Dr.WEB

Desktop Security Suite (Linux)

Руководство пользователя



© «Доктор Веб», 2026. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

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

Dr.Web Desktop Security Suite (Linux)
Версия 11.1
Руководство пользователя
07.10.2026

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте.

ООО «Доктор Веб»

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

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение 9

2. Условные обозначения и сокращения 10

3. О продукте 11

3.1. Основные функции Dr.Web Desktop Security Suite 12

3.2. Структура Dr.Web Desktop Security Suite 15

3.2.1. Базовые антивирусные компоненты 15

3.2.2. Компоненты поиска угроз 18

3.2.3. Сервисные компоненты 20

3.2.4. Интерфейсные компоненты 22

3.3. Помещение в карантин 22

3.4. Полномочия для работы с файлами 24

3.5. Режимы работы 25

4. Системные требования и совместимость 30

5. Лицензирование 35

6. Установка и удаление 36

6.1. Установка Dr.Web Desktop Security Suite 37

6.1.1. Установка универсального пакета 38

6.1.1.1. Установка в графическом режиме 40

6.1.1.2. Установка в режиме командной строки 42

6.1.2. Установка из репозитория 43

6.2. Обновление Dr.Web Desktop Security Suite 47

6.2.1. Получение текущих обновлений 47

6.2.2. Переход на новую версию 48

6.3. Удаление Dr.Web Desktop Security Suite 53

6.3.1. Удаление универсального пакета 53

6.3.1.1. Удаление в графическом режиме 54

6.3.1.2. Удаление в режиме командной строки 55

6.3.2. Удаление Dr.Web Desktop Security Suite, установленного из репозитория 56

6.4. Дополнительно 58

6.4.1. Пакеты и файлы Dr.Web Desktop Security Suite 58

6.4.2. Выборочные установка и удаление компонентов 61

6.5. Настройка подсистем безопасности 66

6.5.1. Настройка политик безопасности SELinux 67

6.5.2. Настройка разрешений PARSEC 70
6.5.3. Настройка Альт 8 СП и других ОС, использующих pam_namespace 74
6.5.4. Настройка запуска в режиме ЗПС (Astra Linux SE, версии 1.6 и 1.7) 76
7. Начало работы 77
7.1. Регистрация и активация 77
7.1.1. Ключевой файл 80
7.1.2. Файл настроек подключения 81
7.2. Проверка работоспособности 82
7.3. Режимы мониторинга файлов 83
8. Работа с Dr.Web Desktop Security Suite 85
8.1. Работа в графическом режиме 86
8.1.1. Интеграция со средой рабочего стола 91
8.1.2. Запуск и завершение работы 96
8.1.3. Поиск и обезвреживание угроз 96
8.1.3.1. Проверка объектов по требованию 97
8.1.3.2. Проверка объектов по расписанию 100
8.1.3.3. Управление списком проверок 102
8.1.3.4. Мониторинг файловой системы 105
8.1.3.5. Мониторинг сетевых соединений 107
8.1.3.6. Просмотр обнаруженных угроз 110
8.1.3.7. Управление карантином 113
8.1.4. Обновление антивирусной защиты 116
8.1.5. Менеджер лицензий 117
8.1.6. Просмотр сообщений от сервера централизованной защиты 127
8.1.7. Управление правами приложения 130
8.1.8. Справочные материалы 132
8.1.9. Настройка работы 132
8.1.9.1. Основные настройки 134
8.1.9.2. Настройки проверки файлов 136
8.1.9.3. Настройки мониторинга файловой системы 138
8.1.9.4. Настройки мониторинга сетевых соединений 140
8.1.9.5. Настройка исключений 144
8.1.9.5.1. Исключение файлов и каталогов 145
8.1.9.5.2. Черный и белый списки сайтов 146
8.1.9.5.3. Исключение сетевых соединений приложений 147
8.1.9.6. Настройка проверки по расписанию 148

8.1.9.7. Настройка защиты от угроз, передаваемых через сеть 150
8.1.9.8. Настройка режима защиты 153
8.1.9.9. Настройка использования Dr.Web Cloud 156
8.1.10. Дополнительно 157
8.1.10.1. Аргументы командной строки 157
8.1.10.2. Запуск автономного экземпляра 158
8.2. Работа из командной строки 159
9. Компоненты Dr.Web Desktop Security Suite 160
9.1. Dr.Web ConfigD 160
9.1.1. Принципы работы 160
9.1.2. Аргументы командной строки 162
9.1.3. Параметры конфигурации 163
9.2. Dr.Web Ctl 166
9.2.1. Формат вызова из командной строки 168
9.2.2. Общие опции 168
9.2.3. Команды 169
9.2.3.1. Команды антивирусной проверки 169
9.2.3.2. Команды управления угрозами и карантином 185
9.2.3.3. Команды управления конфигурацией 191
9.2.3.4. Расширенные команды 193
9.2.3.4.1. Команды управления обновлением и работой в режиме централизованной защиты 194
9.2.3.4.2. Информационные команды 196
9.2.4. Примеры использования 202
9.2.5. Параметры конфигурации 206
9.3. SpIDer Guard 207
9.3.1. Принципы работы 207
9.3.2. Аргументы командной строки 211
9.3.3. Параметры конфигурации 212
9.4. Dr.Web MailD 220
9.4.1. Принципы работы 221
9.4.2. Аргументы командной строки 221
9.4.3. Параметры конфигурации 222
9.5. Dr.Web Anti-Spam 239
9.5.1. Принципы работы 239
9.5.2. Аргументы командной строки 241

9.5.3. Параметры конфигурации 241
9.6. Dr.Web Mail Quarantine 244
9.6.1. Принципы работы 244
9.6.2. Аргументы командной строки 244
9.6.3. Параметры конфигурации 245
9.7. SpIDer Gate 247
9.7.1. Принципы работы 248
9.7.2. Аргументы командной строки 249
9.7.3. Параметры конфигурации 250
9.8. Dr.Web Firewall для Linux 252
9.8.1. Принципы работы 252
9.8.2. Аргументы командной строки 260
9.8.3. Параметры конфигурации 260
9.9. Dr.Web File Checker 290
9.9.1. Принципы работы 290
9.9.2. Аргументы командной строки 291
9.9.3. Параметры конфигурации 292
9.10. Dr.Web Network Checker 294
9.10.1. Принципы работы 294
9.10.2. Аргументы командной строки 296
9.10.3. Параметры конфигурации 297
9.11. Dr.Web Scanning Engine 303
9.11.1. Принципы работы 303
9.11.2. Аргументы командной строки 305
9.11.3. Параметры конфигурации 308
9.12. Dr.Web Updater 312
9.12.1. Принципы работы 312
9.12.2. Аргументы командной строки 313
9.12.3. Параметры конфигурации 314
9.13. Dr.Web ES Agent 321
9.13.1. Принципы работы 321
9.13.2. Аргументы командной строки 322
9.13.3. Параметры конфигурации 323
9.14. Dr.Web MeshD 325
9.14.1. Принципы работы 325
9.14.2. Аргументы командной строки 327

9.14.3. Параметры конфигурации 328
9.15. Dr.Web URL Checker 331
9.15.1. Принципы работы 332
9.15.2. Аргументы командной строки 332
9.15.3. Параметры конфигурации 333
9.16. Dr.Web CloudD 335
9.17. Dr.Web StatD 340
9.17.1. Принципы работы 340
9.17.2. Аргументы командной строки 340
9.17.3. Параметры конфигурации 341
10. Приложения 343
10.1. Приложение А. Виды компьютерных угроз 343
10.2. Приложение Б. Устранение компьютерных угроз 349
10.3. Приложение В. Техническая поддержка 352
10.4. Приложение Г. Конфигурационный файл Dr.Web Desktop Security Suite 355
10.4.1. Структура файла 355
10.4.2. Типы параметров 356
10.5. Приложение Д. Генерация сертификатов SSL 360
10.6. Приложение Е. Сборка модуля ядра для SpIDer Guard 363
10.7. Приложение Ж. Описание известных ошибок 366
10.8. Приложение З. Список сокращений 417

1. Введение

Решение Dr.Web Desktop Security Suite позволит вам обеспечить надежную защиту вашего компьютера от распространения 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 Desktop Security Suite.

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

2. 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 к вводу `$` или `#`, определяющим, какие полномочия пользователя необходимы для выполнения указанной команды. Стандартным для Unix-систем образом подразумевается, что:

`$` — для выполнения команды достаточно обычных прав пользователя.

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

Перечень сокращений приведен в разделе Приложение З. Список сокращений.

3. О продукте

Назначение

Dr.Web Desktop Security Suite создан для защиты файлов и сетевого трафика аппаратных и виртуальных рабочих станций, работающих под управлением ОС семейства GNU/Linux от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения через них угроз для различных платформ. При работе в режиме централизованной защиты Dr.Web Desktop Security Suite контролируется сервером под управлением Dr.Web Enterprise Security Suite.

Защита данных

Основные компоненты (антивирусное ядро и вирусные базы) являются не только крайне эффективными и нетребовательными к системным ресурсам, но и кросс-платформенными, что позволяет специалистам компании «Доктор Веб» создавать надежные антивирусные решения, обеспечивающие защиту компьютеров, работающих под управлением распространенных операционных систем, от угроз, предназначенных для различных платформ. В настоящее время, наряду с Dr.Web Desktop Security Suite, в компании «Доктор Веб» разработаны также и другие антивирусные решения для Unix-подобных операционных систем (GNU/Linux и FreeBSD), macOS и Windows. Кроме того, разработаны антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением ОС Android и «Аврора».

Компоненты Dr.Web Desktop Security Suite постоянно обновляются, а вирусные базы, базы правил спам-фильтрации сообщений электронной почты и базы категорий веб-ресурсов регулярно дополняются новыми записями, что обеспечивает актуальный уровень защищенности файлов и сетевого трафика аппаратных и виртуальных рабочих станций. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре, и обращение к облачному сервису Dr.Web Cloud, хранящему информацию о новейших угрозах, сигнатуры которых еще отсутствуют в базах.

Дополнительно:

- Основные функции Dr.Web Desktop Security Suite
- Структура Dr.Web Desktop Security Suite
- Помещение в карантин
- Полномочия для работы с файлами
- Режимы работы

3.1. Основные функции Dr.Web Desktop Security Suite

Основные функции Dr.Web Desktop Security Suite:

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.

   Эвристический анализатор может ложно срабатывать на программное обеспечение, не являющееся вредоносным. По этой причине объекты, содержащие обнаруженные им угрозы, получают специальный статус «подозрительные». Рекомендуется помещать такие файлы в карантин, а также передавать на анализ в антивирусную лабораторию «Доктор Веб». Подробнее об методах обезвреживания см. Приложение Б. Устранение компьютерных угроз.

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

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

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

Утилита управления из командной строки, входящая в состав Dr.Web Desktop Security Suite, 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 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 Desktop Security Suite. В этом случае спам-проверка сообщений электронной почты не производится.

   Для определения нежелательных ссылок используются как поставляемая вместе с Dr.Web Desktop Security Suite автоматически обновляемая база категорий веб-ресурсов, так и черные и белые списки, ведущиеся пользователем вручную. Дополнительно Dr.Web Desktop Security Suite может обращаться к сервису Dr.Web Cloud, чтобы проверить, не отмечен ли 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 инцидентов, связанных с вредоносным ПО, ведение журнала обнаруженных угроз (доступен только через утилиту управления из командной строки), а также отправка статистики инцидентов, связанных с вредоносным ПО, облачному сервису Dr.Web Cloud.
8. **Обеспечение работы под управлением сервера централизованной защиты** для применения на защищаемом компьютере единых политик безопасности, принятых в антивирусной сети под управлением Dr.Web Enterprise Security Suite, 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 в интернет.

Поскольку для использования информации, хранящейся в облачном сервисе Dr.Web Cloud, необходимо передавать данные об активности пользователя (например, передавать на проверку адреса посещаемых им 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 Dr.Web Desktop Security Suite.

3.2. Структура Dr.Web Desktop Security Suite

Dr.Web Desktop Security Suite представляет собой программный комплекс, состоящий из набора компонентов, каждый из которых выполняет свой набор функций. В соответствии с задачами, решаемыми компонентами, они разделены на категории:

- Базовые антивирусные компоненты, образующие ядро продукта Dr.Web Desktop Security Suite. При отсутствии компонентов этой категории продукт не может выполнять сканирование файлов (и иных данных) на предмет наличия вирусов и иных угроз.
- Компоненты поиска угроз. Данные компоненты используются для решения базовых задач Dr.Web Desktop Security Suite — поиска вредоносных и потенциально опасных объектов. В своей работе компоненты этой категории используют базовые антивирусные компоненты.
- Сервисные компоненты, решающие вспомогательные задачи для поддержки антивирусной защиты (обновление вирусных баз, подключение к серверам централизованной защиты, общая координация работы компонентов Dr.Web Desktop Security Suite и т. д.).
- Интерфейсные компоненты, предоставляющие (пользователю или сторонним приложениям) интерфейс для управления работой Dr.Web Desktop Security Suite.

Перечень компонентов, входящих в состав Dr.Web Desktop Security Suite, перечислен в таблицах ниже.

3.2.1. Базовые антивирусные компоненты

Компонент	Описание
Dr.Web Virus-Finding Engine	Антивирусное ядро. Реализует алгоритмы поиска и распознавания вирусов и прочих вредоносных программ (используя сигнатурный и эвристический анализ). Работает под управлением компонента Dr.Web Scanning Engine Файл библиотеки: `drweb32.dll`. Внутреннее наименование, выводимое в журнал: `CoreEngine`
Dr.Web Scanning Engine	Сканирующее ядро. Компонент, отвечающий за загрузку антивирусного ядра Dr.Web Virus-Finding Engine и вирусных баз. • Передает антивирусному ядру на проверку содержимое файлов и загрузочных записей дисковых устройств. • Организует очередь файлов, ожидающих проверки. • Выполняет лечение тех угроз, для которых данное действие применимо.

Компонент	Описание
	Может работать как под управлением демона Dr.Web ConfigD, так и в автономном режиме. Используется компонентами Dr.Web File Checker и Dr.Web Network Checker. Также может использоваться компонентом Dr.Web MeshD (в некоторых режимах работы) и внешними (по отношению к Dr.Web Desktop Security Suite) приложениями, использующими непосредственно API Dr.Web Scanning Engine Исполняемый файл компонента: `drweb-se`. Внутреннее наименование, выводимое в журнал: `ScanEngine`
Вирусные базы	Автоматически обновляемая база данных сигнатур вирусов и прочих угроз, а также алгоритмов распознавания и нейтрализации вредоносного программного обеспечения. Используется антивирусным ядром Dr.Web Virus-Finding Engine и поставляется совместно с ним
Базы категорий веб-ресурсов	Автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, и используемая для идентификации нежелательных сайтов. Используется компонентами, проверяющими сетевую активность пользователей и приложений, такими как SpIDer Gate, Dr.Web MailD
Dr.Web File Checker	Компонент проверки объектов файловой системы и менеджер карантина. • Принимает от компонента поиска угроз задания на проверку файлов, находящихся в локальной (по отношению к Dr.Web Scanning Engine) файловой системе. • Обходит каталоги файловой системы согласно заданию, передает файлы на проверку сканирующему ядру Dr.Web Scanning Engine и оповещает компоненты-клиенты о ходе проверки. • Выполняет удаление инфицированных файлов, перемещение их в карантин и восстановление из карантина, управляет каталогами карантина. • Организует и содержит в актуальном состоянии кеш, хранящий информацию о ранее проверенных файлах для уменьшения частоты повторных проверок файлов. Используется компонентами, проверяющими объекты файловой системы, такими как SpIDer Guard Исполняемый файл компонента: `drweb-filecheck`. Внутреннее наименование, выводимое в журнал: `FileCheck`
Dr.Web Network Checker	Агент сетевой проверки данных. • Используется для передачи на проверку в сканирующее ядро данных, отправленных компонентами программного комплекса через сеть (это такие компоненты, как SpIDer Gate, Dr.Web MailD).

Компонент	Описание
	• Позволяет Dr.Web Desktop Security Suite организовывать распределенную проверку данных: принимать на проверку данные с удаленных узлов сети и передавать локальные данные на проверку на удаленные узлы сети. Для приема и передачи данных на удаленных узлах также должен функционировать антивирусный продукт Dr.Web для операционных систем семейства Unix. В режиме распределенной проверки позволяет автоматически распределять интенсивность антивирусного сканирования по доступным узлам, снижая нагрузку на узлы с большим объемом проверки (например, выполняющих роль почтовых серверов и интернет-шлюзов). При наличии в сети узлов-партнеров, способных принимать данные на проверку, компоненты, использующие Dr.Web Network Checker для проверки, могут не использовать мощности локального сканирующего ядра Dr.Web Scanning Engine. Таким образом, локальное сканирующее ядро Dr.Web Scanning Engine, Dr.Web Virus-Finding Engine и вирусные базы могут отсутствовать. Для обеспечения безопасности при передаче файлов по сети использует SSL Исполняемый файл компонента: `drweb-netcheck`. Внутреннее наименование, выводимое в журнал: `NetCheck`
Dr.Web URL Checker	Компонент для анализа URL на предмет принадлежности к нежелательным или потенциально опасным категориям Исполняемый файл компонента: `drweb-urlcheck`. Внутреннее наименование, выводимое в журнал: `UrlCheck`
Dr.Web MeshD	Компонент, осуществляющий подключение продукта Dr.Web Desktop Security Suite к локальному облаку, позволяющему продуктам Dr.Web для Unix обмениваться обновлениями, результатами проверки файлов, передавать друг другу на проверку файлы, а также предоставлять услуги сканирующего ядра напрямую. При наличии этого компонента в составе продукта и при наличии в составе локального облака, к которому он подключен, узлов, предоставляющих услуги сканирующего ядра, локальное сканирующее ядро Dr.Web Scanning Engine, Dr.Web Virus-Finding Engine и вирусные базы могут отсутствовать Исполняемый файл компонента: `drweb-meshd`. Внутреннее наименование, выводимое в журнал: `MeshD`

3.2.2. Компоненты поиска угроз

Компонент	Описание
Сканер	Компонент, выполняющий по требованию пользователя или по заданному расписанию проверку объектов файловой системы (файлы, каталоги и загрузочные записи) на наличие в них угроз. Пользователь имеет возможность запускать проверку как из графического режима, так и из командной строки.
SpIDer Guard	Монитор файловой системы GNU/Linux. Работает в фоновом режиме и отслеживает операции с файлами (такие как создание, открытие, закрытие и запуск файла) в файловых системах GNU/Linux. Посылает компоненту Dr.Web File Checker запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ. В зависимости от возможностей ОС использует системный механизм *fanotify* или специализированный модуль ядра, разработанный компанией «Доктор Веб» (LKM-модуль, поставляется совместно с SpIDer Guard в отдельном пакете). При работе через системный механизм *fanotify* монитор может работать в усиленном или «параноидальном» режиме, блокируя доступ к файлам, которые еще не проверены, до момента окончания их проверки. По умолчанию используется обычный режим мониторинга. Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Исполняемый файл компонента: `drweb-spider`. Внутреннее наименование, выводимое в журнал: `LinuxSpider`
Загружаемый модуль ядра Linux для SpIDer Guard	Загружаемый модуль ядра Linux (LKM-модуль), используемый монитором SpIDer Guard для доступа к событиям файловой системы в тех ОС, в которых API fanotify недоступен или реализован с ограниченным набором функций. Компонент поставляется как в скомпилированном виде (для набора ОС, в которых fanotify не реализован или недоступен), так и в виде исходного кода, позволяющего осуществить сборку и установку модуля ядра ОС вручную (инструкция по сборке приведена в разделе Приложение Е. Сборка модуля ядра для SpIDer Guard). Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Для архитектур ARM64, E2K и IBM POWER (ppc64el) работа с модулем ядра не поддерживается.

Компонент	Описание
	Исполняемый файл компонента: `drweb.ko`
SpIDer Gate	Компонент проверки сетевого трафика и URL. Предназначен для проверки данных, загружаемых на локальный узел из сети и передаваемых с него во внешнюю сеть, на наличие угроз, и предотвращения соединения с узлами сети, внесенными как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые пользователем. Для проверки получаемых данных использует компонент Dr.Web Network Checker. Посылает Сканеру на проверку файлы, загружаемые из интернета (с серверов, доступ к которым был разрешен), и блокирует их загрузку, если они содержат угрозы. При наличии соответствующего разрешения от пользователя посылает запрашиваемые им URL на проверку в сервис Dr.Web Cloud. Исполняемый файл компонента: `drweb-gated`. Внутреннее наименование, выводимое в журнал: `GateD`
Dr.Web Firewall для Linux	Менеджер сетевых соединений. Используется SpIDer Gate и обеспечивает прохождение через него соединений, устанавливаемых приложениями, работающими на узле, для проверки передаваемого через них трафика. Исполняемый файл компонента: `drweb-firewall`. Внутреннее наименование, выводимое в журнал: `LinuxFirewall`
Dr.Web MailD	Компонент проверки электронной почты. Разбирает сообщения электронной почты и подготавливает их к проверке на наличие угроз. Может работать в двух режимах. 1) Фильтр для серверов электронной почты (Sendmail, Postfix и т. п.), подключаемый через интерфейс *Milter*, *Spamd* или *Rspamd*. 2) Прозрачный прокси протоколов электронной почты (SMTP, POP3, IMAP). В этом режиме задействуется SpIDer Gate. Для проверки данных, извлекаемых из сообщений электронной почты, использует компонент Dr.Web Network Checker Исполняемый файл компонента: `drweb-maild`. Внутреннее наименование, выводимое в журнал: `MailD`
Dr.Web Anti-Spam	Компонент проверки сообщений электронной почты на наличие признаков спама. Используется компонентом Dr.Web MailD. Может отсутствовать, в зависимости от поставки. Если отсутствует, проверка сообщений

Компонент	Описание
	электронной почты на наличие признаков спама компонентом Dr.Web MailD не осуществляется.  Компонент не поддерживается для архитектур ARM64, E2K и IBM POWER (ppc64el). Исполняемый файл компонента: `drweb-ase`. Внутреннее наименование, выводимое в журнал: `Antispam`

3.2.3. Сервисные компоненты

Компонент	Описание
Dr.Web CloudD	Компонент взаимодействия с облаком Dr.Web Cloud. Отправляет URL, посещаемые пользователем, а также сведения о проверяемых файлах, в облачный сервис Dr.Web Cloud для их проверки на наличие угроз, информация о которых пока отсутствует в вирусных базах Исполняемый файл компонента: `drweb-cloudd`. Внутреннее наименование, выводимое в журнал: `CloudD`
Dr.Web ConfigD	Демон управления конфигурацией комплекса Dr.Web Desktop Security Suite. • Управляет активностью (запуск и остановка) других компонентов программного комплекса в зависимости от настроек. • Перезапускает компоненты, завершившие работу в результате сбоя, запускает одни компоненты комплекса по требованию других, информирует компоненты продукта об изменении состава запущенных компонентов. • Хранит и предоставляет всем компонентам информацию об имеющихся лицензионных ключах и настройках. Получает измененные настройки и ключи от уполномоченных компонентов Dr.Web Desktop Security Suite и оповещает все компоненты об изменении лицензионных ключей и настроек Исполняемый файл компонента: `drweb-configd`. Внутреннее наименование, выводимое в журнал: `ConfigD`
Dr.Web ES Agent	Агент централизованной защиты. Обеспечивает работу программного комплекса в централизованном и мобильном режимах.

Компонент	Описание
	• Организует связь с сервером централизованной защиты, получает от него лицензионный ключевой файл, обновления вирусных баз и антивирусного ядра. • Передает на сервер информацию о составе и состоянии компонентов Dr.Web Desktop Security Suite и накопленную статистику инцидентов, связанных с вредоносным ПО Исполняемый файл компонента: `drweb-esagent`. Внутреннее наименование, выводимое в журнал: `ESAgent`
Dr.Web Mail Quarantine	Компонент проверки электронной почты, отвечающий за организацию очередей проверяемых сообщений. Используется компонентом Dr.Web MailD. Может отсутствовать, в зависимости от поставки. Если отсутствует, режимы SMTP и BCC компонента Dr.Web MailD не поддерживаются. Исполняемый файл компонента: `drweb-mail-quarantine`. Внутреннее наименование, выводимое в журнал: `MailQuarantine`
Dr.Web StatD	Компонент для хранения статистики событий компонентов Dr.Web Desktop Security Suite. Получает и организует хранение событий, поступающих от компонентов программного комплекса, таких как неожиданное завершение работы, обнаружение угрозы и др. Исполняемый файл компонента: `drweb-statd`. Внутреннее наименование, выводимое в журнал: `StatD`
Dr.Web Updater	Компонент обновления. Отвечает за загрузку с серверов обновлений компании «Доктор Веб» обновлений для вирусных баз и баз категорий веб-ресурсов, антивирусного ядра и библиотеки проверки сообщений электронной почты на спам. Обновления могут загружаться как автоматически, по расписанию, так и непосредственно по команде пользователя (через утилиту Dr.Web Ctl) Исполняемый файл компонента: `drweb-update`. Внутреннее наименование, выводимое в журнал: `Update`

3.2.4. Интерфейсные компоненты

Компонент	Описание
Графический интерфейс управления	Компонент, предоставляющий оконный графический интерфейс управления Dr.Web Desktop Security Suite. Позволяет пользователю в графическом режиме запускать проверку объектов файловой системы, управлять работой мониторов SpIDer Guard и SpIDer Gate, просматривать содержимое карантина, выполнять запуск получения обновлений, а также настраивать работу Dr.Web Desktop Security Suite.
Агент уведомлений	Компонент, работающий в фоновом режиме. Отображает всплывающие уведомления о возникающих событиях и индикатор приложения Dr.Web Desktop Security Suite 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.
Dr.Web Ctl	Утилита, обеспечивающая интерфейс управления Dr.Web Desktop Security Suite из командной строки. Позволяет осуществлять запуск проверки файлов, просматривать содержимое карантина и управлять им, запускать обновление вирусных баз, подключать Dr.Web Desktop Security Suite к серверу централизованной защиты и отключаться от него, просматривать и изменять значения параметров конфигурации программного комплекса Исполняемый файл компонента: `drweb-ctl`. Внутреннее наименование, выводимое в журнал: `Ctl`

Более подробно компоненты Dr.Web Desktop Security Suite описаны в разделе Компоненты Dr.Web Desktop Security Suite.

