Dr.WEB

для Linux

Руководство пользователя

Dr.Web для Linux
Версия 11.1
Руководство пользователя
01.09.2023

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12-а

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Введение

Благодарим вас за приобретение Dr.Web 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 UNIX), в установке и использовании Dr.Web для Linux версии 11.1.

Если у вас уже установлен Dr.Web для Linux предыдущей версии, и вы желаете обновить его до версии 11.1, выполните переход на новую версию (см. раздел Переход на новую версию).

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 ввести с клавиатуры в командную строку операционной системы (в терминале или эмуляторе терминала), в руководстве предваряются символом приглашения ко вводу `$` или `#`, определяющим, какие полномочия пользователя необходимы для исполнения указанной 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`.

Перечень сокращений приведен в разделе Приложение Е. Список сокращений.

О продукте

В этом разделе содержится следующая информация о продукте:

- Назначение.
- Основные функции.
- Структура Dr.Web для Linux.
- Размещение карантина.
- Полномочия для работы с файлами.
- Режимы работы.

Назначение

Dr.Web 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 Doctor Web 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 для Linux, в компании Doctor Web разработаны также антивирусные решения для операционных систем семейства UNIX (таких, как FreeBSD), IBM OS/2, Novell NetWare, macOS и Windows. Кроме того, разработаны антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением ОС Android, Symbian, BlackBerry.

Компоненты Dr.Web 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 Dr.Web 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.
- *Облачные технологии обнаружения угроз*. Производится 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 Doctor Web. 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 Dr.Web для Linux, позволяет также проверять на наличие угроз файловые системы удаленных узлов сети, предоставляющих удаленный доступ к ним через SSH или Telnet.

Вы можете использовать удаленное сканирование только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле воспользуйтесь средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров и прочих «умных» устройств вы можете обновить прошивку, а для вычислительных машин — подключиться 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 установленное на них антивирусное ПО (программное обеспечение).

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. Помимо стандартного режима мониторинга имеется возможность включить усиленный («параноидальный») режим, в котором доступ к файлам будет блокироваться монитором до момента окончания их проверки (это позволяет предотвратить случаи доступа к файлу, когда он содержит угрозу, но результат его проверки становится известным уже после того, как приложение успело получить доступ к файлу). Усиленный режим мониторинга повышает уровень безопасности, но замедляет доступ приложений к еще не проверенным файлам.
3. **Мониторинг сетевых соединений**. Отслеживаются попытки обращения к серверам в интернете (веб-серверам, файловым серверам) по протоколам HTTP и FTP для блокировки доступа пользователей к веб-сайтам и узлам, адреса которых отмечены как нежелательные для посещения, а также для предотвращения загрузки вредоносных файлов.
4. **Проверка сообщений электронной почты** для предотвращения получения и отправки сообщений электронной почты, содержащих инфицированные файлы и нежелательные ссылки, а также классифицированных как спам.

   Проверка сообщений электронной почты и файлов, загружаемых по сети, на наличие в них вирусов и других угроз, производится «на лету». В зависимости от поставки, компонент Dr.Web Anti-Spam может отсутствовать в составе Dr.Web для Linux. В этом случае спам-проверка сообщений электронной почты не производится.

   Для определения нежелательных ссылок используются как поставляемая вместе с Dr.Web для Linux автоматически обновляемая база данных категорий веб-ресурсов, так и черные и белые списки, ведущиеся пользователем вручную. Дополнительно Dr.Web для Linux может обращаться к сервису Dr.Web Cloud, чтобы проверить, не отмечен ли веб-сайт, к которому пытается обратиться пользователь, или ссылка на который содержится в сообщении электронной почты, как вредоносный другими антивирусными продуктами Dr.Web.

Если какие-либо сообщения электронной почты неправильно распознаются компонентом Dr.Web Anti-Spam, рекомендуется отправлять их на специальные почтовые адреса для анализа и повышения качества работы спам-фильтра. Для этого каждое такое сообщение сохраните в отдельный файл типа `.eml`. Сохраненные файлы прикрепите к сообщению электронной почты, которое отправьте на соответствующий служебный адрес.

- nonspam@drweb.com — если оно содержит файлы писем, *ошибочно признанных спамом*;
- spam@drweb.com — если оно содержит файлы писем, *ошибочно не определенных как спам*.

5. **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.
6. **Автоматическое обновление** содержимого вирусных баз Dr.Web и антивирусного ядра для поддержания высокого уровня надежности защиты от вредоносных программ.
7. **Сбор статистики** проверок и вирусных инцидентов; ведение журнала обнаруженных угроз (доступен только через утилиту управления из командной строки), а также отправка статистики вирусных инцидентов облачному сервису Dr.Web Cloud.
8. **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 интернету.

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 Dr.Web для Linux

Dr.Web 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

Компонент	Описание
	загрузочные записи) на наличие в них угроз. Пользователь имеет возможность запускать проверку как из графического режима, так и из командной строки.
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 Doctor Web. При работе через системный механизм fanotify монитор может работать в усиленном режиме, блокируя доступ к файлам (всех типов или только к исполняемым файлам), которые еще не проверены, до момента окончания их проверки. По умолчанию усиленный режим мониторинга отключен.
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 интернета (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.
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. В версиях для архитектур ARM64 и E2K компонент отсутствует.
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 Doctor Web обновлений для вирусных баз,

Компонент	Описание
	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 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 для Linux.
Агент уведомлений	Компонент, работающий в фоновом режиме. Отображает всплывающие уведомления о возникающих событиях и индикатор приложения Dr.Web 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 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 UNIX, разработанного компанией Doctor Web (может быть использован в любой ОС семейства GNU/Linux с ядром версии 2.6.x и новее). Для архитектур ARM64 и E2K возможность работы с LKM не поддерживается.

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.

Размещение карантина

Карантин Dr.Web 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 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 SplDer 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 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 этом 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 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» (Quarantine)*, 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 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.
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 для Linux, запущенного в графическом режиме, вы можете воспользоваться соответствующей кнопкой, имеющейся на окне Dr.Web для Linux (она доступна и отображается только в тех случаях, когда повышение прав может потребоваться для успешного выполнения некоторой операции). Для

запуска Dr.Web 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 работы

Dr.Web 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 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 для Linux полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании Doctor Web.
- *В режиме централизованной защиты (centralized protection mode)* защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web 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 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 для Linux, включая статистику вирусных инцидентов. Обновление вирусных баз также выполняется с сервера централизованной защиты.
- *В мобильном режиме (mobile mode)* Dr.Web для Linux получает обновления вирусных баз с серверов обновлений компании Doctor Web, но использует локально хранящиеся настройки и особый лицензионный ключевой файл, полученные от сервера централизованной защиты.

В случае работы Dr.Web 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 SpIDer Guard, а также его включения и выключения при работе Dr.Web 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 для Linux будут недоступны.

Принципы централизованной защиты

Решения компании Doctor Web 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 для Linux), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

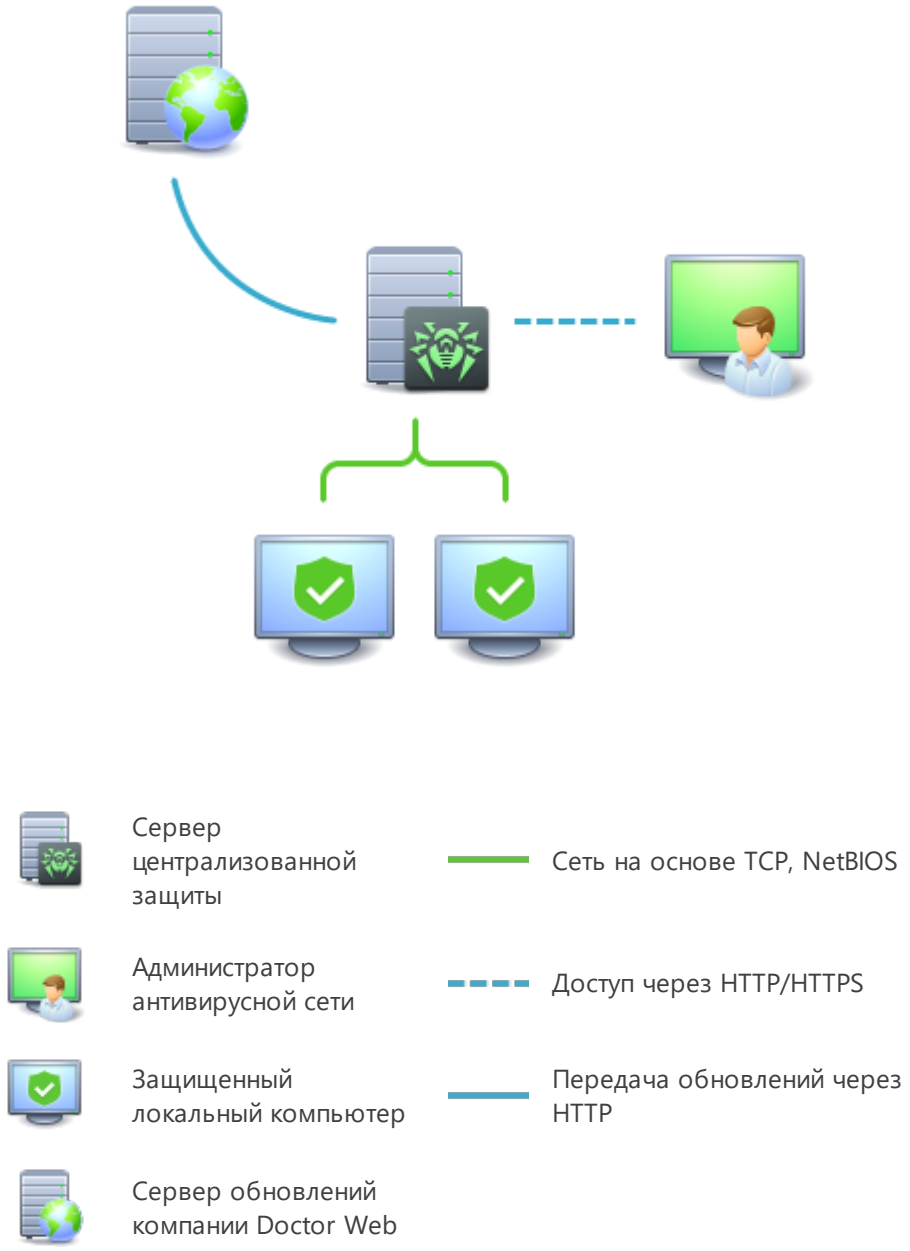

Рисунок 1. Логическая структура антивирусной сети.

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 Doctor Web.

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 для Linux версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

В режиме централизованной защиты возможен экспорт и сохранение отчетов о функционировании Dr.Web для Linux с помощью сервера централизованной защиты. Поддерживается экспорт и сохранение отчетов в форматах HTML, CSV, PDF и XML.

Подключение к антивирусной сети

Dr.Web для Linux может быть подключен к антивирусной сети следующими способами:

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

Отключение от антивирусной сети

Dr.Web для Linux может быть отключен от антивирусной сети следующими способами:

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

Системные требования и совместимость

В этом разделе:

Системные требования

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

Компонент	Требование
Платформа	Поддерживаются процессоры следующих архитектур и систем команд: • Intel/AMD: 32-бит (*IA-32, x86*); 64-бит (*x86-64, x64, amd64*) • ARM64 • E2K (*Эльбрус*) • IBM POWER (*ppc64el*)
Оперативная память (RAM)	Не менее 500 МБ свободной оперативной памяти (рекомендуется 1 ГБ и более).
Место на жестком диске	Не менее 2 ГБ свободного дискового пространства на томе, на котором размещаются каталоги Dr.Web для Linux.
Операционная система	UNIX на основе ядра версии 2.6.37 или более поздней, использующая PAM и библиотеку `glibc` версии 2.13 или более позднюю, систему инициализации `systemd` версии 209 или более позднюю. Перечень поддерживаемых дистрибутивов UNIX приведен ниже.
Прочее	Наличие сетевого подключения: • Подключение к интернету 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.

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.

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

Назначение	Направление	Номера портов
Для получения обновлений	исходящий	80
Для соединения с облачным сервисом Dr.Web Cloud	исходящий	2075 (в том числе для UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

Dr.Web 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 для Linux удалите с компьютера другие антивирусные программы.

Перечень поддерживаемых дистрибутивов ОС

Поддерживаются следующие дистрибутивы UNIX:

Платформа	Поддерживаемые версии GNU/Linux
x86_64	• Astra Linux Special Edition 1.5 (с кумулятивным патчем 20201201SE15), 1.6 (с кумулятивным патчем 20200722SE16), 1.7; • Astra Linux Common Edition (Орел) 2.12; • Debian 9, 10; • Fedora 31, 32; • CentOS 7, 8; • Ubuntu 18.04, 20.04, 22.04; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10;

Платформа	Поддерживаемые версии GNU/Linux
	• Альт 8 СП; • РЕД ОС 7.2 МУРОМ, РЕД ОС 7.3 МУРОМ; • Гослинукс IC6; • SUSE Linux Enterprise Server 12 SP3; • Red Hat Enterprise Linux 7, 8
x86	• CentOS 7; • Debian 10; • Альт Рабочая станция 9, 10; • Альт 8 СП
ARM64	• Ubuntu 18.04; • CentOS 7, 8; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10; • Альт 8 СП; • Astra Linux Special Edition (Новороссийск) 4.7
E2K	• Astra Linux Special Edition (Ленинград) 8.1 (с кумулятивным патчем 20200429SE81); • Альт 8 СП; • Эльбрус-Д МЦСТ 1.4; • ОПО ВК Эльбрус-8.32 ТВГИ.00311-28
ppc64el	• CentOS 8; • Ubuntu 20.04

В ОС Альт 8 СП и Гослинукс 7.1 работа с мандатными уровнями доступа не поддерживается.

Для прочих дистрибутивов UNIX, соответствующих описанным требованиям, полная совместимость с Dr.Web для Linux не гарантируется. При возникновении проблем с совместимостью с вашим дистрибутивом обратитесь в техническую поддержку.

Требуемые дополнительные компоненты и пакеты

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

Для удобной работы с Dr.Web 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 Dr.Web для Linux 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.
  Для архитектур ARM64 и E2K возможность работы с LKM не поддерживается.

Работа SpIDer Guard через 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 SpIDer 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 SpIDer Gate возможно возникновение следующей проблемы, связанной с внутренней ошибкой в реализации NetFilter: при выключении SpIDer 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 SpIDer Gate совместим со всеми пользовательскими приложениями, использующими сеть, включая веб-браузеры и почтовые клиенты. Для корректной проверки защищенных соединений необходимо добавить сертификат Dr.Web для Linux к перечню доверенных сертификатов тех приложений, которые используют защищенные соединения (например, веб-браузеров и почтовых клиентов).
- После внесения изменений в работу монитора SpIDer 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 для Linux не совместим с подсистемой улучшения безопасности SELinux. Кроме того, по умолчанию Dr.Web 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).

Для установки Dr.Web для Linux в системы с SELinux, а также в системы, использующие мандатные модели доступа, может потребоваться дополнительная настройка подсистем безопасности для снятия ограничений в функционировании Dr.Web для Linux. Подробнее см. в разделе Настройка подсистем безопасности.

Лицензирование

Права пользователя на использование копии Dr.Web для Linux подтверждаются и регулируются лицензией, приобретенной пользователем у компании Doctor Web 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 Dr.Web для Linux 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 для Linux.
- Другие ограничения (в частности, количество компьютеров, на которых разрешено использовать приобретенную копию Dr.Web для Linux).

Для предварительного ознакомления с возможностями продукта вы можете активировать *демонстрационный период*. При активации демонстрационного периода вы получаете право на полноценное использование установленной копии Dr.Web для Linux в течение всего этого периода.

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

При отсутствии действующей лицензии или активированного демонстрационного периода (в том числе, если срок действия ранее приобретенной лицензии или демонстрационного периода истек), антивирусные функции Dr.Web для Linux блокируются. Кроме того, недоступен сервис получения обновлений вирусных баз Dr.Web с серверов обновлений компании Doctor Web. Однако имеется возможность активировать Dr.Web 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.

Установка и удаление

В этом разделе описываются процедуры установки и удаления Dr.Web для Linux версии 11.1, а также процедура получения текущих обновлений и процедура перехода на новую версию, если на вашем компьютере уже установлен Dr.Web для Linux предыдущей версии.

Кроме этого, в этом разделе описана процедура выборочной установки и удаления компонентов Dr.Web для Linux (например, для устранения ошибок, возникших в процессе его эксплуатации или для получения установки с ограниченным набором функций) и настройка расширенных подсистем безопасности (таких, как SELinux), что может потребоваться при установке или в процессе эксплуатации Dr.Web для Linux.

- Установка Dr.Web для Linux.
- Обновление Dr.Web для Linux.
- Удаление Dr.Web для Linux.
- Настройка подсистем безопасности.
- Дополнительно:
  - Расположение файлов Dr.Web для Linux.
  - Выборочные установка и удаление компонентов.

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`.

Не гарантируется совместимость Dr.Web 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 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 Dr.Web для файловых серверов UNIX, и вы хотите в дополнение к нему установить Dr.Web для Linux), то предварительно убедитесь, что версия уже установленного продукта *совпадает* с версией того Dr.Web для Linux, которую вы планируете установить. Если версия, которую вы собираетесь установить, новее, чем версия продукта, который уже установлен на вашем компьютере, *перед началом* установки обновите уже установленный продукт до версии того продукта Dr.Web, который вы хотите установить дополнительно.

Установка Dr.Web для Linux

Вы можете установить Dr.Web для Linux одним из двух способов:

1. Загрузив с сайта компании Doctor Web 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 Dr.Web для Linux в виде набора нативных пакетов (для этого потребуется подключиться к соответствующему репозиторию пакетов компании Doctor Web).

В дистрибутивах, использующих устаревшие версии пакетного менеджера (например, Альт 8 СП) рекомендуется устанавливать Dr.Web для Linux из универсального пакета.

После установки Dr.Web для Linux любым из указанных в этом руководстве способов, в начале работы, вам потребуется активировать лицензию или установить ключевой файл. Кроме того, вы можете подключить Dr.Web 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.

Dr.Web для Linux, 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 UNIX для корректной работы Dr.Web для Linux. При возникновении проблем с функционированием отдельных компонентов вы можете выполнить их выборочную установку и удаление, не удаляя Dr.Web для Linux целиком.

Установка универсального пакета

Dr.Web 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 (для 32-битных платформ — `x86`, для 64-битных платформ — `amd64`, `arm64` и `e2s`). Например:

```
drweb-11.1-av-linux-amd64.run
```

Далее имя установочного файла будет указываться как *<имя_файла>*`.run`.

Чтобы установить компоненты Dr.Web для Linux:

1. Загрузите инсталляционный файл с официального сайта компании Doctor Web.
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 для Linux в среде ОС Astra Linux SE версий 1.6 и 1.7, 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, версии 1.6 и 1.7)), 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 повторите 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 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. Если вы *не согласны* с условиями Лицензионного соглашения, вы должны удалить Dr.Web для Linux 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 UNIX 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, 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 Dr.Web для Linux или его компонентов в последующем, без обновления его версии.

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

- **Dr.Web для Linux** для запуска Dr.Web 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 для Linux дополнительно может потребоваться установить пакеты, перечисленные в разделе Системные требования и совместимость (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 для Linux, на экране появится соответствующее окно с перечислением обнаруженных проблем. Вы можете прервать установку, нажав **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 для Linux, нажмите **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 для Linux.

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

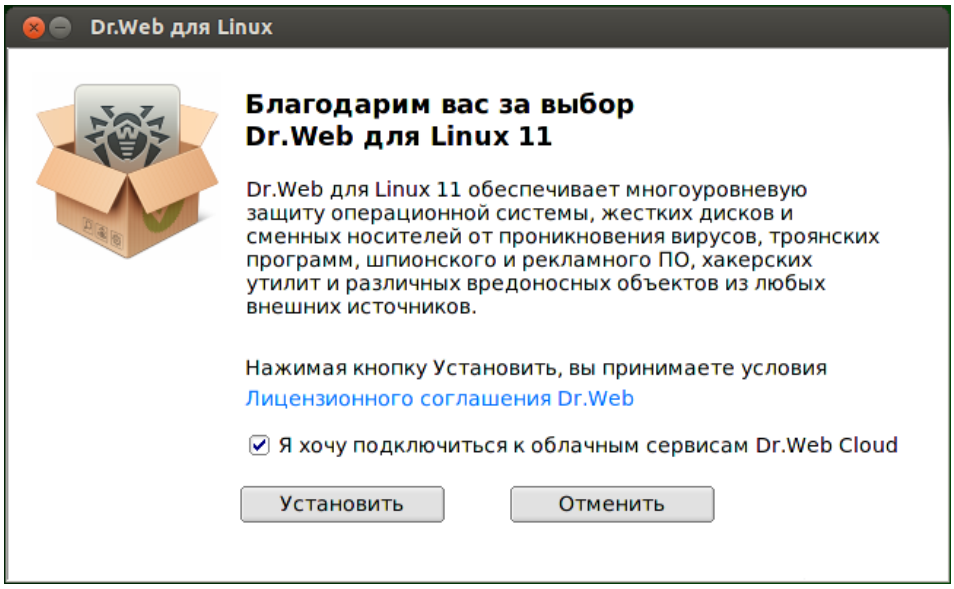

Рисунок 2. Страница приветствия мастера установки

Для установки Dr.Web для Linux на свой компьютер необходимо последовательно выполнить следующие действия:

1. Ознакомьтесь с условиями Лицензионного соглашения компании Doctor Web. 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 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 для Linux использовать облачный сервис Dr.Web Cloud, сбросьте этот флажок. При необходимости вы в любой момент сможете разрешить или запретить Dr.Web для Linux использовать сервис Dr.Web Cloud в настройках программы.
3. Для начала установки нажмите **Установить**. Тем самым вы одновременно подтверждаете, что принимаете условия Лицензионного соглашения компании Doctor Web. Если вы решили отказаться от установки Dr.Web для Linux на свой компьютер, нажмите **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 **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 **ОК**. Если данная операция поддерживается возможностями окружения, на финальном шаге появится страница с предложением запустить Dr.Web для Linux в графическом режиме. Для запуска установите флажок **Запустить Dr.Web для Linux сейчас** и нажмите **ОК**.

Если установка была прервана из-за ошибки, финальная страница мастера будет содержать соответствующее сообщение. В этом случае закройте мастер установки, нажав **ОК**. 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 Doctor Web, 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 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 для Linux воспользуйтесь любым удобным для вас способом запуска.

Если установка была прервана из-за ошибки, устраните проблемы, вызвавшие ошибку установки, и повторите процесс установки заново.

Установка из репозитория

Нативные пакеты Dr.Web 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 интернету.

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`.

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Debian, Mint, Ubuntu (apt).
- ALT Linux, PCLinuxOS (apt-rpm).
- Mageia, OpenMandriva Lx (urpmi).
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf).
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

1. Репозиторий для этих ОС защищен цифровой подписью Doctor Web. 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
8C42FC58D8752769
```

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

```
deb https://repo.drweb.com/drweb/debian 11.1 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/drweb-repo11.1.deb.

3. Для установки Dr.Web 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 11.1/<arch> drweb
```

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

- для 32-разрядной версии: `i386`;
- для архитектуры AMD64: `x86_64`;
- для архитектуры ARM64: `aarch64`;
- для архитектуры E2K: `e2s`.

2. Для установки Dr.Web 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/linux/11.1/<arch>/
```

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

- для 32-разрядной версии: `i386`;
- для 64-разрядной версии: `x86_64`.

2. Для установки Dr.Web 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 - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$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 `$` необходимо экранировать: `\$`.

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

2. Для установки Dr.Web 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 https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. Для установки Dr.Web 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 для Linux

Предусмотрено два режима обновления Dr.Web для Linux:

1. Получение обновлений пакетов и компонентов, выпущенных в рамках эксплуатации текущей версии Dr.Web для Linux (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 Doctor Web выпустила новую версию Dr.Web для Linux, отличающуюся новыми возможностями.

Получение текущих обновлений

В этом разделе:

- Обновление через интернет.
- Обновление без подключения к интернету.

Обновление через интернет

После установки Dr.Web для Linux 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 Dr.Web для Linux.

  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 Dr.Web для Linux, 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).

Обновление без подключения к интернету

В условиях повышенных требований к безопасности, когда подключение к интернету отсутствует или ограничено, обновление вирусных баз и антивирусного ядра можно выполнять без подключения к интернету. В этом случае обновления загружаются на компьютер, подключенный к интернету, копируются на USB-накопитель или сетевой диск, после чего устанавливаются на другой, не подключенный к интернету компьютер.

Процедура обновления выполняется через командную строку.

Для получения обновлений:

1. На компьютере, подключенном к интернету, выполните команду:

   ```
   $ drweb-ctl update --Path <путь к каталогу, куда будут загружены обновления>
   ```

2. Скопируйте полученные обновления на USB-накопитель или сетевой диск.

3. Примонтируйте сетевой диск или накопитель на компьютере, на который требуется установить обновления. Если вы получаете обновления с USB-накопителя, для этого потребуется выполнить команды:

   ```
   # mkdir /mnt/usb
   # mount <путь к устройству> /mnt/usb
   ```

4. Установите обновления с помощью команды:

   ```
   $ drweb-ctl update --From /mnt/usb
   ```

Переход на новую версию

Предварительные замечания

Поддерживается процедура обновления предыдущих версий Dr.Web для Linux до версии 11.1. Переход на новую версию Dr.Web для Linux выполняйте тем же способом, каким был установлена версия Dr.Web для Linux, подлежащая обновлению:

- Если версия Dr.Web для Linux, подлежащая обновлению, была установлена из репозитория, то переход на новую версию выполняйте путем обновлением из репозитория.
- Если версия Dr.Web для Linux, подлежащая обновлению, была установлена из универсального пакета, то для перехода на новую версию установите универсальный пакет, содержащий новую версию.

Чтобы уточнить способ, которым была установлена версия Dr.Web для Linux, подлежащая обновлению, проверьте присутствие в каталоге исполняемых файлов Dr.Web для Linux скрипта программы удаления `remove.sh`. Если этот файл присутствует, текущая версия Dr.Web для Linux была установлена из универсального пакета, а в противном случае — из репозитория.

Если вы не имеете возможности обновить Dr.Web для Linux тем же способом, каким он был установлен изначально, то предварительно удалите текущую версию, а потом выполните установку новой версии любым доступным для вас способом. Способы установки и удаления предыдущих версий Dr.Web для Linux аналогичны способам установки и удаления, рассмотренным в этом руководстве для версии 11.1. Для дополнительной информации обратитесь к Руководству пользователя установленной у вас версии Dr.Web для Linux.

Обратите внимание, что переход с Dr.Web для Linux версии 6.0.2 и меньше на версию 11.1 возможен *только* путем предварительного удаления старой версии Dr.Web для Linux с последующей установкой версии 11.1.

