходимости.

   - Если вы используете 64-битную версию ОС, убедитесь, что у вас установлены библиотеки поддержки 32-битных приложений (см. раздел Системные требования), и установите их в случае необходимости.

   Для проверки наличия библиотеки поддержки 32-битных приложений используйте команду:

   ```
   $ dpkg -l | grep <libname>
   ```

   где <*libname*> – имя библиотеки (**libc6-i386** или **glibc.i686**, в зависимости от вашей системы). Если команда не выведет никакого результата, то библиотеку требуется установить, используя системный менеджер пакетов, иначе установки не требуется и **drweb-se** не доступен по другим причинам.

   После установки библиотеки поддержки 32-битных приложений перезапустите Dr.Web Desktop Security Suite (для Linux), выполнив команду

   ```
   # service drweb-configd restart
   ```

   - Если ваша ОС использует подсистему безопасности **SELinux**, настройте политику безопасности для модуля **drweb-se** (см. раздел Настройка политик безопасности SELinux).

3. При отсутствии настроек компонента в конфигурации, или в случае если предыдущие шаги не помогли, установите или переустановите пакет `drweb-se`.

4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Сканер недоступен*
Код ошибки	`x120`
Описание	Невозможно осуществлять проверку файлов, поскольку отсутствует модуль **drweb-filecheck**, используемый для проверки файлов. Невозможна работа компонентов: Сканер, SplDer Guard.

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-filecheck** и при необходимости исправьте его (параметр **`ExePath`** в секции `[FileCheck]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow FileCheck.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset FileCheck.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset FileCheck.ExePath -r
   ```

2. В случае возникновения ошибки при указании правильного пути:

   - Если вы используете 64-битную версию ОС, убедитесь, что у вас установлены библиотеки поддержки 32-битных приложений (см. раздел Системные требования), и установите их в случае необходимости.

   Для проверки наличия библиотеки поддержки 32-битных приложений используйте команду:

   ```
   $ dpkg -l | grep <libname>
   ```

   где <*libname*> – имя библиотеки (**libc6-i386** или **glibc.i686**, в зависимости от вашей системы). Если команда не выведет никакого результата, то библиотеку требуется установить, используя системный менеджер пакетов, иначе установки не требуется и **drweb-filecheck** не доступен по другим причинам.

   После установки библиотеки поддержки 32-битных приложений перезапустите Dr.Web Desktop Security Suite (для Linux), выполнив команду:

   ```
   # service drweb-configd restart
   ```

   - Если ваша ОС использует подсистему безопасности **SELinux**, настройте политику безопасности для модуля **drweb-filecheck** (см. раздел Настройка политик безопасности SELinux).

3. При отсутствии настроек компонента в конфигурации, или в случае если предыдущие шаги не помогли, установите или переустановите пакет `drweb-filecheck`.

4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*ES Agent недоступен*
Код ошибки	`x121`
Описание	Отсутствует компонент Dr.Web ES Agent (требуется для подключения к серверу централизованной защиты).

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-esagent** и при необходимости исправьте его (параметр **`ExePath`** в секции `[ESAgent]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

     ```
     $ drweb-ctl cfshow ESAgent.ExePath
     ```

   - Для установки нового значения параметра введите команду:

     ```
     # drweb-ctl cfset ESAgent.ExePath <новый путь>
     ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

     ```
     # drweb-ctl cfset ESAgent.ExePath -r
     ```

2. При отсутствии настроек компонента в конфигурации, или если ошибка возникает при указании правильного пути, установите или переустановите пакет `drweb-esagent`.
3. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Компонент Firewall для Linux недоступен*
Код ошибки	`x122`
Описание	Невозможно контролировать сетевые соединения, поскольку отсутствует или не может быть запущен вспомогательный модуль

	drweb-firewall, предназначенный для перенаправления соединений. Невозможна работа компонентов: SplDer Gate.

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-firewall** и при необходимости исправьте его (параметр **ExePath** в секции `[LinuxFirewall]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow LinuxFirewall.ExePath
   ```

   - Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset LinuxFirewall.ExePath <новый путь>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset LinuxFirewall.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web Firewall для Linux в конфигурации, или если ошибка возникает при указании правильного пути, установите или переустановите пакет `drweb-firewall`.
3. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Network Checker недоступен*
Код ошибки	`x123`
Описание	Невозможно контролировать сетевые соединения, поскольку отсутствует или не может быть запущен вспомогательный модуль **drweb-netcheck**, предназначенный для проверки файлов, загруженных по сети. Невозможна работа компонентов: SplDer Gate (частично).