3.3. Помещение в карантин

Карантин Dr.Web Desktop Security Suite представляет собой систему каталогов, предназначенных для надежной изоляции файлов, содержащих выявленные угрозы, которые в данный момент не могут быть обезврежены по каким-либо причинам. Например, обнаруженная угроза может быть неизлечимой, потому что еще неизвестна Dr.Web Desktop Security Suite (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, если он выбрал соответствующее действие в списке обнаруженных угроз или указал его как реакцию на угрозы определенного типа.

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

Каталоги карантина размещаются:

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

Каталоги карантина Dr.Web Desktop Security Suite всегда имеют имя `.com.drweb.quarantine` и создаются по мере необходимости в тот момент, когда к какой-либо угрозе применяется действие «**В карантин**» (`QUARANTINE`), другими словами, 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 файловой системе периодически и в различные точки.

Пользователь может управлять содержимым карантина как в графическом режиме работы, так и из командной строки, используя утилиту Dr.Web Ctl. 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 карантина, располагающийся в его домашнем каталоге, называется *Пользовательским* карантином, а все остальные каталоги карантина считаются *Системным* карантином.

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

Не все антивирусные компоненты Dr.Web Desktop Security Suite используют карантин для изоляции угроз. Например, его не использует компонент Dr.Web MailD.

3.4. Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз Dr.Web Desktop Security Suite (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.

Действие	Требуемые полномочия
Удаление файла из карантина	Пользователь должен иметь разрешение на запись в исходный файл, который был перемещен в карантин.

Для временного повышения прав Dr.Web Desktop Security Suite, запущенного в графическом режиме, используйте соответствующую кнопку на окне Dr.Web Desktop Security Suite (она доступна и отображается только в тех случаях, когда для выполнения какой-либо операции может потребоваться повышение прав).

Для запуска утилиты управления из командной строки Dr.Web Ctl с правами суперпользователя (обычно *root*) используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

3.5. Режимы работы

В этом разделе

- Принципы централизованной защиты
- Подключение к серверу централизованной защиты
- Отключение от сервера централизованной защиты

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

- В *автономном режиме* защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационный и лицензионный ключевой файлы находятся на локальных дисках, а Dr.Web Desktop Security Suite полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании «Доктор Веб».
- В *режиме централизованной защиты* защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web Desktop Security Suite 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 от выбранного сервера централизованной защиты, к которому подключен Dr.Web Desktop Security Suite. Лицензионный или демонстрационный ключевой файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы Dr.Web Desktop Security Suite, включая статистику инцидентов, связанных с вредоносным ПО. Обновление вирусных баз также выполняется с сервера

централизованной защиты. Настройка режима централизованной защиты описана в Руководстве администратора Dr.Web Enterprise Security Suite по управлению Dr.Web Desktop Security Suite.

- В *мобильном режиме* Dr.Web Desktop Security Suite получает обновления вирусных баз с серверов обновлений компании «Доктор Веб», но использует локально хранящиеся настройки и особый лицензионный ключевой файл, полученные от сервера централизованной защиты.

Если Dr.Web Desktop Security Suite работает под управлением сервера централизованной защиты (в том числе и в мобильном режиме), то следующие возможности блокируются:

- удаление лицензионного ключевого файла в Менеджере лицензий;
- запуск обновлений вручную и настройки параметров обновления;
- настройка параметров проверки объектов файловой системы Сканером.

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



В режиме централизованной защиты недоступна проверка по расписанию.

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

Принципы централизованной защиты

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

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

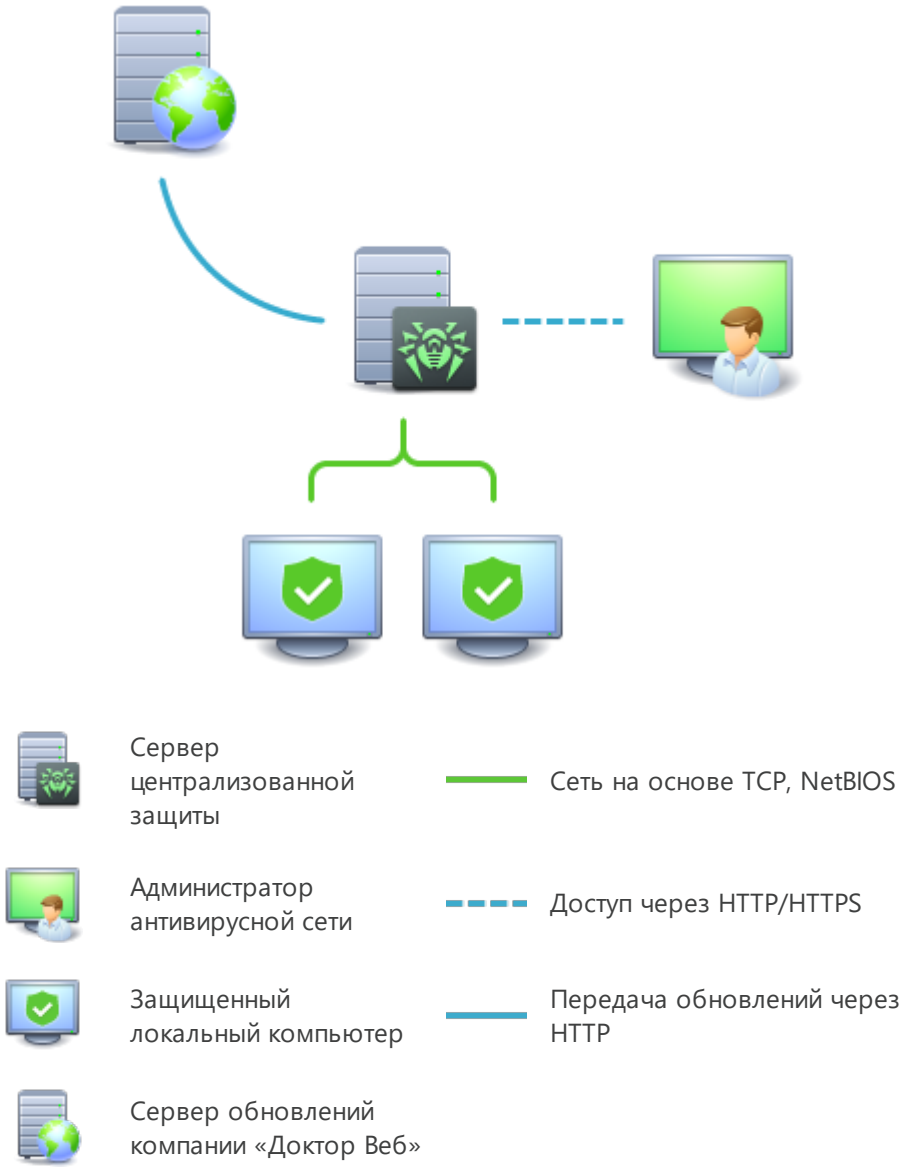


Рисунок 1. Логическая структура антивирусной сети

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

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

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется сервером централизованной защиты по указанию администраторов

антивирусной сети. Администраторы управляют конфигурацией сервера централизованной защиты и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также, при необходимости, задают настройки работы конкретных локальных антивирусных компонентов.



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

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

Подключение к серверу централизованной защиты

Dr.Web Desktop Security Suite может быть подключен к серверу централизованной защиты антивирусной сети следующими способами:

- на вкладке **Режим** страницы настроек окна Dr.Web Desktop Security Suite;
- при помощи команды `esconnect` утилиты управления из командной строки `drweb-ctl`.



Для верификации сервера централизованной защиты используется сертификат, соответствующий уникальному открытому ключу шифрования, используемому сервером. По умолчанию агент централизованной защиты Dr.Web ES Agent не позволит произвести подключение к серверу, если вы не укажете файл сертификата сервера, к которому производится подключение. Файл сертификата необходимо предварительно получить у администратора антивирусной сети, обслуживаемой сервером, к которому вы хотите подключить Dr.Web Desktop Security Suite.

Если Dr.Web Desktop Security Suite подключен к серверу централизованной защиты, то имеется возможность перевести его в мобильный режим и вернуть назад в режим централизованной защиты. Включение и выключение мобильного режима регулируется параметром конфигурации `MobileMode` компонента Dr.Web ES Agent.



Возможность перехода Dr.Web Desktop Security Suite в мобильный режим работы зависит от разрешений, заданных на используемом сервере централизованной защиты.

Отключение от сервера централизованной защиты

Dr.Web Desktop Security Suite может быть отключен от сервера централизованной защиты антивирусной сети следующими способами:

- на вкладке **Режим** страницы настроек окна Dr.Web Desktop Security Suite;
- при помощи команды `esdisconnect` утилиты управления из командной строки `drweb-ctl`.

4. Системные требования и совместимость

В этом разделе

- Системные требования
- Перечень поддерживаемых версий операционных систем
- Требуемые дополнительные компоненты и пакеты
- Совместимость с компонентами операционных систем
- Совместимость с подсистемами безопасности

Системные требования

Использование Dr.Web Desktop Security Suite возможно на компьютере, удовлетворяющем следующим требованиям:

Параметр	Требования
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 POWER9, Power10 (*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 Desktop Security Suite.
Операционная система	GNU/Linux 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 GNU/Linux 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 SplDer 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 Desktop Security Suite 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 Desktop Security Suite несовместим с другими антивирусными программами. Так как установка двух антивирусов на один компьютер может привести к ошибкам в системе и потере важных данных, перед установкой Dr.Web Desktop Security Suite удалите с компьютера другие антивирусные программы.

Перечень поддерживаемых версий операционных систем

Поддерживаются следующие дистрибутивы GNU/Linux:

Платформа	Поддерживаемые версии GNU/Linux
x86_64	• Astra Linux Common Edition (Орел) 2.12; • Astra Linux Special Edition 1.6 (с кумулятивным патчем 20200722SE16), 1.7, 1.8; • CentOS 7, 8; • Debian 9, 10, 11, 12, 13; • Fedora 37, 38; • Red Hat Enterprise Linux 7, 8, 9; • SUSE Linux Enterprise Server 12 SP3; • Ubuntu 18.04, 20.04, 22.04, 22.10, 23.10, 24.04;

Платформа	Поддерживаемые версии GNU/Linux
	• Альт 8 СП; • Альт Рабочая станция 9, 10, 11; • Альт Сервер 9, 10, 11; • Гослинукс IC6; • РЕД ОС 7.2 МУРОМ, РЕД ОС 7.3 МУРОМ, РЕД ОС 8
x86	• CentOS 7; • Debian 10; • Альт 8 СП; • Альт Рабочая станция 9, 10
ARM64	• Astra Linux Special Edition (Новороссийск) 4.7; • CentOS 7, 8; • Debian 11, 12; • Ubuntu 18.04; • Альт 8 СП; • Альт Рабочая станция 9, 10, 11; • Альт Сервер 9, 10, 11
E2K	• Astra Linux Special Edition (Ленинград) 8.1 (с кумулятивным патчем 20200429SE81); • Альт 8 СП; • Альт Рабочая станция 10; • Альт Сервер 10; • ОПО ВК Эльбрус-8.32 ТВГИ.00311-28; • Эльбрус-Д МЦСТ 1.4
ppc64el	• CentOS 8; • Ubuntu 20.04



В ОС Эльбрус-Д МЦСТ 1.4 и Гослинукс IC6 работа с мандатными уровнями доступа не поддерживается.

Для прочих дистрибутивов GNU/Linux, соответствующих описанным требованиям, полная совместимость с Dr.Web Desktop Security Suite не гарантируется. При возникновении проблем с совместимостью с вашим дистрибутивом обратитесь в техническую поддержку.

Требуемые дополнительные компоненты и пакеты

- Для работы Dr.Web Desktop Security Suite 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 на панели Ubuntu Dock 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 Desktop Security Suite также необходимо, чтобы в системе использовался механизм аутентификации PAM.

Для удобной работы с Dr.Web Desktop Security Suite 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 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 Desktop Security Suite поставляются LKM-модули для всех систем GNU/Linux, указанных выше. В случае необходимости вы имеете возможность собрать модуль ядра самостоятельно из поставляемого исходного кода для любой ОС, использующей ядро Linux версии 2.6.x и новее.

Для архитектур ARM64, E2K и IBM POWER (ppc64el) работа с загружаемым модулем ядра (LKM) не поддерживается.

Работа SpIDer Guard через LKM 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 или «параноидальном» режиме (с предварительной блокировкой доступа к еще не проверенным файлам) возможна только через системный механизм 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 приведен в разделе Приложение Ж. 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 приведен в разделе Приложение Ж. 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. Способ устранения указанной проблемы приведен в разделе Приложение Ж. 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 Desktop Security Suite 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 Desktop Security Suite не совместим с подсистемой безопасности SELinux. Кроме того, по умолчанию Dr.Web Desktop Security Suite 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 Desktop Security Suite на системах с SELinux, а также на системы, использующие мандатные модели доступа, может потребоваться дополнительная настройка подсистем безопасности для снятия ограничений в функционировании Dr.Web Desktop Security Suite. Подробнее см. раздел Настройка подсистем безопасности.

5. Лицензирование

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

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование Dr.Web Desktop Security Suite;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать приобретенную копию Dr.Web Desktop Security Suite).

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а на локальном компьютере с лицензией связывается специальный файл, регулирующий работу компонентов Dr.Web Desktop Security Suite в соответствии с параметрами лицензии. Он называется *лицензионным ключевым файлом*.

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 Desktop Security Suite в течение всего этого периода, если не нарушены условия его активации. При этом 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 демонстрационный период истек), антивирусные функции Dr.Web Desktop Security Suite блокируются, кроме того, сервис регулярных обновлений вирусных баз Dr.Web с серверов обновлений компании «Доктор Веб» становится недоступным. Однако имеется возможность активировать Dr.Web Desktop Security Suite, 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 в составе антивирусной сети, возлагается на сервер централизованной защиты.

6. Установка и удаление

В этом разделе описываются процедуры установки и удаления Dr.Web Desktop Security Suite, а также процедура получения текущих обновлений и процедура перехода на новую версию, если на вашем компьютере уже установлен Dr.Web Desktop Security Suite более ранней версии.

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

Для осуществления этих операций необходимы права суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.



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

Если на вашем компьютере уже имеется другой антивирусный продукт Dr.Web, установленный из универсального пакета (`.run`), и вы желаете установить еще один антивирусный продукт Dr.Web (например, у вас из универсального пакета установлен продукт Dr.Web Server Security Suite, и вы хотите в дополнение к нему установить Dr.Web Desktop Security Suite), то предварительно убедитесь, что версия уже установленного продукта совпадает с версией Dr.Web Desktop Security Suite, которую вы планируете установить. Если версия, которую вы собираетесь установить, новее, чем версия продукта, который уже установлен на вашем компьютере, перед началом установки дополнительного продукта обновите уже установленный продукт до версии Dr.Web Desktop Security Suite, которую вы хотите установить дополнительно.

Дополнительно:

- Установка Dr.Web Desktop Security Suite
- Обновление Dr.Web Desktop Security Suite
- Удаление Dr.Web Desktop Security Suite
- Настройка подсистем безопасности
- Пакеты и файлы Dr.Web Desktop Security Suite
- Выборочные установка и удаление компонентов

6.1. Установка Dr.Web Desktop Security Suite

Вы можете установить Dr.Web Desktop Security Suite одним из двух способов:

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



В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, рекомендуется устанавливать Dr.Web Desktop Security Suite из универсального пакета.

После установки Dr.Web Desktop Security Suite подсистема IMA/EVM ОС Альт 8 СП 11100-01 может выдавать предупреждение о возможном нарушении целостности. Чтобы избежать этого предупреждения, после установки Dr.Web Desktop Security Suite выполните команду:

```
# integalert fix
```

ОС Альт 8 СП 11100-02 и ОС Альт 8 СП 11100-03 не подвержены этой проблеме.



После установки Dr.Web Desktop Security Suite 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 Desktop Security Suite к серверу централизованной защиты (подробнее см. раздел Лицензирование). До тех пор, пока вы этого не сделаете, *функции антивирусной защиты будут отключены*. Кроме того, в ряде случаев необходимо выполнить основную настройку базовой функциональности Dr.Web Desktop Security Suite, как описано в разделе Начало работы.

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 Desktop Security Suite, 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 Dr.Web Desktop Security Suite. При необходимости выполните также настройку подсистем безопасности GNU/Linux для корректной работы Dr.Web Desktop Security Suite. При возникновении проблем с функционированием отдельных компонентов вы можете выполнить их выборочную установку и удаление, не удаляя Dr.Web Desktop Security Suite целиком.

6.1.1. Установка универсального пакета

Универсальный пакет Dr.Web Desktop Security Suite распространяется в виде установочного файла с именем `drweb-<версия>-av-linux-<платформа>.run`, где *<платформа>* — строка, указывающая тип платформы, для которой предназначен Dr.Web Desktop Security Suite (для 32-битных платформ — `x86`, для 64-битных платформ — `amd64`, `arm64`, `e2s` и `ppc64el`), например:

```
drweb-11.1.0-av-linux-amd64.run
```



Далее в данном разделе руководства имя установочного файла, соответствующее формату, указанному выше, обозначается как *<имя файла .run>*, а путь к этому файлу — как *<путь к файлу .run>*.

Версия Dr.Web Desktop Security Suite определяется первыми двумя числами, разделенными точкой, в имени универсального пакета.

Чтобы установить компоненты Dr.Web Desktop Security Suite

1. Если у вас отсутствует установочный файл (универсальный пакет), загрузите его с официального сайта компании «Доктор Веб».
2. Сохраните установочный файл на жесткий диск компьютера в любой доступный для записи каталог (например, `/home/<username>`, где *<username>* — имя текущего пользователя).
3. Разрешите исполнение файла, например, командой:

   ```
   # chmod +x <путь к файлу .run>
   ```

4. Запустите его на выполнение командой:

   ```
   # <путь к файлу .run>
   ```

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



В случае установки Dr.Web Desktop Security Suite в среде ОС Astra Linux SE версий 1.6 и 1.7, работающей в режиме *замкнутой программной среды* (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.

При этом 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 утилита `sudo`). Если попытка повышения прав окончится неудачей, установка будет отменена.



Если раздел файловой системы, содержащий временный каталог, не имеет 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 в разделе файловой системы, имеющем достаточное количество свободного места. Также вы можете воспользоваться ключом распаковки в указанный каталог `--target` (см. раздел 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:

```
# <путь к файлу .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).



Использование этой опции означает, что вы соглашаетесь с условиями Лицензионного соглашения Dr.Web. Ознакомиться с текстом Лицензионного соглашения после установки Dr.Web Desktop Security Suite 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, вам следует удалить Dr.Web Desktop Security Suite после установки.

Запуск программы установки в полностью автоматическом режиме требует наличия прав суперпользователя (обычно пользователя *root*). Для повышения прав вы можете использовать команду `su` или `sudo`.



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

```
# setenforce 0
```

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

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



Рекомендуется сохранить файл `.run`, из которого производилась установка, для возможной переустановки Dr.Web Desktop Security Suite 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 Desktop Security Suite** для запуска продукта в графическом режиме.
- **Удалить продукты Dr.Web** для удаления продукта.

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



Для корректной работы Dr.Web Desktop Security Suite 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).

6.1.1.1. Установка в графическом режиме

Если программа установки в начале своей работы обнаружит наличие на компьютере ряда проблем, которые могут в дальнейшем привести к полной или частичной неработоспособности Dr.Web Desktop Security Suite, 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 Desktop Security Suite, 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 Desktop Security Suite.

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

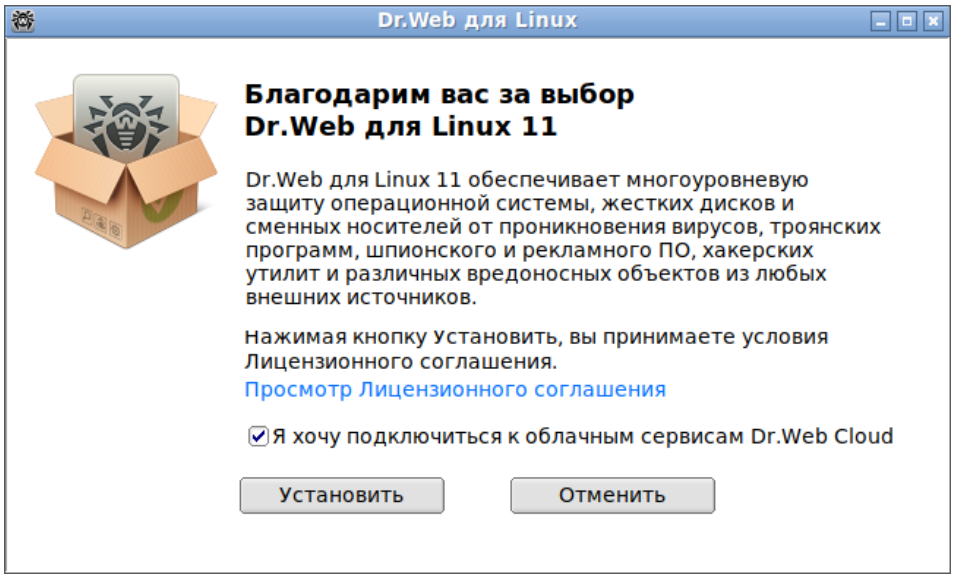


Рисунок 2. Мастер установки

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

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

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

   Чтобы закрыть страницу ознакомления с Лицензионным соглашением и авторскими правами нажмите **ОК**.

2. Перед началом установки вы можете согласиться с тем, что после установки Dr.Web Desktop Security Suite автоматически подключится к облачному сервису Dr.Web Cloud. Для этого установите соответствующий флажок (по умолчанию он установлен в момент запуска мастера установки). Если вы не хотите разрешать Dr.Web Desktop Security Suite использовать облачный сервис Dr.Web Cloud, сбросьте этот флажок. При необходимости вы в любой момент сможете разрешить или запретить Dr.Web Desktop Security Suite 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 «Доктор Веб». Если вы решили отказаться от установки Dr.Web Desktop Security Suite

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 Desktop Security Suite в графическом режиме. Для запуска установите флажок **Запустить Dr.Web Desktop Security Suite 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.

6.1.1.2. Установка в режиме командной строки

После запуска программы установки, работающей в 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 перед началом установки вам необходимо ознакомиться с текстом Лицензионного соглашения компании «Доктор Веб», который будет выведен на экран. Для перелистывания текста соглашения пользуйтесь клавишами ENTER (перелистывание текста на одну строчку вниз) и ПРОБЕЛ (перелистывание текста вниз на экран).

   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 завершена.
4. После принятия условий Лицензионного соглашения автоматически будет запущен процесс установки на компьютер компонентов Dr.Web Desktop Security Suite. 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 завершит свою работу.

В случае возникновения ошибки на экран будет выведено соответствующее сообщение с описанием ошибки, после чего работа программы установки будет завершена. Если установка была прервана из-за ошибки, устраните проблемы, вызвавшие ошибку установки, и повторите процесс установки заново.

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

6.1.2. Установка из репозитория

Нативные пакеты Dr.Web Desktop Security Suite находятся в официальном репозитории Dr.Web. 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, при установке Dr.Web Desktop Security Suite из подключенного репозитория пакетный менеджер ОС обнаруживает обновления всех компонентов Dr.Web и предлагает их установку.



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 (обычно 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):

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

Astra Linux, Debian, Mint, Ubuntu (apt)

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

```
# wget https://repo.drweb.com/drweb/drweb.gpg -O /etc/apt/trusted.gpg.d/drweb.gpg
```

Ключ цифровой подписи «Доктор Веб» ранее устанавливался с помощью утилиты `apt-key`, которая признана устаревшей и не рекомендуется для использования. Кроме того, теперь для хранения ключей подписи разработчики ОС рекомендуют использовать каталог `/etc/apt/trusted.gpg.d` вместо файла `/etc/apt/trusted.gpg`. Ввиду этого при выполнении установки Dr.Web Desktop Security Suite из репозитория, если ключ подписи установлен в каталог `/etc/apt/trusted.gpg`, команда `apt-get update` (см. ниже) выдаст следующее предупреждение: `Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details`. Установка Dr.Web Desktop Security Suite при этом продолжится в обычном режиме, а функциональность продукта не пострадает. Чтобы предупреждение больше не выводилось при установке или переустановке продуктов «Доктор Веб», установите ключ подписи как указано выше.

2. Чтобы подключить репозиторий, выполните команду:

```
# echo "deb https://repo.drweb.com/drweb/debian 11.1 non-free" > /etc/apt/sources.list.d/drweb.list
```

Вы можете выполнить пункты 1 и 2, загрузив специальный DEB-пакет и установив его.

3. Для установки Dr.Web Desktop Security Suite 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.

Альт (apt-rpm)

1. Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.list.d/drweb-apt-rpm-<arch>.list`:

```
rpm http://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`;
- для архитектуры IBM POWER (ppc64el): `ppc64le`.