Если версия Dr.Web для Linux, подлежащая обновлению, работает под управлением сервера централизованной защиты, то перед началом обновления рекомендуется сохранить адрес сервера централизованной защиты, к которому подключен Dr.Web для Linux. Например, для получения адреса сервера централизованной защиты, к которому подключен Dr.Web 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 сертификата сервера.

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

Обновление с версии 9.0 и новее

Обновление установкой универсального пакета

Выполните установку Dr.Web для Linux версии 11.1 из универсального пакета. В случае необходимости, в процессе установки вам будет предложено автоматически удалить имеющиеся компоненты старой версии Dr.Web для Linux.

Обновление из репозитория

Для обновления текущей версии Dr.Web для Linux, установленной из репозитория компании Doctor Web, в зависимости от типа используемых пакетов, выполните следующие действия:

- **В случае использования пакетов RPM (yum)**:
  1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 11.1).

     

     Имя репозитория, хранящего пакеты версии 11.1, см. в разделе Установка из репозитория. Для уточнения способа смены репозиториев обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

  2. Установите новую версию Dr.Web для Linux из репозитория, выполнив команду:

     ```
     # yum update
     ```

     или, если используется менеджер `dnf` (как, например, в ОС Fedora версии 22 и более поздних):

     ```
     # dnf update
     ```

Если в процессе обновления пакетов возникнет ошибка, то выполните удаление и последующую повторную установку Dr.Web для Linux. При необходимости см. разделы Удаление Dr.Web для Linux, 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 11.1).
  2. Обновите пакеты Dr.Web для Linux, 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 для Linux, имеющийся у вас лицензионный ключевой файл будет автоматически установлен в надлежащее место для использования новой версией Dr.Web для Linux.

В случае возникновения проблем с автоматической установкой лицензионного ключевого файла, вы можете выполнить его установку вручную. Dr.Web 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 Doctor Web.

Повторное подключение к серверу централизованной защиты

Если это возможно, то после обновления (если обновляемая версия была подключена к серверу централизованной защиты) подключение будет восстановлено автоматически. В случае если подключение не восстановилось автоматически, для подключения обновленной версии Dr.Web 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 для Linux.
- Используйте команду:

```
$ drweb-ctl esconnect <адрес> --Certificate <путь к файлу сертификата сервера>
```

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

Особенности процесса обновления

- При обновлении из репозитория при работающем Dr.Web для Linux обновляемой версии, после завершения установки пакетов новой версии Dr.Web для Linux, процессы старой версии Dr.Web 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 Dr.Web для Linux.
- При обновлении Dr.Web 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, перезапустите его после завершения обновления для обеспечения проверки входящих писем.

Обновление с версии 6.0.2 и более ранней

Переход с Dr.Web для Linux версии 6.0.2 и более ранней на версию 11.1 возможен только путем предварительного удаления старой версии Dr.Web для Linux с последующей установкой версии 11.1. Для получения дополнительной информации о способах удаления старой версии Dr.Web для Linux обратитесь к Руководству пользователя установленной у вас версии Dr.Web для Linux.

Перенос ключевого файла

Имеющийся у вас лицензионный ключевой файл старой версии Dr.Web для Linux не будет автоматически установлен для использования новой версией, но вы можете выполнить его установку вручную. Dr.Web 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 Doctor Web.

Dr.Web для Linux версии 11.1 не поддерживает карантин Dr.Web 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 для Linux версии 6.0.2 (и менее) 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 для Linux перед началом перехода на новую версию.

Удаление Dr.Web для Linux

В зависимости от способа установки, вы можете удалить Dr.Web 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, установленные из репозитория компании Doctor Web, используя системный менеджер пакетов.

Удаление универсального пакета

Удаление Dr.Web 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 для Linux, но и *все другие* продукты Dr.Web, установленные на вашем компьютере.

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

Удаление Dr.Web для Linux 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 Dr.Web для Linux из командной строки

Запуск программы удаления осуществляется скриптом `remove.sh`, расположенным в каталоге `/opt/drweb.com/bin`. Таким образом, чтобы запустить удаление Dr.Web для Linux, необходимо выполнить 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 команду:

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

Процедура удаления Dr.Web 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`.

В ОС Альт 8 СП во время удаления на консоль могут выводиться сообщения вида:

```
/etc/init.d/drweb-configd: Нет такого файла или каталога
```

На работу системы эти сообщения никак не влияют. Процедура удаления выполняется корректно.

Удаление в графическом режиме

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

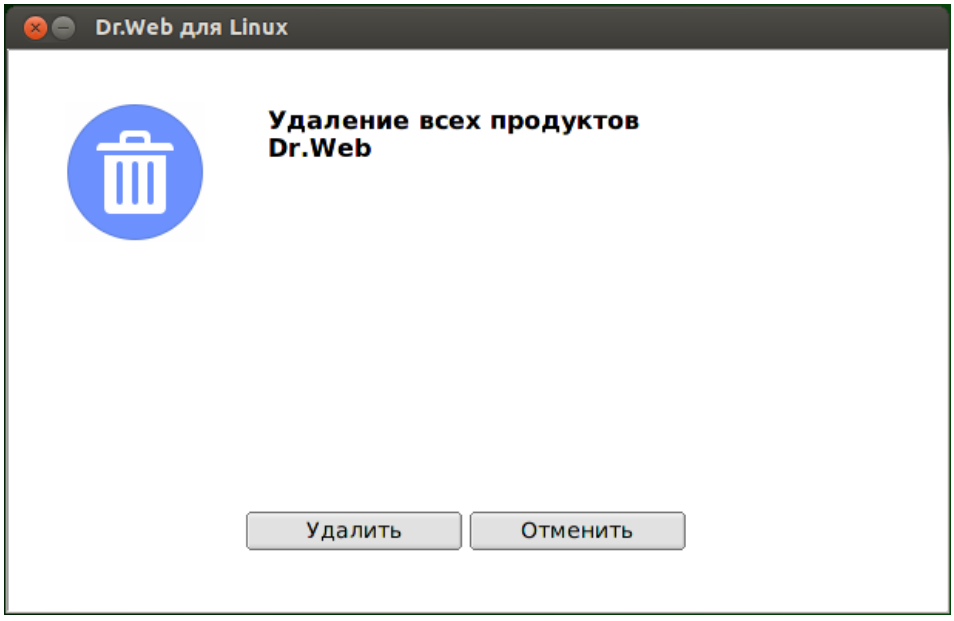

Рисунок 3. Страница приветствия мастера удаления

1. Для удаления продуктов Dr.Web нажмите **Удалить**. Чтобы прекратить работу мастера удаления и отказаться от удаления продуктов Dr.Web с вашего компьютера, нажмите **Отменить**.
2. После начала процесса удаления откроется страница мастера, отражающая ход процесса удаления и содержащая соответствующий индикатор прогресса. Для просмотра сообщений журнала удаления нажмите **Подробнее**.
3. После успешного окончания процесса удаления файлов Dr.Web 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 продуктов Dr.Web с вашего компьютера, введите *No* или *N*. В этом случае работа программы удаления будет завершена.

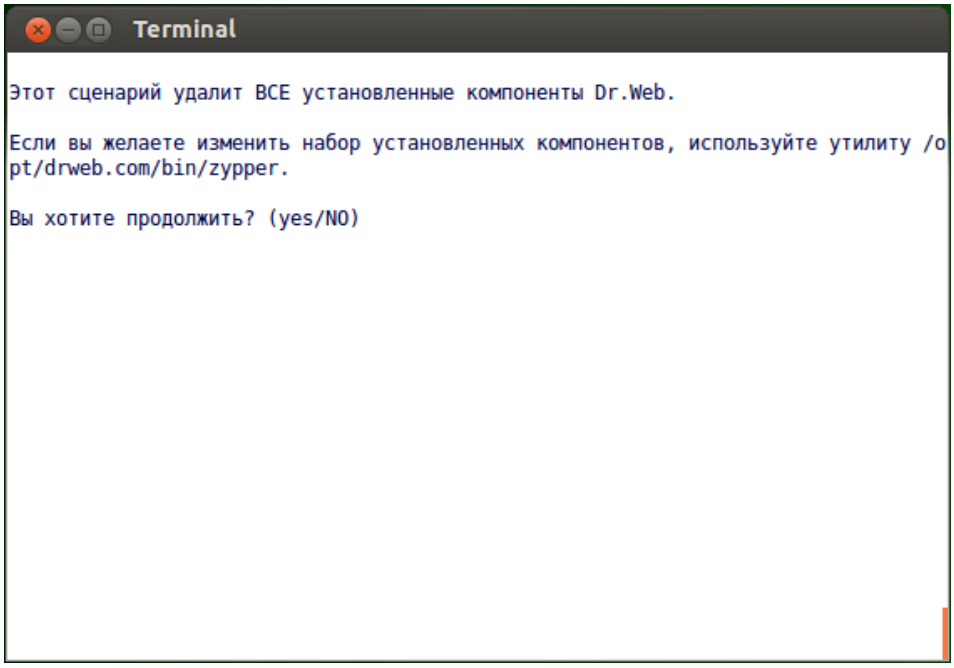

Рисунок 4. Приглашение к удалению

2. После подтверждения удаления запустится процедура удаления всех установленных пакетов Dr.Web. При этом на экран будут выдаваться записи, фиксируемые в журнал и отражающие ход процесса удаления.
3. По окончании процесса программа удаления завершит свою работу автоматически.

Удаление Dr.Web для Linux, 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`.

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Debian, Mint, Ubuntu (apt),
- ALT Linux, PCLinuxOS (apt-rpm),
- Mageia, OpenMandriva Lx (urpmi),
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf),
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

Для удаления корневого метапакета Dr.Web для Linux выполните команду:

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

Для удаления корневого метапакета вместе со всеми зависимостями выполните команду:

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

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 Dr.Web 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 Dr.Web для Linux.

Удалить пакеты Dr.Web для Linux также можно с помощью альтернативных менеджеров (например, Synaptic или aptitude).

ALT Linux, PCLinuxOS (apt-rpm)

Удаление Dr.Web для Linux в этом случае выполняется так же, как и в Debian, Ubuntu (см. выше).

Удалить пакеты Dr.Web для Linux также можно с помощью альтернативных менеджеров (например, Synaptic или aptitude).

В ОС Альт 8 СП во время удаления на консоль могут выводиться сообщения вида:

```
/etc/init.d/drweb-configd: Нет такого файла или каталога
```

На работу системы эти сообщения никак не влияют. Процедура удаления выполняется корректно.

Mageia, OpenMandriva Lx (urpme)

Для удаления Dr.Web 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 Dr.Web для Linux.

Удалить пакеты Dr.Web для Linux также можно 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 Dr.Web для Linux.

Удалить пакеты Dr.Web для Linux также можно с помощью альтернативных менеджеров (например, PackageKit или Yumex).

SUSE Linux (zypper)

Для удаления Dr.Web 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 Dr.Web для Linux.

Удалить пакеты Dr.Web для Linux также можно с помощью альтернативных менеджеров (например, YaST).

Дополнительно

Расположение файлов Dr.Web для Linux

Файлы Dr.Web 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 и основные библиотеки, необходимые для работы Dr.Web для Linux.
`/etc/opt/drweb.com`	Файлы настроек компонентов (по умолчанию) и лицензионный ключевой файл для работы Dr.Web 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 для Linux.

Выборочные установка и удаление компонентов

В случае необходимости вы можете выполнить выборочную установку и удаление отдельных компонентов Dr.Web для Linux, установив или удалив соответствующие пакеты. Выборочную установку и удаление производите тем же способом, каким был установлен Dr.Web для Linux.

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

Установка и удаление компонентов Dr.Web для Linux:

- установленного из репозитория;
- установленного из универсального пакета.

1. Установка и удаление компонентов Dr.Web для Linux, установленного из репозитория

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

1. Чтобы удалить компонент SpIDer Gate (пакет `drweb-gated`) из состава Dr.Web для Linux, установленного в ОС CentOS, используйте команду:

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

2. Чтобы добавить компонент SpIDer Gate (пакет `drweb-gated`) в состав Dr.Web для Linux, установленного в ОС Ubuntu, используйте команду:

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

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

2. Установка и удаление компонентов Dr.Web для Linux, установленного из универсального пакета

Если Dr.Web для Linux 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 Dr.Web для Linux. Если вы не сохранили этот файл, загрузите его с сайта компании Doctor Web.

Распаковка инсталляционного файла

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

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

`--keep` — не удалять установочные файлы Dr.Web для Linux и журнал установки по окончании установки.

`--target` <*каталог*> — распаковать установочные файлы Dr.Web для Linux 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 Dr.Web для Linux перейдите в каталог, содержащий распакованные файлы пакетов Dr.Web для Linux. Если этот каталог отсутствует, выполните команду:

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

В результате в каталоге <*каталог*> появится вложенный каталог <*имя_файла*>, содержащий распакованные файлы пакетов Dr.Web для Linux.

Выборочная установка компонентов

Установочный run-файл содержит пакеты всех компонентов, из которых состоит Dr.Web 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 Dr.Web для Linux. Имена всех пакетов, содержащих компоненты Dr.Web для Linux, начинаются с префикса «drweb».

Для установки пакетов в состав инсталляционного комплекта включен менеджер пакетов `zypper`. Для выборочной установки используйте скрипт `installpkg.sh`. Для этого предварительно распакуйте содержимое инсталляционного пакета в любой удобный для вас 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 Dr.Web для Linux целиком, запустите скрипт автоматической установки, выполнив команду:

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

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

```
# ./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 воспользуйтесь менеджером пакетов `zypper`, автоматически установленным в рамках установки Dr.Web для Linux. Для этого перейдите в каталог `/opt/drweb.com/bin`, и выполните следующую команду:

```
# ./zypper rm <имя_пакета>
```

Например:

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

Если вы хотите удалить Dr.Web для Linux целиком, запустите скрипт 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 подсистем 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 Dr.Web для Linux при настройках по умолчанию. Для обеспечения корректной работы Dr.Web для Linux в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web для Linux.

В этом разделе рассматриваются следующие настройки, обеспечивающие корректную работу Dr.Web для Linux:

- 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, версии 1.6 и 1.7).

Настройка разрешений системы мандатного доступа PARSEC для Dr.Web 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 компонентов Dr.Web для Linux, то вы все равно сможете запускать проверку файлов, используя графический интерфейс Dr.Web 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 Dr.Web для Linux 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 SpIDer Guard и SpIDer 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 ее сервисных компонентов.

Настройка политик безопасности SELinux

Если используемый вами дистрибутив UNIX оснащен подсистемой безопасности SELinux (*Security-Enhanced UNIX — UNIX с улучшенной безопасностью*), то, чтобы служебные компоненты Dr.Web для Linux (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 Dr.Web для Linux 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 компоненты Dr.Web для Linux.

Если попытка установки Dr.Web для Linux 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 защиты:

- *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*, временно (на период установки) переведите 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 Dr.Web для Linux из установочного файла, но до его запуска и активации верните режим *Enforced,* для чего выполните команду:

```
# setenforce 1
```

2. Проблемы функционирования Dr.Web для Linux

В некоторых случаях при работающем SELinux отдельные вспомогательные компоненты Dr.Web 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 для Linux и в системном журнале `syslog` (обычно расположен в каталоге `/var/log/`).

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, скомпилируйте для них специальные политики безопасности.

В некоторых дистрибутивах UNIX 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 для Linux. Если это не так, дождитесь таких инцидентов в процессе работы Dr.Web для Linux, либо создайте разрешающие политики принудительно, воспользовавшись утилитой `policygentool` (см. ниже).

Утилита `audit2allow` находится в пакете `policycoreutils-python` или `policycoreutils-devel` (для ОС Red Hat 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 этом 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 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 Red Hat Enterprise Linux и CentOS, 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 UNIX.

Настройка разрешений PARSEC

В дистрибутивах Linux, оснащенных подсистемой безопасности PARSEC, доступ приложений к файлам зависит от уровня привилегий. Поэтому по умолчанию SpIDer Guard может перехватывать события доступа к файлам ровно в той мере, в которой это предусмотрено его уровнем привилегий.

Кроме того, в случае если пользователь работает на отличном от нуля уровне привилегий, интерфейс пользователя Dr.Web 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.

Если в ОС используется PARSEC и имеются учетные записи пользователей, работающих на уровнях привилегий, отличных от нулевого, необходимо выполнить специальную настройку Dr.Web для Linux, чтобы обеспечить взаимодействие его компонентов, запускаемых на различных уровнях привилегий.

В этом разделе рассматриваются следующие настройки PARSEC, обеспечивающие корректную работу Dr.Web для Linux:

- Настройка взаимодействия компонентов, запущенных на разных уровнях привилегий.
- Настройка автоматического запуска компонентов Dr.Web для Linux на уровне привилегий пользователя.
- Настройка SpIDer Guard для перехвата событий доступа к файлам.

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`.

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 для Linux (`drweb-configd`) правом на использование механизма *privsock*. `drweb-configd` — сервисный компонент Dr.Web для Linux, 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 скрипт запуска демона управления конфигурацией Dr.Web 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 скрипта `/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.

Настройка автоматического запуска компонентов на уровне привилегий пользователя

Для того, чтобы компоненты Dr.Web для Linux, с которыми взаимодействует пользователь, были доступны в его окружении (при работе пользователя на уровне привилегий, отличном от нулевого), внесите изменения в файлы настроек PAM для автоматического запуска требуемых компонентов Dr.Web для Linux при начале сессии пользователя и их завершения при окончании сессии (используется специальный PAM-модуль `pam_drweb_session.so`, разработанный Doctor Web, который запускает компонент-посредник `drweb-session`, связывающий между собой локальные копии компонентов, запущенных в окружении пользователя, с компонентами, работающими на нулевом уровне привилегий и запускающимися автоматически при загрузке ОС).

Для внесения изменений в настройки PAM вы можете использовать утилиту конфигурирования `drweb-configure`, входящую в состав Dr.Web для Linux (рекомендуется), либо внести изменения в необходимые файлы конфигурации вручную.

1. Использование утилиты drweb-configure

Для удобства настройки некоторых сложных параметров, обеспечивающих работоспособность Dr.Web для Linux, разработана специальная вспомогательная утилита `drweb-configure`.

1. Для включения или отключения автоматического запуска необходимых компонентов Dr.Web для Linux в окружении пользователя при его работе на уровне привилегий, отличном от нулевого, используйте следующую команду:

   ```
   $ sudo drweb-configure session <режим>
   ```

   где *<режим>* может принимать одно из следующих значений:

   - `enable` — включить режим автоматического запуска нужных компонентов в сессии пользователя на его уровне привилегий.

- `disable` — отключить режим автоматического запуска нужных компонентов в сессии пользователя на его уровне привилегий (при этом ряд функций Dr.Web для Linux окажется недоступным).

2. Перезапустите систему.

Для получения справки по использованию `drweb-configure` для настройки PAM используйте команду:

```
$ drweb-configure --help session
```

2. Изменение файлов конфигурации PAM вручную

Для Astra Linux и других дистрибутивов, использующих модуль PAM pam_parsec_mac.so

1. Чтобы изменить настройки PAM, нужно отредактировать хранящиеся в каталоге каталоге `/etc/pam.d` конфигурационные файлы, в которых вызывается модуль PAM `pam_parsec_mac.so`. Для получения полного списка таких файлов выполните команду:

   ```
   # grep -R pam_parsec_mac.so /etc/pam.d
   ```

   В каждый файл из списка добавьте добавьте следующие записи типа *session*:

   - Перед первой записью типа *session*:

   ```
   session optional pam_drweb_session.so type=close
   ```

   - После последней записи типа *session*:

   ```
   session optional pam_drweb_session.so type=open
   ```

2. Сохраните измененные файлы.
3. Создайте символическую ссылку на файл `pam_drweb_session.so` из системного каталога, содержащего PAM-модули. Файл `pam_drweb_session.so` располагается в каталоге библиотек Dr.Web для Linux `/opt/drweb.com/lib/` (например, для 64-разрядных ОС — в каталоге `/opt/drweb.com/lib/x86_64-linux-gnu/pam/`).
4. Перезапустите систему.

Для Альт 8 СП и других дистрибутивов, использующих модуль pam_namespace.so

1. Чтобы изменить настройки PAM, нужно отредактировать хранящиеся в каталоге `/etc/pam.d` конфигурационные файлы, в которых вызывается модуль PAM `pam_namespace.so`. Для получения полного списка таких файлов выполните команду:

   ```
   # grep -R pam_namespace.so /etc/pam.d
   ```

2. В каждый файл добавьте такие же записи типа *session*, что и для дистрибутивов, использующих модуль `pam_parsec_mac.so` (см. предыдущий параграф).

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 *Fanotify*.

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

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

Для получения дополнительной информации используйте команду:

```
$ man drweb-spider
```

Настройка запуска в режиме ЗПС (Astra Linux SE, версии 1.6 и 1.7)

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 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 Dr.Web для Linux 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 для Linux в режиме ЗПС в ОС версий 1.6 и 1.7 необходимо выполнить предварительные настройки системы.

Настройка Astra Linux SE версий 1.6 и 1.7 для запуска Dr.Web 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):

```
# cp /opt/drweb.com/share/doc/digsig.gost.gpg /etc/digsig/keys/legacy/keys
```

3. Выполните команду:

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

4. Перезагрузите систему.

Начало работы

1. Выполните активацию Dr.Web для Linux.
2. Проверьте его работоспособность.
3. Задайте режим мониторинга файлов.
4. Определите исключения, если они имеются.

Регистрация и активация

В этом разделе:

- Приобретение и регистрация лицензий.
- Активация Dr.Web для Linux:
  - Демонстрационный период.
  - Установка ключевого файла.
  - Подключение к серверу централизованной защиты.
- Повторная регистрация.

Приобретение и регистрация лицензий

При приобретении лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов обновлений компании Doctor Web, а также получать стандартную техническую поддержку компании Doctor Web 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 возможных вариантах лицензий можно найти на официальном сайте компании «Доктор Веб» https://license.drweb.com/.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем Dr.Web для Linux, и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки.

Активация Dr.Web для Linux

Приобретенная лицензия может быть активирована любым из указанных ниже способов:

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

При активации или продлении лицензии требуется указать серийный номер. Этот номер может поставляться вместе с Dr.Web для Linux 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 для Linux на нескольких компьютерах, то при регистрации имеется возможность указать, что Dr.Web 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.

Демонстрационный период

Пользователям продуктов Dr.Web доступен демонстрационный период сроком на 1 месяц. Его 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 для Linux (как правило, он автоматически запускается сразу после окончания установки). Также вы можете в любой момент запустить процесс регистрации из окна Менеджера лицензий, нажав **Получить новую лицензию** на странице просмотра информации о текущей лицензии.

Для активации при помощи серийного номера требуется подключение к интернету.

В случае активации демонстрационного периода или лицензии 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 после регистрации на сайте установите его 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 лицензионный ключевой файл для серийного номера зарегистрированной лицензии. Описание утилиты `drweb-ctl` приведено в Руководстве Пользователя.

Полная версия Руководства пользователя Dr.Web для Linux доступна:

- На сайте компании Doctor Web по адресу https://download.drweb.com/doc/ (требуется подключение к интернету).
- В виде документа PDF в каталоге `/opt/drweb.com/share/doc` (суффикс в имени файла указывает на язык руководства).

Установка ключевого файла

В случае если уже имеется ключевой файл, соответствующий действующей лицензии (например, он был получен от продавца по электронной почте после регистрации или Dr.Web для Linux переносится на другой компьютер), то имеется возможность активировать Dr.Web 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.

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 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**.

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты лицензионного ключевого файла при наличии активной лицензии. При повторной регистрации укажите 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.

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

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 для Linux. В ключевом файле фиксируются параметры использования Dr.Web для Linux 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 для Linux ключевой файл по умолчанию должен находиться в каталоге `/etc/opt/drweb.com` и называться `drweb32.key`.

Компоненты Dr.Web 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 Dr.Web для Linux 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 Dr.Web для Linux, 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).

Файл настроек подключения

Файл настроек подключения представляет собой специальный файл, хранящий внутри себя параметры подключения Dr.Web 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 для Linux через подключение его к серверу централизованной защиты (в этом случае вы не сможете использовать Dr.Web для Linux в автономном режиме, не приобретя дополнительно лицензию).

Проверка работоспособности

Для проверки работоспособности антивирусных программ, использующих сигнатурные методы обнаружения угроз, используется 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 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 Dr.Web для Linux при помощи тестовой программы EICAR из командной строки:

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

Данная команда выделяет из файла `/opt/drweb.com/share/doc/drweb-se/readme.eicar` (поставляется вместе с Dr.Web для Linux) 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 SplDer 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.

Режимы мониторинга файлов

Общие сведения

Монитор файловой системы SplDer Guard, осуществляющий контроль доступа к файлам, может использовать три режима мониторинга:

- *Обычный* (установлен по умолчанию) — отслеживаются операции по доступу к файлам (создание, открытие, закрытие и запуск файла). Запрашивается проверка файла, доступ к которому был осуществлен, по результатам проверки к файлу могут быть применены действия по нейтрализации угрозы, если она в нем обнаружена. До окончания проверки доступ к файлу со стороны приложений, запросивших доступ, не ограничивается.
- *Усиленный контроль исполняемых файлов* — для файлов, не считающихся исполняемыми, — так же, как и в обычном режиме. Для файлов, считающихся исполняемыми, при попытке доступа SplDer Guard блокирует запрошенную операцию доступа до тех пор, пока не станут известны результаты проверки файла на наличие угроз;

  

  Исполняемыми файлами считаются двоичные файлы форматов PE и ELF, а также текстовые файлы скриптов, содержащие преамбулу «`#!`».

- *«Параноидальный» режим* — при попытке доступа к любому файлу SplDer Guard блокирует запрошенную операцию доступа до тех пор, пока не станут известны результаты проверки этого файла на наличие угроз.

Сканер в течение определенного времени сохраняет результаты проверки файлов в специальном кэше, поэтому при повторном доступе к тому же файлу, при наличии информации в кэше, повторное сканирование файла не производится, в качестве результата проверки этого файла используется результат, извлеченный из кэша. Несмотря на это, использование «параноидального» режима мониторинга приводит к существенному замедлению работы при доступе к файлам.

Изменение режима мониторинга файлов

Режимы усиленного мониторинга файлов с их предварительной блокировкой доступны только если SplDer Guard работает в режиме `FANOTIFY`, а ядро ОС собрано со включенной опцией `CONFIG_FANOTIFY_ACCESS_PERMISSIONS`.

Переключение режимов работы SplDer Guard производится только при помощи команды `cfset` утилиты `drweb-ctl`.

Для переключения режимов работы SplDer Guard необходимо обладать правами суперпользователя. Для получения прав суперпользователя воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

- Для переключения SplDer Guard в режим работы `FANOTIFY` используйте команду:

```
$ sudo drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- Для изменения режима мониторинга используйте команду:

```
$ sudo drweb-ctl cfset LinuxSpider.BlockBeforeScan <режим>
```

  где <*режим*> определяет режим блокировки:

  - `Off` — блокировка доступа не производится, SplDer Guard осуществляет обычный (не блокирующий) режим мониторинга;
  - `Executables` — производится блокировка доступа к исполняемым файлам, SplDer Guard осуществляет усиленный контроль исполняемых файлов;
  - `All` — производится блокировка доступа к любым файлам, SplDer Guard осуществляет «параноидальный» режим мониторинга.