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-netcheck** и при необходимости исправьте его (параметр **ExePath** в секции `[NetCheck]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow NetCheck.ExePath
```

- Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset NetCheck.ExePath <новый путь>
```

- Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset NetCheck.ExePath -r
```

2. При отсутствии настроек компонента в конфигурации, или если ошибка возникает при указании правильного пути, установите или переустановите пакет `drweb-netcheck`.
3. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Компонент CloudD недоступен*
Код ошибки	`x124`
Описание	Отсутствует компонент Dr.Web CloudD (требуется для обращения к облаку Dr.Web Cloud).

Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-cloudd** и при необходимости исправьте его (параметр **`ExePath`** в секции `[CloudD]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   - Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow CloudD.ExePath
```

   - Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset CloudD.ExePath <новый путь>
```

   - Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset CloudD.ExePath -r
```

2. При отсутствии настроек компонента в конфигурации, или если ошибка возникает при указании правильного пути, установите или переустановите пакет `drweb-cloudd`.
3. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Непредвиденная ошибка*
Код ошибки	`x125`
Описание	Возникла непредвиденная ошибка в работе некоторого компонента.

Устранение ошибки:

1. Попробуйте перезапустить программный комплекс, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Ошибки, не имеющие кодов

Симптомы	После установки модуля ядра SplDer Guard работа операционной системы аварийно завершается с ошибкой ядра «*Kernel panic*»
Описание	Работа модуля ядра SplDer Guard невозможна в среде исполнения ядра ОС (например, ОС работает в среде гипервизора **Xen**).

Устранение ошибки:

1. Отмените загрузку модуля ядра SplDer Guard (модуль ядра имеет имя `drweb`), добавив в загрузчике **grub** строку

```
drweb.blacklist=yes
```

   в строку параметров загрузки ядра ОС.
2. После загрузки ОС удалите модуль ядра `drweb.ko` из каталога дополнительных модулей ядра `/lib/modules/`uname -r`/extra`.
3. Установите для SplDer Guard режим работы *AUTO*, выполнив команды:

```
# drweb-ctl cfset LinuxSpider.Mode Auto
# drweb-ctl reload
```

4. Если используемая вами ОС не поддерживает механизм **fanotify**, или использование этого режима не позволяет использовать SplDer Guard для полноценного контроля файловой системы (актуально для систем **GNU/Linux** с мандатными моделями доступа, например – **Astra Linux SE**), и, таким образом, использование режима *LKM* является обязательным для контроля файловой системы, то откажитесь от использования гипервизора **Xen**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы	Главное окно Dr.Web Desktop Security Suite (для Linux) неактивно, индикатор в области уведомлений рабочего стола отображается с символом критической ошибки, а выпадающее меню индикатора содержит только один неактивный пункт **Запуск**
Описание	Dr.Web Desktop Security Suite (для Linux) не может запуститься, поскольку основной сервисный компонент **drweb-configd** недоступен.

Устранение ошибки:

1. Перезапустите Dr.Web Desktop Security Suite (для Linux), выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если эта команда вернет ошибку или не даст никакого эффекта, выполните отдельную установку или переустановку пакета `drweb-configd`.
3. Обратите внимание, что это также может означать, что в системе для аутентификации пользователей не используется **PAM**. Если это так, что установите и настройте его.
4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы	1. Индикатор в области уведомлений рабочего стола не отображается после входа в систему. 2. Попытка выполнить команду запуска графического интерфейса `$ drweb-gui` приводит к запуску главного окна Dr.Web Desktop Security Suite (для Linux).
Описание	Возможно, данная ошибка связана с отсутствием в вашей системе дополнительной библиотеки **libappindicator1**.