2. Перед установкой Dr.Web Desktop Security Suite на компьютере архитектуры E2K под управлением ОС Альт добавьте в файл `/etc/rpmrc` следующие строки:

```
arch_compat: e2kv4: e2s
arch_compat: e2k: e2s
arch_compat: e2s: noarch
```

3. Чтобы установить Dr.Web Desktop Security Suite 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 Desktop Security Suite 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 `$` следует экранировать: `\$`.

Вы можете выполнить пункт 1, загрузив специальный RPM-пакет и установив его.

2. Для установки Dr.Web Desktop Security Suite 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, выполните команду:

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. Для установки Dr.Web Desktop Security Suite из репозитория выполните команды:

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

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

6.2. Обновление Dr.Web Desktop Security Suite

Предусмотрено два режима обновления Dr.Web Desktop Security Suite:

1. Получение текущих обновлений пакетов и компонентов, выпущенных в рамках эксплуатации актуальной версии Dr.Web Desktop Security Suite (как правило, такие обновления содержат исправления ошибок и мелкие улучшения в функционировании компонентов).
2. Переход на новую версию. Этот способ обновления используется, если компания «Доктор Веб» выпустила новую версию Dr.Web Desktop Security Suite, отличающуюся новыми возможностями.



Dr.Web Desktop Security Suite позволяет обновлять вирусные базы и антивирусное ядро даже при отсутствии доступа в интернет на защищаемом сервере.

6.2.1. Получение текущих обновлений

После установки Dr.Web Desktop Security Suite 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 Astra Linux, Debian, Mint, Ubuntu), для работы с пакетами Dr.Web используется отдельная версия менеджера пакетов `zypper`, автоматически установленная в рамках установки Dr.Web Desktop Security Suite.

  Чтобы получить и установить обновленные пакеты Dr.Web этим менеджером, перейдите в каталог `/opt/drweb.com/bin` и выполните 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 и OpenMandriva Lx используйте команду `urpmi`;
  - в Альт, Astra Linux, Debian, Mint, Ubuntu используйте команду `apt-get`.

Вы также можете использовать 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 Desktop Security Suite, пакеты, содержащие его компоненты, помещаются в раздел репозитория Dr.Web, соответствующий новой версии. В этом случае для обновления необходимо переключить менеджер пакетов на новый раздел репозитория Dr.Web (см. раздел Переход на новую версию).

6.2.2. Переход на новую версию

В этом разделе

- Предварительные замечания
- Обновление с версии 9.0 и новее
  - Обновление установкой универсального пакета
  - Обновление из репозитория
  - Перенос ключевого файла
  - Повторное подключение к серверу централизованной защиты
  - Особенности процесса обновления
- Обновление с версии 6.0.2 и более ранней
  - Перенос ключевого файла

Предварительные замечания

Поддерживается процедура обновления предыдущих версий Dr.Web Desktop Security Suite до новой версии. Переход на новую версию Dr.Web Desktop Security Suite выполняйте тем же способом, каким была установлена версия Dr.Web Desktop Security Suite, подлежащая обновлению:

- Если версия Dr.Web Desktop Security Suite, подлежащая обновлению, была установлена из репозитория, то переход на новую версию выполняйте путем обновлением из репозитория.
- Если версия Dr.Web Desktop Security Suite, 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 Desktop Security Suite, подлежащая обновлению, проверьте наличие в каталоге исполняемых файлов Dr.Web Desktop Security Suite скрипта программы удаления `uninst.sh`. Если этот файл присутствует, текущая версия Dr.Web Desktop Security Suite была установлена из универсального пакета, а в противном случае — из репозитория.

Если вы не имеете возможности обновить Dr.Web Desktop Security Suite 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 Desktop Security

Suite аналогичны способам установки и удаления, рассмотренным в этом руководстве. Для дополнительной информации обратитесь к Руководству пользователя по установленной у вас версии Dr.Web Desktop Security Suite.



Переход с Dr.Web Desktop Security Suite версии 6.0.2 и меньше на новую версию возможен *только* путем предварительного удаления старой версии Dr.Web Desktop Security Suite с последующей установкой новой версии.

Если версия Dr.Web Desktop Security Suite, подлежащая обновлению, работает под управлением сервера централизованной защиты, то перед началом обновления рекомендуется сохранить адрес этого сервера. Например, для получения адреса сервера централизованной защиты, к которому подключен Dr.Web Desktop Security Suite с версией новее 6.0.2, выполните команду:

```
$ 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 Desktop Security Suite, а также к администратору вашей антивирусной сети.

Обновление с версии 9.0 и новее

Обновление установкой универсального пакета

Выполните установку новой версии Dr.Web Desktop Security Suite из универсального пакета. В случае необходимости в процессе установки вам будет предложено автоматически удалить имеющиеся компоненты старой версии Dr.Web Desktop Security Suite.

Обновление из репозитория

Чтобы обновить текущую версию Dr.Web Desktop Security Suite, установленную из репозитория компании «Доктор Веб»

В зависимости от типа используемых пакетов, выполните следующие действия:

- **В случае использования пакетов RPM (yum, dnf):**

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов новой версии).



Имя репозитория, хранящего пакеты новой версии, 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 Desktop Security Suite 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 Desktop Security Suite. При необходимости см. разделы Удаление Dr.Web Desktop Security Suite, 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 новой версии).
  2. Обновите пакеты Dr.Web Desktop Security Suite, выполнив команды:

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

Перенос ключевого файла

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



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

Повторное подключение к серверу централизованной защиты

Если это возможно, то после обновления (если обновляемая версия была подключена к серверу централизованной защиты) подключение будет восстановлено автоматически. Если подключение не восстановилось автоматически, для подключения обновленной версии Dr.Web Desktop Security Suite к антивирусной сети воспользуйтесь любым из следующих способов:

- Установите флажок на вкладке **Режим** окна настроек Dr.Web Desktop Security Suite.
- Выполните команду:

```
$ drweb-ctl esconnect <адрес сервера> --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 Desktop Security Suite обновляемой версии, после завершения установки пакетов новой версии Dr.Web Desktop Security Suite, процессы старой версии Dr.Web Desktop Security Suite 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 Desktop Security Suite.
- При обновлении Dr.Web Desktop Security Suite 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 Desktop Security Suite версии 6.0.2 и более ранней на более позднюю версию возможен только путем предварительного удаления старой версии Dr.Web Desktop Security Suite с последующей установкой более поздней версии. Для получения дополнительной информации о способах удаления старой версии Dr.Web Desktop Security Suite обратитесь к Руководству пользователя установленной у вас версии Dr.Web Desktop Security Suite.

Перенос ключевого файла

Имеющийся у вас лицензионный ключевой файл старой версии Dr.Web Desktop Security Suite не будет автоматически установлен для использования новой версией, но вы можете выполнить его установку вручную. Dr.Web Desktop Security Suite версии 6.0.2 и

ранее хранит ключевой файл в каталоге `/home/<username>/.drweb` (каталог имеет атрибут «скрытый»). В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки компании «Доктор Веб».



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

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

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

6.3. Удаление Dr.Web Desktop Security Suite

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

- запустив программу удаления универсального пакета (для графического режима или режима командной строки, в зависимости от возможностей окружения);
- удалив пакеты, установленные из репозитория компании «Доктор Веб», используя системный менеджер пакетов.

6.3.1. Удаление универсального пакета

В этом разделе

- Удаление Dr.Web Desktop Security Suite через меню приложений
- Удаление Dr.Web Desktop Security Suite из командной строки

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



Программа удаления удалит не только Dr.Web Desktop Security Suite, но и *все другие* продукты Dr.Web, установленные на вашем компьютере.

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

Удаление Dr.Web Desktop Security Suite через меню приложений

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

Удаление Dr.Web Desktop Security Suite из командной строки

Запуск программы удаления осуществляется скриптом `remove.sh`, расположенным в каталоге `/opt/drweb.com/bin`. Таким образом, чтобы запустить удаление Dr.Web Desktop Security Suite, 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, выполните команду:

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

Процедура удаления Dr.Web Desktop Security Suite рассмотрена в соответствующих разделах:

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

Чтобы запустить программу удаления в полностью автоматическом режиме без показа интерфейса пользователя (включая диалоги программы удаления для режима командной строки), выполните команду:

```
# env DRWEB_NON_INTERACTIVE=yes /opt/drweb.com/bin/uninst.sh
```



В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, 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.

6.3.1.1. Удаление в графическом режиме

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

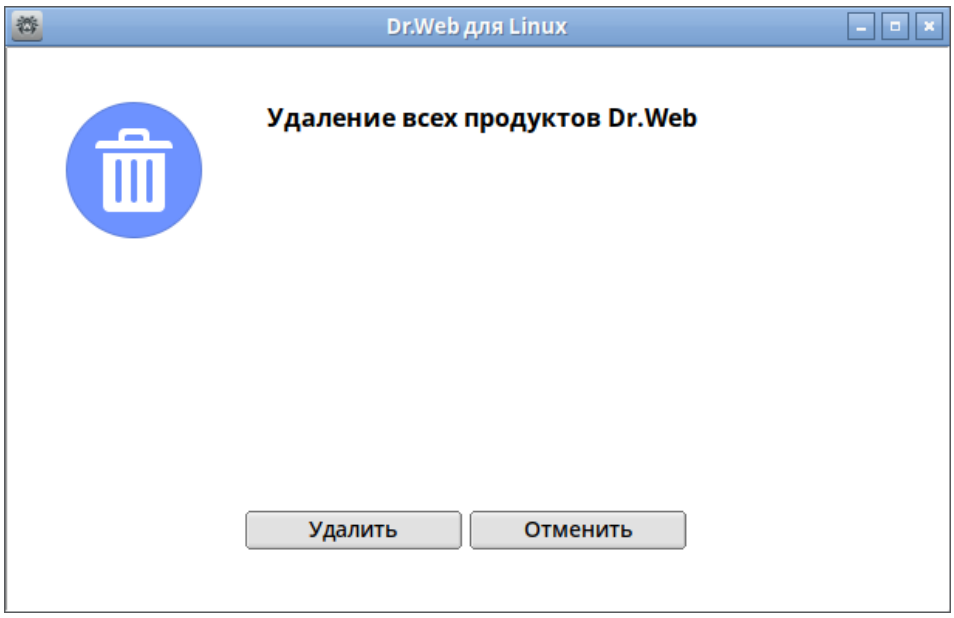


Рисунок 3. Мастер удаления

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 Desktop Security Suite и внесения необходимых изменений в системные настройки, откроется финальная страница мастера с сообщением об успешном удалении.
4. Для закрытия окна мастера удаления нажмите **ОК**.

6.3.1.2. 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.

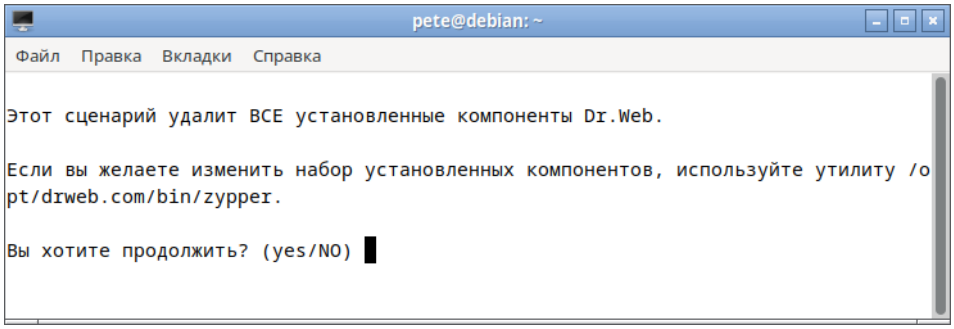


Рисунок 4. Приглашение к удалению

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.

6.3.2. Удаление Dr.Web Desktop Security Suite, установленного из репозитория

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Astra Linux, Debian, Mint, Ubuntu (apt);
- Альт (apt-rpm);
- Mageia, OpenMandriva Lx (urpme);
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf);
- SUSE Linux (zypper).

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

Astra Linux, Debian, Mint, Ubuntu (apt)

Чтобы удалить корневой метапакет Dr.Web Desktop Security Suite, выполните команду:

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

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить корневой метапакет вместе со всеми зависимостями, выполните команду:

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

При этом будут удалены все более не требуемые пакеты (а не только пакеты Dr.Web Desktop Security Suite), которые были автоматически установлены для удовлетворения зависимостей других пакетов.

Если корневой метапакет уже был удален, то чтобы автоматически удалить из системы все более не используемые пакеты, выполните команду:

```
# apt-get autoremove
```

Вы также можете удалить пакеты Dr.Web Desktop Security Suite с помощью альтернативных менеджеров (например, Synaptic или aptitude).

Альт (apt-rpm)

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

Вы также можете удалить пакеты Dr.Web Desktop Security Suite 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)

Чтобы удалить корневой метапакет Dr.Web Desktop Security Suite, выполните команду:

```
# urpme drweb-workstations
```

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить корневой метапакет вместе со всеми зависимостями, выполните команду:

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

При этом будут удалены все более не требуемые пакеты (а не только пакеты Dr.Web Desktop Security Suite), которые были автоматически установлены для удовлетворения зависимостей других пакетов.

Вы также можете удалить пакеты Dr.Web Desktop Security Suite с помощью альтернативных менеджеров (например, `rpmdrake`).

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

Чтобы удалить все установленные пакеты Dr.Web, выполните команду (в некоторых системах символ * требуется экранировать: *):

```
# yum remove drweb*
```

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

```
# dnf remove drweb*
```



Эти команды удалят из системы все пакеты, название которых начинается на `drweb` (стандартное наименование для пакетов программных продуктов Dr.Web). Будут удалены все пакеты с таким именем, а не только пакеты Dr.Web Desktop Security Suite.

Вы также можете удалить пакеты Dr.Web Desktop Security Suite с помощью альтернативных менеджеров (например, PackageKit или Yumex).

SUSE Linux (zypper)

Чтобы удалить корневой метапакет Dr.Web Desktop Security Suite, выполните команду:

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

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить все установленные пакеты Dr.Web, выполните команду (в некоторых системах символ * требуется экранировать: *):

```
# zypper remove drweb*
```



Эта команда удалит из системы все пакеты, название которых начинается на `drweb` (стандартное наименование для пакетов программных продуктов Dr.Web). Будут удалены все пакеты с таким именем, а не только пакеты Dr.Web Desktop Security Suite.

Вы также можете удалить пакеты Dr.Web Desktop Security Suite с помощью альтернативных менеджеров (например, YaST).

6.4. Дополнительно

6.4.1. Пакеты и файлы Dr.Web Desktop Security Suite

В этом разделе

- Пакеты

- Файлы

Пакеты

Dr.Web Desktop Security Suite состоит из следующих пакетов:

Пакет	Содержимое
drweb-ase	Файлы компонента Dr.Web Anti-Spam Engine. Может отсутствовать, в зависимости от поставки
drweb-bases	Файлы вирусных баз
drweb-boost	Библиотеки Boost
drweb-cloudd	Файлы компонента Dr.Web CloudD
drweb-common	Основной конфигурационный файл drweb.ini, основные библиотеки, документация и структура каталогов Dr.Web Desktop Security Suite, утилита сбора данных о конфигурации продукта и системном окружении. В процессе установки данного пакета также будут созданы пользователь drweb и группа drweb
drweb-configd	Файлы компонента Dr.Web ConfigD
drweb-configure	Файлы вспомогательной утилиты настройки Dr.Web Desktop Security Suite
drweb-ctl	Файлы компонента Dr.Web Ctl
drweb-documentation	Файлы документации в формате HTML по продуктам Dr.Web для Unix
drweb-dws	Файлы базы категорий веб-ресурсов
drweb-engine	Файлы антивирусного ядра Dr.Web Virus-Finding Engine
drweb-esagent	Файлы компонента Dr.Web ES Agent
drweb-filecheck	Файлы компонента Dr.Web File Checker
drweb-workstations-doc	Документация в формате PDF
drweb-workstations	Корневой метапакет Dr.Web Desktop Security Suite
drweb-gated	Файлы компонента SpIDer Gate
drweb-firewall	Файлы компонента Dr.Web Firewall для Linux

Пакет	Содержимое
drweb-icu	Библиотеки поддержки интернационализации и Unicode
drweb-libs	Файлы основных библиотек
drweb-maild	Файлы компонента Dr.Web MailD
drweb-netcheck	Файлы компонента Dr.Web Network Checker
drweb-openssl	Библиотеки OpenSSL
drweb-protobuf	Библиотеки Google Protobuf
drweb-se	Файлы компонента Dr.Web Scanning Engine
drweb-spider	Файлы компонента SpIDer Guard
drweb-update	Файлы компонента Dr.Web Updater
drweb-antispam-engine	Файлы антиспам-библиотеки. Может отсутствовать, в зависимости от поставки

В разделе Выборочные установка и удаление компонентов приведены типовые наборы компонентов для выборочной установки, обеспечивающие решение типовых задач Dr.Web Desktop Security Suite.

Файлы

Файлы Dr.Web Desktop Security Suite размещаются в каталогах /opt, /etc и /var дерева файловой системы.

Структура используемых каталогов:

Каталог	Содержимое
/etc/init.d/	Управляющий скрипт drweb-configd для демона управления конфигурацией Dr.Web ConfigD
/etc/opt/drweb.com/	Общий конфигурационный файл drweb.ini и ключевой файл drweb32.key. Кроме этого, содержит:
certs/	– файлы используемых сертификатов.
/opt/drweb.com/	Основной каталог Dr.Web Desktop Security Suite. Содержит в себе:

Каталог	Содержимое
bin/	– исполняемые файлы всех компонентов (за исключением Dr.Web Virus-Finding Engine);
include/	– заголовочные файлы используемых библиотек;
lib/	– используемые библиотеки;
man/	– файлы системной справки man;
share/	– вспомогательные файлы, в том числе:
doc/	▫ документация Dr.Web Desktop Security Suite (текст Лицензионного соглашения и руководства администратора, если пакеты с документацией установлены),
drweb-bases/	▫ файлы вирусных баз Dr.Web (исходные образы, поставляемые при установке),
scripts/	▫ файлы вспомогательных скриптов.
/var/opt/drweb.com/	Вспомогательные и временные файлы, в том числе:
bases/	– файлы вирусных баз Dr.Web (актуальная обновленная версия);
cache/	– кеш обновлений;
drl/	– списки используемых серверов обновлений;
dws/	– файлы базы категорий веб-ресурсов;
lib/	– антивирусное ядро Dr.Web Virus-Finding Engine в виде динамически загружаемой библиотеки drweb32.dll и настройки режима работы с сервером централизованной защиты. Также здесь располагается библиотека проверки писем на спам, если она включена в состав Dr.Web Desktop Security Suite;
update/	– каталог для временного хранения обновлений в процессе их получения.

6.4.2. Выборочные установка и удаление компонентов

В этом разделе

- Типовые комплекты компонентов для выборочной установки
- Установка и удаление компонентов Dr.Web Desktop Security Suite, установленного из репозитория

- Установка и удаление компонентов Dr.Web Desktop Security Suite, установленного из универсального пакета
  - Распаковка установочного файла
  - Выборочная установка компонентов
  - Выборочное удаление компонентов

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

Для переустановки какого-либо компонента вы можете сначала удалить его, а потом установить заново.

Типовые комплекты компонентов для выборочной установки

Если требуется установить Dr.Web Desktop Security Suite с ограниченной функциональностью, вместо установки корневого метапакета из репозитория или из универсального пакета, вы можете установить только пакеты компонентов, обеспечивающих необходимую функциональность. Пакеты, требуемые для разрешения зависимостей, будут установлены автоматически. В таблице ниже приведены комплекты компонентов, предназначенные для решения типовых задач Dr.Web Desktop Security Suite. В столбце **Пакеты для установки** перечислены пакеты, которые необходимо установить для получения указанного комплекта компонентов.

Выборочный комплект компонентов	**Пакеты для установки**	**Будут установлены**
Минимальный комплект для консольного сканирования	• `drweb-filecheck`, • `drweb-se`	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • Вирусные базы
Комплект для мониторинга файловой системы GNU/Linux	• `drweb-se`, • `drweb-spider`	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • SpIDer Guard, • Вирусные базы

Установка и удаление компонентов Dr.Web Desktop Security Suite, установленного из репозитория

Если Dr.Web Desktop Security Suite был установлен из репозитория, для установки или удаления отдельного компонента используйте соответствующую команду менеджера пакетов вашей ОС, например:

1. Чтобы удалить компонент Dr.Web Network Checker (пакет `drweb-netcheck`) из состава Dr.Web Desktop Security Suite, установленного в ОС CentOS, выполните команду:

   ```
   # yum remove drweb-netcheck
   ```

2. Чтобы добавить компонент Dr.Web Network Checker (пакет `drweb-netcheck`) в состав Dr.Web Desktop Security Suite, установленного в ОС Ubuntu, выполните команду:

   ```
   # apt-get install drweb-netcheck
   ```

При необходимости воспользуйтесь справкой по менеджеру пакетов вашей ОС.

Установка и удаление компонентов Dr.Web Desktop Security Suite, установленного из универсального пакета

Если Dr.Web Desktop Security Suite был установлен из универсального пакета, и вы хотите дополнительно установить или переустановить пакет какого-либо компонента, вам понадобится установочный файл (с расширением `.run`), из которого был установлен Dr.Web Desktop Security Suite. Если вы не сохранили этот файл, загрузите его с сайта компании «Доктор Веб».

Распаковка установочного файла

При запуске файла `.run` вы можете использовать следующие параметры командной строки:

`--noexec` — распаковать установочные файлы Dr.Web Desktop Security Suite вместо запуска процесса установки;

`--keep` — не удалять установочные файлы Dr.Web Desktop Security Suite и журнал установки по окончании установки;

`--target` <*каталог*> — распаковать установочные файлы Dr.Web Desktop Security Suite в указанный каталог <*каталог*>.

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

```
$ ./<имя файла .run> --help
```

Для выборочной установки компонентов Dr.Web Desktop Security Suite предварительно распакуйте содержимое установочного файла. Для этого выполните команду:

```
$ ./<имя файла .run> --noexec --target <каталог>
```

Выборочная установка компонентов

Установочный файл `.run` содержит пакеты всех компонентов, из которых состоит Dr.Web Desktop Security Suite (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 Desktop Security Suite. Имена всех пакетов, содержащих компоненты Dr.Web Desktop Security Suite, начинаются с префикса `drweb`.

Для установки пакетов в состав установочного комплекта включен менеджер пакетов `zypper`. Для выборочной установки используйте служебный скрипт `installpkg.sh`. Для этого предварительно распакуйте содержимое установочного файла в любой каталог, доступный для записи.



Для установки пакетов необходимы права суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Чтобы выполнить установку пакета компонента, перейдите в каталог, содержащий распакованный установочный файл, и выполните в командной строке или эмуляторе терминала команду:

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

Например:

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

Если требуется установить Dr.Web Desktop Security Suite целиком, запустите скрипт установки, выполнив команду:

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

Кроме этого, вы можете установить все пакеты Dr.Web Desktop Security Suite (в том числе, чтобы установить недостающие компоненты, или компоненты, удаленные по ошибке), запустив установку корневого метапакета:

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

Выборочное удаление компонентов

Если в вашей ОС используется формат пакетов RPM, для выборочного удаления пакета какого-либо компонента выполните соответствующую команду удаления менеджера пакетов вашей операционной системы:

- в Red Hat Enterprise Linux и CentOS выполните команду `yum remove` <*имя_пакета*>;
- в Fedora выполните команду `yum remove` <*имя_пакета*> или `dnf remove` <*имя_пакета*>;
- в SUSE Linux выполните команду `zypper remove` <*имя_пакета*>;
- в Mageia, OpenMandriva Lx выполните команду `urpme` <*имя_пакета*>;
- в Альт выполните команду `apt-get remove` <*имя_пакета*>.