- Для изменения срока актуальности результатов проверки файлов, хранимых Сканером в кэше, используйте команду:

```
$ sudo drweb-ctl cfset FileCheck.RescanInterval <период>
```

  где <*период*> определяет период актуальности предыдущих результатов проверки, находящихся в кэше. Допустимо значение от `0s` до `1m` (включительно). Если указан период менее 1 секунды, то файл будет проверяться при любом запросе.

Работа с Dr.Web для Linux

Работа пользователя с Dr.Web 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 для Linux выберите пункт **Dr.Web для Linux** в системном меню **Приложения**, или введите в командной строке операционной системы команду:

  ```
  $ drweb-gui
  ```

  После этого, если окружение графического рабочего стола доступно, будет запущен графический интерфейс управления Dr.Web 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 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.
- Включение режима усиленного мониторинга файлов монитором SpIDer Guard описано в разделе Режимы мониторинга файлов.

После установки Dr.Web для Linux любым из описанных в этом руководстве способов, при начале работы, вам потребуется активировать лицензию, либо установить ключевой файл, если он у вас уже имеется, или подключить Dr.Web для Linux к серверу централизованной защиты (см. раздел Регистрация и активация). 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

В этом разделе:

- Общие сведения.
- Агент уведомлений.
- Графический интерфейс управления.

Общие сведения

За работу Dr.Web для Linux в окружении рабочего стола отвечают 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 Dr.Web для Linux, а также предоставляет индикатор состояния Dr.Web для Linux в области системных уведомлений и основное меню для взаимодействия с ним.
- Графический интерфейс — компонент, работающий в окружении графического рабочего стола и предоставляющий оконный интерфейс для управления работой Dr.Web для Linux.

Агент уведомлений

Агент уведомлений Dr.Web для Linux предназначен для:

1. Отображения индикатора состояния Dr.Web 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 для Linux позволяет решать следующие задачи:

1. Просмотр состояния работы Dr.Web для Linux, включая актуальность имеющихся вирусных баз и срока действия лицензии.
2. Запуск и остановка монитора файловой системы SpIDer Guard.
3. Запуск и остановка монитора сетевых соединений SpIDer 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 для Linux.

5. Обзор всех угроз, обнаруженных Dr.Web 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 для Linux, включая следующие параметры:
   - Действия, которые Сканер и SplDer Guard будут автоматически применять к обнаруженным угрозам (в зависимости от их типа).
   - Перечень каталогов и файлов, которые не будут проверяться Сканером и не будут 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 интернета 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).
9. Просмотр сообщений о состоянии антивирусной сети, рассылаемых сервером централизованной защиты (только если Dr.Web для Linux работает в составе антивирусной сети и только если администратор антивирусной сети задаст соответствующую настройку на сервере централизованной защиты).

Для корректной работы Dr.Web 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 для Linux представлен на рисунке ниже.

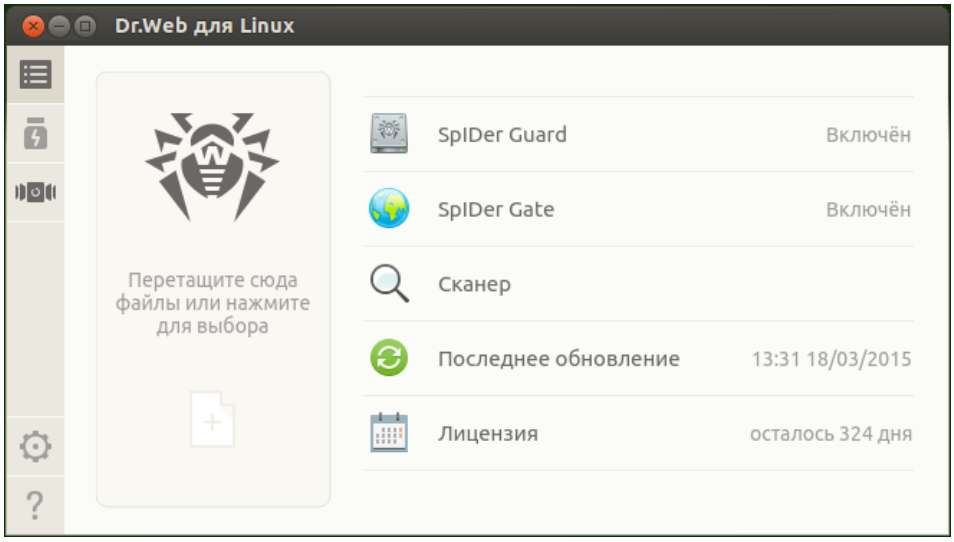

Рисунок 5. Графический интерфейс управления Dr.Web для Linux

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 для Linux, в частности: • Сканера объектов файловой системы. • Монитора файловой системы SpIDer Guard. • Монитора сетевых соединений SpIDer Gate.

Кнопка	Описание
	• Запуска проверок по расписанию. Кроме того, здесь может быть настроена работа в режиме централизованной защиты.
	Предоставляет доступ к справочным материалам и вспомогательным ресурсам компании Doctor Web: • 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 SplDer 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. *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 SplDer Guard. *При переходе на любую другую страницу главного окна, страница управления SplDer Guard будет автоматически закрыта, а кнопка убрана с навигационной панели.*

Кнопка	Описание
	Присутствует на навигационной панели только в случае если открыта и активна страница управления SplDer Gate. *При переходе на любую другую страницу главного окна, страница управления SplDer 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.*
	Открывает страницу просмотра сообщений от сервера централизованной защиты. *Присутствует на навигационной панели только если Dr.Web для Linux работает в режиме централизованной защиты и администратор антивирусной сети настроил отправку сообщений на эту рабочую станцию.*

Главная страница

На главной странице окна графического интерфейса управления Dr.Web 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 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:

- **SplDer Guard** — отображает текущее состояние, в котором находится монитор файловой системы SplDer Guard. При нажатии открывает страницу управления, на которой можно запустить или остановить SplDer 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 для Linux поддерживает четыре способа интеграции с графическим окружением рабочего стола:

- Отображение в области уведомлений рабочего стола значка приложения, служащего индикатором состояния, и позволяющего открыть контекстное меню приложения;
- Вызов контекстного меню с основными командами проверки файлов при щелчке правой кнопки мыши по значку 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 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 в виде значка с логотипом Dr.Web для Linux. Индикатор используется для отображения статуса приложения, а также доступа к контекстному меню Dr.Web для Linux. При наличии каких-либо проблем в работе (например, устарели вирусные базы или заканчивается срок действия лицензии) на индикаторе поверх логотипа Dr.Web для Linux отображается символ восклицательного знака:  .

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

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

При щелчке мышью по значку индикатора на экране открывается контекстное меню Dr.Web для Linux.

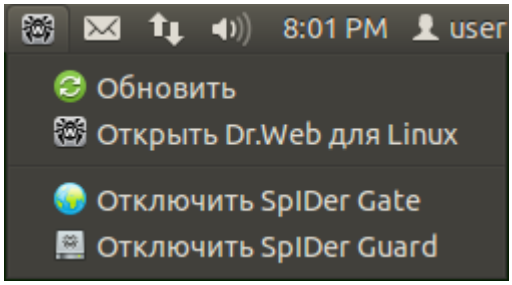

Рисунок 6. Контекстное меню индикатора Dr.Web для Linux

При выборе пункта меню **Открыть Dr.Web для Linux** на экране появляется окно графического интерфейса управления Dr.Web 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 для Linux, то в меню значок 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 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 значки в выпадающем меню.

Контекстное меню значка 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 для Linux, на панели задач появится кнопка со значком приложения. Для этого рекомендуется запускать приложение через выбор пункта **Dr.Web для Linux** в меню

Приложения. Щелчок правой кнопки мыши по кнопке запущенного приложения откроет на экране контекстное меню, примерный вид которого показан на рисунке ниже (меню для Unity Launcher в ОС Ubuntu).

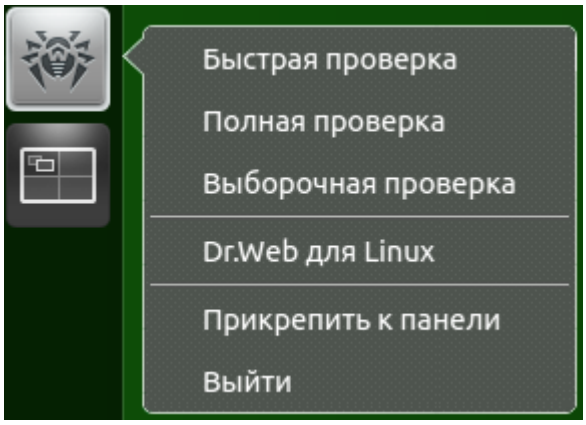

Рисунок 7. Контекстное меню Dr.Web для Linux в панели задач

- 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 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 со значком 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 значка в панели задач

Если значок 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 для Linux** меню **Приложения** (вместо запуска через исполнение команды `drweb-gui` в эмуляторе терминала или выбора пункта **Открыть Dr.Web для Linux** в меню индикатора приложения в области уведомлений).

Проверка файлов и каталогов через контекстное меню файлового менеджера

Dr.Web 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 для Linux**.

Как правило, после первого использования Dr.Web 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 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 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 для Linux**. Для исправления этой ситуации отмените настроенную ассоциацию между файлами и **Dr.Web для Linux**.

Перетаскивание файлов и каталогов на окно графического интерфейса управления

Dr.Web 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 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 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 для Linux

Для запуска графического интерфейса управления Dr.Web для Linux необходимо:

- Выбрать в системном меню **Приложения** пункт **Dr.Web для Linux**.

или

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

Вы также можете запустить графический интерфейс управления Dr.Web для Linux из командной строки, введя команду `drweb-gui`. Это возможно только в том случае, если графическое окружение доступно при работе с командной строкой, например — из эмулятора терминала.

Завершение работы графического интерфейса управления Dr.Web для Linux

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

Обратите внимание, что при завершении работы графического интерфейса Dr.Web для Linux сервисные компоненты, включая агент уведомлений, мониторы SplDer Guard и SplDer 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 SplDer Guard и сетевых соединений SplDer Gate.

- Включение и выключение SplDer Guard и SplDer 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 SplDer 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 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 для Linux работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то страница **Сканер** окна Dr.Web 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

В этом разделе:

- Типы выполняемых проверок.
- Запуск проверки.
- Добавление и удаление объектов из списка выборочной проверки.
- Запуск выборочной проверки из списка.

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 для Linux.
- *Выборочная проверка* — проверка объектов файловой системы, или некоторых объектов специального типа, непосредственно указанных пользователем.

> Если Dr.Web для Linux работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то эта страница окна Dr.Web 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 **Сканер** на главной странице окна.

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

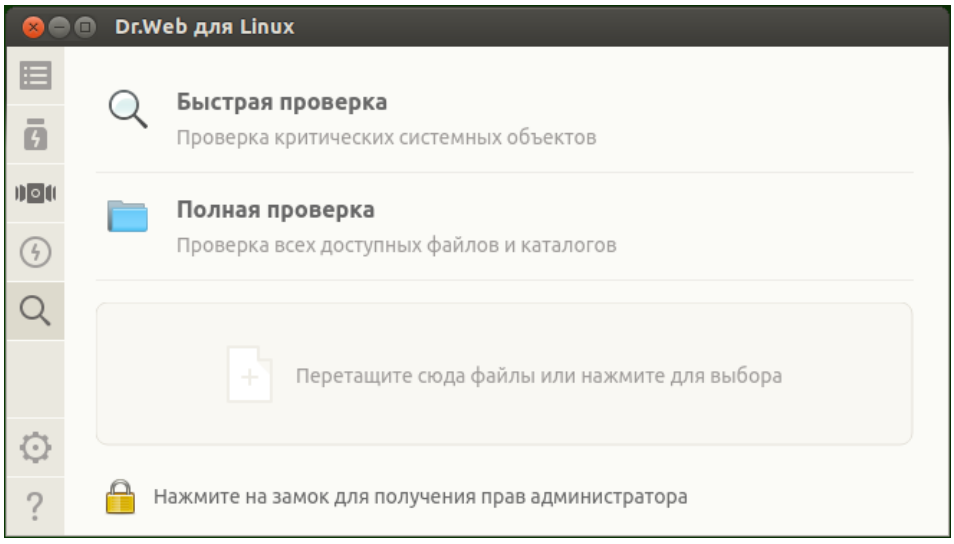

Рисунок 8. Страница выбора типа проверки

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 для Linux. Чтобы обеспечить проверку всех требуемых файлов, владельцем которых вы не являетесь, перед началом проверки повысьте права приложения. 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 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.

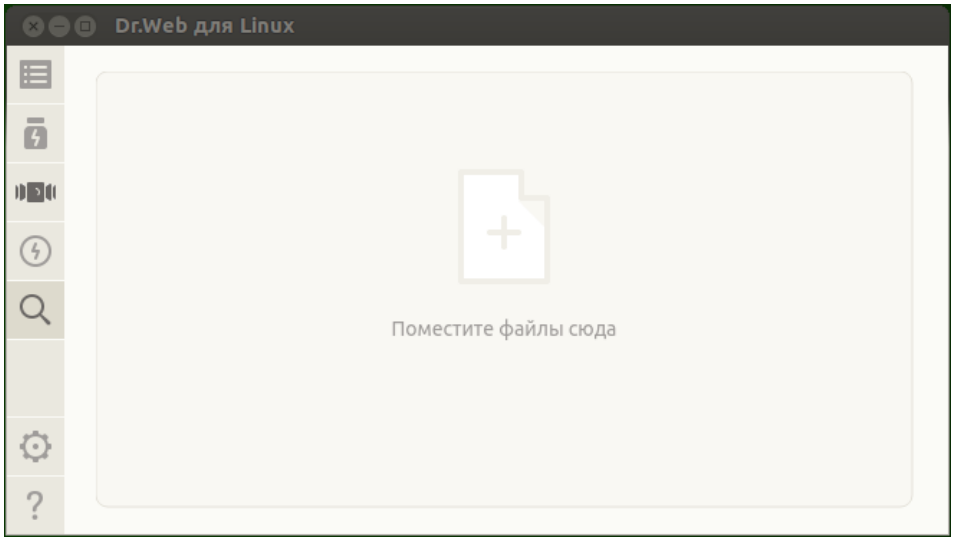

Рисунок 9. Мишень для файлов, подлежащих проверке

- **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.

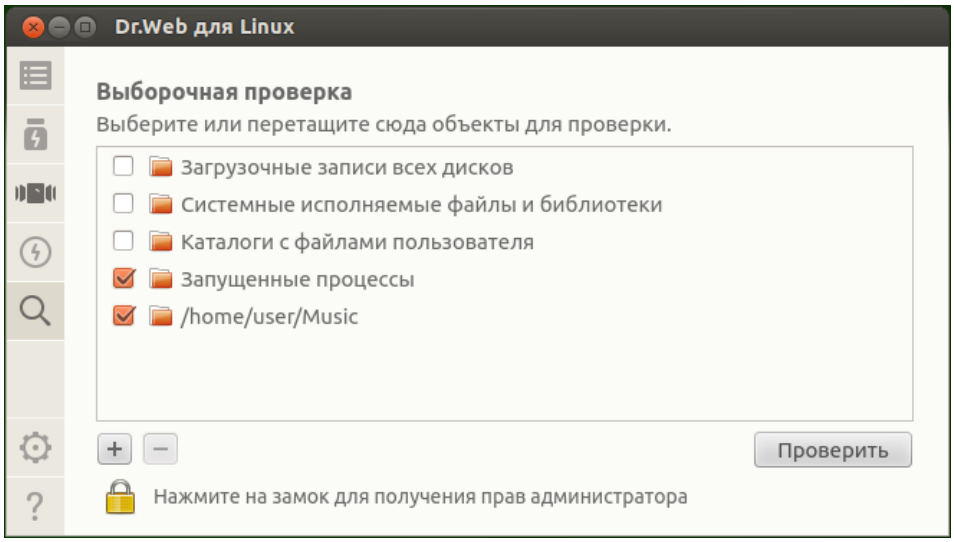

Рисунок 10. Список объектов для выборочной проверки

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 `+` под списком. В этом случае откроется стандартное окно выбора файлов и каталогов. Выберите требуемый объект (файл или каталог) и нажмите **Открыть**.

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

Нажмите `–` под списком для удаления из списка всех выделенных путей (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, установите в списке флажки у всех объектов, подлежащих проверке, и нажмите **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 для Linux может выполнять автоматический запуск периодических проверок заданного перечня объектов файловой системы по указанному расписанию.

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

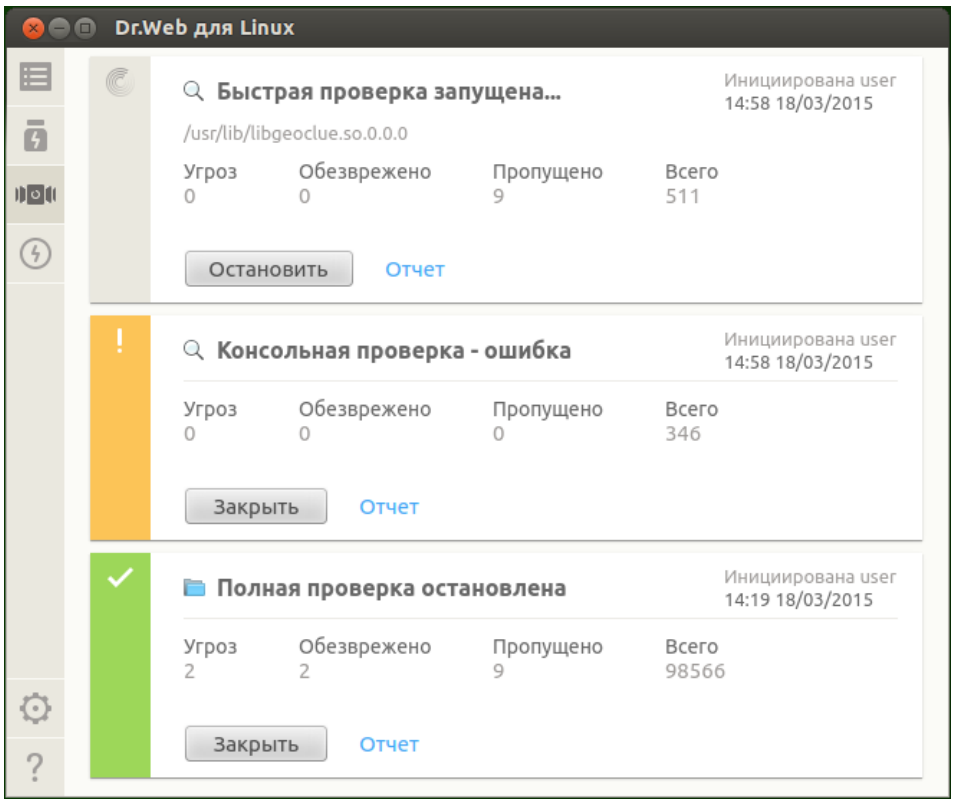

Рисунок 11. Страница просмотра списка проверок

Для каждой задачи выводится следующая информация:

- Тип проверки (в списке могут присутствовать не только *Быстрая проверка, Полная проверка* и *Выборочная проверка*, но и проверки дополнительных типов, см. ниже).
- 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 только те проверки, выполняемые Сканером, которые были непосредственно инициированы пользователем в окне Dr.Web для Linux, а также проверки, запущенные автоматически по заданному расписанию.

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.

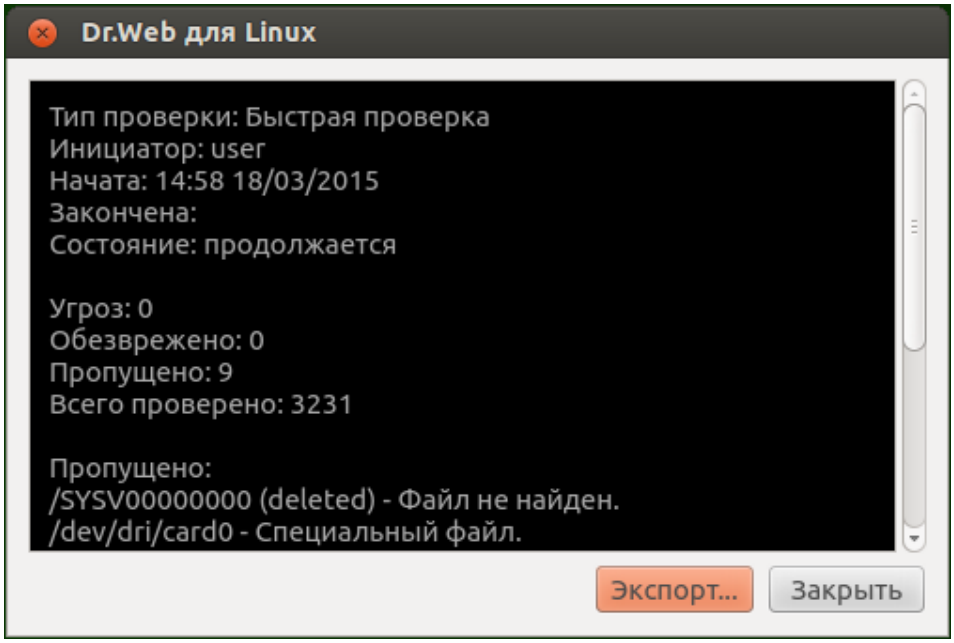

Рисунок 12. Детальная информация о проверке

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 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 Doctor Web, требуется наличие подключения к интернету).

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

К угрозам, обнаруженным Сканером в процессе любой проверки, запущенной через окно Dr.Web 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

В этом разделе:

- Общие сведения.
- Управление работой монитора файловой системы.
- Настройка работы монитора файловой системы.
- Проблемы в работе SpIDer Guard.

Общие сведения

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

Графический интерфейс управления Dr.Web 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 для Linux. Чтобы перейти на страницу управления мониторингом, нажмите **SpIDer Guard** на главной странице.

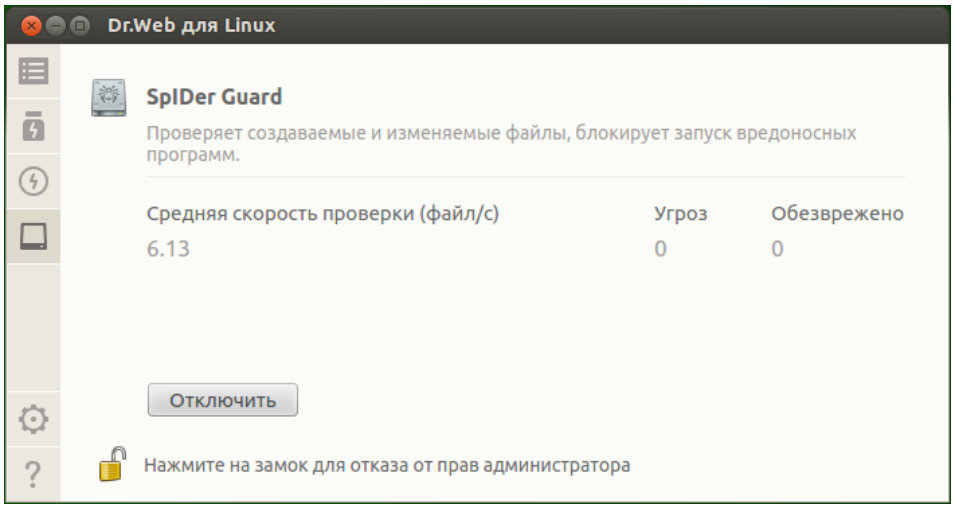

Рисунок 13. Страница управления работой SpIDer Guard

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 **Включить**. Чтобы отключить мониторинг, если он включен, нажмите **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 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 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 SpIDer Guard описано в разделе Режимы мониторинга файлов.

Проблемы в работе SpIDer Guard

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

Мониторинг сетевых соединений

В этом разделе:

- Общие сведения.
- Управление работой монитора сетевых соединений.
- Настройка работы SpIDer Gate.
- Проблемы в работе SpIDer Gate.

Общие сведения

Функция постоянного контроля установленных сетевых соединений реализуется монитором SpIDer 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, SpIDer Gate выполняет проверку:

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

В случае обнаружения угроз в проверенном объекте, SpIDer Gate блокирует его прием или передачу.

Графический интерфейс управления Dr.Web для Linux позволяет управлять работой SpIDer Gate:

- Запускать и останавливать мониторинг сетевых соединений.
- Просматривать количество проверенных и заблокированных объектов и попыток доступа к сайтам.
- Настраивать следующие параметры мониторинга сетевых соединений:
  - Выбирать тип проверяемого трафика (веб-трафик, FTP-трафик).
  - Перечень категорий сайтов и узлов, доступ к которым запрещается.
  - Персональные черные и белые списки пользователя для сайтов и узлов.
  - Параметры проверки файлов, загружаемых из интернета.

Угрозы, содержащиеся в сообщенияях электронной почты, могут быть обнаружены работающим монитором файловой системы SpIDer 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 для Linux. Чтобы перейти на страницу управления мониторингом сетевых соединений, нажмите **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 интернета.
  - Количество проверенных объектов (сообщений электронной почты, файлов, загруженных из интернета, а также URL).
  - Количество заблокированных обращений к сайтам и объектов, содержащих угрозы.

Чтобы включить мониторинг, если он отключен, нажмите **Включить**. Чтобы отключить мониторинг, если он включен, нажмите **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 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 интернету).
	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 SpIDer Gate

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 SpIDer Gate

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 Dr.Web для Linux. В этом случае спам-проверка сообщений не производится.

Если какие-либо сообщения электронной почты неправильно распознаются компонентом Dr.Web Anti-Spam, рекомендуется отправлять их на специальные почтовые адреса для анализа и повышения качества работы спам-фильтра. Для этого каждое такое сообщение сохраните в отдельный файл типа `.eml`. Сохраненные файлы прикрепите к сообщению электронной почты, которое отправьте на соответствующий служебный адрес.

- nonspam@drweb.com — если оно содержит файлы писем, *ошибочно признанных спамом*;
- spam@drweb.com — если оно содержит файлы писем, *ошибочно не определенных как спам*.

Просмотр обнаруженных угроз

В этом разделе:

- Общие сведения.
- Обезвреживание обнаруженных угроз.
- Просмотр информации об угрозах.

Общие сведения

Список угроз, обнаруженных Сканером и монитором файловой системы SpIDer Guard во время текущего сеанса работы Dr.Web 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  на навигационной панели.