Устранение ошибки:

1. Проверьте наличие в вашей системе пакета `libappindicator1`, выполнив команду:

   ```
   # dpkg -l | grep libappindicator1
   ```

2. Если команда не выведет никакого результата, то установите этот пакет, используя любой из имеющихся в системе менеджер пакетов. После этого выполните повторный вход в систему (*log in*).

3. Обратите внимание, что это также может означать, что в системе для аутентификации пользователей не используется **PAM**. Если это так, что установите и настройте его.
4. Если предыдущие действия не помогли, удалите Dr.Web Desktop Security Suite (для Linux) целиком, после чего установите его повторно.

   Инструкции по установке и удалению продукта и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite (для Linux) и Удаление Dr.Web Desktop Security Suite (для Linux).

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы	1. После отключения SpIDer Gate перестают работать сетевые соединения (как исходящие, так, возможно, и входящие – по протоколам SSH, FTP). 2. Поиск в правилах **NetFilter** (**iptables**) с использованием команды `# iptables-save | grep "comment --comment --comment"` выдает непустой результат.
Описание	Данная ошибка связана с некорректной работой **NetFilter** (**iptables**) версии младше 1.4.15, заключающейся в том, что правила с уникальной меткой (комментарием) добавляются некорректно, вследствие чего SpIDer Gate при завершении своей работы не может удалить добавленные им правила перенаправления сетевых соединений.

Устранение ошибки:

1. Повторно включите SpIDer Gate, чтобы он выполнял проверку.
2. Если SpIDer Gate требуется оставить выключенным, удалите некорректные правила **NetFilter** (**iptables**), выполнив команду:

   ```
   # iptables-save | grep -v "comment --comment --comment" | iptables-restore
   ```

   Обратите внимание, что вызов команд **iptables-save** и **iptables-restore** требует наличия прав суперпользователя. Для получения прав суперпользователя вы можете воспользоваться командами **su** и **sudo**. Также обратите внимание, что указанная команда удалит из перечня правил все правила с некорректно добавленным комментарием, например, добавленные другими приложениями, выполняющими корректировку маршрутизации соединений.

Дополнительная информация:

- Для предотвращения возникновения данной ошибки в дальнейшем рекомендуется обновить операционную систему (или, как минимум, **NetFilter** до версии 1.4.15 или новее).
- Кроме этого вы можете включить ручной режим перенаправления соединений для SpIDer Gate, задавая требуемые правила вручную при помощи утилиты **iptables** (не рекомендуется).
- Дополнительные сведения см. в документации **man**: `drweb-firewall(1)`, `drweb-gated(1)`, `iptables(8)`.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы	Двойной щелчок по значку файла или каталога в графическом файловом менеджере вместо его открытия запускает проверку в **Dr.Web Desktop Security Suite (для Linux)**.
Описание	Графическая оболочка выполнила автоматическую ассоциацию файлов некоторого типа и/или каталогов с действием **Открыть в Dr.Web Desktop Security Suite (для Linux)**.

Устранение ошибки:

1. Отмените ассоциацию между файлами данного типа и приложением **Dr.Web Desktop Security Suite (для Linux)**. Настроенные ассоциации фиксируются в файле `mimeapps.list` или `defaults.list`. Файлы, определяющие локальные настройки, измененные в профиле пользователя, хранятся в каталоге `~/.local/share/applications/` или `~/.config/` (обычно эти каталоги имеют атрибут «скрытый»).
2. Откройте файл `mimeapps.list` или `defaults.list` в любом текстовом редакторе (обратите внимание, что для редактирования системного файла ассоциаций вам потребуются полномочия суперпользователя, при необходимости используйте команды **su** или **sudo**).
3. Найдите в файле секцию `[Default Applications]`, а в ней строки ассоциаций вида *<MIME-тип>*`=drweb-gui.desktop`, например:

   ```
   [Default Applications]
   inode/directory=drweb-gui.desktop
   text/plain=drweb-gui.desktop;gedit.desktop
   ```

4. Если в правой части (после равенства) строки ассоциации кроме `drweb-gui.desktop` содержатся также ссылки на другие приложения, удалите из строки только ссылку на приложение **drweb-gui** (`drweb-gui.desktop`). Если ассоциация содержит ссылку только на приложение **drweb-gui**, удалите строку ассоциации полностью.
5. Сохраните измененный файл.