Например, для Red Hat Enterprise Linux:

```
# yum remove drweb-netcheck
```

Если ваша ОС использует пакеты формата DEB, либо если в составе системы не имеется менеджера пакетов, для выборочного удаления воспользуйтесь менеджером пакетов `zypper`, поставляемым с Dr.Web Desktop Security Suite. Для этого перейдите в каталог `/opt/drweb.com/bin` и выполните команду:

```
# ./zypper remove <имя_пакета>
```

Например:

```
# ./zypper remove drweb-netcheck
```

Если вы хотите удалить Dr.Web Desktop Security Suite целиком, запустите скрипт удаления, выполнив команду:

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

Для переустановки какого-либо компонента вы можете сначала удалить его, а потом установить, запустив выборочную или полную установку.

6.5. 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 Desktop Security Suite при настройках по умолчанию. Для обеспечения корректной работы Dr.Web Desktop Security Suite в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web Desktop Security Suite.



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

Даже если вы не настроите разрешения системы мандатного доступа PARSEC для Dr.Web Desktop Security Suite, то вы все равно сможете запускать проверку файлов, используя графический интерфейс Dr.Web Desktop Security Suite в режиме автономного экземпляра. 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`).

В режиме автономного экземпляра 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 автономного экземпляра 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 Desktop Security Suite подключен к серверу централизованной защиты, автономный экземпляр *не сообщает* серверу централизованной защиты об угрозах, обнаруженных при запуске в режиме автономного экземпляра.
- Все вспомогательные компоненты, обслуживающие работу автономного экземпляра, 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. Этот каталог создается запущенным автономным экземпляром в каталоге временных файлов (указанном в системной переменной окружения `TMPDIR`).
- Автономно запущенный экземпляр 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.
- Число одновременно работающих автономных экземпляров не ограничено.
- При завершении работы автономно запущенного экземпляра комплект обслуживающих его сервисных компонентов также завершает работу.

6.5.1. Настройка политик безопасности SELinux

В этом разделе

- Проблемы при установке универсального пакета
- Проблемы функционирования Dr.Web Desktop Security Suite

Если используемый вами дистрибутив GNU/Linux оснащен подсистемой безопасности SELinux (*Security-Enhanced Linux — Linux с улучшенной безопасностью*), то, чтобы служебные компоненты Dr.Web Desktop Security Suite (такие как сканирующее ядро) работали корректно после установки компонентов, вам, возможно, потребуется внести изменения в политики безопасности, используемые SELinux.

Проблемы при установке универсального пакета

При включенном SELinux установка Dr.Web Desktop Security Suite 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 Desktop Security Suite.

Если попытка установки Dr.Web Desktop Security Suite 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:

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

Если SELinux работает в режиме *Enforcing*, временно (на период установки Dr.Web Desktop Security Suite) переведите ее в режим *Permissive*. Для этого выполните команду:

```
# setenforce 0
```

Указанная команда 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 Desktop Security Suite из установочного файла, но до его запуска и активации верните режим *Enforcing*, для чего выполните команду:

```
# setenforce 1
```

Проблемы функционирования Dr.Web Desktop Security Suite

В некоторых случаях при работающем SELinux отдельные компоненты Dr.Web Desktop Security Suite (такие как `drweb-se` и `drweb-filecheck`) не смогут запуститься, вследствие чего сканирование объектов и мониторинг файловой системы станут невозможны. Признаком того, что эти компоненты не могут быть запущены, является появление сообщений об ошибках 119 и 120 на главном окне Dr.Web Desktop Security Suite и в системном журнале, который ведет служба `syslog` (обычно этот журнал 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 хранится 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 компоненты сканирования не функционируют из-за того, что они блокируются SELinux, скомпилируйте для них специальные *политики безопасности*.



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

Чтобы настроить политики 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.

Этот способ можно использовать только в том случае, когда в системном журнале аудита уже зарегистрированы инциденты нарушения политик безопасности SELinux компонентами Dr.Web Desktop Security Suite. Если это не так, дождитесь таких инцидентов в процессе работы Dr.Web Desktop Security Suite или 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 данном примере утилита `audit2allow` производит поиск в файле `/var/log/audit/audit.log` сообщений об отказе в доступе для компонента `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`.

По умолчанию утилита `audit2allow` в качестве результата своей работы выводит на экран готовый вызов команды `semodule`. Скопировав его в командную строку и выполнив, вы выполните пункт 4. Перейдите к пункту 2, только если вы хотите внести изменения в политики, автоматически сформированные для компонентов Dr.Web Desktop Security Suite.

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

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 компонента `drweb-se`:

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

- для компонента `drweb-filecheck`:

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

Вам будет предложено указать несколько общих характеристик домена, после чего для каждого компонента 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.



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 GNU/Linux.

6.5.2. Настройка разрешений PARSEC

В этом разделе

- Настройка взаимодействия компонентов, запущенных на разных уровнях привилегий
  - Использование утилиты drweb-configure
  - Изменение файлов конфигурации вручную
- Настройка автоматического запуска компонентов на уровне привилегий пользователя
  - Использование утилиты drweb-configure
  - Изменение файлов конфигурации PAM вручную
- Настройка SpIDer Guard для перехвата событий доступа к файлам

В дистрибутивах GNU/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 Desktop Security Suite не может взаимодействовать со SplDer 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 Desktop Security Suite, чтобы обеспечить взаимодействие его компонентов, запускаемых на различных уровнях привилегий.



Для осуществления этих операций необходимы права суперпользователя (пользователя *root*). Для получения прав суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Настройка взаимодействия компонентов, запущенных на разных уровнях привилегий

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. `drweb-configd` — сервисный компонент Dr.Web Desktop Security Suite, обеспечивающий взаимодействие всех антивирусных компонентов между собой.

Чтобы демон управления конфигурацией Dr.Web Desktop Security Suite (`drweb-configd`) получил право на использование механизма *privsock*, необходимо внести изменения в системный файл `/etc/parsec/privsock.conf`. Для внесения изменений вы можете использовать утилиту конфигурирования `drweb-configure`, входящую в состав Dr.Web Desktop Security Suite (рекомендуется), либо внести изменения в необходимые файлы конфигурации вручную.

Использование утилиты drweb-configure

Требуемые изменения будут внесены автоматически после выполнения команды:

```
# drweb-configure session <режим>
```

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

- `enable` — использовать механизм *privsock*;
- `disable` — не использовать механизм *privsock*.

Изменение файлов конфигурации вручную

Для ОС Astra Linux SE версии 1.6 и более поздней

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.

Настройка автоматического запуска компонентов на уровне привилегий пользователя

Для того, чтобы компоненты Dr.Web Desktop Security Suite, 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 Desktop Security Suite при начале сессии пользователя и их завершения при окончании сессии (используется специальный PAM-модуль `pam_drweb_session.so`, разработанный «Доктор Веб», который запускает компонент-посредник `drweb-session`, связывающий между собой компоненты, запущенные 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 Desktop Security Suite (рекомендуется), либо внести изменения в необходимые файлы конфигурации вручную.

Использование утилиты drweb-configure

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

1. Для включения или отключения автоматического запуска необходимых компонентов Dr.Web Desktop Security Suite в окружении пользователя при его работе на уровне привилегий, отличном от нулевого, выполните команду:

   ```
   # 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 Desktop Security Suite окажется недоступным).

2. Перезапустите систему.



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

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

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 `/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 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 Desktop Security Suite `/opt/drweb.com/lib/` (например, для 64-разрядных ОС — в каталоге `/opt/drweb.com/lib/x86_64-linux-gnu/pam/`).
4. Перезапустите систему.

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 команду:

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

Для получения дополнительной информации выполните команду:

```
$ man drweb-spider
```

6.5.3. Настройка Альт 8 СП и других ОС, использующих pam_namespace

В этом разделе

- Использование утилиты drweb-configure
- Изменение файлов конфигурации PAM вручную

Для того, чтобы компоненты Dr.Web Desktop Security Suite, с которыми взаимодействует пользователь, были доступны в его окружении, внесите изменения в файлы настроек PAM для автоматического запуска требуемых компонентов Dr.Web Desktop Security Suite при начале сессии пользователя и их завершения при окончании сессии.



Для ОС Альт 8 СП изменения требуются для всех уровней привилегий, а для других ОС, использующих `pam_namespace`, — при работе пользователя на уровне привилегий, отличном от нулевого.

Специальный PAM-модуль `pam_drweb_session.so`, разработанный компанией «Доктор Веб», запускает компонент-посредник `drweb-session`, связывающий между собой локальные экземпляры 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 Desktop Security Suite (рекомендуется), либо внести изменения в необходимые файлы конфигурации вручную.



До внесения изменений на ОС Альт 8 СП 11100-02 необходимо выполнить следующие действия:

1. Выполнить вход под пользователем *officer*.
2. Получить права суперпользователя:

   ```
   $ su -
   ```

3. Выполнить установку политики:

   ```
   # semodule -i /opt/drweb.com/share/drweb.pp
   ```

4. Обновить контексты безопасности файлов в соответствии с установленной политикой:

   ```
   # restorecon -r /opt/drweb.com
   ```

Использование утилиты drweb-configure

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

1. Для включения или отключения автоматического запуска необходимых компонентов Dr.Web Desktop Security Suite в окружении пользователя при его работе на уровне привилегий, отличном от нулевого, выполните команду:

   ```
   # 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 Desktop Security Suite окажется недоступным).

2. Перезапустите систему.



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

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

Изменение файлов конфигурации PAM вручную

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
   ```

   В каждый файл из списка 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 Desktop Security Suite `/opt/drweb.com/lib/` (например, для 64-разрядных ОС — в каталоге `/opt/drweb.com/lib/x86_64-linux-gnu/pam/`). Пример команды для 64-разрядной ОС Альт 8 СП:

```
# ln -s /opt/drweb.com/lib/x86_64-linux-
gnu/pam/pam_drweb_session.so /lib64/security/pam_drweb_session.so
```

Для ОС Альт 8 СП 11100-02 и Альт 8 СП 11100-03 необходимо дополнительно выполнить следующее:

1. В файле /etc/pam.d/newrole вместо строки

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

   укажите следующее:

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

2. Отредактируйте файлы `/etc/pam.d/su` и `/etc/pam.d/sudo`, добавив в конец следующую строку:

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

3. Сохраните измененные файлы.
4. Выполните команду:

   ```
   # cp /opt/drweb.com/share/drweb-session/drweb-
   session.sh /etc/profile.d/
   ```

4. Перезапустите операционную систему.

6.5.4. 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 этом режиме запускаются только приложения, исполняемые файлы которых подписаны цифровой подписью разработчика, чей открытый ключ добавлен в перечень ключей, которым доверяет ОС.

Начиная с версии 1.6, в ОС Astra Linux SE механизм подписи был изменен. Запуск Dr.Web Desktop Security Suite в режиме ЗПС требует предварительной настройки Astra Linux SE 1.6 и 1.7.

Чтобы настроить Astra Linux SE версий 1.6 и 1.7 для запуска Dr.Web Desktop Security Suite в режиме ЗПС

1. Установите пакет `astra-digsig-oldkeys`, если он еще не установлен, с установочного диска ОС.
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.

7. Начало работы

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

7.1. Регистрация и активация

В этом разделе

- Приобретение и регистрация лицензии
- Активация Dr.Web Desktop Security Suite
  - Запрос демонстрационного периода
  - Установка ключевого файла
  - Подключение к серверу централизованной защиты
- Повторная регистрация

Приобретение и регистрация лицензии

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

Приобрести любой антивирусный продукт Dr.Web или серийный номер для него вы можете у наших партнеров или через интернет-магазин. Дополнительную информацию о возможных вариантах лицензий можно найти на официальном сайте компании «Доктор Веб».

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

Активация Dr.Web Desktop Security Suite

Приобретенная лицензия может быть активирована любым из указанных ниже способов:

- при помощи мастера регистрации, входящего в состав Менеджера лицензий;
- непосредственно на сайте компании «Доктор Веб».

При активации или продлении лицензии требуется указать серийный номер. Этот номер может поставляться вместе с Dr.Web Desktop Security Suite или по электронной почте, при покупке или продлении лицензии онлайн.



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

Запрос демонстрационного периода

Пользователям продуктов Dr.Web доступен демонстрационный период в 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 Desktop Security Suite (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 использовать мастер регистрации (например, из-за отсутствия графической оболочки ОС), вы можете использовать команду `license` утилиты командной строки Dr.Web Ctl (`drweb-ctl`), которая позволяет автоматически получить демонстрационный ключевой файл или лицензионный ключевой файл для серийного номера зарегистрированной лицензии.

Установка ключевого файла

Если уже имеется ключевой файл, соответствующий действующей лицензии на этот продукт (например, он был получен от продавца по электронной почте после регистрации или Dr.Web Desktop Security Suite переносится на другой компьютер), имеется возможность активировать Dr.Web Desktop Security Suite, 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 архиву `.zip`.
- Вручную, для этого:
  1. Распакуйте ключевой файл, если он был вами получен в архиве.
  2. Далее выполните любое из указанных ниже действий.
     - Скопируйте его в каталог `/etc/opt/drweb.com` и переименуйте в `drweb32.key`.
     - В файле конфигурации Dr.Web Desktop Security Suite установите значение параметра `KeyPath` таким образом, чтобы он указывал на ключевой файл. В этом случае название ключа может отличаться от `drweb32.key`.
  3. Перезагрузите конфигурацию Dr.Web Desktop Security Suite, выполнив команду:

     ```
     # drweb-ctl reload
     ```

     для применения внесенных изменений.

Вы также можете выполнить команду:

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

В последнем случае дополнительно перезагружать конфигурацию Dr.Web Desktop Security Suite не требуется. Ключевой файл не будет скопирован в каталог `/etc/opt/drweb.com`, а останется в 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 Desktop Security Suite, 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 компании «Доктор Веб». Ключевой файл будет выслан на адрес электронной почты, который был указан при первой регистрации.

После получения ключевого файла по электронной почте вам необходимо выполнить процедуру его установки.

7.1.1. Ключевой файл

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

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

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

При нарушении любого из этих условий ключевой файл становится недействительным.



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

Компоненты Dr.Web Desktop Security Suite 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 Desktop Security Suite 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 архивы `.zip`. Архив, содержащий ключевой файл для активации Dr.Web Desktop Security Suite, обычно имеет имя `agent.zip`. Если в сообщении электронной почты 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).

7.1.2. Файл настроек подключения

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

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

7.2. 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 угрозы.

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 файла `.com` для ОС MS-DOS/Windows, в результате исполнения которого в консоль или на экран эмулятора терминала 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 текстовый файл, состоящий из приведенной выше строки, то в результате получится программа, которая и будет описанным «вирусом».

В случае корректной работы Dr.Web Desktop Security Suite 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 Desktop Security Suite при помощи тестовой программы EICAR:

```
$ echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' > testfile
&& drweb-ctl scan testfile && rm testfile
```

Данная команда записывает строку, представляющую собой тело тестовой программы EICAR, в файл `testfile` в текущий каталог, выполняет проверку полученного файла, после чего удаляет созданный файл.



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

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

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

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



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

7.3. Режимы мониторинга файлов

В этом разделе

- Общие сведения
- Изменение режима мониторинга файлов

Общие сведения

Монитор файловой системы SpIDer 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). 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. SpIDer Guard блокирует запрошенную операцию доступа к исполняемому файлу до тех пор, пока не станут известны результаты его проверки на наличие угроз.



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

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

Сканер в течение определенного времени сохраняет результаты проверки файлов в специальном кеше, поэтому при повторном доступе к тому же файлу, при наличии информации в кеше, повторное сканирование файла не производится, в качестве результата проверки этого файла используется результат, извлеченный из кеша. 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 используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

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

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

- Для изменения режима мониторинга выполните команду:

```
# 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 кеше, выполните команду:

```
# drweb-ctl cfset FileCheck.RescanInterval <период>
```

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

8. Работа с Dr.Web Desktop Security Suite

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

- Для запуска графического интерфейса управления Dr.Web Desktop Security Suite выберите пункт **Dr.Web Desktop Security Suite** в системном меню **Приложения** или введите в эмуляторе терминала команду:

  ```
  $ drweb-gui &
  ```

  После этого, если окружение графического рабочего стола доступно, будет запущен графический интерфейс управления Dr.Web Desktop Security Suite. Для запуска проверки при старте графического интерфейса или для запуска его в режиме автономного экземпляра выполните данную команду с аргументами.
- Управление работой Dr.Web Desktop Security Suite из командной строки рассмотрено в разделе Dr.Web Ctl.
- Для графических сред рабочего стола также поддерживается запуск проверки файлов из панели задач (такой как Ubuntu Dock) 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 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 Desktop Security Suite любым из описанных в этом руководстве способов в начале работы вам потребуется активировать лицензию, либо установить ключевой файл, если он у вас уже имеется, или подключить Dr.Web Desktop Security Suite к серверу централизованной защиты (см. раздел Регистрация и активация). До тех пор, пока вы этого не сделаете, *функции антивирусной защиты будут отключены*.

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.

8.1. Работа в графическом режиме

В этом разделе

- Общие сведения
- Агент уведомлений
- Графический интерфейс управления
  - Внешний вид графического интерфейса управления
  - Главная страница

Общие сведения

За работу Dr.Web Desktop Security Suite 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 Desktop Security Suite, а также предоставляет индикатор состояния Dr.Web Desktop Security Suite 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 Desktop Security Suite.

Агент уведомлений

Агент уведомлений Dr.Web Desktop Security Suite предназначен для:

- отображения индикатора состояния Dr.Web Desktop Security Suite;
- управления мониторами и обновлением, запуска графического интерфейса управления;
- показа всплывающих уведомлений о событиях;
- запуска проверок по заданному расписанию.

Графический интерфейс управления

Графический интерфейс управления Dr.Web Desktop Security Suite позволяет решать следующие задачи:

1. Просмотр состояния работы Dr.Web Desktop Security Suite, 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 Desktop Security Suite.
5. Обзор всех угроз, обнаруженных Dr.Web Desktop Security Suite во время текущего сеанса работы в графическом режиме, включая обзор нейтрализованных и пропущенных угроз, а также объектов, перемещенных в карантин.
6. Обзор объектов, перемещенных в карантин, с возможностью их окончательного удаления или восстановления.
7. Настройка параметров работы компонентов Dr.Web Desktop Security Suite, включая следующие параметры:
   - Действия, которые Сканер и SpIDer 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 SpIDer Guard.
   - Черные и белые списки сайтов и нежелательных категорий веб-ресурсов, используемые монитором SpIDer 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 Desktop Security Suite работает в составе антивирусной сети и только если администратор антивирусной сети задаст соответствующую настройку на сервере централизованной защиты).

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

Внешний вид графического интерфейса управления

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

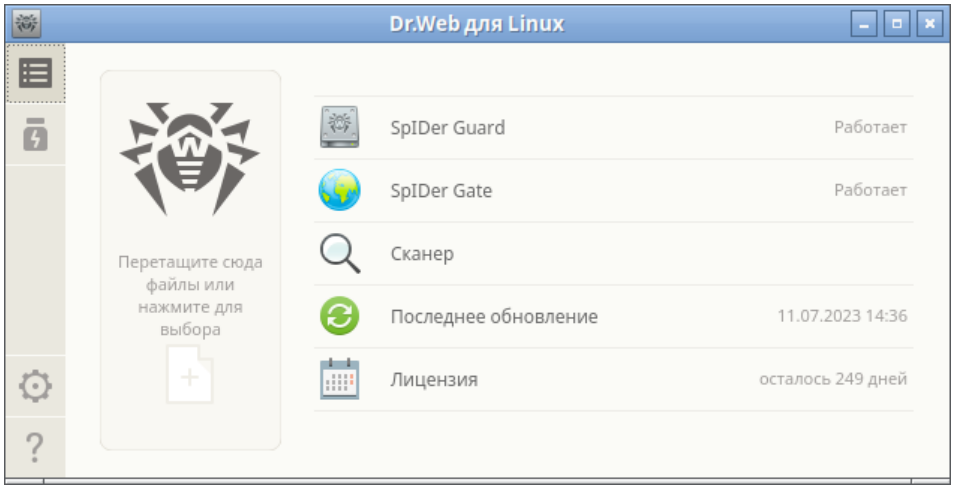


Рисунок 5. Графический интерфейс управления Dr.Web Desktop Security Suite

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

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.

Кнопка	Описание
	Открывает окно настройки работы Dr.Web Desktop Security Suite, в частности: • сканера объектов файловой системы; • монитора файловой системы SpIDer Guard; • монитора сетевых соединений SpIDer Gate; • запуска проверок по расписанию. Кроме того, здесь может быть настроена работа в режиме централизованной защиты.
	Предоставляет доступ к справочным материалам и вспомогательным ресурсам компании «Доктор Веб»: • информация о продукте; • руководство пользователя; • форум Dr.Web; • техническая поддержка; • персональный кабинет пользователя **Мой Dr.Web**. Все ссылки открываются в браузере, установленном в системе.
2. Появляющиеся в зависимости от условий	
	Открывает страницу списка задач проверки, 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, угроз не найдено, или все найденные угрозы обезврежены; 2) красная — имеются необезвреженные угрозы; 3) желтая — какая-либо из проверок завершилась вследствие ошибки. *Присутствует на навигационной панели только в случае если запускалась хотя бы одна проверка.*
	Открывает страницу просмотра угроз, обнаруженных при проверке файлов сканером или монитором файловой системы SpIDer Guard. *Присутствует на навигационной панели только в случае если имеются обнаруженные угрозы.*
	Присутствует на навигационной панели только в случае если открыта и активна страница запуска сканирования. *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.*

Кнопка	Описание
	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.*
	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 Desktop Security Suite 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 Desktop Security Suite расположена целевая область («мишень») для перетаскивания файлов и каталогов, подлежащих проверке. Она отмечена надписью **Перетащите сюда файлы или нажмите для выбора**. При перетаскивании и отпускании файлов и каталогов из окна файлового менеджера на главную страница окна Dr.Web Desktop Security Suite 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 SpIDer 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.

8.1.1. Интеграция со средой рабочего стола

В этом разделе

- Индикатор приложения в области уведомлений
  - Проблемы в работе индикатора приложения
- Контекстное меню значка панели задач
  - Проблемы в работе значка в панели задач
- Проверка файлов и каталогов через контекстное меню файлового менеджера
  - Проблемы с использованием контекстного меню файлового менеджера
- Перетаскивание файлов и каталогов на окно графического интерфейса управления

Dr.Web Desktop Security Suite 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 нажатии значка приложения в панели задач правой кнопкой мыши;
- запуск проверки файлов и каталогов при помощи команды контекстного меню в графическом файловом менеджере;
- запуск проверки файлов и каталогов при перетаскивании их мышью на главное окно Dr.Web Desktop Security Suite.

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 Desktop Security Suite. Индикатор используется для отображения состояния приложения, а также для доступа к контекстному меню Dr.Web Desktop Security Suite. При наличии каких-либо проблем в

работе (например, устарели вирусные базы или заканчивается срок действия лицензии) на индикаторе поверх логотипа Dr.Web Desktop Security Suite отображается символ восклицательного знака: .

Помимо индикатора состояния, агент уведомлений также отображает всплывающие уведомления, информирующие пользователя о важных событиях в работе Dr.Web Desktop Security Suite, таких как:

- обнаружена угроза (в том числе, резидентными мониторами SpIDer Guard и SpIDer Gate);
- заканчивается срок действия лицензии.

При нажатии значка индикатора на экране открывается контекстное меню Dr.Web Desktop Security Suite:

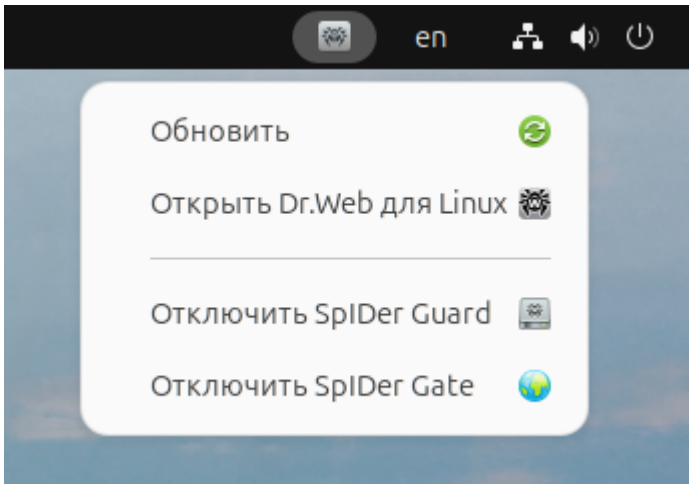


Рисунок 6. Контекстное меню индикатора Dr.Web Desktop Security Suite

При выборе пункта меню **Открыть Dr.Web Desktop Security Suite** на экране появляется окно графического интерфейса управления Dr.Web Desktop Security Suite, т. е. происходит его запуск. Выбор пунктов меню **Включить SpIDer Gate** или **Отключить SpIDer Gate** и **Включить SpIDer Guard** или **Отключить SpIDer Guard** позволяет запустить или завершить работу соответствующего монитора.

Для выключения любого монитора необходимо пройти аутентификацию, указав логин и пароль пользователя, обладающего административными правами (см. Управление правами приложения).