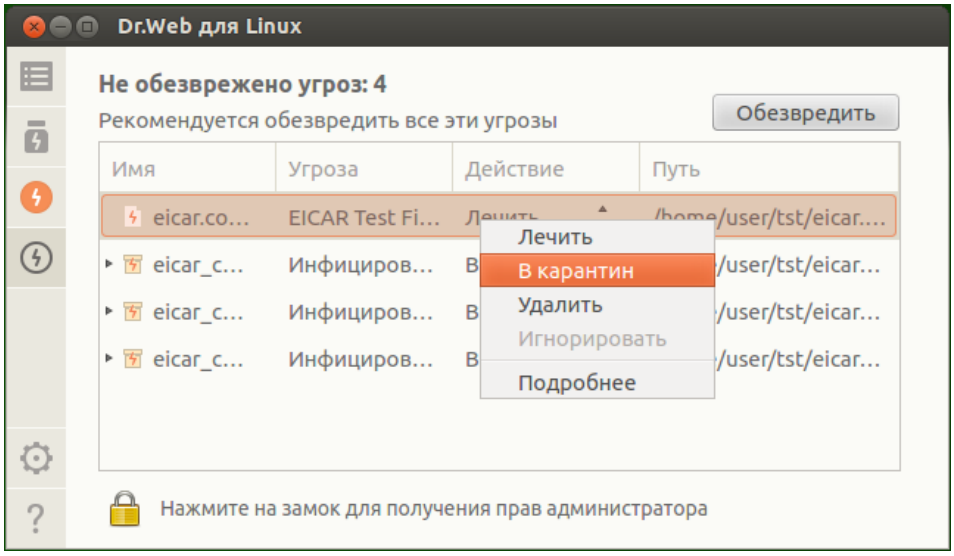

Рисунок 15. Страница обзора угроз

В списке для каждой обнаруженной угрозы выводится следующая информация:

- Имя объекта, содержащего угрозу.
- Имя угрозы, содержащейся в объекте (по классификации Doctor Web).
- 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 SpIDer Guard, могут быть изменены на соответствующих вкладках окна настроек.

Если в настройках Сканера или SplDer Guard было для некоторого типа угроз выбрано действие *Сообщать*, то все угрозы этого типа будут отображены в списке угроз с действием *Нет действия*. Для нейтрализации таких угроз необходимо указать для каждой из них действие в поле **Действие**.

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

Угрозы, к которым применено действие *Игнорировать*, будут отображаться в списке до перезапуска графического интерфейса управления.

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.

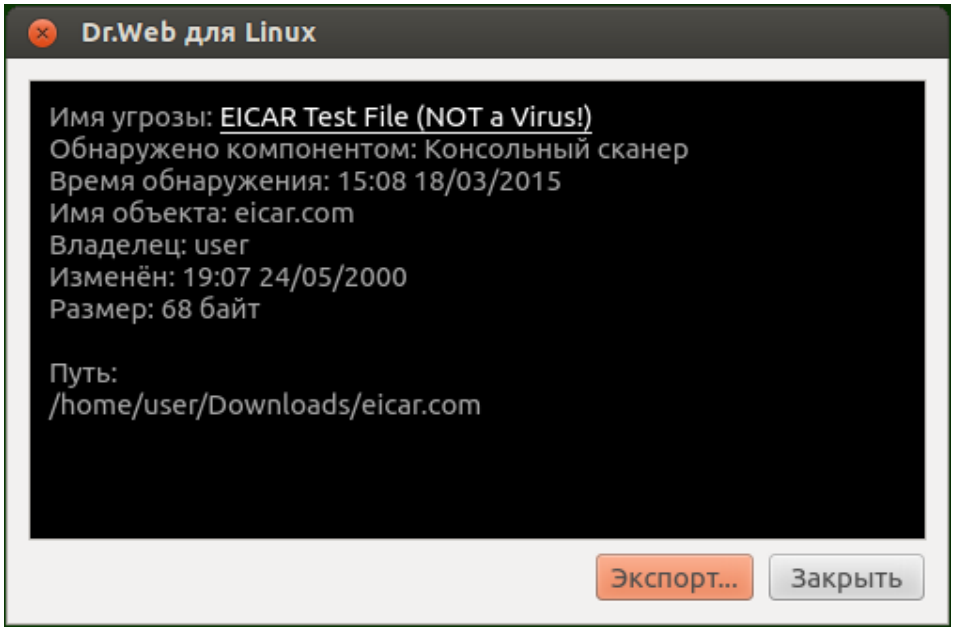

Рисунок 16. Информация об угрозе

В этом окне отображается следующая информация:

- Имя угрозы (по классификации Doctor Web).
- Название компонента Dr.Web 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 Doctor Web, требуется подключение к интернету).

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

Управление карантином

В этом разделе:

- Общие сведения.
- Применение действий к изолированным объектам.

- Просмотр информации об изолированных объектах.

Общие сведения

Список объектов, изолированных Dr.Web для Linux в карантин, отображается на специальной странице. Чтобы ее открыть, нажмите  на навигационной панели.

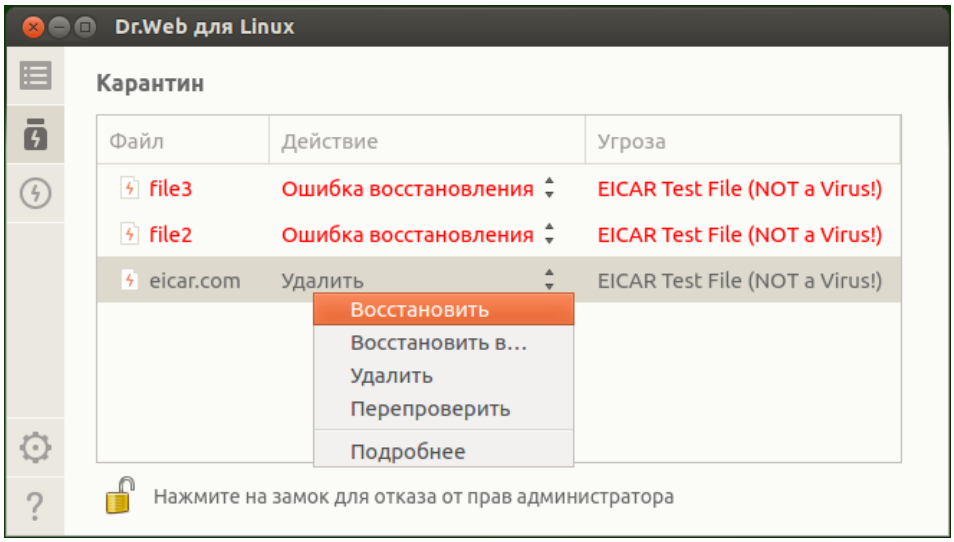

Рисунок 17. Страница управления карантином

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

- Имя объекта, содержащего угрозу.
- Действие, которое требуется применить к объекту в карантине.
- Имя угрозы, содержащейся в объекте (по классификации Doctor Web).

Применение действий к изолированным объектам

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

- При удержании клавиши 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 щелкните правой кнопкой мыши по строке информации об этом объекте и выберите в 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, выделите их в списке перед вызовом контекстного меню.

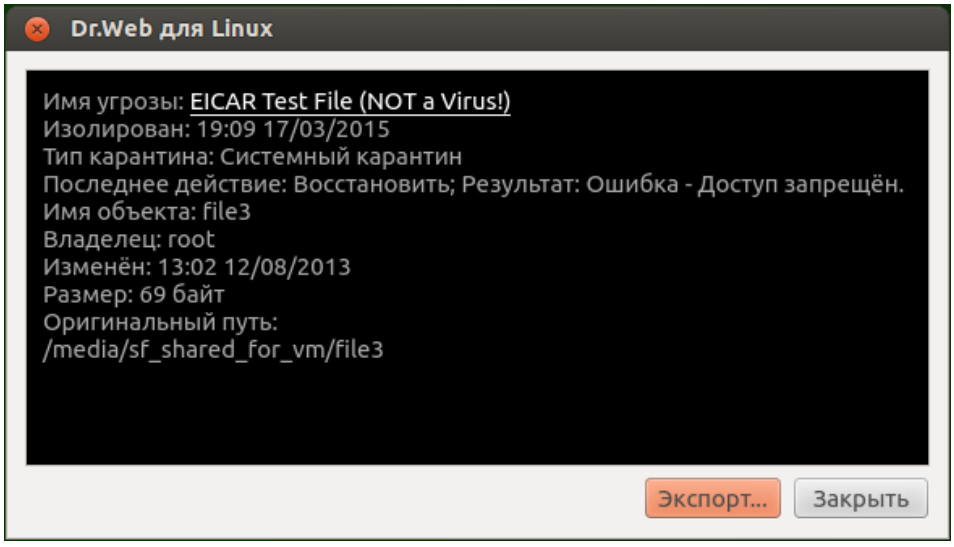

Рисунок 18. Информация об изолированном объекте

В этом окне отображается следующая информация:

- Имя угрозы (по классификации Doctor Web).
- 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 Doctor Web, требуется подключение к интернету).

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

Обновление антивирусной защиты

В этом разделе:

- Общие сведения.
- Настройка обновлений.
- Проблемы в работе компонента обновлений.
- Обновление антивирусной защиты без подключения к Интернету.

Общие сведения

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 для Linux. Чтобы перейти на страницу управления обновлением, нажмите **Последнее обновление** на главной странице.

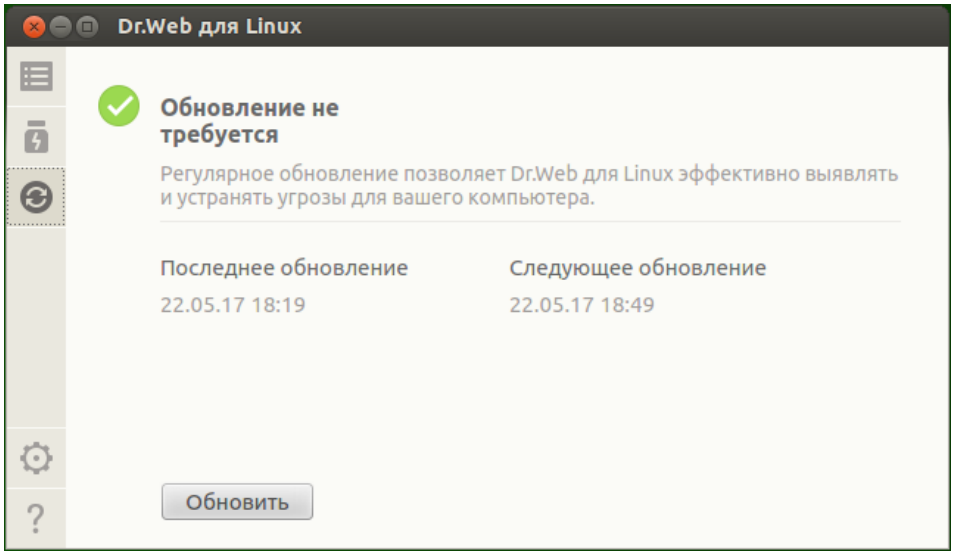

Рисунок 19. Страница управления обновлением

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 **Обновить**. Для закрытия страницы управления обновлением достаточно перейти к любой другой странице при помощи кнопок навигационной панели.

Если Dr.Web для Linux работает в режиме централизованной защиты, эта страница будет заблокирована.

Настройка обновлений

Настройка обновлений Dr.Web 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

В этом разделе:

Общие сведения

Менеджер лицензий позволяет просмотреть в графическом режиме информацию о текущей лицензии, которая выдана пользователю Dr.Web для Linux. Данные лицензии, выданной пользователю, хранятся в лицензионном ключевом файле, обеспечивающем работу Dr.Web для Linux на компьютере пользователя. В случае отсутствия на компьютере лицензионного или демонстрационного ключевого файла все антивирусные функции Dr.Web для Linux (проверка и мониторинг объектов файловой системы, обновление вирусных баз) будут заблокированы.

Запуск Менеджера лицензий

Менеджер лицензий интегрирован в окно Dr.Web для Linux. Чтобы открыть страницу Менеджера лицензий, нажмите **Лицензия** на главной странице окна.

Если на компьютере уже установлен ключевой файл, связанный с некоторой лицензией на использование Dr.Web 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.

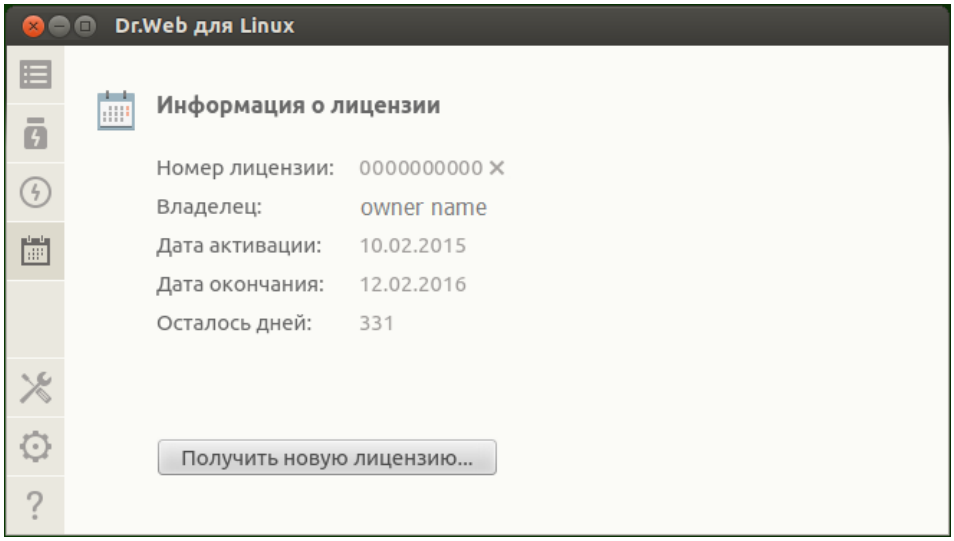

Рисунок 20. Информация о лицензии

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

Чтобы активировать лицензию при помощи Менеджера лицензий (в том числе — приобрести новую лицензию или продлить текущую) или демонстрационный период, и получить на компьютер соответствующий ключевой файл, обеспечивающий работу Dr.Web для Linux, нажмите **Получить новую лицензию**. После этого на экране появится мастер регистрации. Обратите внимание, что мастер регистрации также отображается автоматически при первом запуске Dr.Web 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 интернету.

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 **Активировать**.

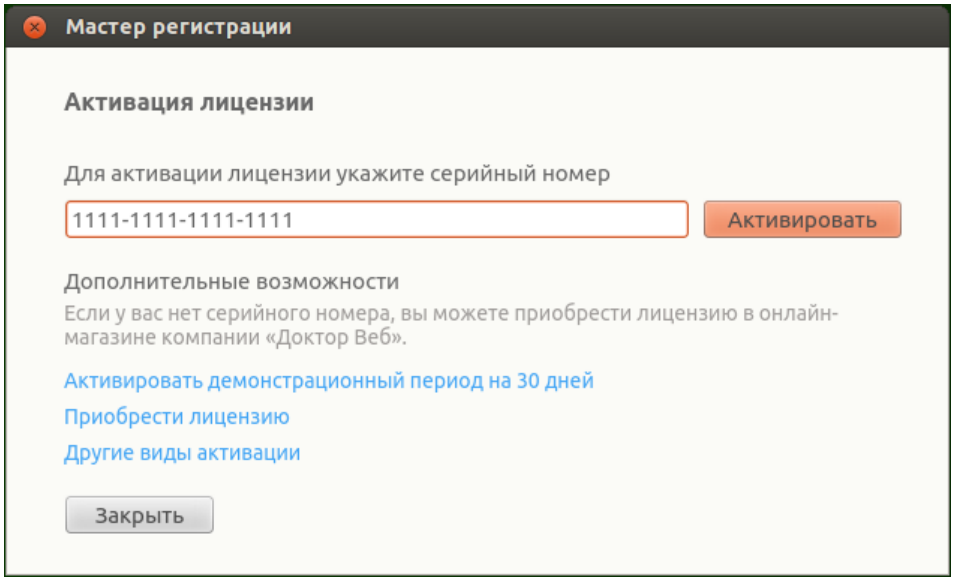

Рисунок 21. Регистрация при помощи серийного номера

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

О дополнительных способах приобретения лицензии на продукты Dr.Web см. в разделе Регистрация и активация.

После того, как вы нажмете **Активировать**, будет произведено подключение к серверу регистрации компании Doctor Web.

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 Dr.Web для Linux. 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).

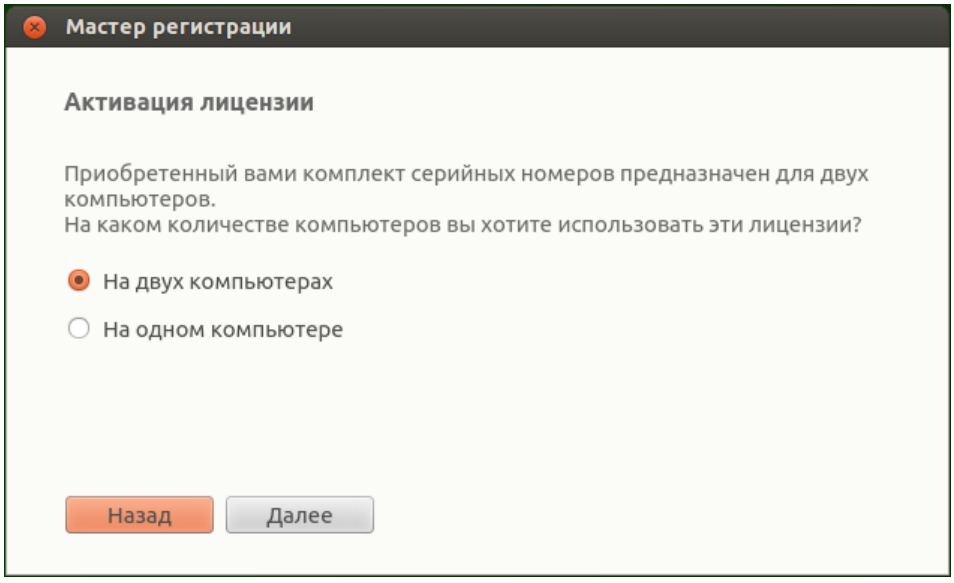

Рисунок 22. Выбор количества компьютеров

После выбора количества компьютеров, для которого может быть активирована лицензия, нажмите **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**.

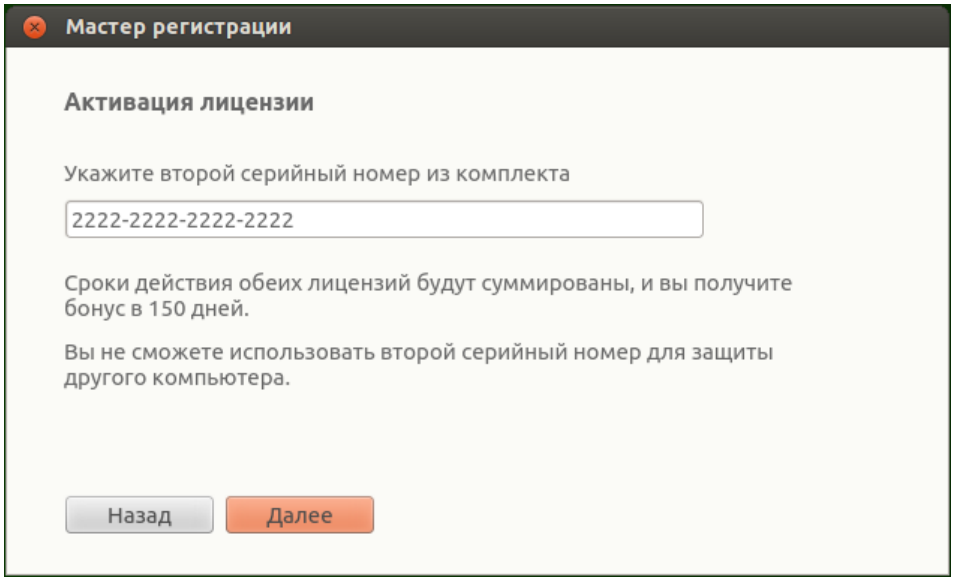

Рисунок 23. Указание второго серийного номера из комплекта

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**.

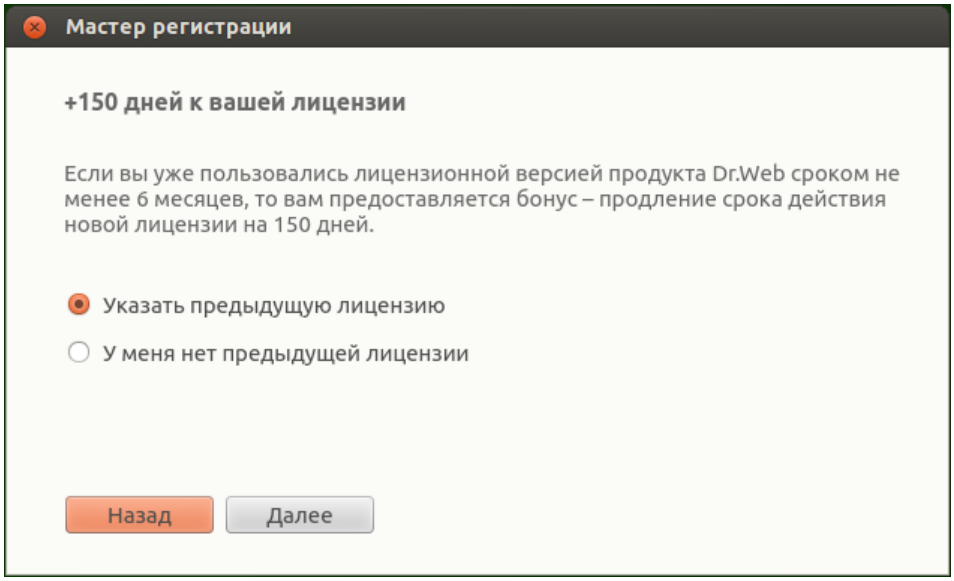

Рисунок 24. Получение бонуса

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.

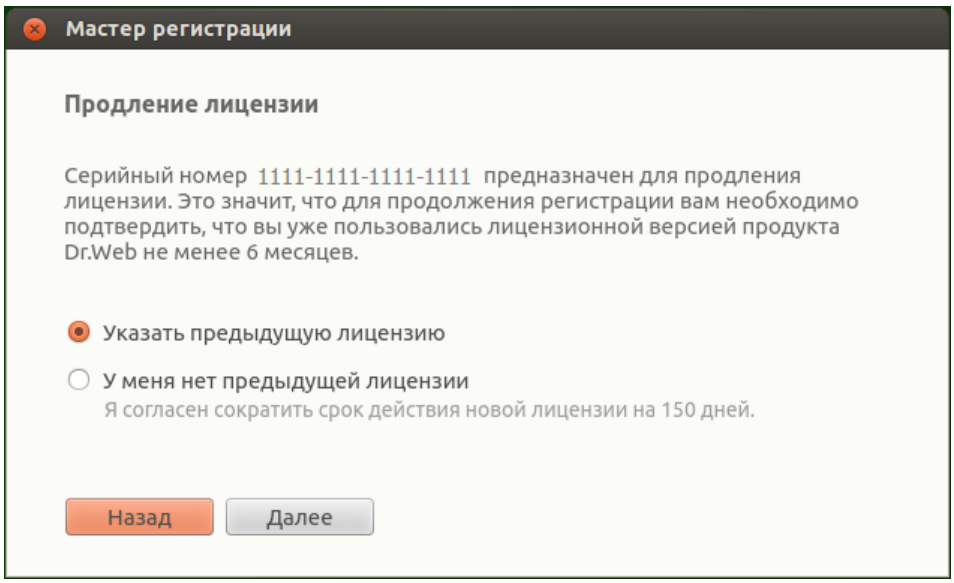

Рисунок 25. Продление лицензии

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

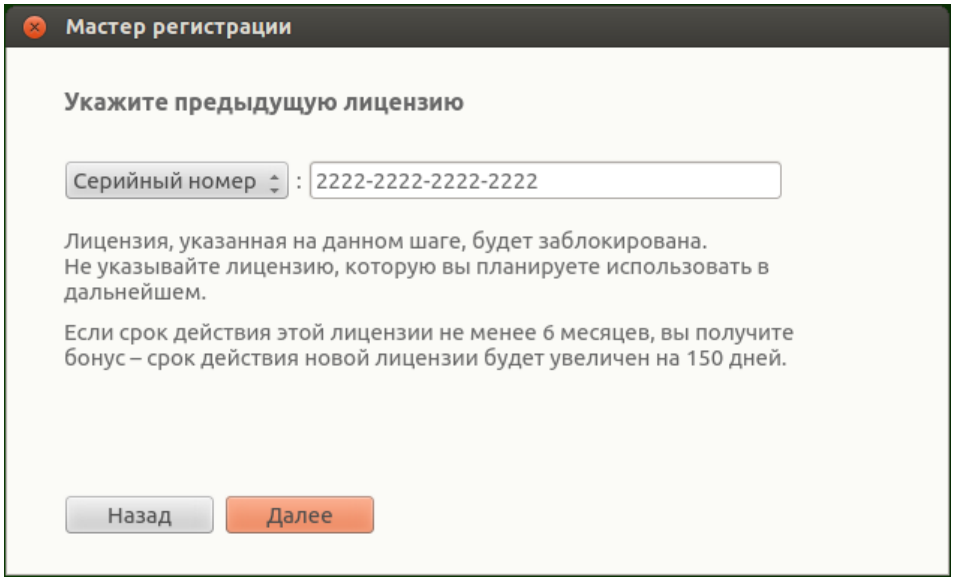

Рисунок 26. Указание предыдущей лицензии

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 150 бонусных дней для первого компьютера вы должны использовать на этом 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 150 бонусных дней для второго компьютера вы должны использовать на этом 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 прибавляются 150 бонусных дней (первый серийный номер дает бонус для второго номера). Кроме этого, если на этом шаге вы дополнительно укажете предыдущую лицензию, выданную для этого компьютера (если она имеется), то к удвоенному сроку действия активируемой лицензии также прибавятся 150 бонусных дней и остаток срока действия указанной лицензии.

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 **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 **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.