Дополнительная информация:

- Для проверки текущих ассоциаций вы можете воспользоваться утилитами **xdg-mime**, **xdg-open** и **xdg-settings** (входят в состав пакета `xdg-utils`).
- Сведения о работе утилит **xdg** см. в документации **man**: `xdg-mime(1)`, `xdg-open(1)`, `xdg-settings(1)`.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Приложение Д. Сборка модуля ядра для SpIDer Guard

Если операционная система не предоставляет механизм **fanotify**, используемый SpIDer Guard для мониторинга действий с объектами файловой системы, он может использовать специальный загружаемый модуль, работающий в пространстве ядра (LKM-модуль).

По умолчанию в составе SpIDer Guard поставляется скомпилированный модуль ядра для ОС, не предоставляющих сервис **fanotify**. Также совместно со SpIDer Guard поставляется архив в формате `tar.bz2`, содержащий исходные файлы загружаемого модуля ядра, чтобы его можно было собрать вручную.

> LKM-модуль, используемый SpIDer Guard, предназначен для работы с ядрами **GNU/Linux** версий 2.6.* и новее.

Архив с исходными кодами загружаемого модуля ядра располагается в каталоге основных файлов Dr.Web Desktop Security Suite (для Linux) (по умолчанию – `/opt/drweb.com`), в подкаталоге `share/drweb-spider-kmod/src`, и имеет имя вида `drweb-spider-kmod-<версия>-<дата>.tar.bz2`. Также в каталоге `drweb-spider-kmod` имеется сценарий проверки `check-kmod-install.sh`, запустив который, вы получите информацию, поддерживает ли используемая вами операционная система предварительно скомпилированные версии модулей ядра, уже включенные в состав продукта. В случае если нет, на экран будет выведена рекомендация выполнить ручную сборку.

Если указанный каталог `drweb-spider-kmod` отсутствует, установите пакет `drweb-spider-kmod`.

> Для выполнения ручной сборки LKM-модуля из исходных кодов необходимо обладать правами суперпользователя. Для получения прав суперпользователя при сборке воспользуйтесь командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

Инструкция по сборке модуля ядра

1. Распакуйте архив с исходными кодами в любой каталог. Например, команда

   ```
   # tar -xf drweb-spider-kmod-<версия>-<дата>.tar.bz2
   ```

   распакует архив непосредственно в каталог, содержащий сам архив, создав в нем подкаталог с именем файла архива (обратите внимание, что для записи в каталог, содержащий архив, необходимы права суперпользователя).
2. Перейдите в созданный каталог с исходными кодами и выполните команду:

   ```
   # make
   ```

В случае возникновения ошибок на этапе *make* следует их устранить (см. ниже) и выполнить компиляцию повторно.

3. После успешного окончания этапа *make* выполните следующие команды:

```
# make install
# depmod
```

4. После успешной сборки модуля ядра и его регистрации в системе, выполните дополнительно настройку SplDer Guard, указав ему режим работы с модулем ядра, выполнив команду

```
# drweb-ctl cfset LinuxSpider.Mode LKM
```

Также допускается установка значения `AUTO` вместо значения `LKM`. В этом случае SplDer Guard будет пробовать использовать не только модуль ядра, но и системный механизм **fanotify**. Для получения дополнительной информации используйте документацию **man**: `drweb-spider(1)`.

Возможные ошибки сборки

На этапе выполнения сборки *make* могут возникать ошибки. В случае возникновения ошибок проверьте следующее:

- Для успешной сборки требуется наличие **Perl** и компилятора **GCC**. Если они отсутствуют, установите их.
- В некоторых ОС может потребоваться предварительная установка пакета `kernel-devel`.
- В некоторых ОС сборка может завершиться ошибкой из-за неправильно определенного пути к каталогу исходных кодов ядра. В этом случае используйте команду **make** с параметром `KDIR=<`*путь к исходным кодам ядра*`>`. Обычно они размещаются в каталоге `/usr/src/kernels/<`*версия ядра*`>`.

Обратите внимание, что версия ядра, выдаваемая командой **uname** `-r`, может не совпадать с именем каталога `<`*версия ядра*`>`.

Предметный указатель

Предметный указатель

Предметный указатель