Выбор пункта **Обновить** принудительно запускает процедуру получения обновлений.

Если индикатор указывает на наличие проблем в функционировании Dr.Web Desktop Security Suite, 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 Desktop Security Suite 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

Запустить приложение можно путем выбора пункта **Dr.Web Desktop Security Suite** в меню **Приложения**. Если окружение рабочего стола поддерживает использование панели задач, то при запуске графического интерфейса Dr.Web Desktop Security Suite на панели задач появится кнопка со значком приложения. Нажатие кнопки запущенного приложения правой кнопки мыши откроет на экране контекстное меню, примерный вид которого показан на рисунке ниже (меню панели Ubuntu Dock).

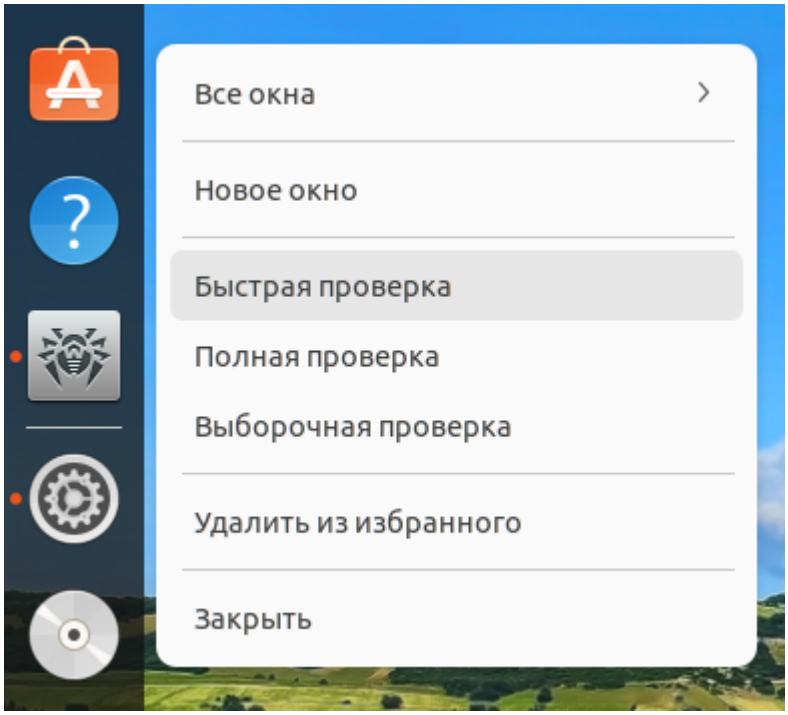


Рисунок 7. Контекстное меню Dr.Web Desktop Security Suite в панели задач

- Выбор пунктов меню **Быстрая проверка**, **Полная проверка** и **Выборочная проверка** позволяет запустить соответствующую задачу проверки (для **Выборочная проверка** — открыть страницу выбора объектов, подлежащих проверке).
- Выбор пункта меню **Dr.Web Desktop Security Suite** запускает графический интерфейс (если он 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 Desktop Security Suite** меню **Приложения** (вместо запуска через выполнение команды `drweb-`

`gui` в эмуляторе терминала или выбора пункта **Открыть Dr.Web Desktop Security Suite** в меню индикатора приложения в области уведомлений).

Проверка файлов и каталогов через контекстное меню файлового менеджера

Dr.Web Desktop Security Suite позволяет выполнять проверку файлов и каталогов непосредственно из окна графического файлового менеджера, например, Nautilus. Для проверки файлов и каталогов необходимо:

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

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



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

Если в файловом менеджере при помощи пункта контекстного меню **Открыть в другой программе** выбрать Dr.Web Desktop Security Suite, то некоторые графические среды для ОС GNU/Linux могут автоматически настроить ассоциацию файлов или каталогов (по MIME-типу этих объектов) с Dr.Web Desktop Security Suite. В этом случае открытие таких файлов и каталогов в файловом менеджере будет приводить к запуску Dr.Web Desktop Security Suite. Для исправления этой ситуации отмените настроенную ассоциацию.

Перетаскивание файлов и каталогов на окно графического интерфейса управления

Dr.Web Desktop Security Suite позволяет выполнять проверку файлов и каталогов путем перетаскивания их указателем мыши из окна обзора файлов и каталогов графического файлового менеджера на окно Dr.Web Desktop Security Suite. Чтобы началась проверка файлов и каталогов, перенесенных на окно приложения, необходимо, чтобы окно было открыто на главной странице или на странице выбора типа проверки. Если на странице окна Dr.Web Desktop Security Suite есть область с надписью **Перетащите сюда файлы**

или нажмите для выбора, то на эту страницу можно перетаскивать файлы и каталоги для проверки.

8.1.2. Запуск и завершение работы

Запуск графического интерфейса управления Dr.Web Desktop Security Suite

Для запуска графического интерфейса управления Dr.Web Desktop Security Suite необходимо:

- выбрать в системном меню **Приложения** пункт **Dr.Web Desktop Security Suite**, либо
- нажать правой кнопкой мыши на индикатор Dr.Web Desktop Security Suite в области уведомлений рабочего стола и выбрать в выпадающем меню пункт **Открыть Dr.Web Desktop Security Suite**.

Вы также можете запустить графический интерфейс управления Dr.Web Desktop Security Suite из командной строки, введя команду `drweb-gui&` в эмуляторе терминала.

Завершение работы графического интерфейса управления Dr.Web Desktop Security Suite

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



При завершении работы графического интерфейса Dr.Web Desktop Security Suite сервисные компоненты, включая агент уведомлений, мониторы SplDer Guard и SplDer Gate продолжают свою работу (если они не были отключены пользователем).

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

8.1.3. 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 SpIDer Guard, отображаются в виде списка на странице просмотра обнаруженных угроз.
- Управление угрозами, помещенными в карантин, осуществляется на странице работы с карантином.
- Настройка реакции Dr.Web Desktop Security Suite на обнаруженные угрозы осуществляется в окне настроек. Там же имеется возможность включить и настроить расписание периодических проверок, а также настроить проверку зашифрованных соединений.

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

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

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

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

Запуск проверки

Запустите процесс проверки объектов файловой системы, 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.

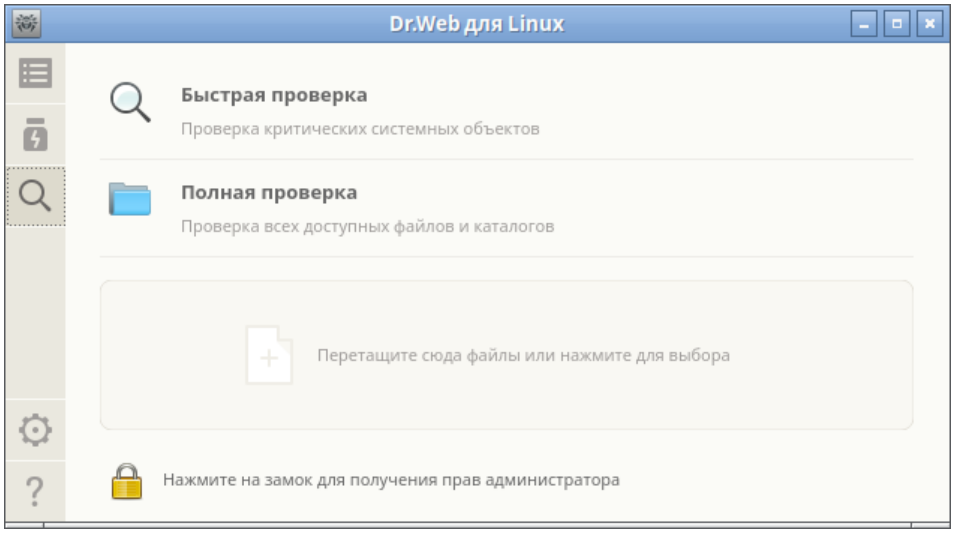


Рисунок 8. Выбор типа проверки

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

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

- **Перетаскивание указателем мыши**

  Файлы и каталоги, подлежащие проверке, можно перетащить мышью из окна файлового менеджера на открытую страницу выбора типа проверки (в зону,

отмеченную надписью **Перетащите сюда файлы или нажмите для выбора**). Также можно перетащить их на главную страницу окна Dr.Web Desktop Security Suite.

При перемещении файлов или каталогов указателем мыши на окно на нем отображается область, содержащая надпись **Поместите файлы сюда**. Для начала проверки выбранных файлов достаточно «бросить» их на страницу, отпустив кнопку мыши. После этого проверка начнется автоматически.

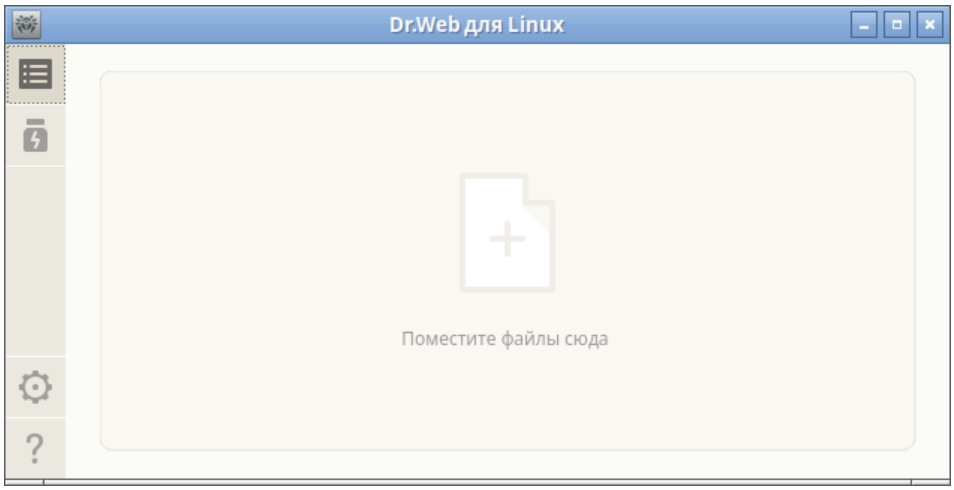


Рисунок 9. Область добавления файлов

- **Формирование списка объектов для выборочной проверки**

  Для формирования списка объектов для выборочной проверки необходимо нажать на область добавления файлов. В этом случае на экране откроется список объектов для выборочной проверки.

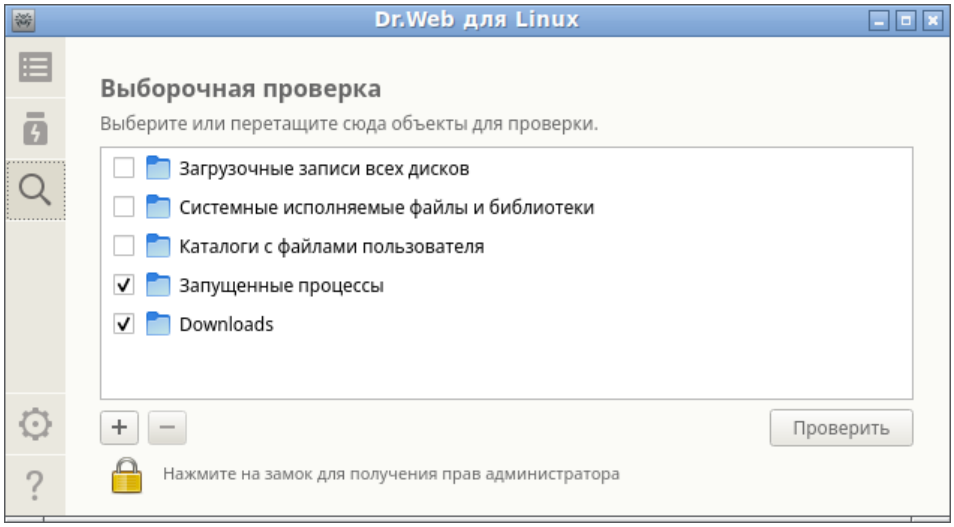


Рисунок 10. Список объектов для выборочной проверки

В списке есть четыре специальных пункта, задающих предопределенные группы объектов:

- *Загрузочные записи всех дисков* — все загрузочные записи всех доступных в системе дисков.
- *Системные исполняемые файлы и библиотеки* — все каталоги, содержащие системные исполняемые файлы (`/bin`, `/sbin` и т. д.).

- *Каталоги с файлами пользователя* — каталоги, содержащие файлы пользователя и текущего сеанса работы (домашний каталог `/home/<username>` (~), `/tmp`, `/var/mail`, `/var/tmp`).
- *Запущенные процессы* — 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, будут автоматически 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**.

Нажмите `–` под списком для удаления всех выделенных путей из списка (путь считается выделенным, если выделена строка списка, содержащая путь). Чтобы выделить более одного пути, выделяйте элементы списка с нажатой клавишей SHIFT или CTRL.

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.

Первые четыре предопределенных пункта удалить из списка нельзя.

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.

8.1.3.2. Проверка объектов по расписанию

В этом разделе

- Типы выполняемых проверок

- Запуск проверки

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

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

Типы выполняемых проверок

По расписанию можно выполнять следующие типы проверок:

- *Быстрая проверка* — проверка только жестко определенного набора критических системных объектов, подверженных наибольшему риску (загрузочные записи дисков, системные файлы и т. п.).
- *Полная проверка* — проверка всех объектов локальной файловой системы, доступных пользователю, от имени которого запущен Dr.Web Desktop Security Suite.
- *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.

8.1.3.3. Управление списком проверок

Перечень созданных и выполняющихся Сканером задач проверки объектов файловой системы и их результатов доступен на специальной странице окна Dr.Web Desktop Security Suite. 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).

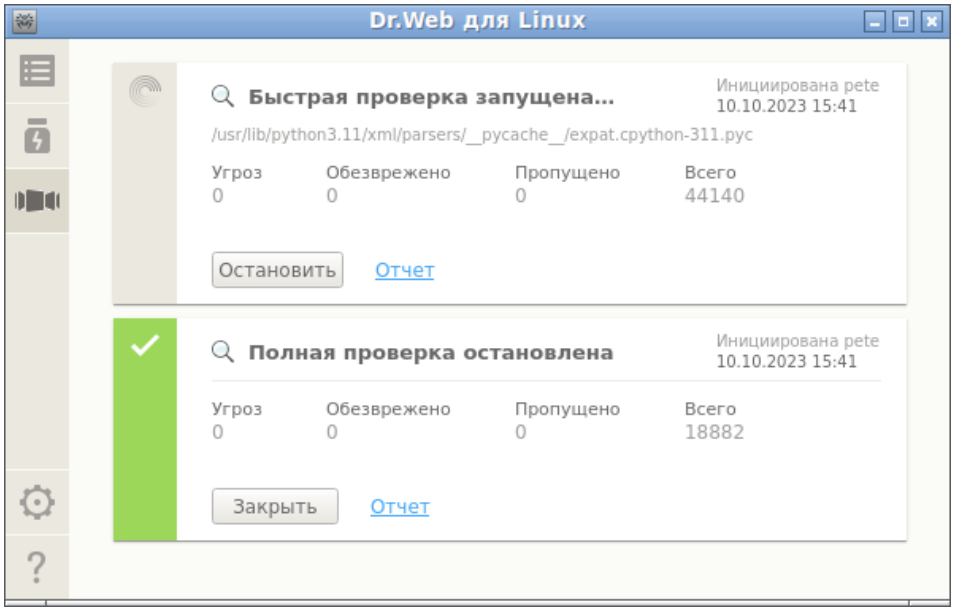


Рисунок 11. Список проверок

Для каждой задачи выводится следующая информация:

- тип проверки (*Быстрая проверка*, *Полная проверка*, *Выборочная проверка* или Проверка по расписанию);
- 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.



В списке отображаются только те проверки, выполняемые Сканером, которые были непосредственно инициированы пользователем в окне Dr.Web Desktop Security Suite, 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.

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

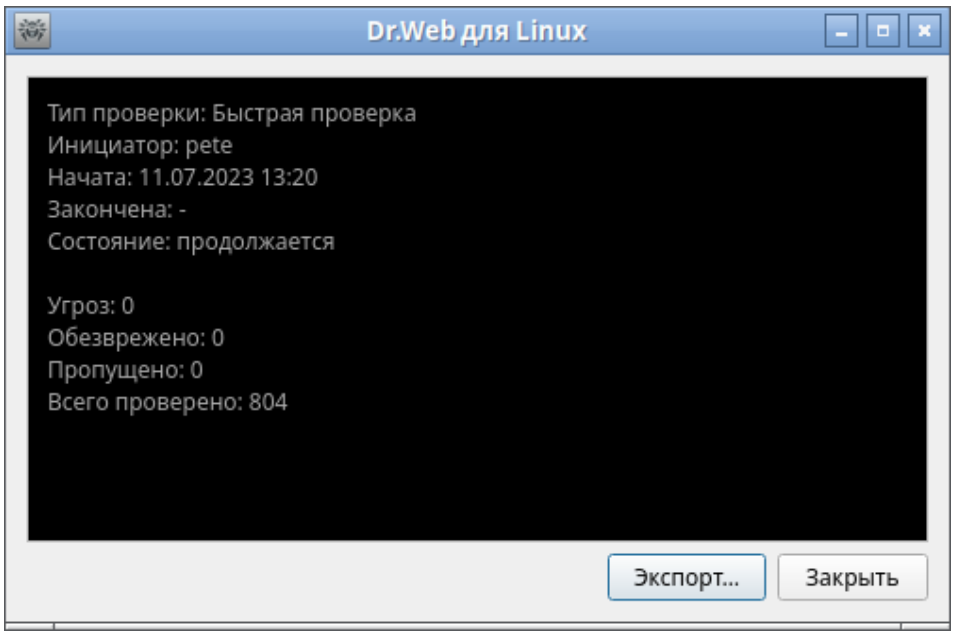


Рисунок 12. Детальная информация о проверке

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

Нажатие ссылки с названием обнаруженной угрозы откроет в веб-браузере, заданном по умолчанию, страницу с информацией об угрозе (производится переход на сайт компании «Доктор Веб», 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 Desktop Security Suite (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 проверки*.

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

8.1.3.4. 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 Desktop Security Suite позволяет управлять работой SpIDer Guard, а именно:

- запускать и останавливать монитор файловой системы;
- просматривать статистику работы компонента и перечень обнаруженных угроз;
- настраивать следующие параметры работы монитора файловой системы:
  - реакция на обнаружение угроз;
  - перечень исключений из проверки.

Управление работой монитора файловой системы

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

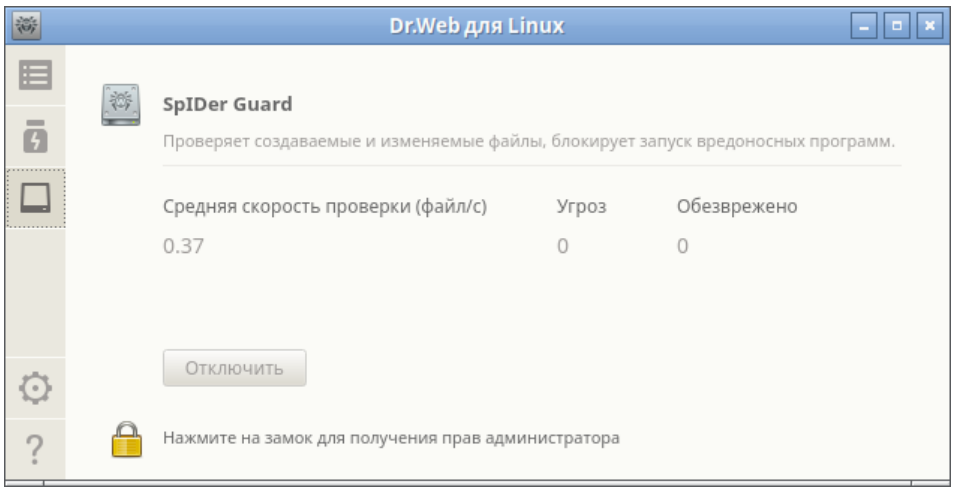


Рисунок 13. Управление работой SpIDer Guard

На странице управления мониторингом файловой системы выводится следующая информация:

- состояние монитора файловой системы SpIDer Guard (включен или отключен), а также сведения о произошедшей в процессе его работы ошибке, если она имела место;
- 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 Desktop Security Suite 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 он отключен пользователем или произошла ошибка.

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

Перечень угроз, обнаруженных SpIDer Guard в текущем сеансе работы Dr.Web Desktop Security Suite, 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 Ж.

8.1.3.5. 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, а также приложенных к письму вложений (в том числе на наличие признаков спама);
- файлов, загружаемых из интернета.

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

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

Графический интерфейс управления Dr.Web Desktop Security Suite 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:
  - 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 сообщениях 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 Desktop Security Suite. Чтобы перейти на эту страницу, нажмите **SpIDer Gate** на главной странице.



Рисунок 14. Управление 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. раздел Управление правами приложения.

Возможность включения и выключения монитора сетевых соединений SpIDer Gate при работе Dr.Web Desktop Security Suite 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 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 Ж. Описание известных ошибок.

8.1.3.6. 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 Desktop Security Suite, отображается на специальной странице окна, которая доступна только в том случае, если была обнаружена хотя бы одна угроза.

Если были обнаружены угрозы, то, чтобы открыть страницу со списком угроз, нажмите  на навигационной панели.

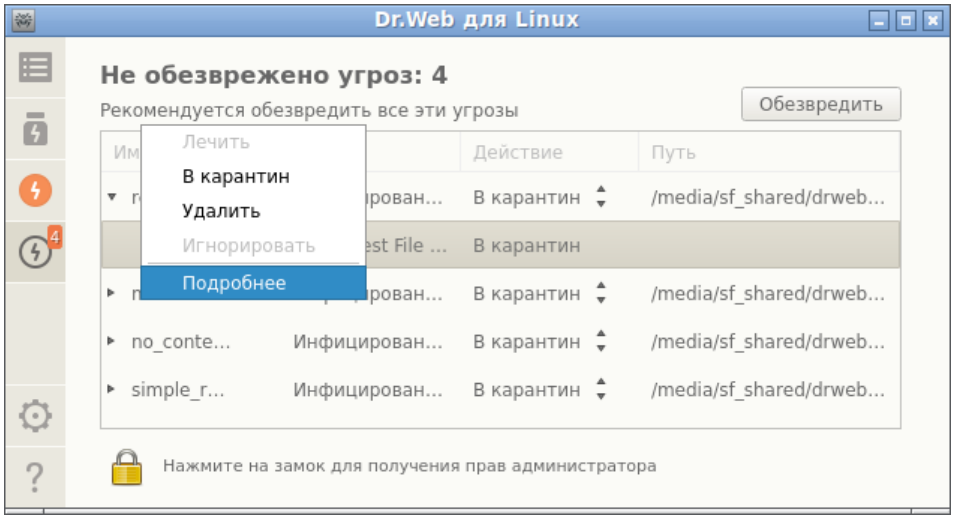


Рисунок 15. Обзор угроз

В списке для каждой обнаруженной угрозы выводится следующая информация:

- имя объекта, содержащего угрозу;
- имя угрозы, содержащейся в объекте, по классификации компании «Доктор Веб»;

- действие, которое будет применено к объекту для нейтрализации угрозы (или уже было применено, если угроза нейтрализована);
- путь к объекту файловой системы, в котором эта угроза была обнаружена.

Уже обезвреженные угрозы в списке представлены в списке неактивными строками.

Обезвреживание обнаруженных угроз

Если в списке имеются необезвреженные угрозы, то на странице, непосредственно над списком, будет доступна кнопка **Обезвредить**, при нажатии которой к каждой необезвреженной угрозе, представленной в списке, будет применено действие по ее обезвреживанию, указанное в поле **Действие**. 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 SpIDer 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 угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), то контейнер будет не удален, а помещен в карантин.

Если требуется применить к угрозе действие, отличное от представленного в списке, нажмите поле **Действие** в строке угрозы и выберите требуемое действие в контекстном меню.

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 выделения и выберите требуемое действие в появившемся выпадающем списке. Выбранное действие будет применено ко всем выделенным угрозам.

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.

При 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 строку информации об угрозе правой кнопкой мыши 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 их в списке мышью, удерживая нажатой клавишу CTRL перед вызовом контекстного меню.