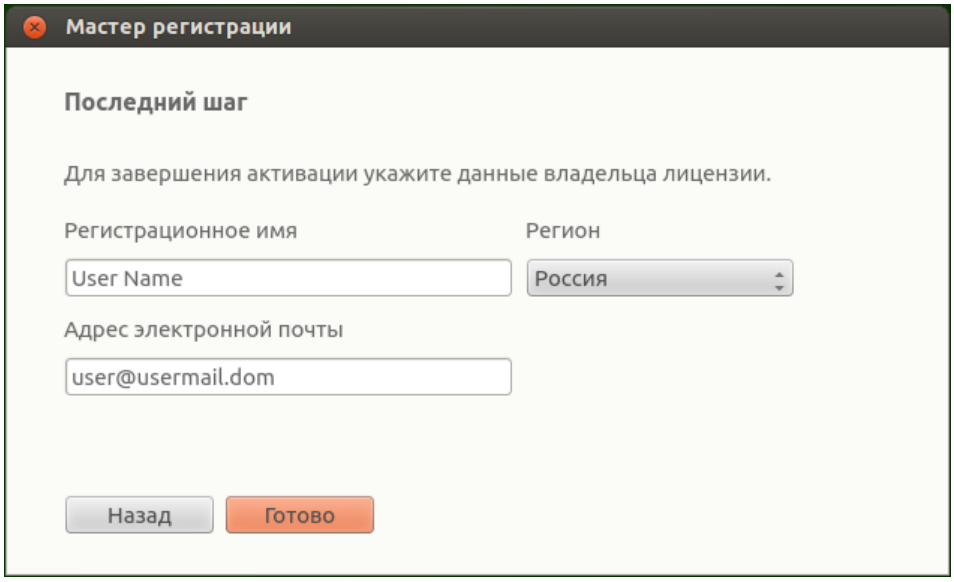

Рисунок 27. Регистрационная информация пользователя

После заполнения всех полей формы нажмите **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 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.

3. Установка имеющегося ключевого файла

Если вы уже имеете действующую лицензию и связанный с ней ключевой файл (возможно, полученный от компании Doctor Web или ее партнеров по электронной почте), то вы можете активировать Dr.Web 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.

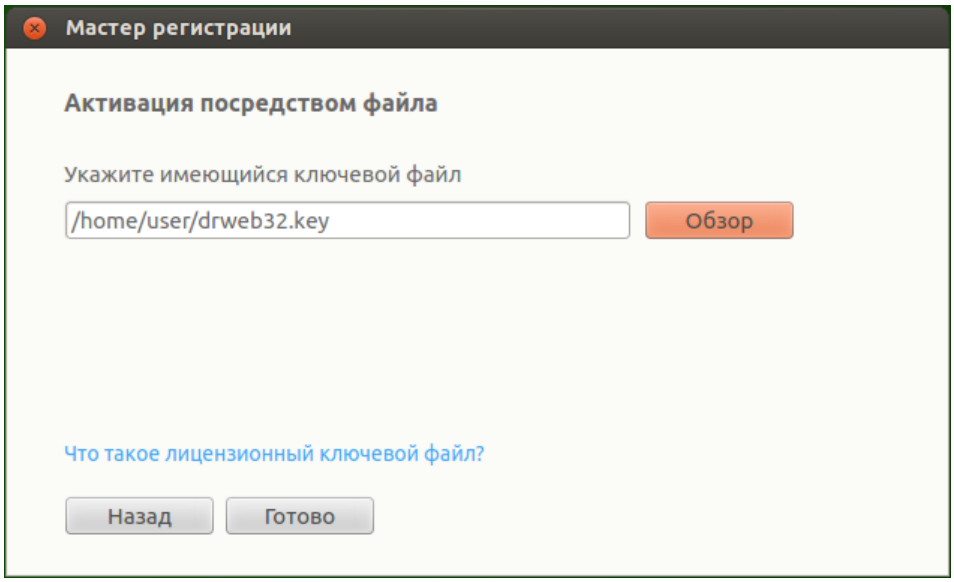

Рисунок 28. Активация посредством ключевого файла

Для указания ключевого файла вы можете:

- Ввести путь к нему непосредственно в строку ввода.
- Воспользоваться стандартным окном выбора файлов графической оболочки, нажав **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 **Готово** для автоматической установки ключевого файла. Ключевой файл будет при необходимости распакован и скопирован в каталог служебных файлов Dr.Web для Linux. Подключения к интернету в этом 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 **ОК** для закрытия мастера регистрации и возвращения на главную страницу окна Dr.Web для Linux.

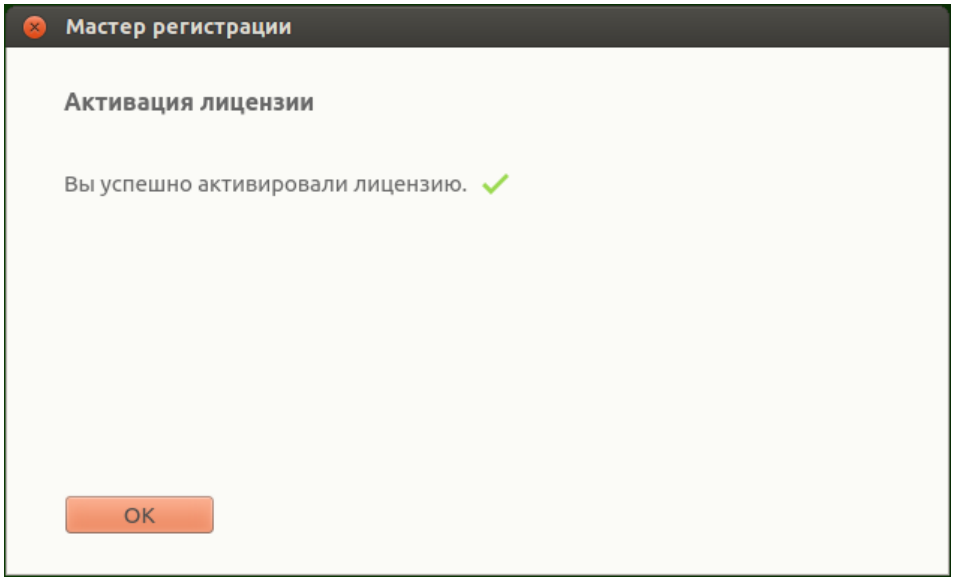

Рисунок 29. Сообщение об успешной активации

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.

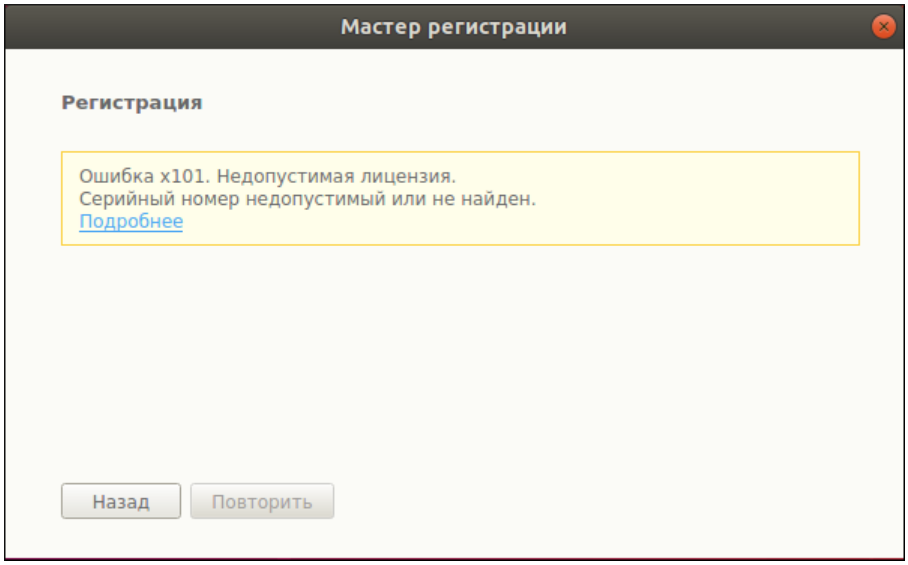

Рисунок 30. Сообщение об ошибке

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 **Назад**.

В случае если ошибка связана с временной неполадкой, например, временным сбоем в сети, то вы можете попытаться повторить этот шаг, нажав **Повторить**. В случае необходимости вы можете нажать **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 Doctor Web для проверки введенного серийного номера, будет показана страница с соответствующим сообщением об ошибке.

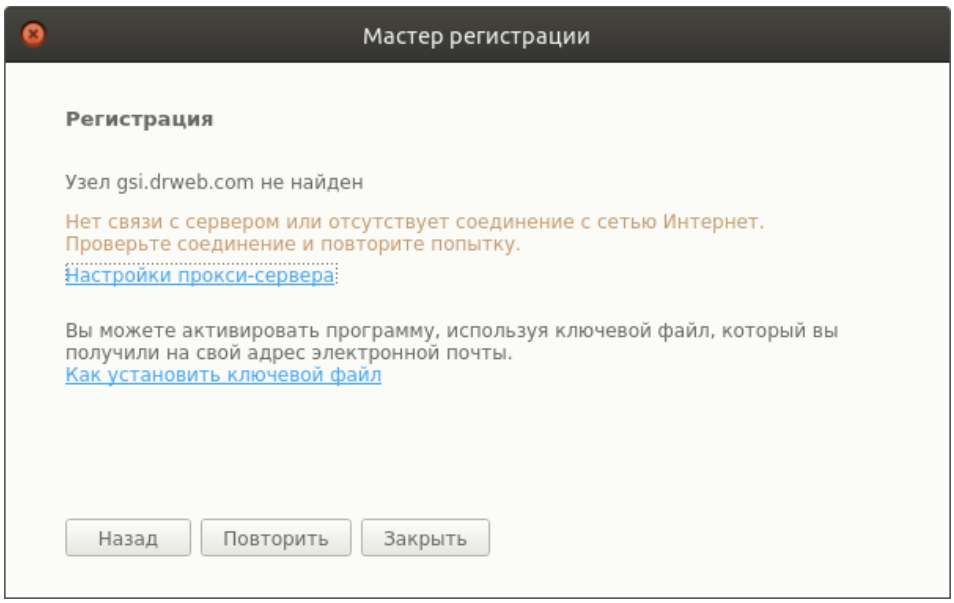

Рисунок 31. Ошибка подключения к серверу регистрации

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

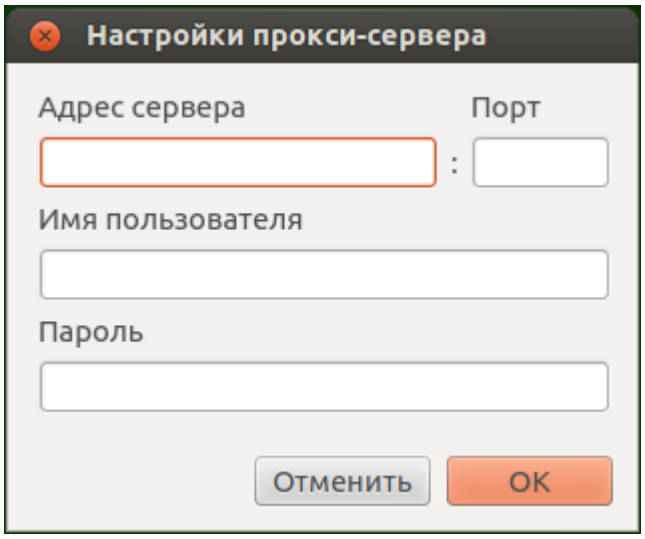

Рисунок 32. Настройки прокси-сервера

В этом окне укажите параметры доступа к прокси-серверу и нажмите **OK**. Затем повторите попытку подключения к серверу регистрации компании Doctor Web, нажав **Повторить**.

При активации новой лицензии и формировании нового ключевого файла, предыдущий ключевой файл, который использовался Dr.Web 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 для Linux на этом компьютере, а перенести его на другой компьютер) можно удалить установленный на компьютере лицензионный ключевой файл, управляющий работой Dr.Web 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 **Да**. Если вы решили отказаться от удаления с данного компьютера лицензионного ключевого файла, нажмите **Нет**.

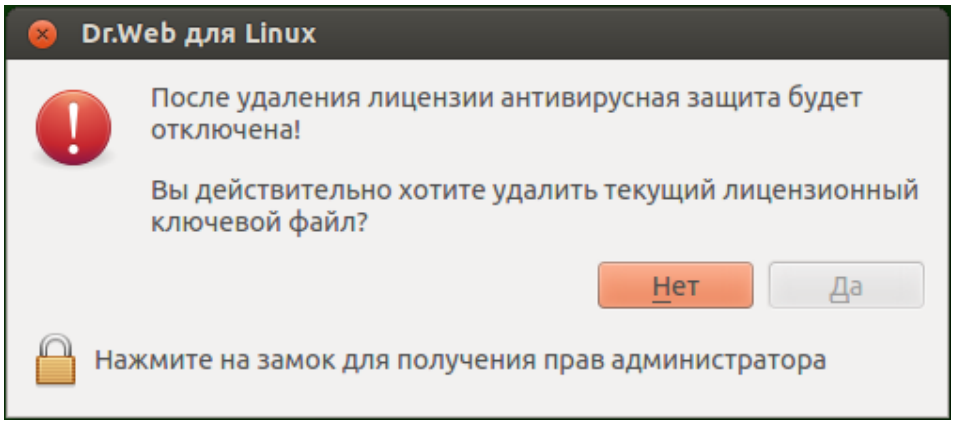

Рисунок 33. Окно подтверждения удаления лицензионного ключевого файла

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 для Linux

(проверка файлов, обновление вирусных баз, антивирусного ядра и баз категорий веб-ресурсов, мониторинг файловой системы) будут заблокированы.

Просмотр сообщений от сервера централизованной защиты

В этом разделе:

- Общие сведения.
- Применение действий к сообщениям.
- Фильтрация сообщений.

Общие сведения

Если Dr.Web для Linux работает под управлением сервера централизованной защиты, доступен интерфейс для просмотра сообщений о состоянии антивирусной сети, рассылаемых сервером на управляемые им станции. Данный инструмент может быть использован администратором антивирусной сети для отслеживания состояния сети и важных событий в работе сервера централизованной защиты.

> Сообщения о состоянии и событиях антивирусной сети будут поступать, только если администратор антивирусной сети настроил отправку сообщений на вашу рабочую станцию на том сервере централизованной защиты, к которому подключен Dr.Web для Linux. В противном случае просмотр сообщений недоступен и соответствующая страница не отображается на главном окне Dr.Web для Linux.

Интерфейс просмотра сообщений от сервера отображается на специальной странице.

Чтобы ее открыть, нажмите  на навигационной панели.

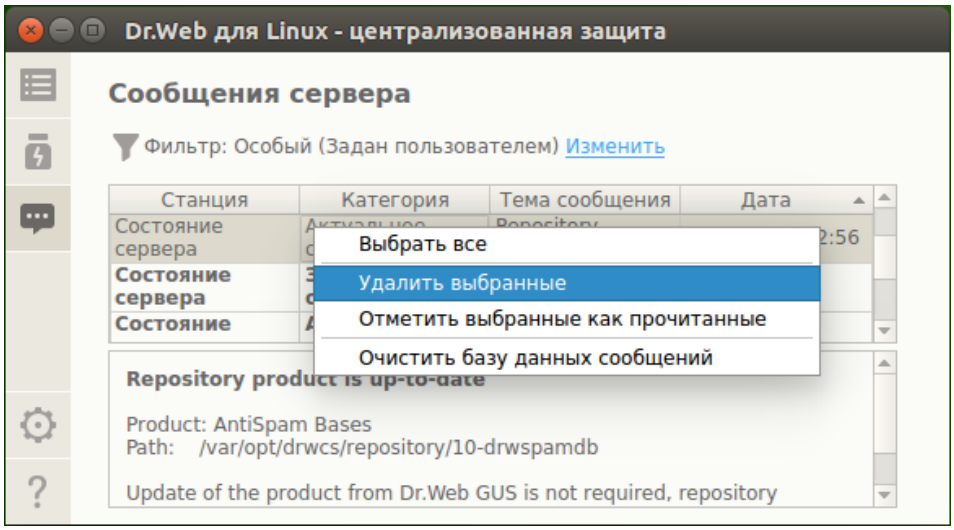

Рисунок 34. Страница просмотра сообщений сервера централизованной защиты

В списке для каждого сообщения выводится следующая информация:

- Имя (адрес) станции, информация о которой содержится в сообщении.
- Категория сообщения.
- Заголовок (тема) сообщения.
- Дата и время отправки сообщения сервером.

Для просмотра сообщения необходимо выделить его в списке, после этого текст выделенного сообщения будет отображен в панели под списком сообщений. Не просмотренные сообщения выделяются в списке жирным шрифтом.

Текст сообщений о состоянии и событиях антивирусной сети формируется на том языке, который задан в настройках сервера централизованной защиты.

Применение действий к сообщениям

Для выполнения какого-либо действия с сообщением щелкните правой кнопкой мыши в строке, содержащей информацию о сообщении, и выберите требуемое действие в контекстном меню. Если нужно совершить некоторое действие с несколькими сообщениями, выделите их в списке перед вызовом контекстного меню. Выделение осуществляется мышью при нажатой клавише CTRL или SHIFT:

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

Для выделения всех сообщений нажмите комбинацию клавиш CTRL+A.

В меню доступны следующие действия:

- Выделение в списке всех сообщений, подпадающих под текущий фильтр.
- Удаление выделенных сообщений.
- Отметка выделенных сообщений как прочитанные.
- Очистка базы данных сообщений.

При очистке базы данных сообщений будут удалены все поступившие сообщения (в том числе — не прочитанные).

Обратите внимание, что для сообщений, поступивших от сервера централизованной защиты, в настройках задается предельный срок их хранения в базе данных, после чего они удаляются автоматически.

Фильтрация сообщений

В связи с тем, что от сервера может поступать значительное число сообщений, предусмотрена возможность их фильтрации как по адресу сервера-отправителя, или имени станции антивирусной сети, так и по категории интересующих сообщений и периоду времени их поступления. По умолчанию заданный фильтр отображает в списке сообщения всех категорий, поступившие от всех серверов в течение текущего дня.

При необходимости вы можете изменить фильтр показа сообщений. Для этого нажмите на ссылку **Изменить**. После этого в верхней части откроется панель изменения фильтра.

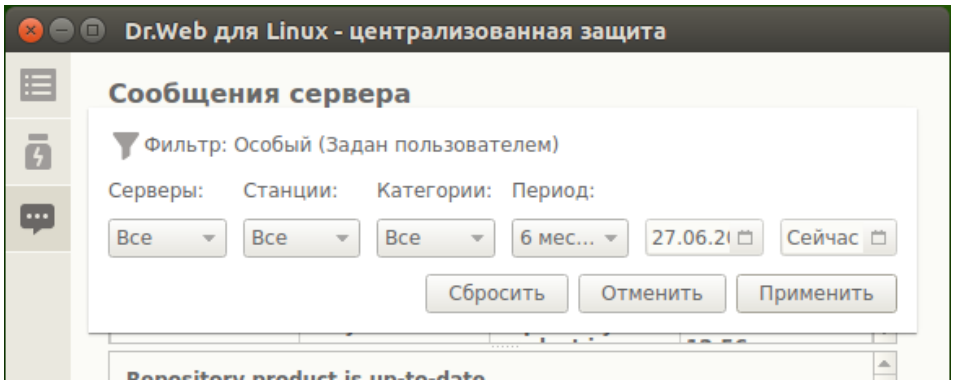

Рисунок 35. Панель фильтра сообщений

В панели фильтра вы можете указать следующие параметры фильтрации сообщений:

- **Серверы** — список серверов, сообщения от которых будут показаны.
- **Станции** — список станций, сообщения про которые будут показаны.
- **Категории** — список категорий сообщений, которые будут показаны.
- **Период** — период формирования сообщений, которые будут показаны (кроме выбора типового периода из списка, вы можете указать конкретные моменты начала и окончания периода формирования сообщений сервером).

Для применения изменений, внесенных в фильтр, нажмите **Применить**. Чтобы закрыть панель фильтра, не применяя изменения, нажмите **Отменить**. Для сброса значений фильтра к значениям по умолчанию нажмите **Сбросить**.

Управление правами приложения

Некоторые действия в окне Dr.Web 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 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 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 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.

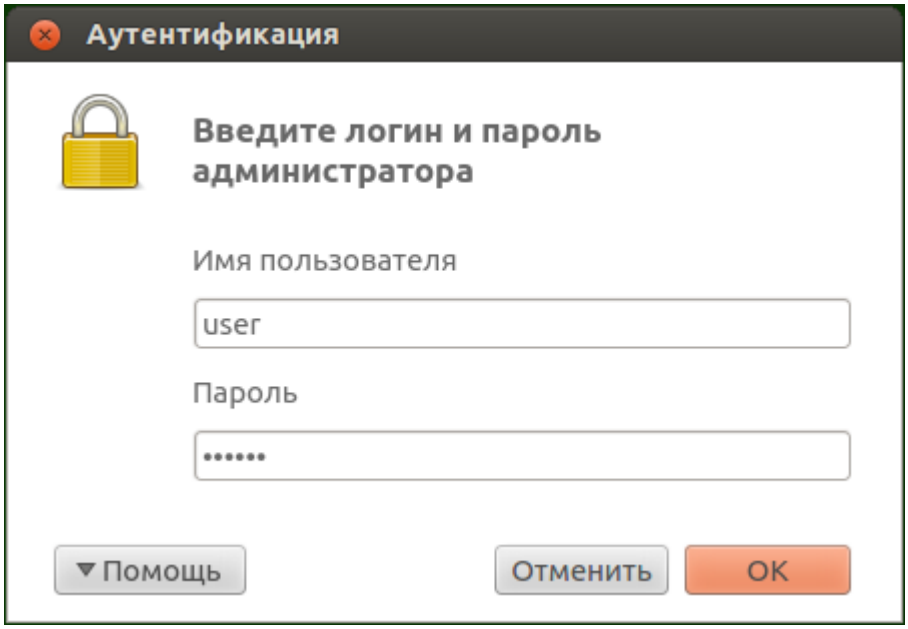

Рисунок 36. Окно аутентификации

Для получения приложением прав суперпользователя укажите имя (логин) и пароль любого пользователя, включенного в группу пользователей, указанную в настройках

Dr.Web для Linux как *группа администраторов*, или логин и пароль суперпользователя (учетная запись *root*), и нажмите **ОК**. Чтобы отказаться от повышения прав, закройте окно, нажав **Отменить**. Для просмотра или скрытия краткой подсказки по аутентификации нажмите **Справка**.

> По умолчанию при установке Dr.Web 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 нажмите  на навигационной панели окна Dr.Web для Linux.

На экране появится выпадающее меню, содержащее следующие пункты:

- **Справка** — открыть краткое Руководство пользователя Dr.Web для Linux.
- **Форум Dr.Web** — открыть в браузере страницу форума пользователей продуктов компании Doctor Web (требуется подключение к интернету).
- **Техническая поддержка** — открыть в браузере страницу службы технической поддержки компании Doctor Web (требуется подключение к интернету).
- **Мой Dr.Web** — открыть в браузере персональную страницу пользователя продуктов компании Doctor Web (требуется подключение к интернету).
- **О программе** — открыть окно с краткой информацией об Dr.Web для Linux и его версии.

Кроме того, когда на любой странице главного окна Dr.Web 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 для Linux на обнаруженные угрозы при проверках по требованию Сканером и при обнаружении их монитором файловой системы SpIDer Guard.

- Перечень объектов, исключаемых Сканером и SpIDer 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 для Linux.

Для доступа к окну настроек нажмите  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 для Linux на угрозы, обнаруживаемые Сканером в процессе проверки по требованию и по расписанию.
- SpIDer Guard — позволяет настроить реакцию Dr.Web для Linux на угрозы, обнаруживаемые монитором файловой системы SpIDer Guard.
- SpIDer Gate — позволяет настроить параметры контроля сетевых соединений монитором SpIDer Gate.
- Исключения — позволяет настроить список объектов, которые должны быть исключены из проверки по требованию и по расписанию, а также из перечня объектов, наблюдаемых SpIDer Guard и контролируемых SpIDer Gate.
- Планировщик — позволяет настроить периодический запуск проверок по заданному расписанию.
- Сеть — позволяет включить или отключить для SpIDer 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 для Linux.
- Dr.Web Cloud — позволяет разрешить или запретить Dr.Web для Linux использовать сервис Dr.Web Cloud.

Для получения справки нажмите  на соответствующей странице окна настроек.

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

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

Основные настройки

В этом разделе:

- Общие сведения.
- Настройки прокси-сервера, используемого для получения обновлений.

Общие сведения

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

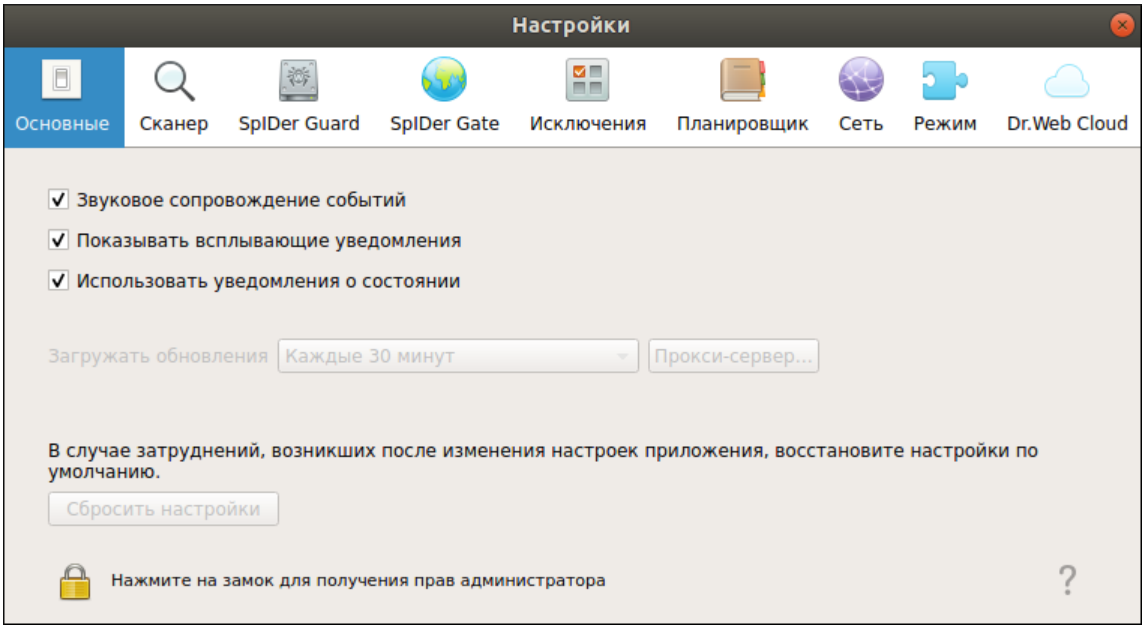

Рисунок 37. Вкладка основных настроек

Элемент управления	Действие
Флажок **Звуковое сопровождение событий**	Установка этого флажка предписывает Dr.Web для Linux проигрывать звуковые уведомления при возникновении таких событий, как: • обнаружена угроза (как Сканером так и SpIDer Guard); • ошибка проверки объекта; • и т. п.
Флажок **Показывать всплывающие уведомления**	Установка этого флажка предписывает Dr.Web 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.

Элемент управления	Действие
Флажок **Использовать уведомления о состоянии**	Установка этого флажка предписывает Dr.Web для Linux показывать всплывающие уведомления при изменении состояния компонентов (например, в случае их включения или отключения).
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 будет использоваться для получения обновлений.
- Порт для подключения к прокси-серверу.
- Имя пользователя и пароль, используемые для аутентификации на прокси-сервере.