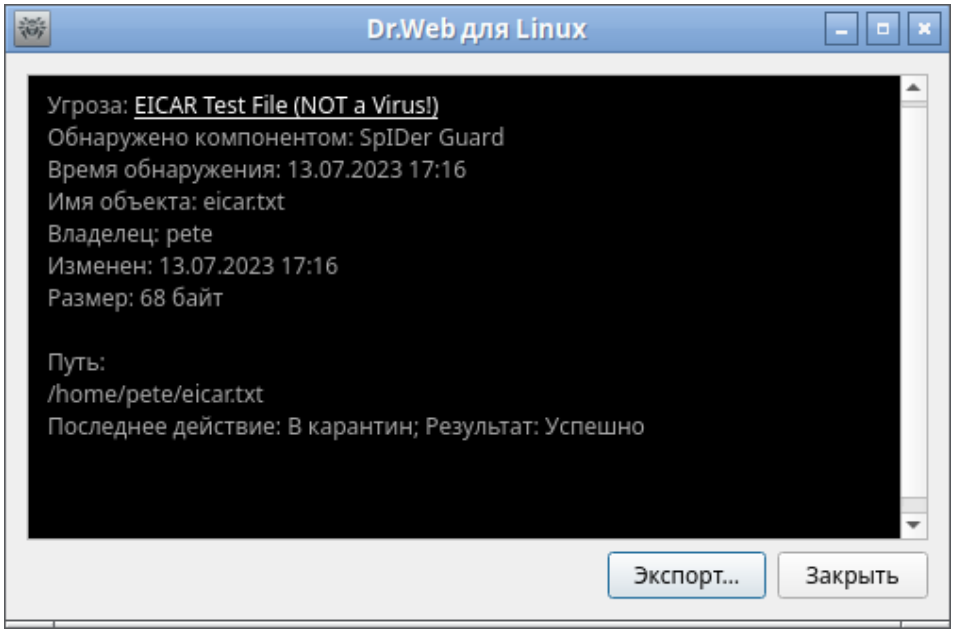


Рисунок 16. Информация об угрозе

В этом окне отображается следующая информация:

- имя угрозы по классификации компании «Доктор Веб»;
- название компонента Dr.Web Desktop Security Suite, 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 странице окна настроек).

Нажмите ссылку с именем угрозы, чтобы открыть веб-страницу с ее описанием (происходит переход на сайт компании «Доктор Веб», 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**.

8.1.3.7. Управление карантином

В этом разделе

- Общие сведения
- Применение действий к изолированным объектам
- Просмотр информации об изолированных объектах

Общие сведения

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

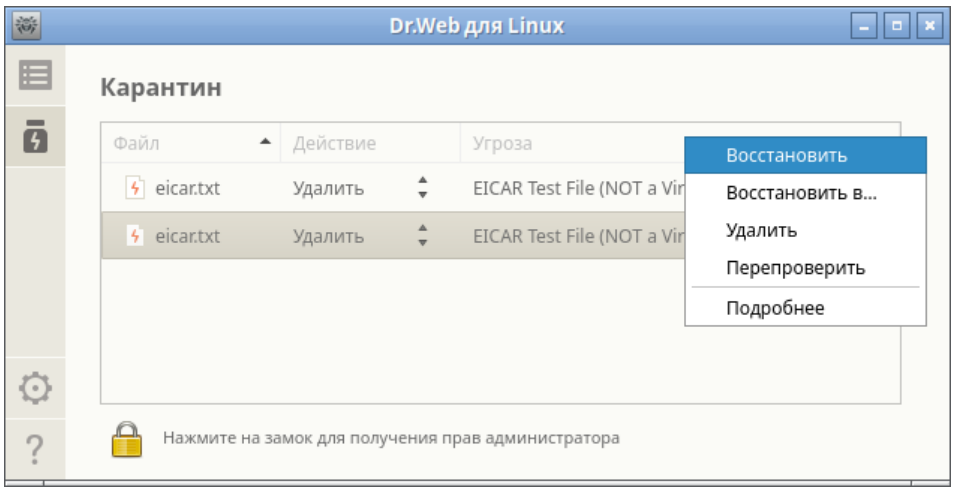


Рисунок 17. Управление карантином

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 компании «Доктор Веб».

Применение действий к изолированным объектам

Для применения какого-либо действия к изолированному в карантине объекту нажмите строку, содержащую информацию об объекте, правой кнопкой мыши и выберите требуемое действие в контекстном меню. Если требуется применить какое-либо действие к нескольким изолированным объектам, 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 контекстном 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 лечение, если это возможно.

Если выбранное действие применяется к выделенному объекту успешно, его строка исчезает из таблицы. Если попытка оказывается неудачной, то 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 другим пользователем.

Просмотр информации об изолированных объектах

Для получения детальной информации о любом изолированном объекте нажмите строку информации об этом объекте правой кнопкой мыши 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.

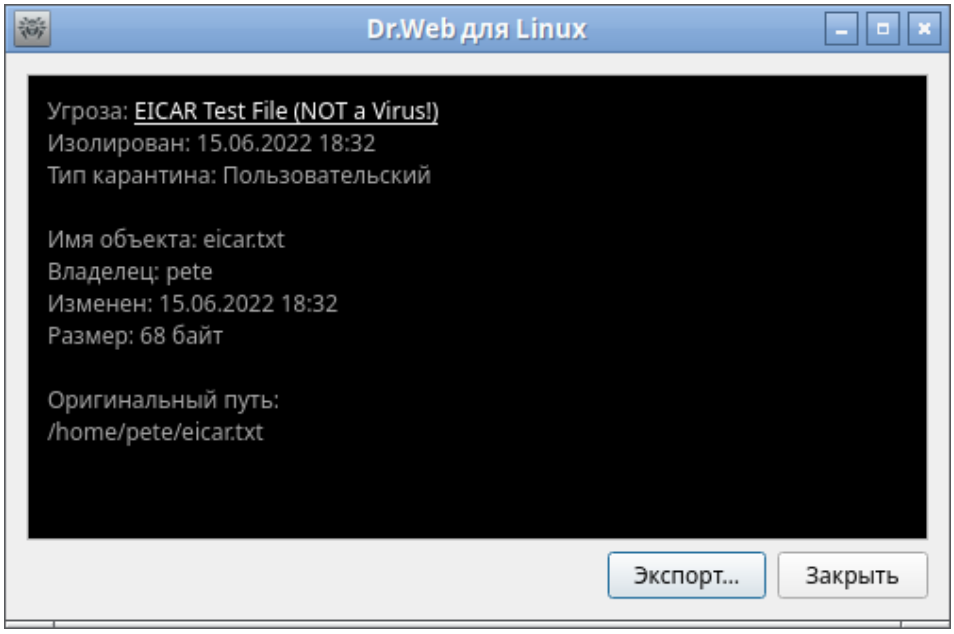


Рисунок 18. Информация об изолированном объекте

В этом окне отображается следующая информация:

- имя угрозы по классификации компании «Доктор Веб»;
- дата и время изоляции объекта в карантине;
- тип карантина, в котором 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.

Нажмите ссылку с именем угрозы, чтобы открыть веб-страницу с ее описанием (происходит переход на сайт компании «Доктор Веб», требуется подключение к интернету).

Нажмите **Экспорт**, чтобы сохранить информацию, показанную в окне, в текстовый файл (откроется окно выбора файла). Чтобы закрыть окно с подробной информацией об угрозе и содержащем ее объекте, нажмите **Закрыть**.

8.1.4. Обновление антивирусной защиты

В этом разделе

- Общие сведения
- Настройка обновлений
- Обновление без подключения к интернету
- Проблемы в работе компонента обновлений

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 Desktop Security Suite. Вирусные базы считаются устаревшими спустя сутки с момента последнего успешного обновления. Чтобы перейти на страницу управления обновлением, нажмите **Последнее обновление** на главной странице.

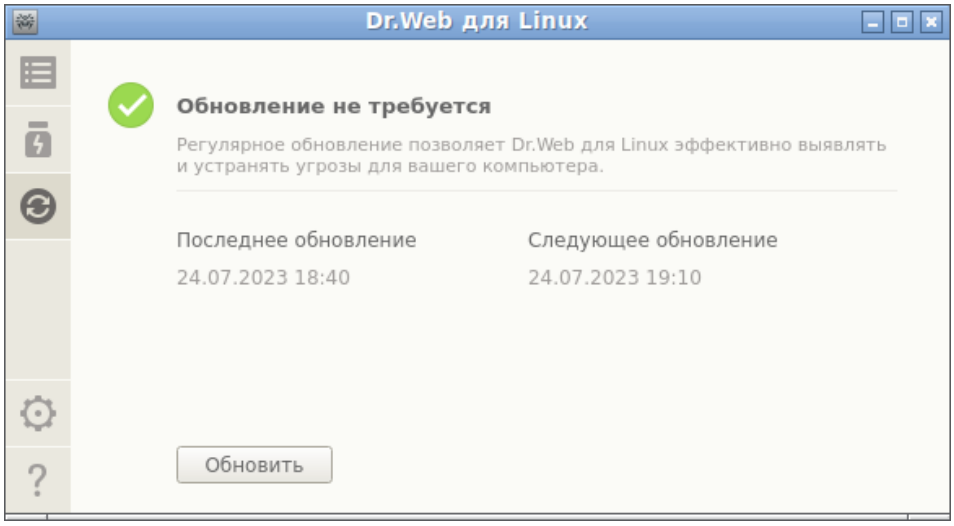


Рисунок 19. Управление обновлением

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 Desktop Security Suite работает в режиме централизованной защиты, эта страница будет заблокирована.

Настройка обновлений

Настройка обновлений Dr.Web Desktop Security Suite производится в окне настроек на вкладке **Основные**.

Обновление без подключения к интернету

Обновление антивирусной защиты без подключения к интернету доступно только при использовании командной строки. Примеры команд можно найти в соответствующем разделе.

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 Ж.

8.1.5. Менеджер лицензий

В этом разделе

- Общие сведения
- Запуск Менеджера лицензий
- Активация лицензии
  - Активация лицензии или демонстрационного периода при помощи серийного номера
  - Получение демонстрационного периода
  - Установка имеющегося ключевого файла
- Удаление лицензионного ключевого файла

Общие сведения

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

Запуск Менеджера лицензий

Менеджер лицензий интегрирован в окно Dr.Web Desktop Security Suite. 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 Desktop Security Suite, 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.

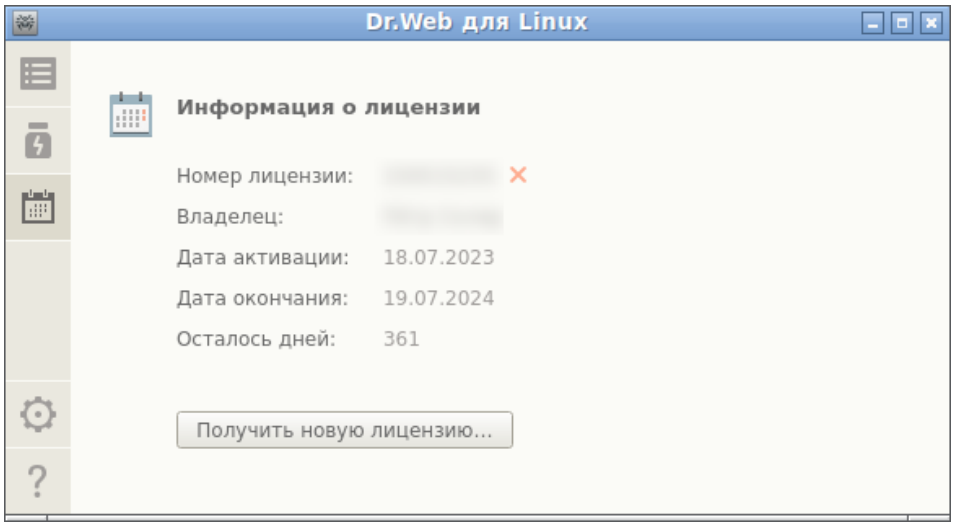


Рисунок 20. Информация о лицензии

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 Desktop Security Suite, нажмите **Получить новую лицензию**. После этого на экране появится мастер регистрации. Мастер регистрации также отображается автоматически при первом запуске Dr.Web Desktop Security Suite после его установки.

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.

Активация лицензии или демонстрационного периода при помощи серийного номера

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

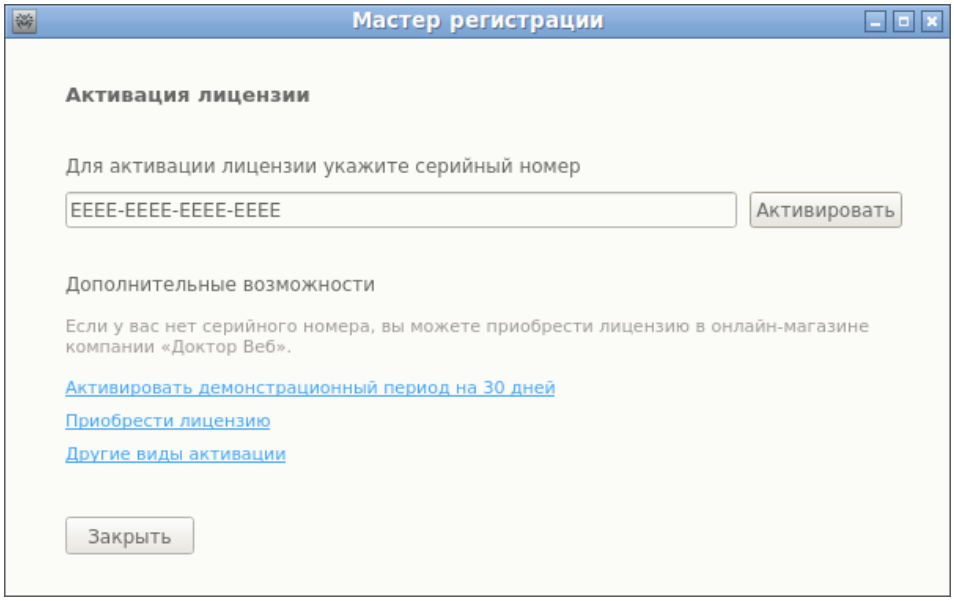


Рисунок 21. Регистрация при помощи серийного номера

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

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 Desktop Security Suite. Если вы выберете вариант **На двух компьютерах**, то второй серийный номер из этого комплекта вы сможете активировать еще на одном компьютере и получить второй лицензионный ключевой файл. При этом для обоих компьютеров выданные лицензии будут действительны в течение одинакового срока (например, 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).

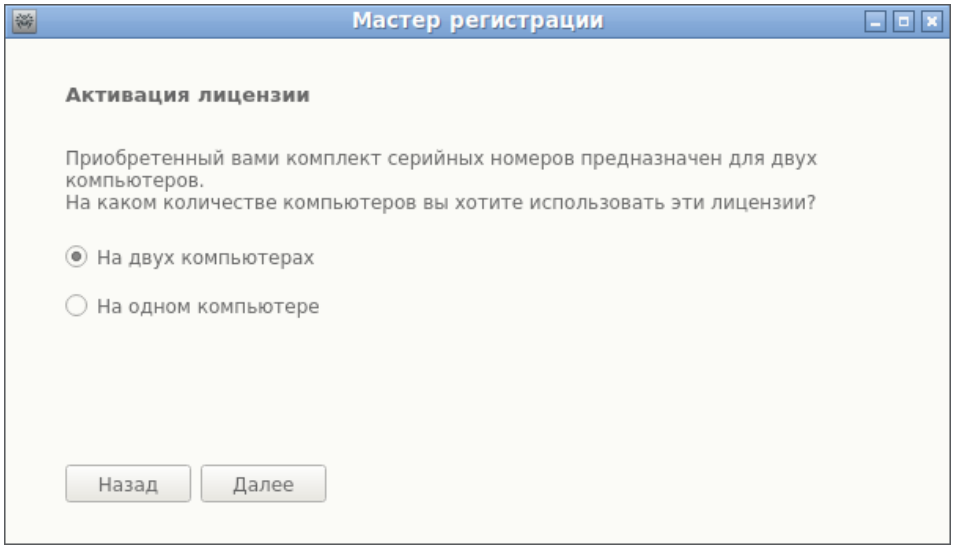


Рисунок 22. Выбор количества компьютеров

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**.

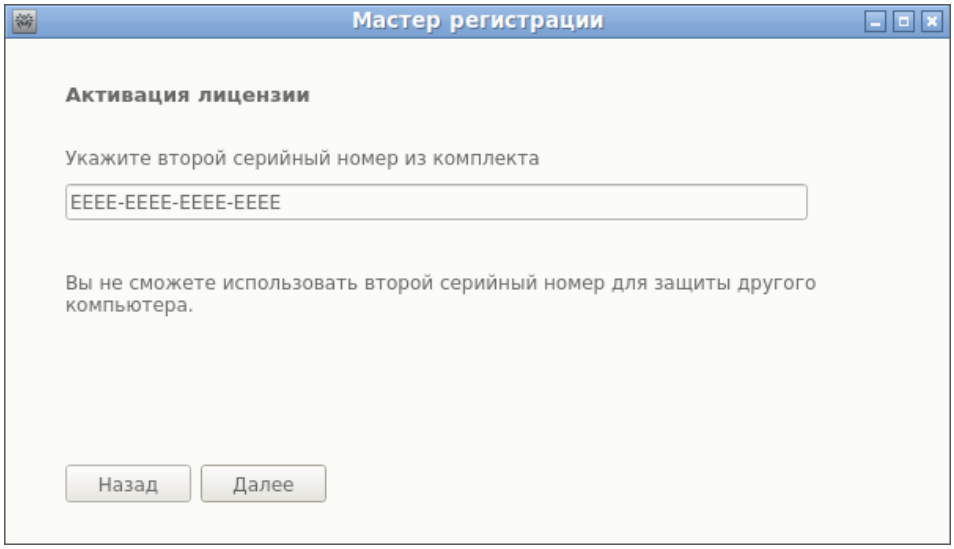


Рисунок 23. Указание второго серийного номера из комплекта

Для продолжения активации нажмите **Далее**.

На следующем шаге вам будет предложено указать предыдущую лицензию.

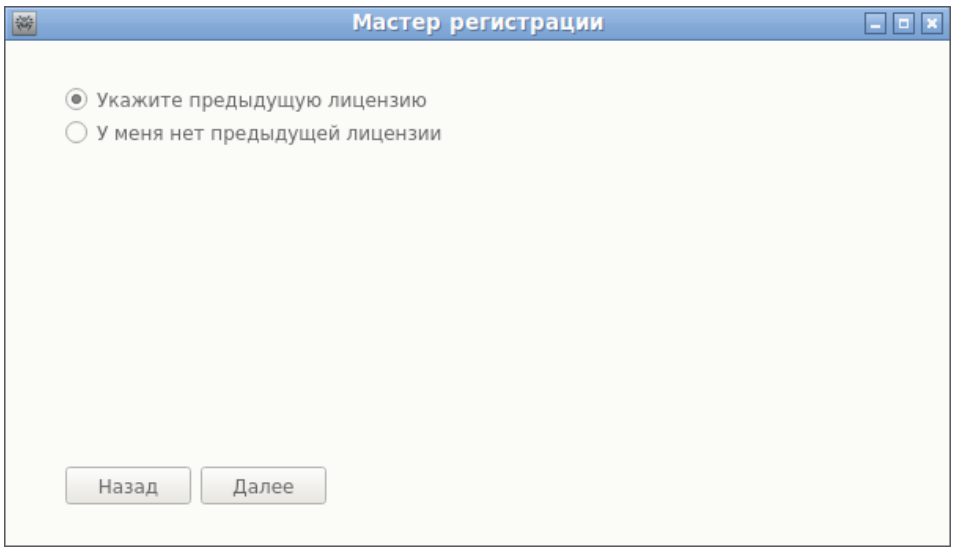


Рисунок 24. Предложение указать предыдущую лицензию

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

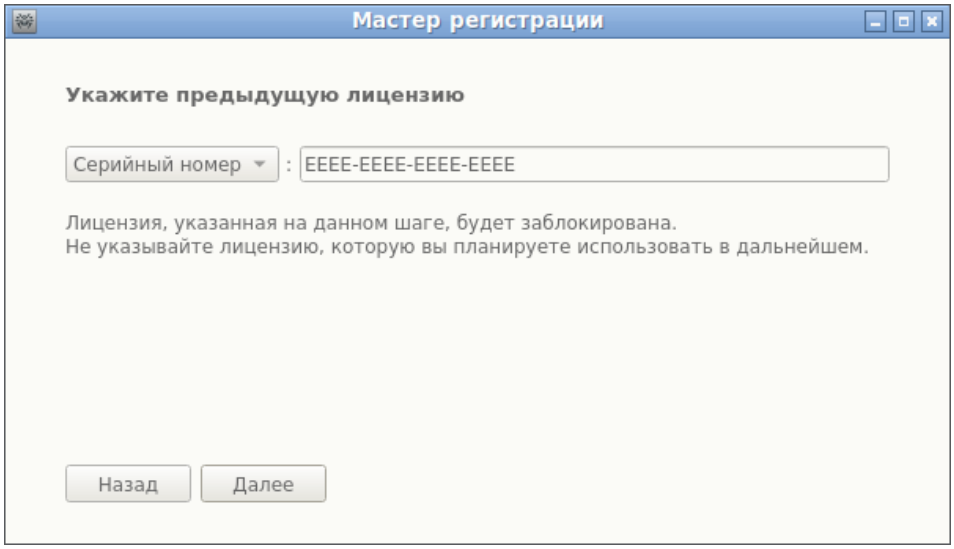


Рисунок 25. Указание предыдущей лицензии

Если вы укажете на этом шаге лицензию, срок действия которой еще не истек, то срок действия активируемой лицензии будет дополнительно продлен на остаток срока действия старой лицензии.

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

- ввести путь к нему непосредственно в поле ввода;
- воспользоваться стандартным окном выбора файлов графической оболочки, нажав **Обзор**;
- перетащить его мышью на страницу мастера регистрации из окна файлового менеджера.

Можно указать файл архива `.zip`, 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.

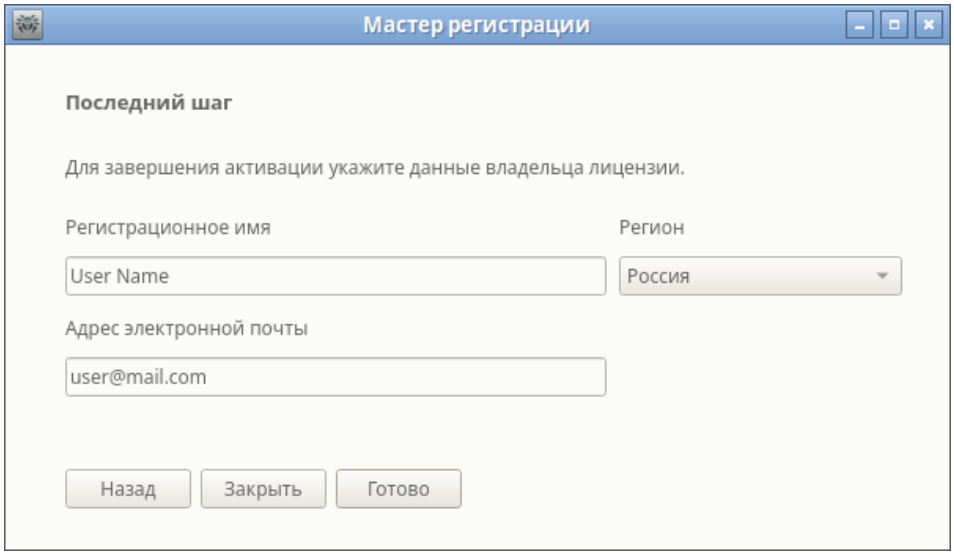


Рисунок 26. Регистрационная информация пользователя

После заполнения всех полей формы нажмите **Готово** для подключения к серверу и получения лицензионного ключевого файла. При необходимости вы можете перенести полученный лицензионный ключевой файл на любой компьютер при условии, что вы удалите его с текущего компьютера.

Получение демонстрационного периода

Если требуется получить демонстрационный период для работы Dr.Web Desktop Security Suite 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.

Установка имеющегося ключевого файла

Если вы уже имеете действующую лицензию и связанный с ней ключевой файл (возможно, полученный от компании «Доктор Веб» или ее партнеров по электронной почте), то вы можете активировать Dr.Web Desktop Security Suite, 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.

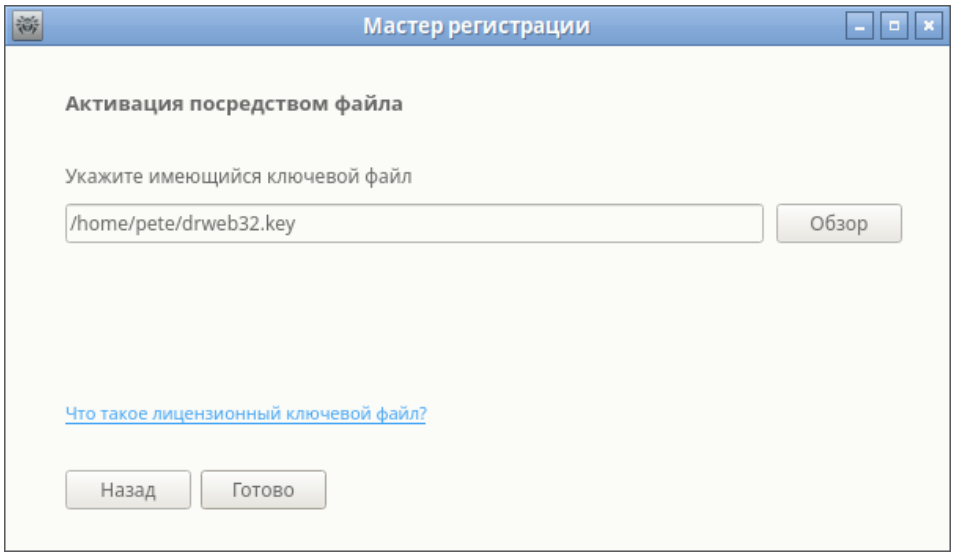


Рисунок 27. Активация посредством ключевого файла

Для указания ключевого файла вы можете:

- ввести путь к нему непосредственно в поле ввода;
- воспользоваться стандартным окном выбора файлов графической оболочки, нажав **Обзор**;
- перетащить его мышью на страницу мастера из окна файлового менеджера.