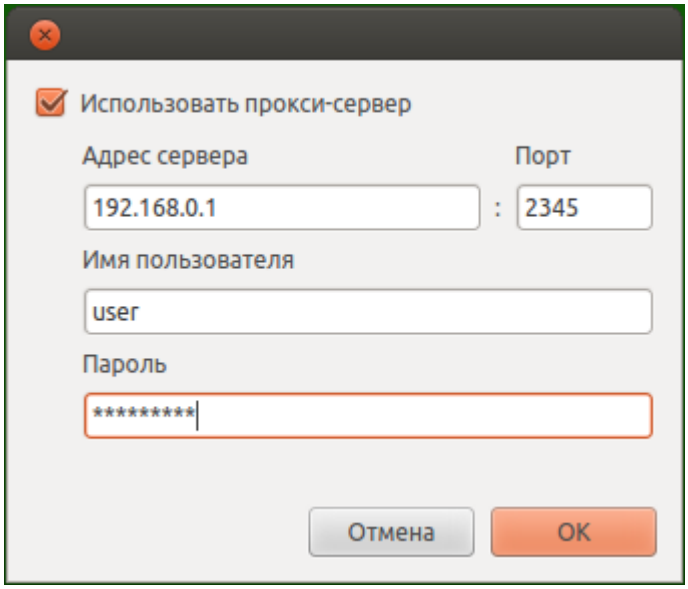

Рисунок 38. Настройки прокси-сервера

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

В этом разделе:

- Общие сведения.
- Дополнительные настройки проверки файлов.

Общие сведения

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

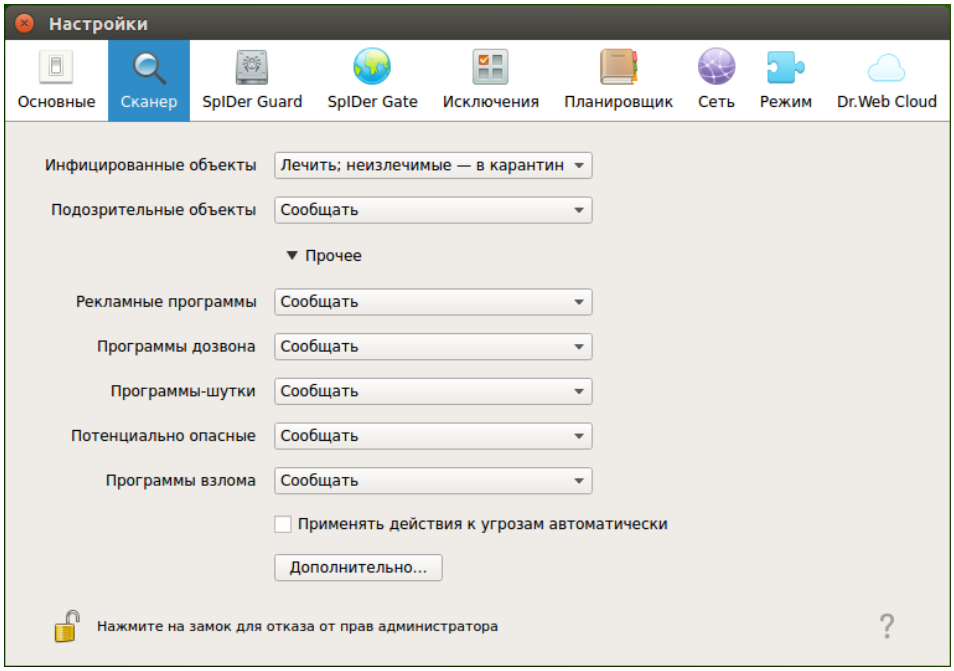

Рисунок 39. Вкладка настроек проверки файлов Сканером

В выпадающих списках выберите действия, которые Dr.Web для Linux будет применять к объектам при обнаружении в них любой из угроз соответствующего типа.

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

Установите флажок **Применять действия к угрозам автоматически**, если вы хотите, чтобы Dr.Web для Linux применял указанные действия сразу в момент обнаружения угроз Сканером в ходе проверки по требованию или по расписанию (вы будете проинформированы о нейтрализации угрозы, а информация о ней будет доступна в списке угроз). Если этот флажок сброшен, угроза, обнаруженная Сканером, будет только добавлена в список обнаруженных угроз, и вам придется самостоятельно выбрать, какое действие применить к объекту, содержащему обнаруженную угрозу.

Нажмите **Дополнительно**, чтобы открыть 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 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.

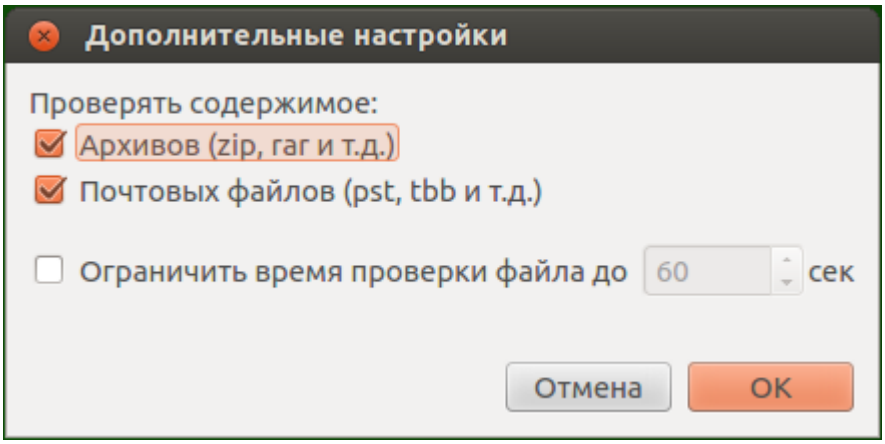

Рисунок 40. Дополнительные настройки проверки файлов

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 **OK**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

Настройки мониторинга файловой системы

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

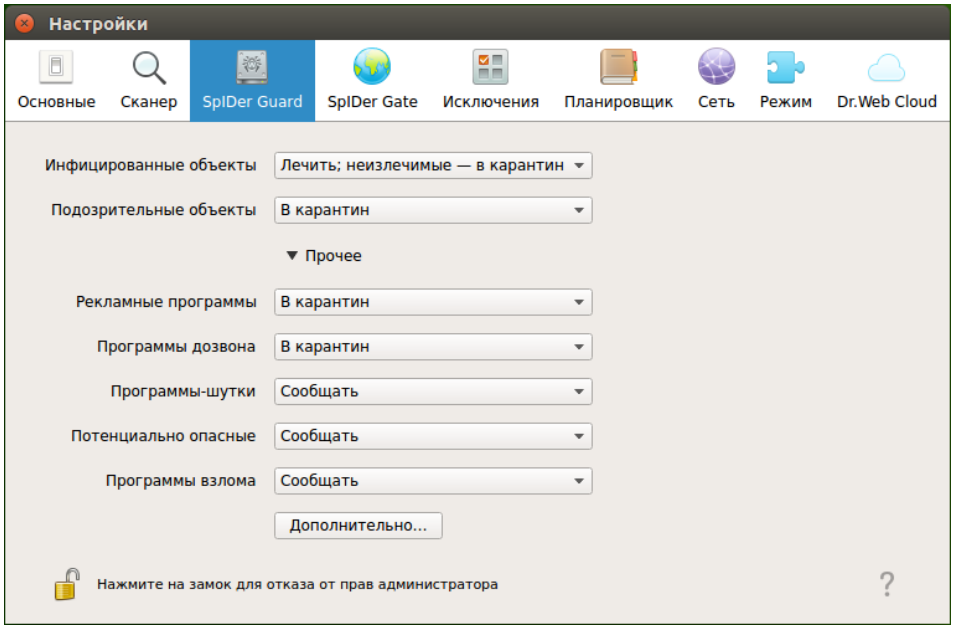

Рисунок 41. Вкладка настроек мониторинга файловой системы

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 SplDer Guard производится на вкладке **Исключения**.
- Включение усиленного режима мониторинга файлов монитором SplDer Guard описано в разделе Режимы мониторинга файлов.
- Реакции на обнаружение угроз, заданные для монитора SplDer Guard, не влияют на поведение Сканера. Его реакции на угрозы задаются на соответствующей странице.

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

Возможность настройки SplDer Guard при работе Dr.Web для Linux под управлением сервера централизованной защиты может быть заблокирована, если это запрещено сервером.

Настройки мониторинга сетевых соединений

В этом разделе:

- Общие сведения.
- Выбор категорий веб-сайтов.
- Управление параметрами проверки файлов.

Общие сведения

На вкладке **SpIDer Gate** вы можете настроить политики безопасности, которые монитор сетевых соединений SpIDer Gate будет использовать при контроле обращений к интернету.

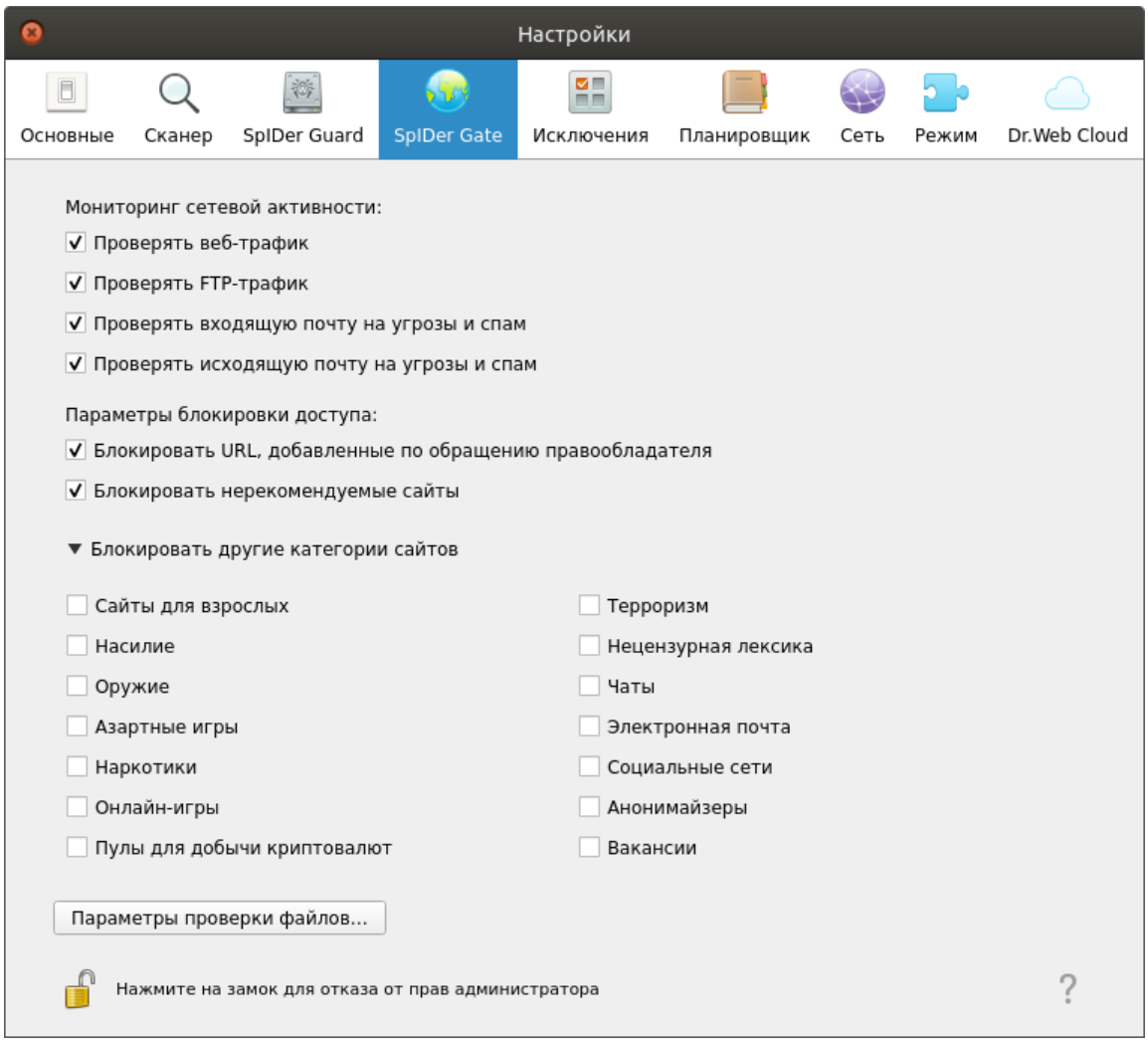

Рисунок 42. Вкладка настроек контроля доступа к сети

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

Выбор категорий веб-сайтов

Переключатели в разделе **Параметры мониторинга** определяют, доступ к веб-сайтам и узлам каких категорий блокируется (это относится не только к попыткам доступа к этим сайтам через браузер, но и к попыткам обращения к FTP-серверам). Устанавливая или снимая соответствующие переключатели, вы можете запретить или разрешить доступ к веб-сайтам и узлам 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 террористической направленности
Электронная почта	Сайты бесплатных почтовых служб
Социальные сети	Сайты социальных сетей
Онлайн-игры	Сайты, на которых размещены игры, использующие постоянное соединение с интернетом.
Анонимайзеры	Сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам.
Пулы для добычи криптовалют	Сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи («майнинга») криптовалют.

Категория	Описание
Вакансии	Сайты для поиска работы

База категорий веб-ресурсов поставляется в составе Dr.Web 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 SpIDer Gate будет блокировать доступ к веб-сайту или узлу, если он попадает хотя бы в одну из категорий, включенных для запрета доступа. Щелкните по надписи **Блокировать другие категории сайтов** чтобы показать или скрыть перечень доступных категорий.

Если нужно заблокировать доступ к некоторому веб-сайту или узлу, не относящемуся ни к одной из указанных категорий, включите его в черный список. Если наоборот, нужно разрешить доступ к некоторому веб-сайту или узлу, не смотря на то, что он относится к какой-либо из нежелательных категорий, включите его в белый список. Также вы можете настроить список приложений, чьи сетевые соединения не контролируются монитором SpIDer Gate.

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

Существует особая категория — *Источники распространения вирусов*. Доступ к веб-сайтам и узлам из этой категории запрещается в любом случае, даже если они включены в белый список.

Управление параметрами проверки файлов

Для управления параметрами, которые монитор SpIDer Gate будет применять при проверке файлов, загруженных из интернета, нажмите **Параметры проверки файлов**.

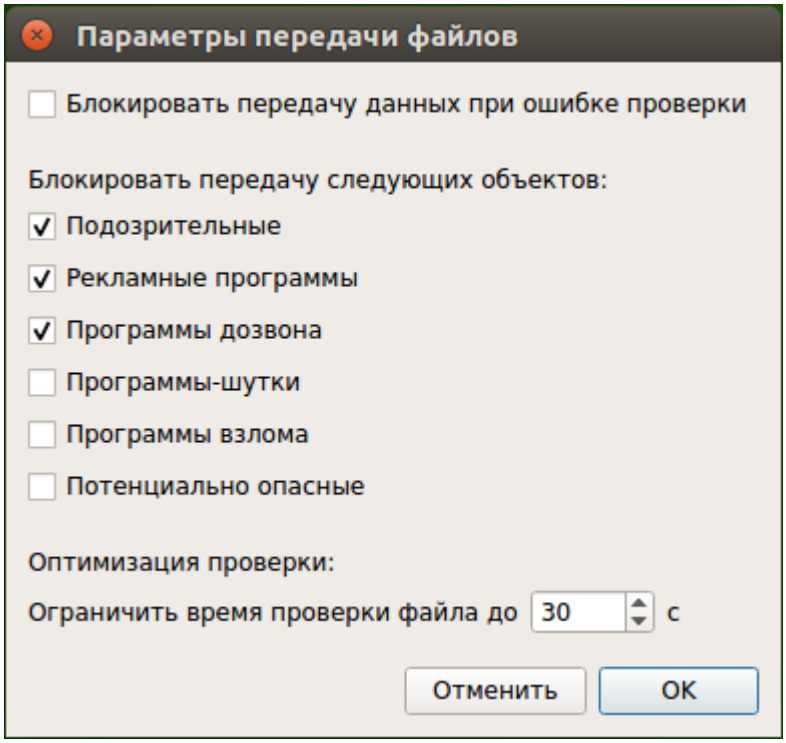

Рисунок 43. Окно управления настройками проверки файлов

В появившемся окне вы можете указать, какие категории вредоносных объектов нужно блокировать при попытке их передачи. Если некоторый переключатель включен, то файлы, содержащие угрозу соответствующего типа, будут отвергаться при попытке их загрузки на компьютер. Если переключатель отключен, то файлы, содержащие угрозы этого типа, будут загружаться из интернета. Также вы можете также установить максимальный интервал времени, отводимый на проверку загружаемых файлов. Если включен переключатель **Блокировать передачу данных при ошибке проверки**, то файлы, которые не удалось проверить из-за возникновения ошибки, будут блокироваться при загрузке. Для разрешения загрузки непроверенных файлов переключатель можно отключить (не рекомендуется).

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

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

Для изменения настроек монитора сетевых соединений SpIDer 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 SpIDer 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 SpIDer Gate.
- **Приложения** — открывает окно перечисления приложений, сетевые соединения которых не будут контролироваться монитором сетевых соединений SpIDer Gate.

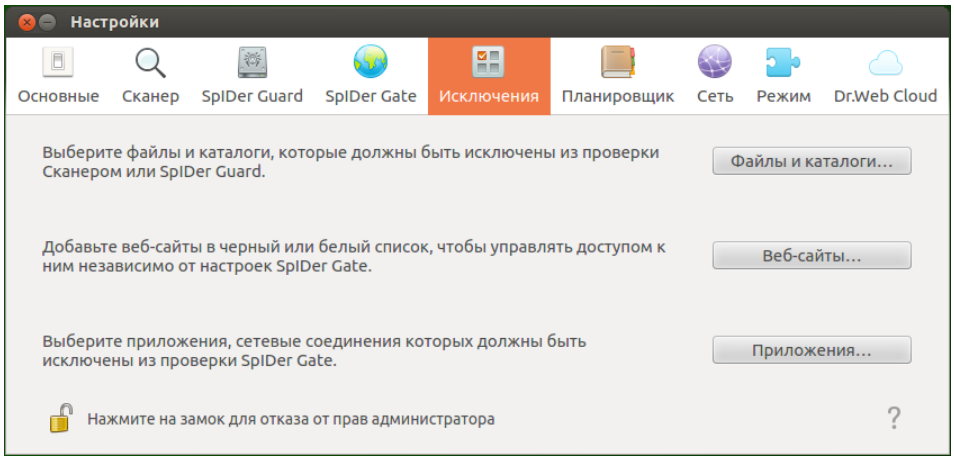

Рисунок 44. Вкладка настройки исключений

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

Исключение файлов и каталогов

В этом разделе:

- Общие сведения.
- Добавление и удаление объектов из списков исключений.

Общие сведения

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

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

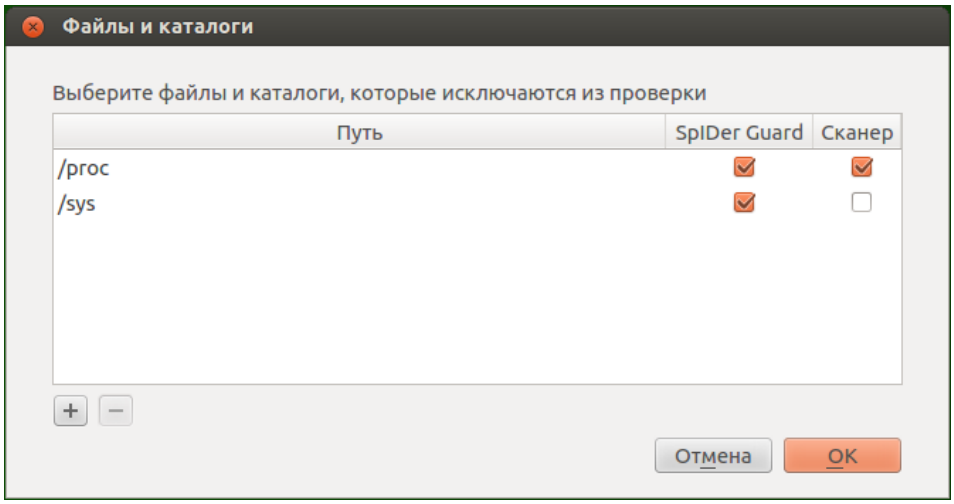

Рисунок 45. Настройка исключений файлов и каталогов

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, установите соответствующий флажок в строке объекта. Чтобы исключить объект, представленный в списке, из перечня объектов, исключаемых из проверки Сканером или SplDer Guard, сбросьте соответствующий флажок в строке объекта.
- Чтобы добавить в список новый объект, нажмите + под списком объектов, и выберите объект в появившемся окне выбора каталогов и файлов. Также вы можете добавить объекты в список, перетащив их мышью из окна файлового менеджера.
- Чтобы удалить объект из списка, выделите его строку в списке и нажмите – 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

В этом разделе:

- Общие сведения.
- Добавление и удаление приложений из списка исключений.

Общие сведения

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

Здесь вы можете указать перечень путей к исполняемым файлам приложений, чьи сетевые соединения не должны контролироваться монитором сетевых соединений SpIDer Gate.

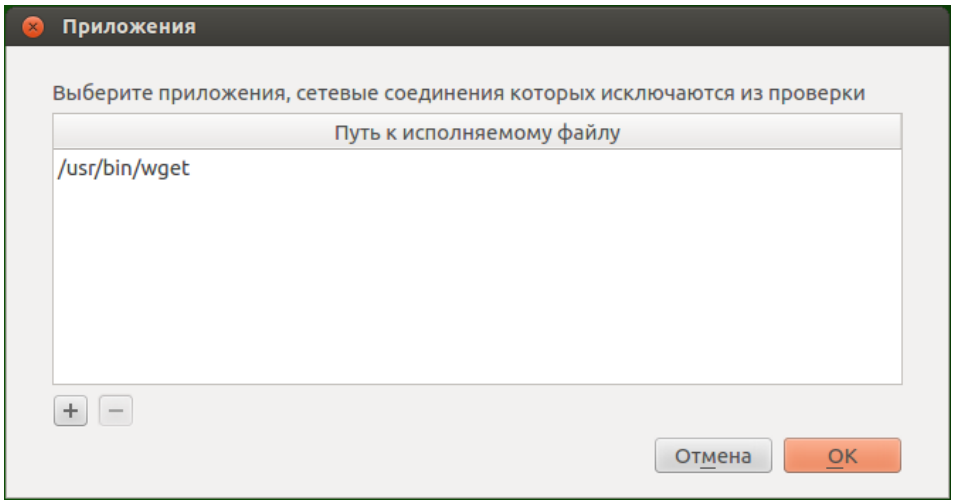

Рисунок 46. Настройка исключений сетевых соединений приложений

Добавление и удаление приложений из списка исключений

- Чтобы добавить в список новое приложение, нажмите + под списком приложений и выберите 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, выделите его строчку в списке и нажмите − под списком.

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

Черный и белый списки веб-сайтов

В этом разделе:

- Общие сведения.
- Добавление и удаление веб-сайтов из черного и белого списка.

Общие сведения

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

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

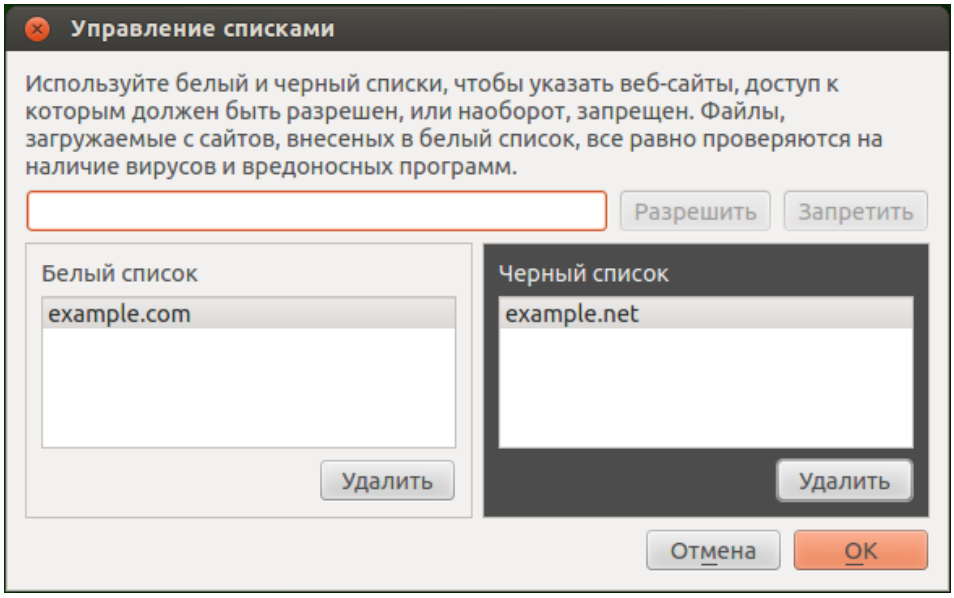

Рисунок 47. Окно управления черным и белым списками

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, наоборот, запрещает доступ ко всем ресурсам, расположенным на этом домене.
- Для удаления веб-сайта из белого или черного списка выделите его в соответствующем списке и нажмите **Удалить**.

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

Настройка проверки по расписанию

В этом разделе:

- Общие сведения.
- Настройка проверки по расписанию.

Общие сведения

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

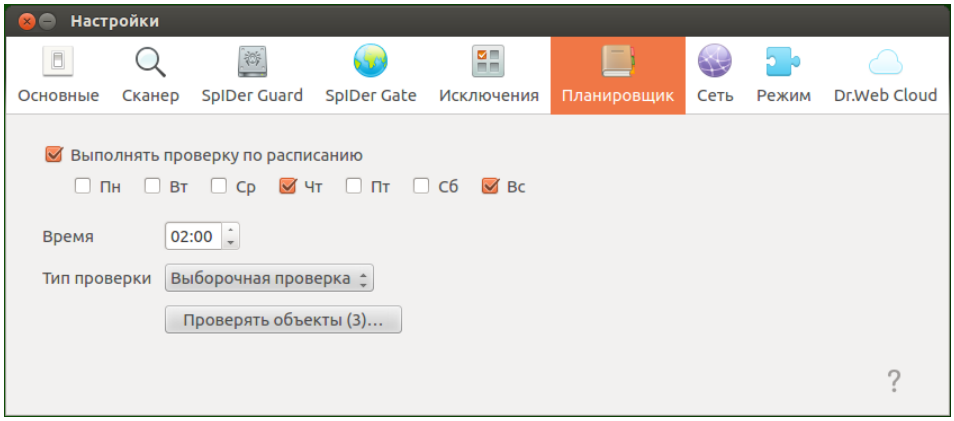

Рисунок 48. Вкладка настройки расписания

Для включения автоматической проверки по расписанию установите флажок **Выполнять проверку по расписанию**. В этом случае Dr.Web 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 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 для запуска проверки (для этого установите соответствующие флажки).
- Задать время (часы и минуты) начала проверки.
- Выбрать 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 **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, нажимая `+`, либо 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

В этом разделе:

- Общие сведения.
- Настройка проверки защищенных сетевых соединений.
- Добавление сертификата Dr.Web в списки доверенных сертификатов приложений.
- Добавление сертификата Dr.Web в список доверенных сертификатов через командную строку .

Общие сведения

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

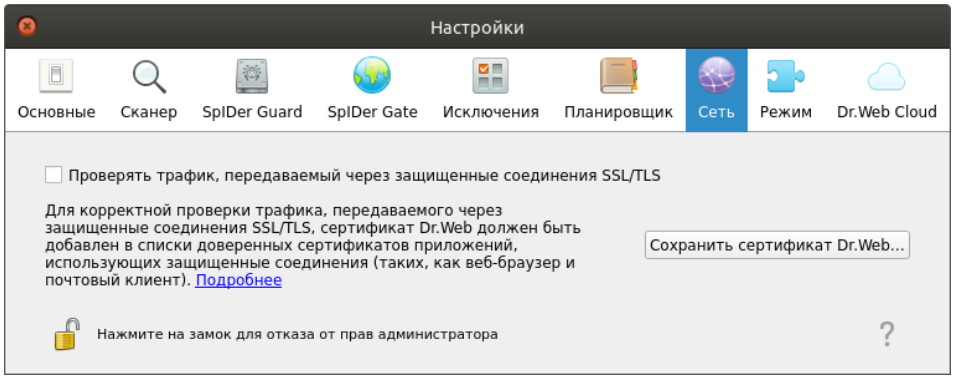

Рисунок 49. Вкладка настройки защиты от угроз, передаваемых через сеть

Настройка проверки защищенных сетевых соединений

Для разрешения монитору SpIDer 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 требуется 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 **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 вручную добавьте сохраненный файл сертификата Dr.Web 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 **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 **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 окно настроек почтового клиента, нажав **Закрыть**.
7) Перезапустите почтовый клиент.

Добавление сертификата Dr.Web в список доверенных сертификатов через командную строку

Сертификат можно добавить не только через графический интерфейс, но и через командную строку. Чтобы сгенерировать сертификат, выполните команду (необходимо указать имя файла, в который будет сохранен файл в формате PEM):

```
$ drweb-ctl certificate > <cert_name>.pem
```

Далее добавьте сертификат в системное хранилище. В разных дистрибутивах Linux эта операция выполняется с помощью разных команд.
В Ubuntu, Debian, Mint:

```
# cp <cert_name>.pem /etc/ssl/certs/
# c_rehash
```

В CentOS и Fedora:

```
# cp <cert_name>.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust extract
```

Настройка режима защиты

В этом разделе:

- Общие сведения.
- Подключение к серверу централизованной защиты.
- Дополнительные настройки.

Общие сведения

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

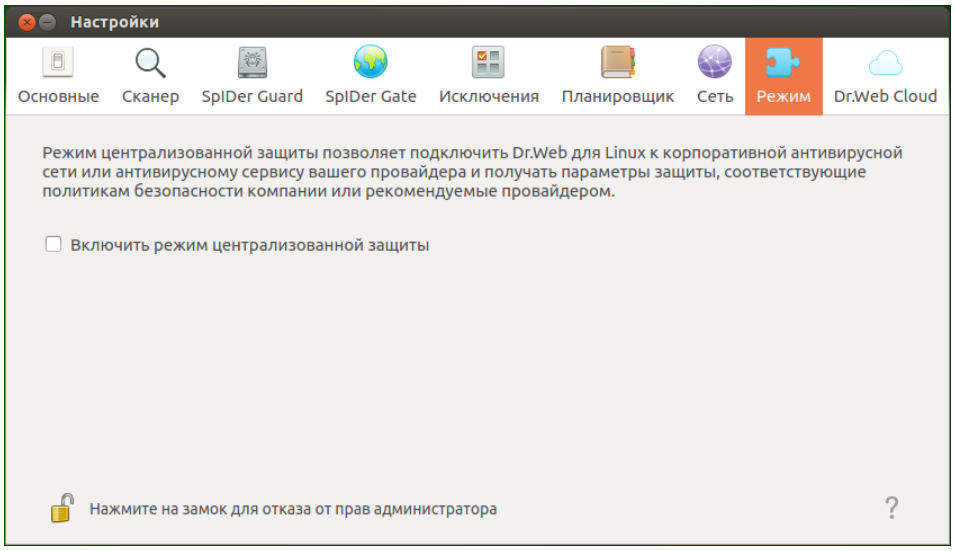

Рисунок 50. Вкладка управления режимом работы

Чтобы подключить Dr.Web для Linux к серверу централизованной защиты или отключиться от него, установите или сбросьте соответствующий флажок.

Для подключения Dr.Web 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:

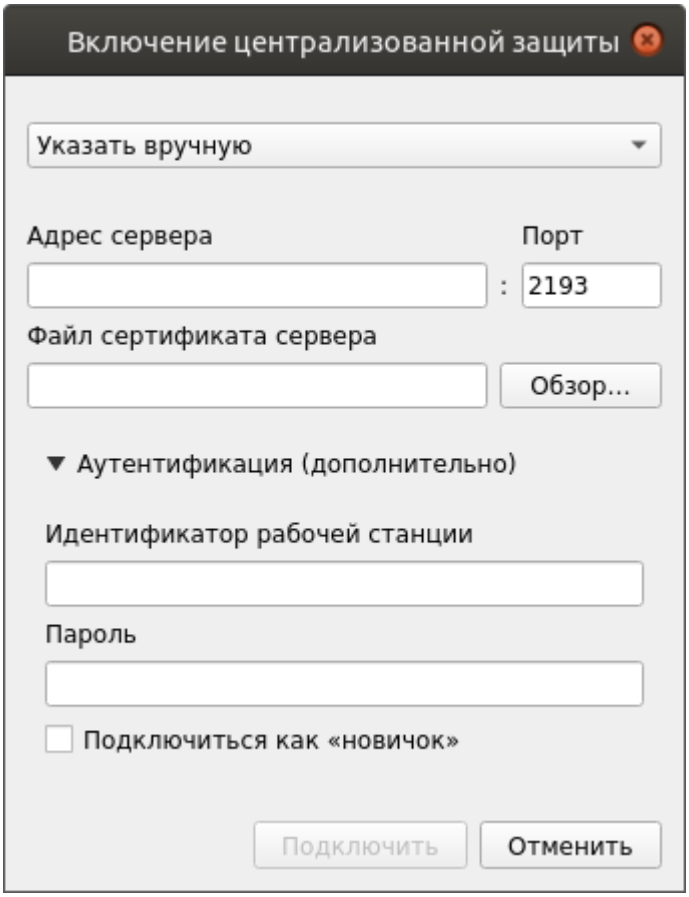

Рисунок 51. Окно подключения к серверу централизованной защиты

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 вариантов *Указать вручную* и *Определить автоматически* укажите адрес и порт для подключения к серверу

централизованной защиты, а также путь к файлу сертификата (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 задавайте в строгом соответствии с инструкциями, предоставленными администратором антивирусной сети или провайдером.

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

После того, как вы подключили Dr.Web 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 работы.

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

Дополнительные настройки

В выпадающем списке **Максимальное время хранения сообщений от сервера** вы можете указать предельный срок хранения сообщений о состоянии и событиях антивирусной сети, поступающих на эту рабочую станцию с сервера централизованной защиты, к которому подключен Dr.Web для Linux. По истечении указанного срока сообщения будут удаляться автоматически, даже если они не были прочитаны.

Сообщения о состоянии и событиях антивирусной сети будут поступать, только если администратор антивирусной сети настроил отправку сообщений на вашу рабочую станцию на том сервере централизованной защиты, к которому подключен Dr.Web для Linux. В противном случае просмотр сообщений недоступен и выпадающий список **Максимальное время хранения сообщений от сервера** не отображается на странице настроек режима защиты.

Настройка использования Dr.Web Cloud

На вкладке **Dr.Web Cloud** вы можете разрешить или запретить Dr.Web для Linux использовать сервис Dr.Web Cloud.

Подключение к Dr.Web Cloud позволяет Dr.Web для Linux использовать свежую информацию об угрозах, обновляемую на серверах компании Doctor Web 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.

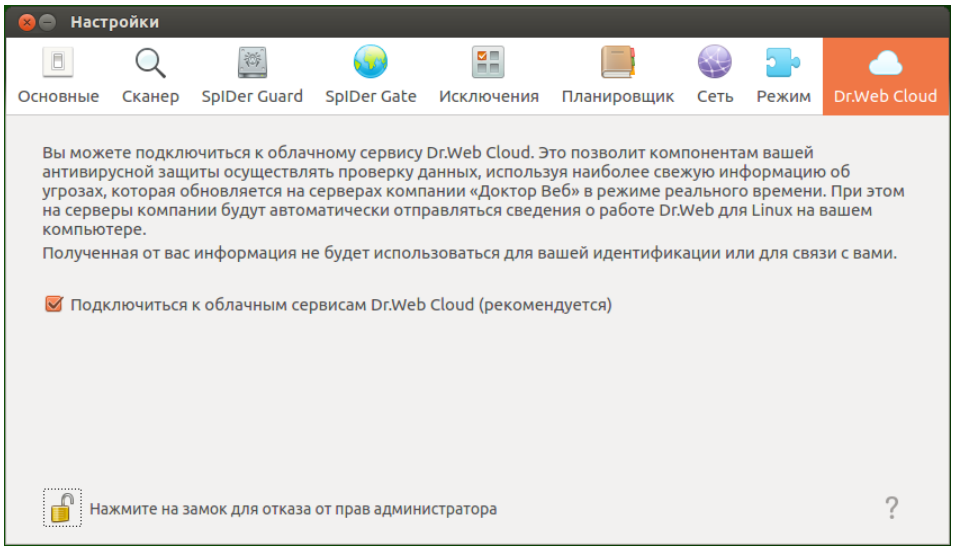

Рисунок 52. Вкладка управления использованием Dr.Web Cloud

Чтобы разрешить или наоборот, запретить Dr.Web для Linux использовать сервис Dr.Web Cloud, установите или сбросьте соответствующий флажок.

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

Для разрешения или запрещения Dr.Web 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 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 для Linux в режиме автономной копии.
- `--FullScan` — запустить полную проверку при старте графического интерфейса управления Dr.Web для Linux.
- `--ExpressScan` — запустить быструю проверку при старте графического интерфейса управления Dr.Web для Linux.
- `--CustomScan` — запустить выборочную проверку при старте графического интерфейса управления Dr.Web для Linux (открыть страницу выбора объектов, подлежащих проверке).

Пример:

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

Данная команда запустит графический интерфейс управления Dr.Web 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 для Linux поддерживает работу в особом режиме — режиме *автономной копии*.

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

- Для запуска графического интерфейса управления Dr.Web 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 Dr.Web для Linux 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 SpIDer Guard и SpIDer 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 ее сервисных компонентов.

Работа из командной строки

В этом разделе:

- Общие сведения.
- Удаленная проверка узлов.

Общие сведения

Имеется возможность управлять работой Dr.Web для Linux из командной строки операционной системы. Для этого в его состав входит специальная утилита Dr.Web Ctl (`drweb-ctl`). С ее помощью вы можете 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 антивирусных компонентов (вирусных баз, антивирусного ядра, и прочих, в зависимости от поставки).
- Просмотр и изменение параметров конфигурации Dr.Web для Linux.
- Просмотр состояния компонентов Dr.Web для Linux и статистики обнаруженных угроз.
- Просмотр карантина и управление его содержимым.
- Подключение к серверу централизованной защиты и отключение от него.

Чтобы команды управления Dr.Web для Linux, вводимые пользователем, имели эффект, должны быть запущены сервисные компоненты Dr.Web 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 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.

Коды всех имеющихся ошибок приведены в разделе Приложение Г. Описание известных ошибок.

Удаленная проверка узлов

Dr.Web для Linux позволяет проверять на наличие угроз файлы, находящиеся 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 требуется, чтобы удаленный узел предоставлял возможность удаленного доступа к нему через *SSH* (*Secure Shell*) или *Telnet*. Для доступа к устройству вы должны знать его IP-адрес или доменное имя, имя и пароль пользователя, который может совершить удаленный доступ к системе через *SSH* или *Telnet*. 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 невозможно. Для устранения обнаруженных угроз на удаленном узле воспользуйтесь средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров и прочих «умных» устройств вы можете обновить прошивку, а для вычислительных машин — подключиться к ним (в том числе — в удаленном терминальном режиме) и произвести соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустить установленное на них антивирусное ПО.

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 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 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 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.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-ctl`

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:

Команда	Описание
	<путь> — путь к файлу или каталогу, который нужно проверить (может быть относительным). *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 Dr.Web для Linux 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). `--Exclude` *<путь>* — путь, исключаемый из проверки. Может быть относительным и включать в себя файловую маску (содержащую символы '`?`' и '`*`', а также символьные классы '`[ ]`', '`[! ]`', '`[^ ]`'). *Необязательная опция; может быть указана более одного раза.* `--Report` *<тип>* — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет. • `DEBUG` — подробный отчет. • `JSON` — сериализованный отчет в формате JSON. 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*

Команда	Описание
	`--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* `--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*. `--MaxSizeToExctract` <size> — установить ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (b, kb, mb, gb). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *нет* `--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз. Если указано *No*, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: *No* Значение по умолчанию: *3000* `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: *On* `--OnKnownVirus` <*действие*> — действие, которое нужно выполнить, если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: *Report, Cure, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnIncurable` <*действие*> — действие, которое нужно выполнить, если лечение (`Cure`) обнаруженной угрозы окончилось неудачей или оно невозможно.

Команда	Описание
	Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnSuspicious` <*действие*> — действие, которое нужно выполнить, если эвристический анализ обнаружит подозрительный объект. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnAdware` <*действие*> — действие, которое нужно выполнить, если обнаружена рекламная программа. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnDialers` <*действие*> — действие, которое нужно выполнить, если обнаружена программа дозвона. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnJokes` <*действие*> — действие, которое нужно выполнить, если обнаружена программа-шутка. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnRiskware` <*действие*> — действие, которое нужно выполнить, если обнаружена потенциально опасная программа. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnHacktools` <*действие*> — действие, которое нужно выполнить, 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*). `--FollowSymlinks` — автоматически разрешать символические ссылки
`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

Команда	Описание
	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` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если Dr.Web для Linux работает под его управлением. `--Report` <*тип*> — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет. • `DEBUG` — подробный отчет. • `JSON` — сериализованный отчет в формате JSON. 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,

Команда	Описание
	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 Dr.Web для Linux работает под его управлением. `--Report` <*тип*> — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет. • `DEBUG` — подробный отчет. • `JSON` — сериализованный отчет в формате JSON. 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 нужно выполнить, если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: *Report, Cure, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnIncurable` <*действие*> — действие, которое нужно выполнить, если лечение (`Cure`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnSuspicious` <*действие*> — действие, которое нужно выполнить, если эвристический анализ обнаружит подозрительный объект. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnAdware` <*действие*> — действие, которое нужно выполнить, если обнаружена рекламная программа. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnDialers` <действие> — действие, которое нужно выполнить, если обнаружена программа дозвона. Возможные действия: *Report, Quarantine, Delete*.

Команда	Описание
	Значение по умолчанию: *Report* `--OnJokes` <*действие*> — действие, которое нужно выполнить, если обнаружена программа-шутка. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnRiskware` <*действие*> — действие, которое нужно выполнить, если обнаружена потенциально опасная программа. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* `--OnHacktools` <*действие*> — действие, которое нужно выполнить, если обнаружена программа взлома. Возможные действия: *Report, Quarantine, Delete*. Значение по умолчанию: *Report* При обнаружении угроз в исполняемом файле все запущенные из него процессы принудительно завершаются Dr.Web для Linux.
`remotescan` <*узел*> <*путь*>	Назначение: Инициировать проверку указанного файла или каталога на указанном удаленном узле, подключившись к нему через *SSH* или *Telnet*. 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:

Команда	Описание
	<*узел*> — IP-адрес или доменное имя узла, к которому необходимо подключиться для проверки. <*путь*> — путь к файлу или каталогу, который нужно проверить (должен быть абсолютным). Опции: `-m [--Method]` <*SSH*|*Telnet*> — метод (протокол) подключения к удаленному узлу. *Если метод не указан, будет использован SSH.* `-l [--Login]` <*имя*> — логин (имя пользователя) для авторизации на удаленном узле через выбранный протокол. *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 выбранный протокол. `-p [--Port]` <*число*> — номер порта на удаленном узле для подключения через выбранный протокол. Значение по умолчанию: *порт по умолчанию для выбранного протокола (22 — для SSH, 23 — для Telnet)*. `--ForceInteractive` — Использовать интерактивную сессию SSH (только для метода подключения *SSH*). *Необязательная опция.* `--TransferListenAddress` <*адрес*> — Адрес, прослушиваемый для приема файлов, передаваемых на проверку удаленным устройством. *Необязательная опция. Если не указана, используется произвольный адрес.* `--TransferListenPort` <*порт*> — Порт, прослушиваемый для приема файлов, передаваемых на проверку удаленным устройством. *Необязательная опция. Если не указана, используется случайный порт.* `--TransferExternalAddress` <*адрес*> — Адрес для передачи файлов на проверку, сообщаемый удаленному устройству. *Необязательная опция. Если не указана, используется значение опции `--TransferListenAddress`, либо исходящий адрес уже установленной сессии.* `--TransferExternalPort` <*порт*> — Порт для передачи файлов на проверку, сообщаемый удаленному устройству. *Необязательная опция. Если не указана, используется порт, определенный автоматически.* `--Password` <*пароль*> — пароль для аутентификации указанного пользователя через выбранный протокол. *Обратите внимание, что пароль передается в открытом виде.*

Команда	Описание
	`--Exclude` <*путь*> — путь, который необходимо исключить из проверки. Может включать в себя файловую маску (содержащую символы '?' и '*', а также символьные классы '[ ]', '[!]', '[^]'). Путь (в том числе содержащий маску) должен быть абсолютным. *Необязательная опция; может быть указана более одного раза.* `--Report` <*тип*> — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет. • `DEBUG` — подробный отчет. • `JSON` — сериализованный отчет в формате JSON. 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* `--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*. `--MaxSizeToExctract` <size> — установить ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (b, kb, mb, gb). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *нет*

Команда	Описание
	`--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз. Если указано *No*, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: *No* Значение по умолчанию: *3000* `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`

`checkmail` <*путь к файлу*>	Назначение: Выполнить (при помощи компонента проверки писем) проверку почтового сообщения, сохраненного в файл, на наличие угроз, признаков спама, вредоносных ссылок или несоответствия правилам обработки писем. В поток вывода консоли (*stdout*) будут возвращены результаты проверки письма, а также — какое действие было бы применено к данному письму при его проверке компонентом проверки писем.
	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.
	• *JSON* — сериализованный отчет в формате JSON.
	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, а именно:
	`threat_category in (KnownVirus, VirusModification, UnknownVirus, Adware, Dialer) : REJECT`
	`total_spam_score gt 0.80 : REJECT`
	`url_category in (InfectionSource, NotRecommended, CopyrightNotice) : REJECT`
	При этом, если компонент Dr.Web Anti-Spam не установлен, то правило проверки на спам (вторая строка) будет автоматически исключено из набора.
	`-c [--Connect]` <*IP*>:<*port*> — указать сетевой сокет, который будет использован как адрес, с которого подключился отправитель проверяемого сообщения.

Команда	Описание
	`-e [--Helo]` <*имя*> — указать идентификатор клиента, отправившего сообщение (IP-адрес или FQDN узла, как для SMTP-команды HELO/EHLO). `-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.*  Если компонент проверки писем не установлен, вызов данной команды вернет ошибку.

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 антивирусных компонентов (вирусных баз и антивирусного ядра, и прочих, в зависимости от поставки) с серверов обновлений компании Doctor Web или из локального облака, прервать уже запущенный процесс обновления или откатить результаты последнего обновления, восстановив предыдущие версии обновленных файлов.  Команда не имеет эффекта, если Dr.Web для Linux работает под управлением сервера централизованной защиты. Аргументы: Нет. Опции: `-l [--local-cloud]` — использовать для загрузки обновлений локальное облако, к которому подключен Dr.Web для Linux. Если опция

Команда	Описание
	не указана, обновления загружаются с серверов обновлений компании Doctor Web (поведение по умолчанию). `--From` <*путь*> — выполнить обновление из указанного каталога без подключения к интернету. `--Path` <*путь*> — сохранить в указанный каталог файлы, которые будут использоваться для обновления без подключения к интернету; если в этот каталог уже были загружены файлы, то они будут обновлены. `--Rollback` — откатить последнее обновление и восстановить последние сохраненные копии обновленных файлов. `--Stop` — прервать уже идущий процесс обновления.
`esconnect` <*сервер*>`[:`<*порт*>`]`	Назначение: Подключить Dr.Web для Linux к указанному серверу централизованной защиты (например, Dr.Web Enterprise Server). О режимах работы см. в разделе Режимы работы. 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: `--Certificate` <*путь*> — путь к файлу сертификата 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).

Команда	Описание
	Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`esdisconnect`	Назначение: Отключить Dr.Web для Linux от сервера централизованной защиты и перевести его в одиночный режим работы. Команда не имеет эффекта, если Dr.Web для Linux уже работает в одиночном режиме (standalone mode). Аргументы: Нет. Опции: Нет. Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). 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 Dr.Web для Linux. Аргументы: • *<секция>* — имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент. • *<параметр>* — имя изменяемого параметра. Обязательный аргумент. • *<значение>* — новое значение параметра. Обязательный аргумент.

Команда	Описание
	 Для задания значения параметров всегда используется формат <*секция*>.<*параметр*> <*значение*>, знак присваивания '=' не используется. Если вы хотите задать несколько значений параметра, то нужно повторить вызов команды `cfset` столько раз, сколько значений параметра вы хотите добавить. При этом для добавления нового значения в список значений параметра необходимо использовать опцию `-a` (см. ниже). Нельзя указывать в качестве аргумента последовательность <*параметр*> <*значение 1*>, <*значение 2*>, так как строка "<*значение 1*>, <*значение 2*>" будет считаться единым значением параметра <*параметр*>. Описание конфигурационного файла доступно в документации `man 5 drweb.ini`. 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 необходимо использовать для добавления новых групп параметров с тегом. `-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 Dr.Web для Linux. Для вывода параметров по умолчанию используется формат <*секция*>.<*параметр*> = <*значение*>. Секции и параметры не установленных компонентов по умолчанию не выводятся.

Команда	Описание
	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, 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 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. Информация об угрозах выводится в соответствии с форматом, заданным необязательной

Команда	Описание
	опцией `--Format`. Если опция `--Format` не указана, то для каждой угрозы выводится следующая информация: • Идентификатор, присвоенный угрозе (порядковый номер). • Полный путь к инфицированному файлу. • Информация об угрозе (имя, тип по классификации компании Doctor Web). • Информация о файле: размер, пользователь-владелец, дата последнего изменения. • История действий с инфицированным файлом: обнаружение, применявшиеся действия и т. п. Аргументы: Нет. Опции: `--Format "<`*строка формата*`>"` — выводить информацию об угрозах в указанном формате. Описание строки формата приведено ниже. *Если эта опция указана совместно с любой из опций-действий, она игнорируется.* `-f [--Follow]` — выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (CTRL+C прерывает ожидание). *Если эта опция указана совместно с любой из опций-действий, она игнорируется.* `--Directory <`*список каталогов*`>` — выводить только те угрозы, которые были обнаружены в файлах в каталогах из *<список каталогов>*. *Если эта опция указана совместно с любой из опций, приведенных ниже, 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 действие ко всем обнаруженным угрозам, вместо *<список угроз>* укажите `All`. Например, команда: `$ drweb-ctl threats --Quarantine All` перемещает в карантин все обнаруженные объекты с угрозами.

Команда	Описание
`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. Информация об изолированных объектах выводится в соответствии с форматом, заданным необязательной опцией `--Format`. Если опция `--Format` не указана, то 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 Doctor Web). Аргументы: Нет. Опции: `-a [--Autonomous]` — запустить отдельную копию Сканера для выполнения заданного действия с карантином, завершив ее работу после окончания действия. *Эта опция может быть применена совместно с любой из опций, указанных ниже.* `--Format "<строка формата>"` — выводить информацию об объектах, находящихся в карантине, в указанном формате. Описание строки формата приведено ниже. *Если эта опция указана совместно с любой из опций-действий, она игнорируется.* `-f [--Follow]` — выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (CTRL+C прерывает ожидание). *Если эта опция указана совместно с любой из опций-действий, она игнорируется.* `--Discovery [<список каталогов>,]` — произвести поиск каталогов карантина в указанном списке каталогов и добавить их к консолидированному карантину в случае обнаружения. Если *<список каталогов>* не указан, то произвести поиск каталогов карантина в стандартных местах файловой системы (точки монтирования томов и домашние каталоги пользователей). *Эта опция может быть указана совместно не только с опцией `-a` (`--Autonomous`) (см. выше), но и с любой из опций-действий, перечисленных ниже. Более того, если команда `quarantine` запускается в режиме автономной копии, т. е. с опцией `-a` (`--`*

Команда	Описание

	`Autonomous`), *но без опции* `--Discovery`, *то это равносильно вызову:*
	`quarantine --Autonomous --Discovery`
	`--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 воспользуйтесь опцией восстановления `--Restore`.
	`--Restore` <*объект*> — восстановить указанный объект из карантина в исходное место.
	Обратите внимание, что для выполнения этого действия 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). Может быть указан как абсолютный, так и относительный (относительно текущего каталога) путь.
	Обратите внимание, что опция применяется только совместно с опцией восстановления `--Restore`.
	В качестве <*объект*> используется идентификатор объекта в карантине. Если требуется применить действие ко всем объектам, находящимся в карантине, вместо <*объект*> укажите `All`. Например, команда:
	`$ drweb-ctl quarantine --Restore All --TargetPath test`
	восстанавливает из карантина все имеющиеся в нем объекты, помещая их в подкаталог `test`, находящийся в текущем каталоге, из которого запущена команда `drweb-ctl`.
	Обратите внимание, что для варианта `--Restore All` *дополнительная опция* `--TargetPath`, *если указана, должна задавать путь к каталогу, а не к файлу.*

Форматированный вывод данных для команд threats и quarantine

Формат вывода задается строкой формата, указанной в качестве аргумента необязательной опции `--Format`. Строка формата обязательно указывается в кавычках. Строка формата может включать в себя как обычные символы (будут выведены на экран «как есть»), так и специализированные маркеры, которые при выводе будут заменены на соответствующую информацию. Доступны следующие маркеры:

1. Общие для команд `threats` и `quarantine`:

Маркер	Описание
`%{n}`	Перевод строки
`%{t}`	Табуляция
`%{threat_name}`	Имя обнаруженной угрозы (вируса) по классификации компании Doctor Web
`%{threat_type}`	Тип угрозы («known virus» и т. д.) по классификации компании Doctor Web
`%{size}`	Размер исходного файла
`%{origin}`	Полное имя исходного файла с путем
`%{path}`	Синоним для `%{origin}`
`%{ctime}`	Дата/время модификации исходного файла в формате "*%Y-%b-%d %H:%M:%S*" (например, "`2018-Jul-20 15:58:01`")
`%{timestamp}`	То же, что и `%{ctime}`, но в формате времени *UNIX timestamp*
`%{owner}`	Пользователь-владелец исходного файла
`%{rowner}`	Удаленный пользователь-владелец исходного файла (если не применимо или значение неизвестно — заменяется на `?`)

2. Специфические для команды `threats`:

Маркер	Описание
`%{hid}`	Идентификатор записи об угрозе в реестре истории событий, связанных с угрозой
`%{tid}`	Идентификатор угрозы
`%{htime}`	Дата/время события, связанного с угрозой
`%{app}`	Идентификатор компонента Dr.Web для Linux, обработавшего угрозу
`%{event}`	Последнее событие, связанное с угрозой: • `FOUND` — угроза была обнаружена; • `Cure` — угроза была вылечена; • `Quarantine` — файл с угрозой был перемещен в карантин;

Маркер	Описание
	• `Delete` — файл с угрозой был удален; • `Ignore` — угроза была проигнорирована; • `RECAPTURED` — угроза была обнаружена повторно другим компонентом.
`%{err}`	Текст сообщения об ошибке (если ошибки нет — заменяется на пустую строку)

3. Специфические для команды `quarantine`:

Маркер	Описание
`%{qid}`	Идентификатор объекта в карантине
`%{qtime}`	Дата/время перемещения объекта в карантин
`%{curetime}`	Дата/время попытки лечения объекта, перемещенного в карантин (если не применимо или значение неизвестно — заменяется на `?`)
`%{cureres}`	Результат попытки лечения объекта, перемещенного в карантин: • `cured` — угроза вылечена; • `not cured` — угроза не вылечена либо попыток лечения не производилось.