Можно указать файл архива `.zip`, 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 Desktop Security Suite. 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 Desktop Security Suite.

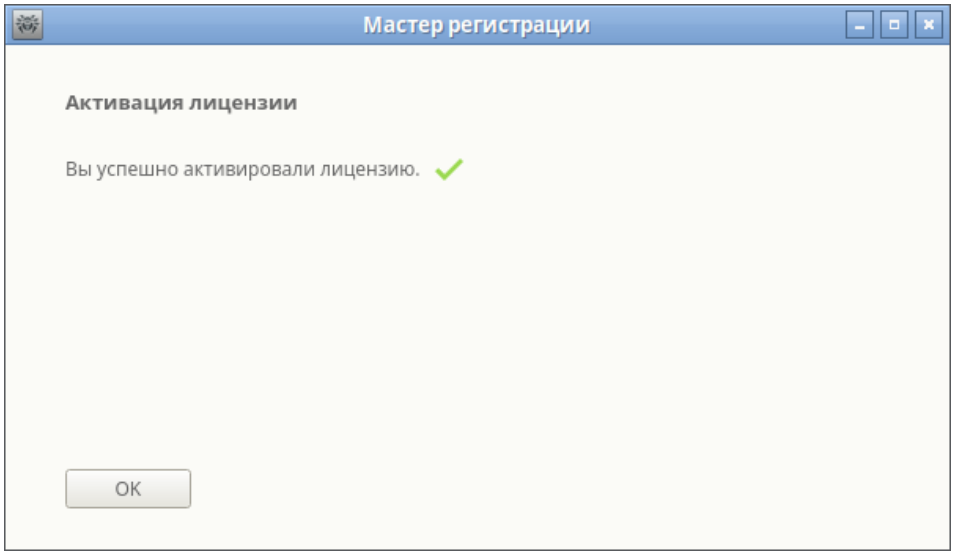


Рисунок 28. Сообщение об успешной активации

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.

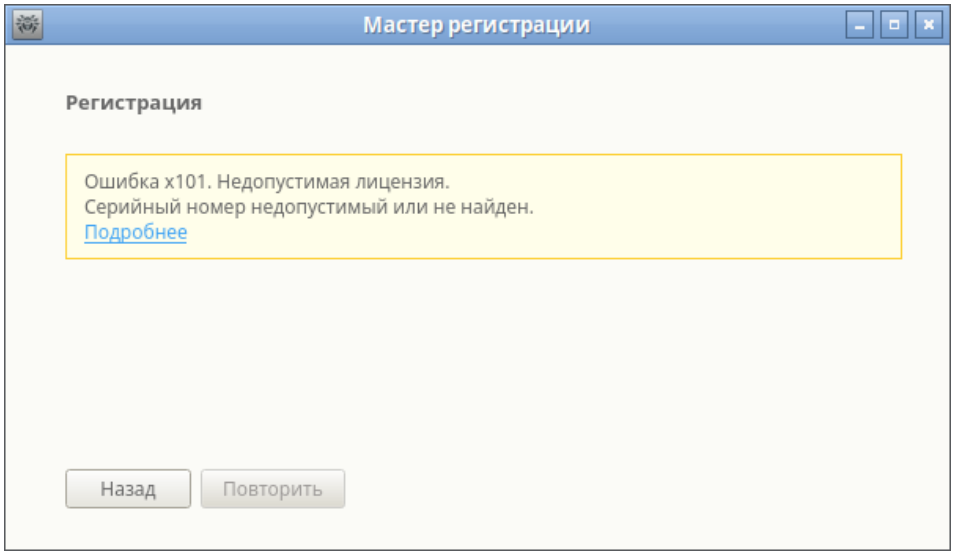


Рисунок 29. Сообщение об ошибке

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

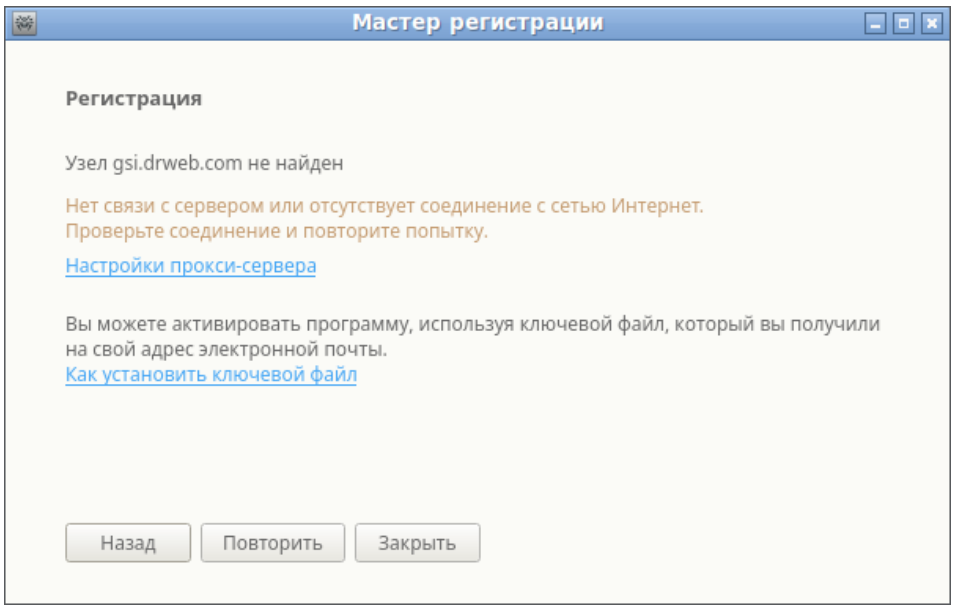


Рисунок 30. Ошибка подключения к серверу регистрации

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:

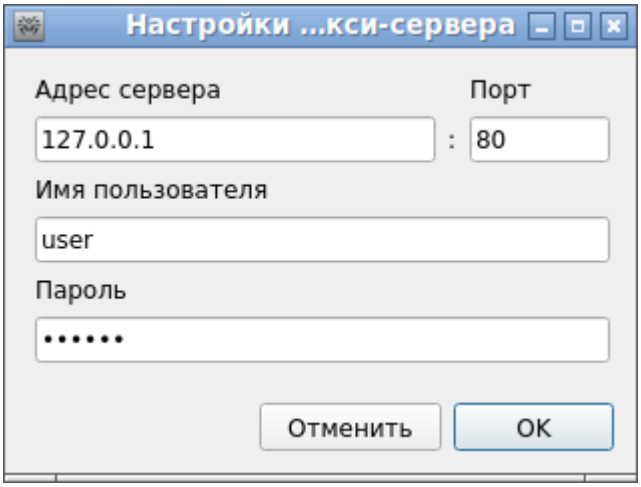


Рисунок 31. Настройки прокси-сервера

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

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

Удаление лицензионного ключевого файла

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

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

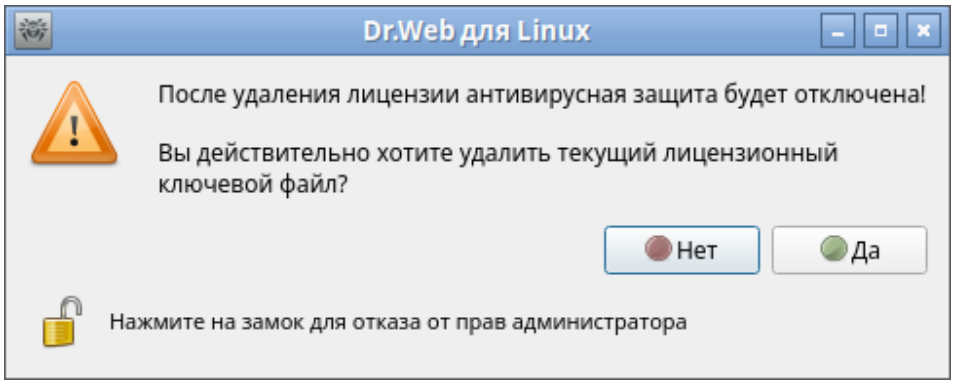


Рисунок 32. Подтверждение удаления ключевого файла

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

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

8.1.6. Просмотр сообщений от сервера централизованной защиты

В этом разделе

- Общие сведения
- Применение действий к сообщениям

- Фильтрация сообщений

Общие сведения

Если Dr.Web Desktop Security Suite работает под управлением сервера централизованной защиты, доступен интерфейс для просмотра сообщений о состоянии антивирусной сети, рассылаемых сервером на управляемые им станции. Этот 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 Desktop Security Suite. В противном случае просмотр сообщений недоступен и соответствующая страница не отображается на главном окне Dr.Web Desktop Security Suite.

Интерфейс просмотра сообщений от сервера отображается на специальной странице.

Чтобы ее открыть, нажмите  на навигационной панели.

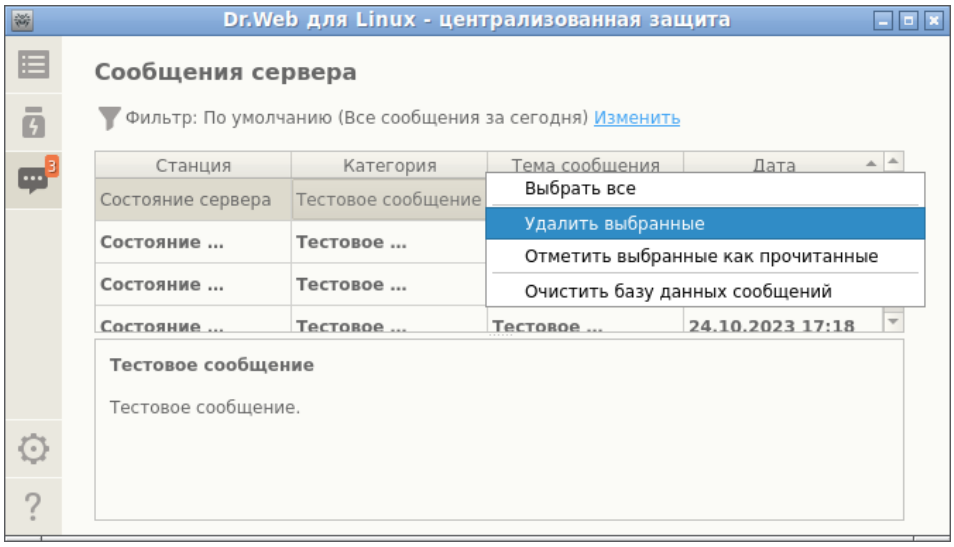


Рисунок 33. Сообщения сервера централизованной защиты

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. Непросмотренные 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 применения какого-либо действия к сообщению нажмите строку, содержащую информацию о сообщении, правой кнопкой мыши и выберите требуемое действие в контекстном меню. Если нужно применить какое-либо действие к нескольким сообщениям, 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 контекстном 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, непрочитанные).

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 искомых 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.

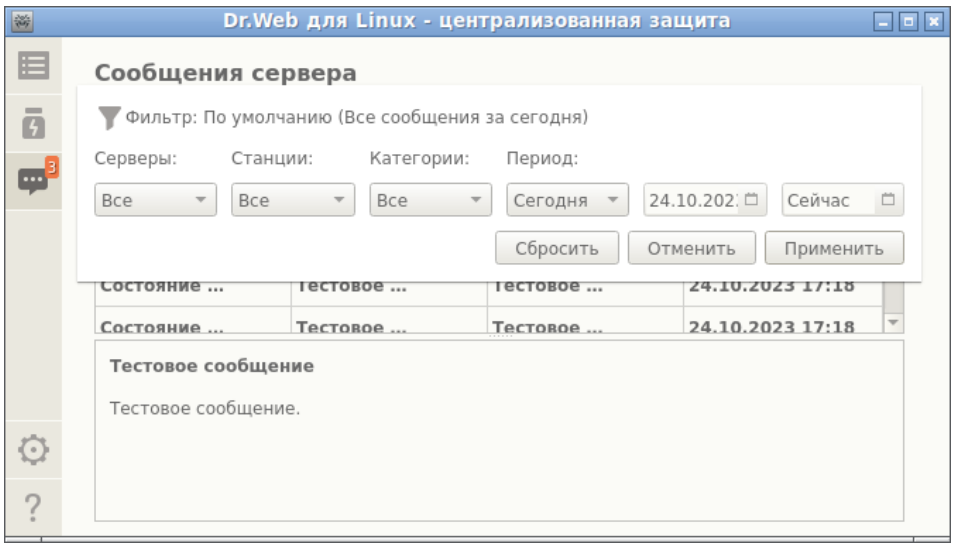


Рисунок 34. Панель фильтра сообщений

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**.

8.1.7. Управление правами приложения

Некоторые действия в окне Dr.Web Desktop Security Suite 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:

- управление объектами, помещенными в системный карантин (а именно, в каталог карантина, не принадлежащий пользователю, запустившему Dr.Web Desktop Security Suite);
- проверка файлов и каталогов, принадлежащих другим пользователям (в частности, суперпользователю);
- выключение монитора файловой системы SpIDer Guard;
- выключение монитора сетевых соединений SpIDer Gate;

- удаление лицензионного ключевого файла, подключение и отключение от сервера централизованной защиты.

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

На всех страницах окна Dr.Web Desktop Security Suite, функциональность которых зависит от наличия у приложения повышенных прав, расположена специальная кнопка с изображением замка. Состояние замка показывает, обладает ли в данный момент окно Dr.Web Desktop Security Suite 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, а именно, к отказу от прав суперпользователя и возврату к исходным правам обычного пользователя.

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

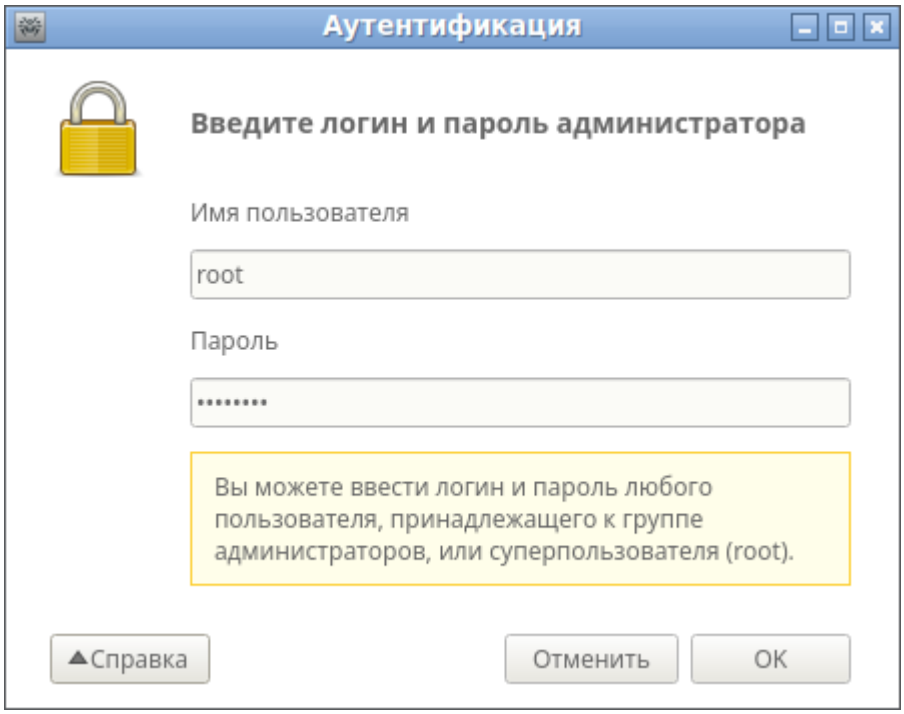


Рисунок 35. Окно аутентификации

Для получения приложением прав суперпользователя укажите имя (логин) и пароль любого пользователя, включенного в группу пользователей, указанную в настройках Dr.Web Desktop Security Suite как *группа администраторов*, или логин и пароль суперпользователя (пользователя *root*), и нажмите **OK**. 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 Desktop Security Suite 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 (пользователя *root*).

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

8.1.8. Справочные материалы

Для доступа к справочным материалам нажмите  на навигационной панели окна Dr.Web Desktop Security Suite.

На экране появится выпадающее меню, содержащее следующие пункты:

- **Справка** — открыть краткое Руководство пользователя Dr.Web Desktop Security Suite.
- **Форум Dr.Web** — открыть в браузере страницу форума пользователей продуктов компании «Доктор Веб» (требуется подключение к интернету).
- **Техническая поддержка** — открыть в браузере страницу службы технической поддержки компании «Доктор Веб» (требуется подключение к интернету).
- **Мой Dr.Web** — открыть в браузере персональную страницу пользователя продуктов компании «Доктор Веб» (требуется подключение к интернету).
- **О программе** — открыть окно с краткой информацией о Dr.Web Desktop Security Suite и его версии.

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

8.1.9. Настройка работы

В окне настроек Dr.Web Desktop Security Suite можно настроить следующие параметры работы:

- периодичность выполнения обновлений;
- реакцию Dr.Web Desktop Security Suite 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 или централизованный);
- использование сервиса Dr.Web Cloud.

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 Desktop Security Suite на угрозы, обнаруживаемые Сканером в процессе проверки по требованию и по расписанию.
- SpIDer Guard — позволяет настроить реакцию Dr.Web Desktop Security Suite 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 или централизованный), в котором работает Dr.Web Desktop Security Suite.
- Dr.Web Cloud — позволяет разрешить или запретить Dr.Web Desktop Security Suite 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 Desktop Security Suite работает в режиме централизованной защиты, то некоторые настройки могут быть заблокированы и недоступны для изменения.

8.1.9.1. 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.

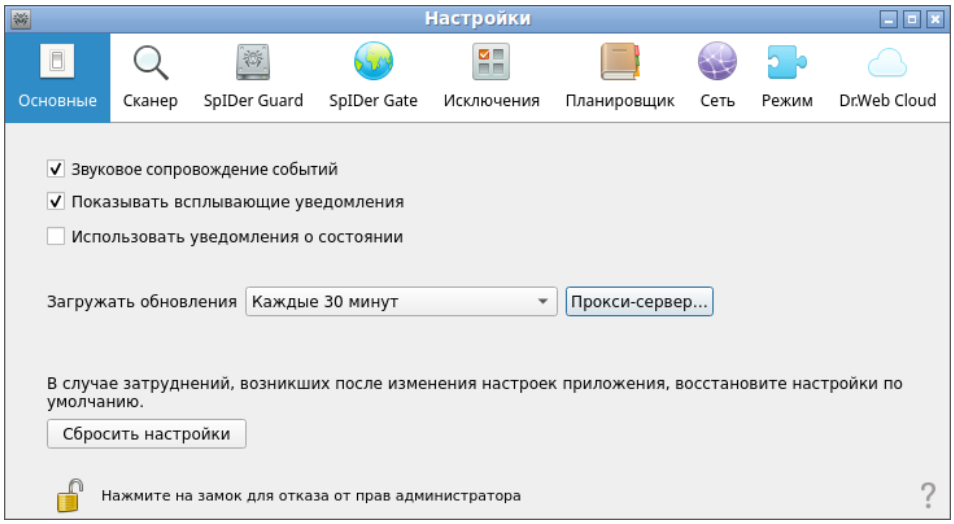


Рисунок 36. Основные настройки

Элемент управления	Действие
Флажок **Звуковое сопровождение событий**	Установка этого флажка предписывает Dr.Web Desktop Security Suite проигрывать звуковые уведомления при возникновении таких событий, как: • обнаружение угрозы (Сканером или SpIDer Guard); • ошибка проверки объекта; • и т. п.
Флажок **Показывать всплывающие уведомления**	Установка этого флажка предписывает Dr.Web Desktop Security Suite при работе в режиме графического рабочего стола отображать на экране всплывающие уведомления при возникновении таких событий, как: • обнаружение угрозы; • ошибка проверки; • и т. п.
Флажок **Использовать уведомления о состоянии**	Установка этого флажка предписывает Dr.Web Desktop Security Suite показывать всплывающие уведомления при изменении состояния компонентов (например, в случае их включения или отключения). Используется альтернативный механизм отображения

Элемент управления	Действие
	всплывающих уведомлений, что может быть полезно, например, если среда рабочего стола не поддерживает отображение значка Dr.Web Desktop Security Suite в области уведомлений. Если эта функция не поддерживается средой рабочего стола, то на вкладке **Основные** этого флажка не будет.
Выпадающий список **Загружать обновления**	Позволяет выбрать периодичность автоматического обновления вирусных баз, баз категорий веб-ресурсов и антивирусного ядра.
Кнопка **Прокси-сервер**	Открывает окно настройки прокси-сервера для получения обновлений. Прокси-сервер может понадобиться, 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. раздел Управление правами приложения).

Настройки прокси-сервера, используемого для получения обновлений

В окне настройки прокси-сервера 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.

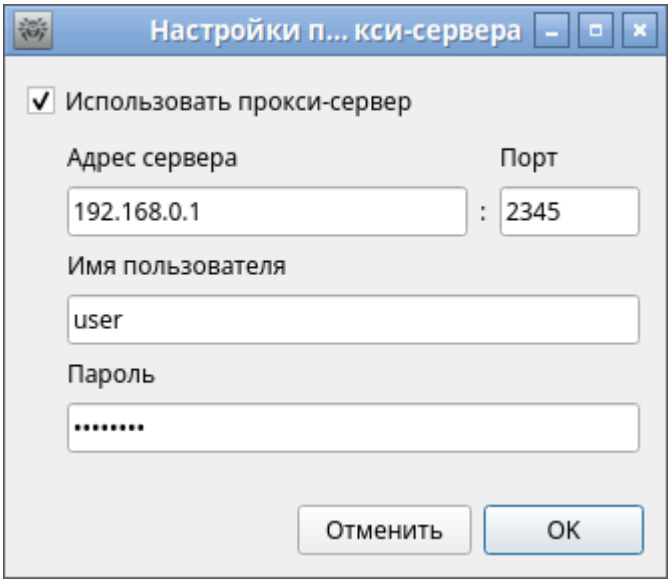


Рисунок 37. Настройки прокси-сервера

Обязательно укажите адрес и порт для использования прокси-сервера. В качестве адреса можно использовать как IP-адрес, так и FQDN узла, на котором работает прокси-сервер. 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**.

8.1.9.2. Настройки проверки файлов

В этом разделе

- Общие сведения
- Дополнительные настройки проверки файлов

Общие сведения

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

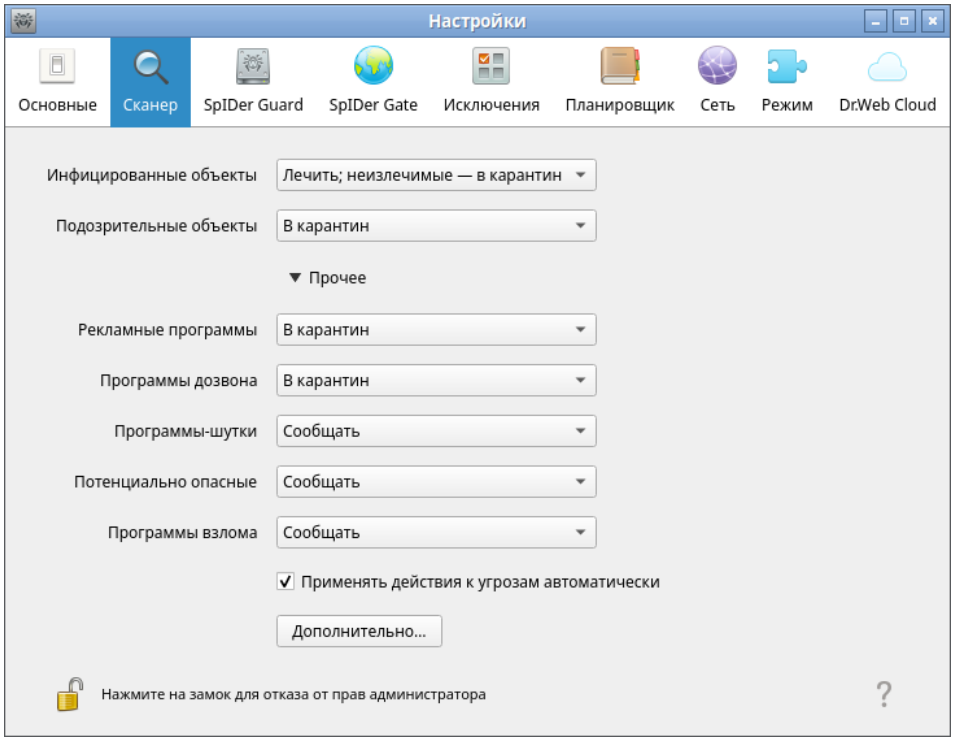


Рисунок 38. Настройки Сканера

В выпадающих списках выберите действия, которые Dr.Web Desktop Security Suite 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 Desktop Security Suite 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, то 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 SpIDer 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. раздел Управление правами приложения).