Пример

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

Данная команда выведет содержимое карантина в виде записей следующего вида:

```
{
 <путь к файлу>: <имя угрозы> - <дата перемещения в карантин>
}
…
```

3.5. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	Назначение: Вывести на экран информацию о работающих компонентах Dr.Web для Linux. Для каждого запущенного компонента выводится следующая информация: • Внутреннее имя. • Идентификатор процесса GNU/Linux (PID). • Состояние (запущен, остановлен и т. п.).

Команда	Описание
	• 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: `-l [--List]` — вывести полный список загруженных файлов вирусных баз данных и число вирусных записей в каждом файле.
`certificate`	Назначение: Вывести на экран содержимое доверенного сертификата Dr.Web, который используется Dr.Web 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.
`events`	Назначение: Просмотреть события Dr.Web для Linux. Кроме этого команда позволяет выполнить управление событиями (отметка как «прочитанные», удаление).

Команда	Описание
	Аргументы: Нет. Опции: `--Report` <*тип*> — установить тип отчета о событиях. Возможные значения: • `BRIEF` — краткий отчет. • `DEBUG` — подробный отчет. • `JSON` — сериализованный отчет в формате JSON. `-f [--Follow]` — выполнять ожидание поступления новых событий и выводить их на экран сразу, как только они будут поступать (нажатие CTRL+C прерывает ожидание). `-s [--Since]` <*дата, время*> — показывать события, произошедшие не ранее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-u [--Until]` <*дата, время*> — показывать события, произошедшие не позднее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-t [--Types]` <*список типов*> — показывать события только перечисленных типов (типы событий перечисляются через запятую). Доступны следующие типы событий: • `Mail` — обнаружена угроза в сообщении электронной почты; • `UnexpectedAppTermination` — аварийное завершение работы некоторого компонента. Для вывода событий всех типов используйте `All`. `--ShowSeen` — показать также и уже прочитанные события. `--Show` <*список событий*> — вывести на экран перечисленные события (идентификаторы событий перечисляются через запятую). `--Delete` <*список событий*> — удалить перечисленные события (идентификаторы событий перечисляются через запятую). `--MarkAsSeen` <*список событий*> — отметить перечисленные события как «прочитанные» (идентификаторы событий перечисляются через запятую). Если требуется отметить как «прочитанные» или удалить все события, вместо <*список событий*> укажите `All`. Например, команда: `$ drweb-ctl events --MarkAsSeen All` отметит как «прочитанные» все имеющиеся события.
`report` <*тип*>	Назначение: Сформировать отчет о событиях Dr.Web для Linux в виде HTML-страницы (тело страницы выводится в указанный файл). Аргументы:

Команда	Описание
	<тип> — тип событий, для которых формируется отчет (указывается один тип). Возможные значения см. в описании опции `--Types` команды `events` выше. Обязательный аргумент. Опции: `-o [--Output]` *<путь к файлу>* — сохранить отчет в указанный файл. Обязательная опция. `-s [--Since]` *<дата, время>* — включить в отчет события, произошедшие не ранее указанного момента времени (*<дата, время>* указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-u [--Until]` *<дата, время>* — включить в отчет события, произошедшие не позднее указанного момента времени (*<дата, время>* указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `--TemplateDir` *<путь к каталогу>* — путь к каталогу, в котором находятся файлы шаблонов HTML-страницы отчета. Опции `-s`, `-u` и `--TemplateDir` являются необязательными. Например, команда: `$ drweb-ctl report Mail -o report.html` сформирует отчет по всем имеющимся событиям обнаружения угроз в сообщениях электронной почты на основе шаблона по умолчанию и сохранит результат в файл `report.html` в текущем каталоге.
`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).

Команда	Описание
	`--Proxy http://`*<имя пользователя>*`:`*<пароль>*`@`*<адрес сервера>*`:`*<номер порта>* — получить лицензионный ключ через прокси-сервер (используется только совместно с одной из предыдущих опций — `--GetDemo` или `--GetRegistered`). *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. Для регистрации серийного номера и для получения демонстрационного периода требуется наличие подключения к интернету.
`log`	Назначение: Вывести на экран консоли (в поток *stdout*) последние записи журнала Dr.Web для Linux (аналогично команде `tail`). Аргументы: Нет. Опции: `-s [--Size]` *<число>* — число последних записей журнала, которые нужно вывести на экран. `-c [--Components]` *<список компонентов>* — список идентификаторов компонентов, записи которых будут выведены. Указываются через запятую. Если параметр не указан, выводятся все доступные последние записи, отправленные в журнал любым из компонентов. *Актуальные идентификаторы установленных компонентов (т. е. внутренние имена компонентов, выводимые в журнал) вы можете узнать, используя команду `appinfo` (см. выше).* `-f [--Follow]` — выполнять ожидание поступления новых записей в журнал и выводить их на экран консоли сразу же, как только они будут поступать (нажатие CTRL+C прерывает ожидание).

Примеры использования

В этом разделе приведены примеры использования утилиты Dr.Web Ctl (`drweb-ctl`):

- Проверка объектов:
  - Простые команды проверки.
  - Проверка файлов, отобранных по критериям.
  - Проверка дополнительных объектов.
- Управление конфигурацией.

- Управление угрозами.
- Пример работы в режиме автономной копии.

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 файлов 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 Dr.Web для Linux, 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 SpIDer Guard):

```
# drweb-ctl cfset LinuxSpider.Start No
```

Обратите внимание, что для этого 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 Dr.Web для Linux:

```
$ drweb-ctl update
```

5. Выполнить перезагрузку конфигурации для компонентов Dr.Web для Linux:

```
# drweb-ctl reload
```

Обратите внимание, что для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl reload
```

6. Подключить Dr.Web для Linux к серверу централизованной защиты, работающему на узле *192.168.0.1*, при условии, что сертификат сервера располагается в файле `/home/user/cscert.pem`:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. Подключить Dr.Web для Linux к серверу централизованной защиты, используя файл настроек подключения settings.cfg:

```
$ drweb-ctl esconnect --cfg <путь к файлу settings.cfg>
```

8. Отключить Dr.Web для Linux от сервера централизованной защиты:

```
# drweb-ctl esdisconnect
```

Обратите внимание, что для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl esdisconnect
```

9. Просмотреть последние записи, внесенные компонентами `drweb-update` и `drweb-configd` в журнал Dr.Web для Linux:

```
# drweb-ctl log -c Update,ConfigD
```

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 (также в режиме автономной копии) и удалит все содержащиеся в нем объекты.

Приложения

Приложение А. Виды компьютерных угроз

Под термином *«угроза»* в этой классификации понимается 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 Doctor Web 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 скриптов и в большинстве случаев инфицируют другие файлы скрипты (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение скриптов, пользуясь уязвимыми скриптами 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 скриптов и т. д.) и по инфицируемым ими операционным системам.

Компьютерные черви

В последнее время вредоносные программы типа «компьютерный червь» стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через интернет) и рассылает свои функциональные копии на другие компьютеры. Для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

В компании Doctor Web 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 Doctor Web 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 действий является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т. д.).
- *Кликеры* переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак).
- *Прокси-трояны* предоставляют злоумышленнику анонимный выход в интернет через компьютер жертвы.

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (файерволах, брандмауэрах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут пользоваться администраторы для проверки надежности своих сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например в веб-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

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

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-серверы и т. д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым 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 Doctor Web.

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.
- Действия с угрозами.

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 Doctor Web 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.

Облачные технологии обнаружения угроз

Облачные методы обнаружения позволяют проверить любой объект (файл, приложение, расширение для браузера и т. п.) по *хеш-сумме*. Она представляет собой уникальную последовательность цифр и букв заданной длины. При анализе по хеш-сумме объекты проверяются по существующей базе и затем классифицируются на категории: чистые, подозрительные, вредоносные и т.д.

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

Таким образом, облачный сервис Dr.Web Cloud собирает информацию от многочисленных пользователей и оперативно обновляет данные о ранее неизвестных угрозах, тем самым повышая эффективность защиты устройств.

Действия с угрозами

В антивирусных 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/.

Для упрощения работы службы технической поддержки по анализу возникшей у вас проблемы рекомендуется предварительно сформировать пакет информации об установленном у вас продукте, его настройках и системном окружении. Для этого предназначена специализированная утилита, входящая в состав Dr.Web для Linux.

Для сбора информации для службы технической поддержки введите следующую команду:

```
# /opt/drweb.com/bin/support-report.sh
```

Для сбора информации для службы технической поддержки рекомендуется запустить утилиту с правами суперпользователя (пользователя *root*). Для получения прав суперпользователя воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

В процессе работы утилита собирает и упаковывает в архив следующую информацию:

- Информация об ОС (название, архитектура, вывод команды `uname -a`);
- Список установленных в системе пакетов, в том числе — пакетов Doctor Web;
- Содержимое журналов:
  - журналы Dr.Web для Linux (если настроены для отдельных компонентов);

  - журнал, ведущийся демоном журналирования `syslog` (`/var/log/syslog`, `/var/log/messages`);
  - журнал системного пакетного менеджера (`apt`, `yum` и т. п.);
  - журнал `dmesg`;
- Результаты запуска следующих команд: `df`, `ip a` (`ifconfig -a`), `ldconfig -p`, `iptables-save`, `nft export xml`.
- Информация о настройках и конфигурации Dr.Web для Linux:
  - перечень загруженных вирусных баз (`drweb-ctl baseinfo -l`);
  - перечень файлов из каталогов Dr.Web для Linux и их MD5-хеши;
  - версия и MD5-хеш файла антивирусного ядра Dr.Web Virus-Finding Engine;
  - параметры конфигурации Dr.Web для Linux (в том числе: содержимое файла `drweb.ini`, правила и файлы значений, используемые в правилах, Lua-процедуры и т. д.);
  - Информация о пользователе и разрешениях, извлеченная из ключевого файла, если Dr.Web для Linux работает не в режиме централизованной защиты.

Сформированный архив с информацией о продукте и системном окружении будет сохранен в домашний каталог пользователя, запустившего утилиту, и будет называться следующим образом:

```
drweb.report.<timestamp>.tgz
```

где <*timestamp*> — полная метка времени создания отчета, включая миллисекунды, например: `20190618151718.23625`.

Приложение Г. Описание известных ошибок

В данном разделе представлены:

- Рекомендации по идентификации ошибок
- Коды ошибок
- Ошибки без кода

Если описание возникшей у вас ошибки здесь отсутствует, рекомендуем обратиться в техническую поддержку, сообщив код ошибки и описав обстоятельства ее появления.

Рекомендации по идентификации ошибок

- Для уточнения возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для Linux (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

- 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
```

Коды ошибок

Сообщение об ошибке	*Ошибка связи с монитором*
Код ошибки	x1
Описание	Ошибка связи одного из нескольких компонентов 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 Dr.Web для Linux в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>/drweb.ini (при этом рекомендуется сохранить резервную копию 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 этого перезапустите демон управления конфигурацией.
4. Если демон управления конфигурацией запустить не удается, попробуйте переустановить пакет drweb-configd.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Операция уже выполняется*

Код ошибки	x2
Описание	Запрошенная операция уже выполняется.
Устранение ошибки: 1. Дождитесь завершения операции и при необходимости повторите требуемое действие позже.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Операция ожидает выполнения*
Код ошибки	x3
Описание	Запрошенная операция ожидает выполнения (возможно, в текущий момент устанавливается сетевое соединение или происходит загрузка и инициализация какого-либо компонента, требующая продолжительного времени).
Устранение ошибки: 1. Дождитесь начала операции и при необходимости повторите требуемое действие позже.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Прервано пользователем*
Код ошибки	x4
Описание	Действие было прервано пользователем.
Устранение ошибки: 1. Повторите требуемое действие позже.	
Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.	

Сообщение об ошибке	*Операция отменена*
Код ошибки	x5
Описание	Действие было отменено.
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 одним из компонентов Dr.Web для Linux разорвано (возможно, компонент завершил свою работу из-за простоя или по команде пользователя).

Устранение ошибки:

1. Если операция не было завершена, повторите ее еще раз. 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 Dr.Web для Linux, 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 Dr.Web для Linux, 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 позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Компонент не установлен*
Код ошибки	`x10`
Описание	Компонент, необходимый для выполнения требуемой функции, не установлен..

Устранение ошибки:

1. Установите отдельно или переустановите пакет, содержащий требуемый компонент:
   - `drweb-filecheck`, если не установлен Сканер.
   - `drweb-spider`, если не установлен SplDer Guard.
   - `drweb-gated`, если не установлен SplDer Gate.
   - `drweb-update`, если не установлен Компонент обновления.
2. Если ошибка повторится, или если вы не можете определить, какой компонент отсутствует, удалите Dr.Web для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 Dr.Web для Linux, 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.

Устранение ошибки:

1. Перезапустите Dr.Web для Linux, 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	Подсистема Dr.Web для Linux, необходимая для выполнения операции, находится в неизвестном состоянии.

Устранение ошибки:

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web для Linux, 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	Указан относительный путь к файлу или каталогу вместо абсолютного.

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.

Устранение ошибки:

1. Попробуйте увеличить объем памяти, доступной процессам Dr.Web для Linux (например, изменив лимиты при помощи команды `ulimit`), перезапустить его 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 примонтируйте его 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	Попытка обращения к несуществующему файлу или каталогу.

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 запрещен*
Код ошибки	`x24`
Описание	Недостаточно прав для доступа к указанному объекту 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	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 поврежден*
Код ошибки	x26
Описание	Запрашиваемые данные повреждены.

Устранение ошибки:

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web для Linux, 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	Файл с указанным 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	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	Ошибка сети (возможно, внезапно перестал отвечать удаленный узел или не удается установить 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 изменен*
Код ошибки	x32
Описание	Проверяемый файл 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	Запрашиваемый объект файловой системы не является регулярным файлом (это может быть каталог, сокет или другой объект).
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	Объект с указанным 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 отключен*
Код ошибки	x35
Описание	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 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	Восстановление файла предполагает перемещение между двумя разными точками 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	Вирусные базы повреждены.

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 **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	*Неподдерживаемая версия вирусных баз*
Код ошибки	x41
Описание	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 **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	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 **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	Действие «Лечить» было применено к неизлечимому объекту

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	*Неподдерживаемая комбинация вирусных баз*
Код ошибки	`x44`
Описание	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 **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	Текущий пользователь не имеет прав на выполнение требуемой операции.
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 Dr.Web для Linux 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	Команда не может быть выполнена, так как 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	Для выполнения требуемого действия необходимы полномочия 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 можно выполнить только при работе Dr.Web для Linux в одиночном (standalone) режиме.

Устранение ошибки:

1. Переведите Dr.Web для Linux в одиночный режим и повторите операцию снова.
2. Для этого:
   - 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	*Неподдерживаемая ОС*
Код ошибки	`x64`

Описание	Операционная система, установленная на узле, не поддерживается Dr.Web для Linux.

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	Запрашиваемые функции компонента недоступны в текущей версии.

Устранение ошибки:

1. Выполните сброс настроек Dr.Web для Linux 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 Dr.Web для Linux, 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 неподдерживаемые в текущей версии Dr.Web для Linux.

Устранение ошибки:

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` в любом текстовом редакторе, удалите строку, содержащую недопустимый параметр, сохраните файл и Перезапустите Dr.Web для Linux, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки Dr.Web для Linux в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию 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 Dr.Web для Linux.

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 Dr.Web для Linux.

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 Dr.Web для Linux, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки Dr.Web для Linux 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 Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимое значение параметра*
Код ошибки	`x68`
Описание	Для одного или нескольких параметров в файле конфигурации указаны недопустимые значения.

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 Dr.Web для Linux, выполнив команду:

```
# service drweb-configd restart
```

3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web для Linux 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 Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимое состояние*
Код ошибки	`x69`
Описание	Недопустимое состояние компонента или Dr.Web для Linux в целом для выполнения запрошенной операции.

Устранение ошибки:

1. Повторите требуемое действие позже.
2. При повторении ошибки перезапустите Dr.Web для Linux, 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	Для параметра параметра, который может иметь только одно значение, в конфигурационном файле задано значение в виде списка.

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 Dr.Web для Linux, выполнив команду:

```
# service drweb-configd restart
```

3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web для Linux 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 Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Запись не найдена*
Код ошибки	`x80`
Описание	Информация о найденной угрозе отсутствует (возможно, угроза уже была обработана другим компонентом).

Устранение ошибки:

1. Обновите список угроз позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Запись обрабатывается в данный момент*
Код ошибки	`x81`
Описание	Угроза уже обрабатывается другим компонентом.

Устранение ошибки:

1. Обновите список угроз позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Файл уже находится в карантине*
Код ошибки	`x82`
Описание	Файл уже находится в карантине. Возможно, угроза уже была обработана другим компонентом.

Устранение ошибки:

1. Обновите список угроз позже.

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 сохранить резервную копию подлежащих обновлению 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 **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 Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый DRL-файл*
Код ошибки	`x90`
Описание	Нарушена структура одного из файлов со списками серверов обновлений.

Устранение ошибки:

1. Проверьте правильность пути к файлу списка серверов и при необходимости исправьте его (параметры с именем вида `*DrlDir` в секции `[Update]` файла конфигурации. Для этого воспользуйтесь командами утилиты управления из командной строки.
   - Для просмотра текущего значения параметра введите команду (<**DrlDir*> 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[.<*DrlDir>]
     ```

   - Для установки нового значения параметра введите команду (<**DrlDir*> нужно заменить на имя конкретного параметра):

     ```
     # drweb-ctl cfset Update.<*DrlDir> <новый путь>
     ```

   - Для сброса значения параметра в значение по умолчанию введите команду (<**DrlDir*> нужно заменить на имя конкретного параметра):

     ```
     # drweb-ctl cfset Update.<*DrlDir> -r
     ```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите **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 для Linux целиком, после чего установите его повторно.

Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый LST-файл*
Код ошибки	`x91`
Описание	Нарушена структура файла с перечнем обновляемых вирусных баз.

Устранение ошибки:

1. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите **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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимый сжатый файл*
Код ошибки	`x92`
Описание	Нарушена структура загруженного файла с обновлениями.

Устранение ошибки:

1. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите **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 **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 `*DrlDir` в секции `[Update]` файла конфигурации. Обратите внимание, что если параметры вида `*CustomDrlDir` указывают на существующий корректный файл списка серверов, то указанные там серверы будут использоваться вместо серверов стандартной зоны обновления (значение, указанное в соответствующем параметре `*DrlDir`, игнорируется).

   Для просмотра и задания параметров подключения вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду (<*DrlDir> 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[.<*DrlDir>]
```

   Для установки нового значения параметра введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> <новый путь>
```

   Для сброса значения параметра в значение по умолчанию введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

4. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите **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 лицензии истек.

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	Истекло время ожидания сетевого соединения (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.
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	Нарушена контрольная сумма загруженного файла с обновлениями.

Устранение ошибки:

1. Повторите попытку обновления позже любым из указанных ниже способов:
   - Нажмите **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	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	Текущая лицензия заблокирована (возможно, нарушены условия лицензионного соглашения на использование Dr.Web для Linux).

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 лицензия предназначена для другого программного продукта или не содержит необходимых разрешений для работы компонентов Dr.Web для Linux.

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	Компонент Dr.Web для Linux 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 поддерживаемых дистрибутивов UNIX (см. раздел Системные требования и совместимость).

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 Dr.Web для Linux, 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 Dr.Web для Linux 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 Dr.Web для Linux, 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	Невозможно запустить компонент. Исполняемый файл поврежден или путь к нему указан неверно.

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 Dr.Web для Linux (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 для Linux целиком, после чего установите его повторно.

Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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	Файл антивирусного ядра Dr.Web Virus-Finding Engine отсутствует или недоступен.

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 **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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Вирусные базы отсутствуют*

Код ошибки	`x106`
Описание	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 **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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 Dr.Web для Linux 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 Dr.Web для Linux, 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 по причине сбоя.

Устранение ошибки:

1. Попробуйте повторить 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 Dr.Web для Linux 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 Dr.Web для Linux, выполнив команду:

   ```
   # service drweb-configd restart
   ```
4. Если ошибка повторится после сброса настроек Dr.Web для Linux, попробуйте переустановить пакет компонента.
5. Если предыдущие действия не помогли, удалите Dr.Web для Linux целиком, после чего установите его повторно.

Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 Dr.Web для Linux 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 SpIDer 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 для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Недопустимая библиотека*
Код ошибки	`x110`
Описание	Отсутствует, недоступен или испорчен файл антиспам-библиотеки (требуется при проверке электронной почты).

Устранение ошибки:

1. Проверьте правильность пути к файлу библиотеки и при необходимости исправьте его (параметр `AntispamCorePath` 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.AntispamCorePath
   ```

   - Для установки нового значения параметра введите команду

   ```
   # drweb-ctl cfset Root.AntispamCorePath <новый путь>
   ```

   - Для сброса значения параметра в значение по умолчанию введите команду

   ```
   # drweb-ctl cfset Root.AntispamCorePath -r
   ```

2. Обновите вирусные базы любым из указанных ниже способов:
   - Нажмите **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 для Linux целиком, после чего установите его повторно.

Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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	Отсутствуют базы категорий веб-ресурсов.

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 **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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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	SplDer 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 SplDer Guard.

   

   Обратите внимание, что работа компонента SplDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список поддерживаемых дистрибутивов UNIX (см. раздел Системные требования и совместимость).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*SplDer Gate недоступен*
Код ошибки	`x117`
Описание	Отсутствует компонент SplDer 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 SplDer 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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Scanning Engine недоступен*
Код ошибки	`x119`

Описание	Компонент Dr.Web Scanning Engine отсутствует или не может быть запущен.

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 Dr.Web для Linux и получите лицензию. Если лицензия вами получена, то проверьте наличие ключевого файла и установите его при необходимости.

   - 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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Сканер недоступен*
Код ошибки	`x120`
Описание	Компонент Dr.Web File Checker отсутствует или не может быть запущен.

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 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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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	Отсутствует компонент Dr.Web Firewall для Linux, необходимый для проверки сетевых соединений.

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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web для Linux.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке	*Network Checker недоступен*
Код ошибки	`x123`
Описание	Отсутствует компонент Dr.Web Network Checker, необходимый для проверки файлов по сети.

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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 одного или нескольких компонентов

Устранение ошибки:

1. Попробуйте перезапустить Dr.Web для Linux, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Ошибки без кода

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 и режим *LKM* становится обязательным, то откажитесь от использования гипервизора Xen.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы: Главное окно Dr.Web 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 для Linux не может запуститься, поскольку основной сервисный компонент `drweb-configd` недоступен.

Устранение ошибки

1. Перезапустите Dr.Web 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`.

   Обратите внимание, что это также может означать, что в системе для аутентификации пользователей не используется PAM. Если это так, что установите и настройте его.

3. Если предыдущие действия не помогли, удалите Dr.Web для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 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*).

Обратите внимание, что это также может означать, что в системе для аутентификации пользователей не используется PAM. Если это так, что установите и настройте его.

3. Если предыдущие действия не помогли, удалите Dr.Web для Linux целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для Linux и его компонентов см. в разделах Установка Dr.Web для Linux и Удаление Dr.Web 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 для Linux.

Описание: Графическая оболочка выполнила автоматическую ассоциацию файлов некоторого типа и/или каталогов с действием **Открыть в Dr.Web для Linux**.

Устранение ошибки

1. Отмените ассоциацию между файлами данного типа и приложением Dr.Web 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

В этом разделе:

Общие сведения

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.

Для архитектур ARM64 и E2K возможность работы с LKM не поддерживается.

Архив с исходными кодами загружаемого модуля ядра располагается в каталоге основных файлов Dr.Web 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 скрипт 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 Dr.Web для Linux. 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 требуются права 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*, устраните их (см. ниже) и выполните 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 SpIDer 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 SpIDer 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 этом случае 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>*.

Приложение E. Список сокращений

В данном руководстве следующие сокращения использованы без расшифровки:

Обозначение	Расшифровка
FQDN	Fully Qualified Domain Name
GNU	Проект GNU (GNU is Not Unix)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure (через SSL/TLS)
ID	Идентификатор
IMAP	Internet Message Access Protocol (протокол электронной почты)
IP	Internet Protocol
MBR	Master Boot Record
NSS	Novell Storage Services
PID	Process ID (системный идентификатор процесса)
PAM	Pluggable Authentication Modules
POP	Post Office Protocol (протокол электронной почты)
RPM	Red Hat Package Manager (формат пакетов)
SMTP	Simple Mail Transfer Protocol (протокол электронной почты)
SP	Service Pack
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User ID (системный идентификатор пользователя)
URL	Uniform Resource Locator
VBR	Volume Boot Record

Обозначение	Расшифровка
ОС	Операционная система

Предметный указатель

Предметный указатель

П

Р

С

Т

У

Предметный указатель

Ф

Ц

Ч