Возможность настройки Сканера при работе Dr.Web Desktop Security Suite 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.

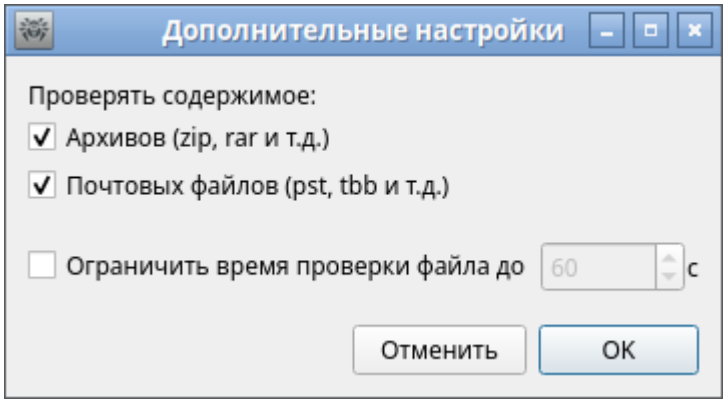


Рисунок 39. Дополнительные настройки проверки файлов

Если флажки проверки содержимого контейнеров не включены, то 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**.

8.1.9.3. Настройки мониторинга файловой системы

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

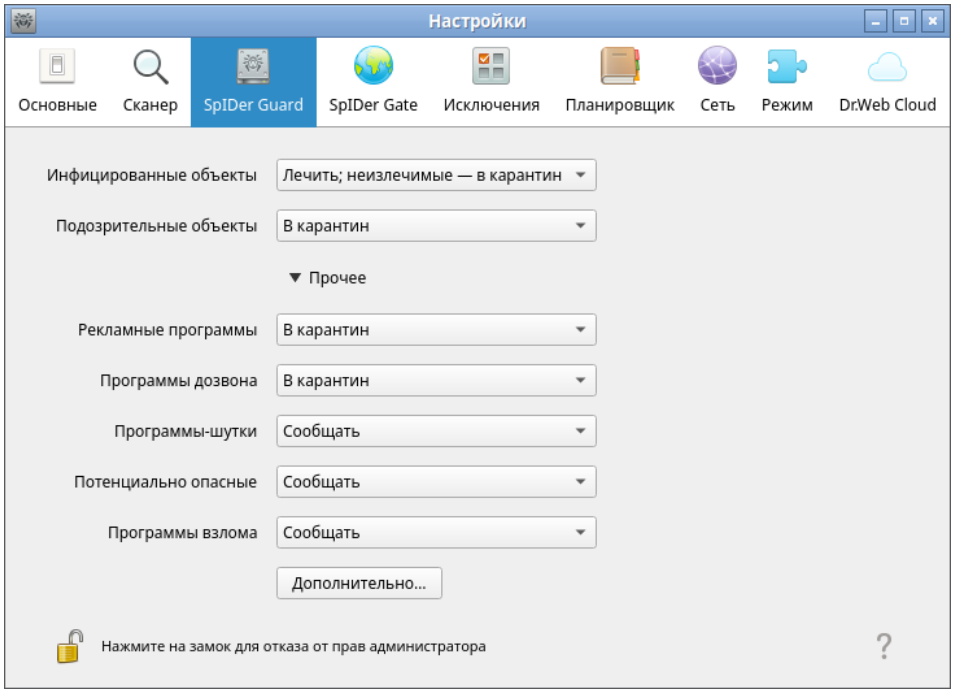


Рисунок 40. Настройки мониторинга файловой системы

Эта вкладка, включая окно дополнительных настроек, аналогична вкладке **Сканер**, где заданы настройки проверки файлов.

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

Замечания:

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

Для изменения настроек монитора файловой системы SpIDer Guard необходимо, чтобы приложение обладало повышенными правами (см. раздел Управление правами приложения).

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

8.1.9.4. Настройки мониторинга сетевых соединений

В этом разделе

- Общие сведения
- Выбор категорий 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.

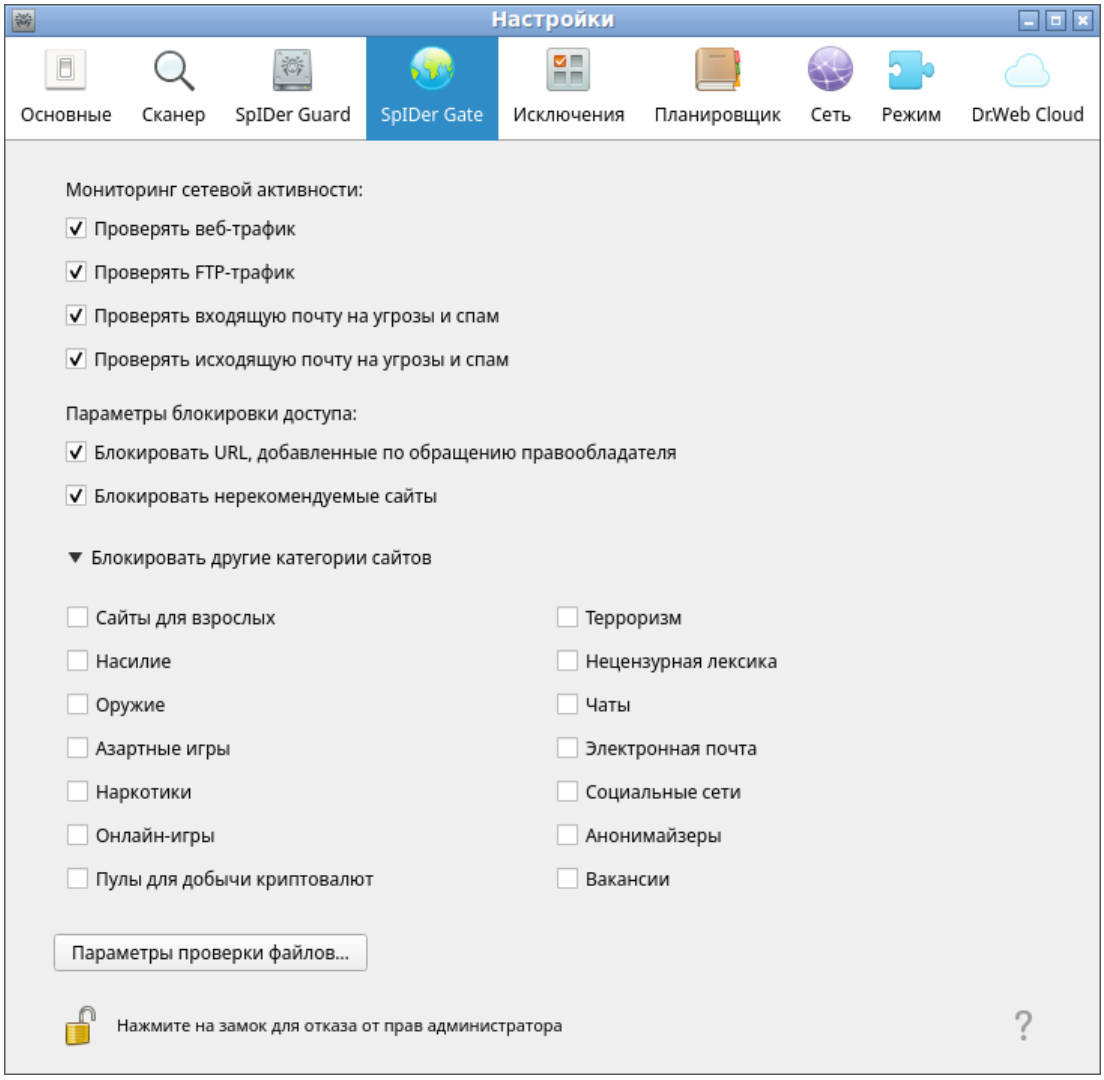


Рисунок 41. Настройки контроля доступа к сети

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

Выбор категорий сайтов

Флажки в разделе **Параметры мониторинга** определяют, доступ к 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 флажки, вы можете запретить или разрешить доступ к 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

Категория	Описание
Пулы для добычи криптовалют	Сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи («майнинга») криптовалют
Вакансии	Сайты для поиска работы



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

Один и тот же сайт может быть отнесен сразу к нескольким различным категориям. Монитор сетевых соединений SpIDer Gate будет блокировать доступ к сайту или узлу, если он попадает хотя бы в одну из категорий, включенных для запрета доступа. Нажмите надпись **Блокировать другие категории сайтов**, чтобы показать или скрыть перечень доступных категорий.

Если нужно заблокировать доступ к какому-либо сайту или узлу, не относящемуся ни к одной из указанных категорий, включите его в черный список. Если же нужно разрешить доступ к некоторому сайту или узлу, несмотря 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 должны контролироваться монитором SpIDer Gate.

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



Существует особая категория — *Источники распространения угроз*. Доступ к 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**.

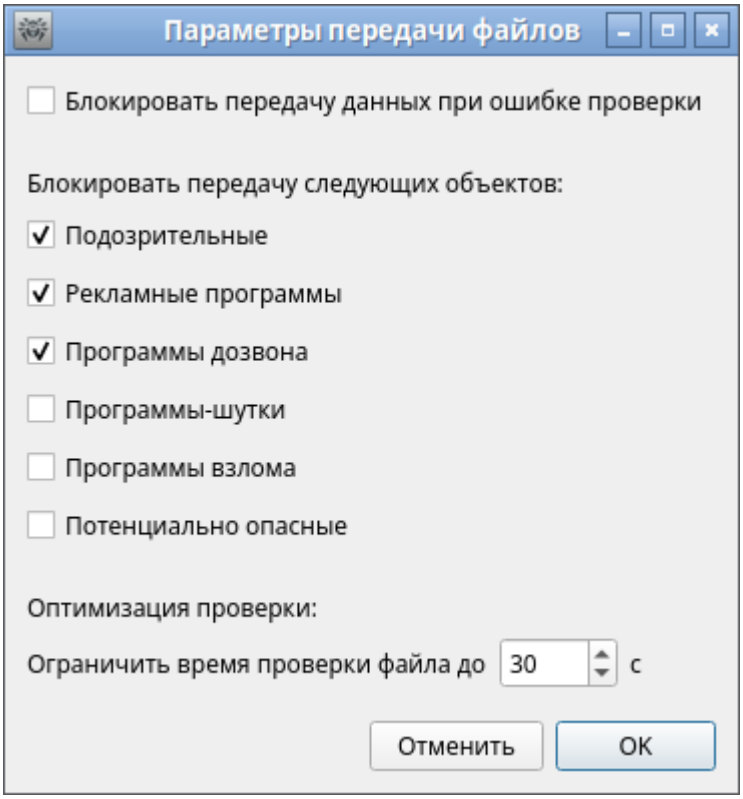


Рисунок 42. Настройки проверки файлов

В появившемся окне вы можете указать, какие категории вредоносных объектов нужно блокировать при попытке их передачи. Если флажок установлен, то загрузка файлов, содержащих угрозу соответствующего типа, будет блокироваться. Если флажок снят, то файлы, содержащие угрозы этого типа, будут загружаться из интернета. Также вы можете также установить максимальный интервал времени, отводимый на проверку загружаемых файлов. Если установлен флажок **Блокировать передачу данных при ошибке проверки**, то файлы, которые не удалось проверить из-за возникновения ошибки, будут блокироваться при загрузке.

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

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.

Правила мониторинга сетевых соединений могут быть отредактированы вручную. Настройка компонента вручную описана в Руководстве администратора Dr.Web Gateway Security Suite, раздел Компоненты Dr.Web Gateway Security Suite ⇒ Dr.Web Firewall для Linux ⇒ Параметры конфигурации ⇒ Правила проверки трафика и блокировки доступа. Внесение изменений вручную может повлиять на стандартную настройку фильтров, выполненную до этого посредством графического интерфейса.

8.1.9.5. Настройка исключений

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

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

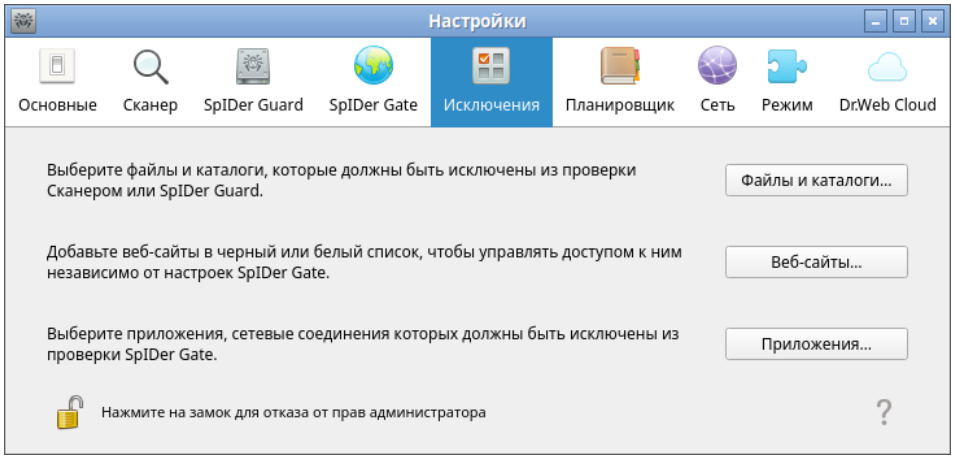


Рисунок 43. Настройка исключений

Для добавления и удаления объектов из списка исключений необходимо, чтобы приложение обладало повышенными правами (см. раздел Управление правами приложения).

8.1.9.5.1. 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 SpIDer Guard. Если указан каталог, то будет пропущено все содержимое этого каталога, включая подкаталоги и вложенные файлы.

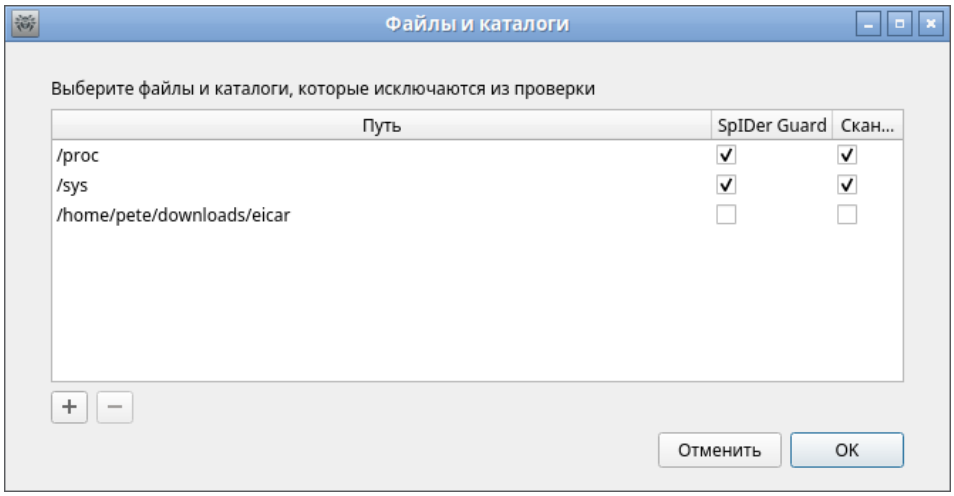


Рисунок 44. Настройка исключений файлов и каталогов

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 SpIDer 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 SpIDer Guard, установите соответствующий флажок в строке объекта. Чтобы исключить объект, представленный в списке, из перечня объектов, исключаемых из проверки Сканером или SpIDer 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 **ОК**; для закрытия окна без сохранения внесенных изменений нажмите **Отменить**.

8.1.9.5.2. Черный и белый списки сайтов

В этом разделе

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

Общие сведения

Управление черными и белыми списками сайтов осуществляется в окне **Управление списками**. Для открытия окна нажмите **Сайты** на вкладке **Исключения**.

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

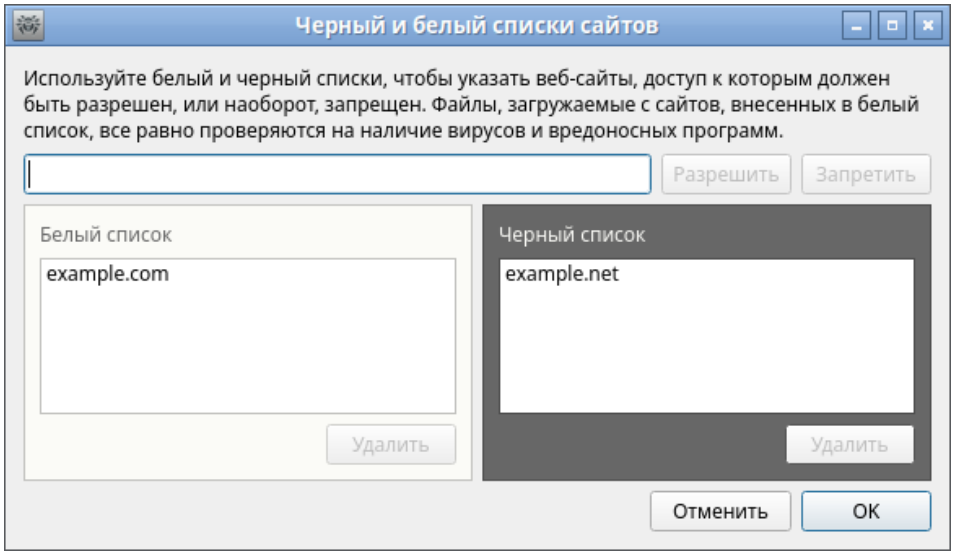


Рисунок 45. Окно управления черным и белым списками

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

Чтобы блокировать сайты из черного списка, использующие протокол HTTPS, разрешите монитору SplDer Gate проверять трафик, передаваемый через защищенные сетевые соединения.

Добавление и удаление сайтов из черного и белого списка

- Для добавления 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 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**.

8.1.9.5.3. 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.

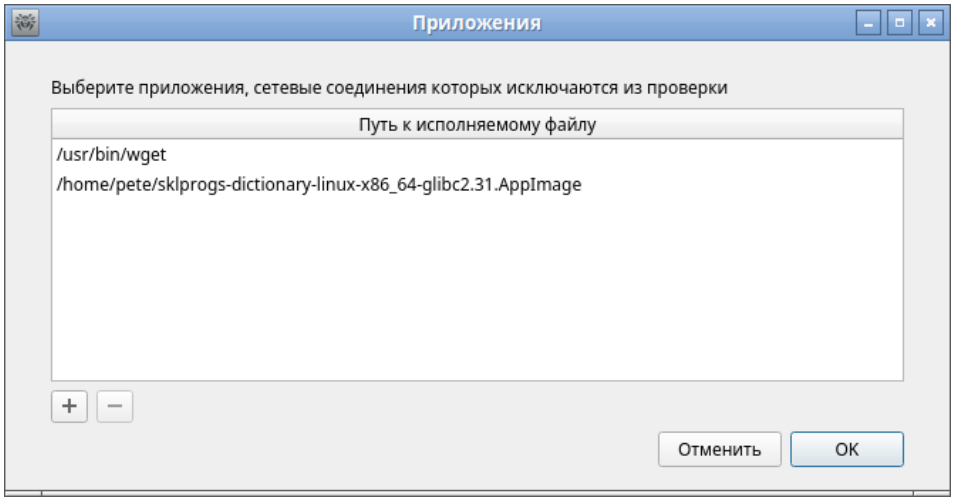


Рисунок 46. Настройка исключений сетевых соединений приложений

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**.

8.1.9.6. 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.

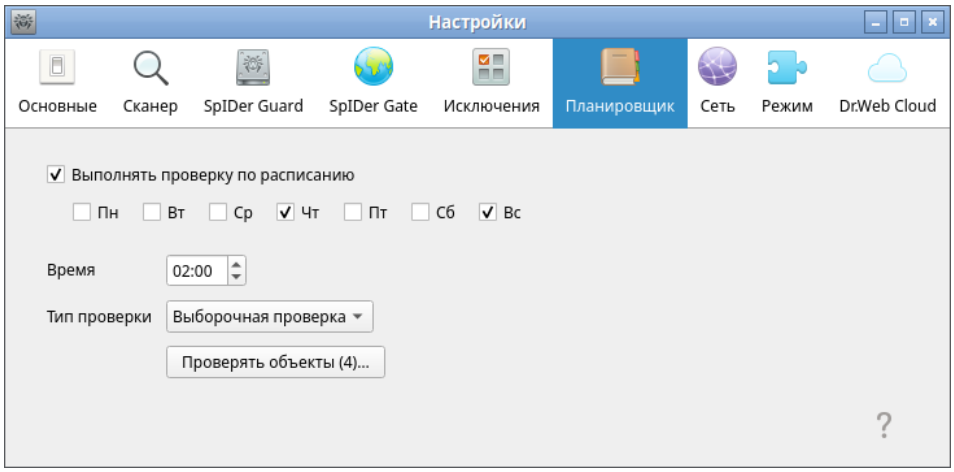


Рисунок 47. Настройка проверки по расписанию

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

Проверки по заданному расписанию будут запускаться с указанной периодичностью агентом уведомлений, либо непосредственно графическим интерфейсом управления, если он запущен в момент начала проверки. Проверки по расписанию не запускаются, если Dr.Web Desktop Security Suite работает под управлением сервера централизованной защиты или 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 выборочной проверки объектов по расписанию, аналогичное окну выборочной проверки по требованию. Вы можете

добавить объекты в список, нажав +, либо перетащив 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.

8.1.9.7. 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.

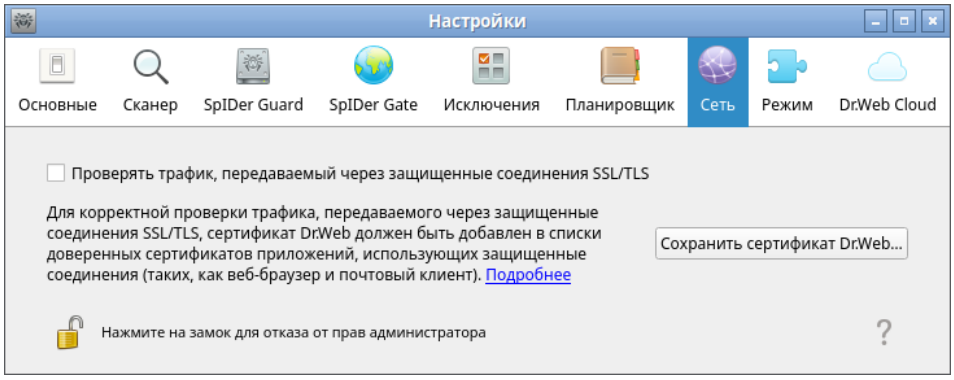


Рисунок 48. Настройка защиты от угроз, передаваемых через сеть

Настройка проверки защищенных сетевых соединений

Чтобы разрешить 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 какого-либо 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 путь 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 сайтов, для идентификации пользователей электронной почты и 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 путь 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 сайтов, для идентификации пользователей электронной почты и 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 для сохранения в формате PEM):

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

Далее добавьте сертификат в системное хранилище. В разных дистрибутивах GNU/Linux эта операция выполняется с помощью разных команд.

- В Ubuntu, Debian, Mint:

```
# apt-get update
# apt-get install ca-certificates
# mkdir -p /usr/local/share/ca-certificates
# cp <cert_name>.pem /usr/local/share/ca-certificates/<cert_name>.crt
# update-ca-certificates
```

- В CentOS и Fedora:

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

8.1.9.8. 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 Desktop Security Suite к серверу централизованной защиты (переведя его в режим централизованной защиты) или отключиться от сервера централизованной защиты (в этом случае Dr.Web Desktop Security Suite будет работать в автономном режиме).

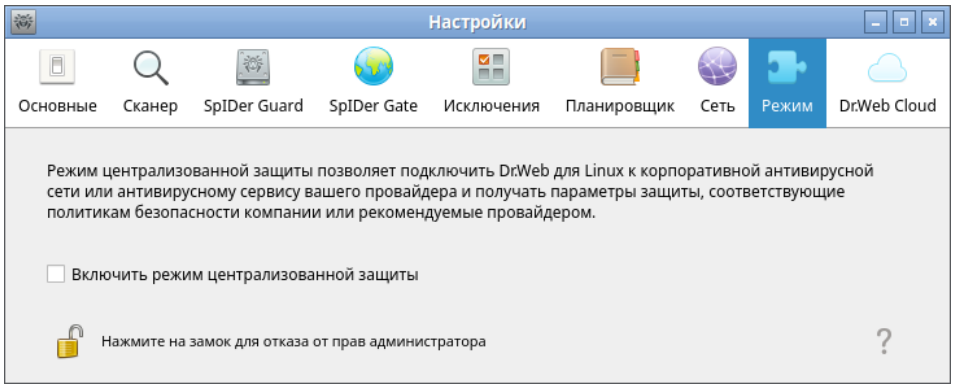


Рисунок 49. Управление режимом работы

Чтобы подключить Dr.Web Desktop Security Suite к серверу централизованной защиты или отключиться от него, установите или сбросьте соответствующий флажок.

Для подключения Dr.Web Desktop Security Suite 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:

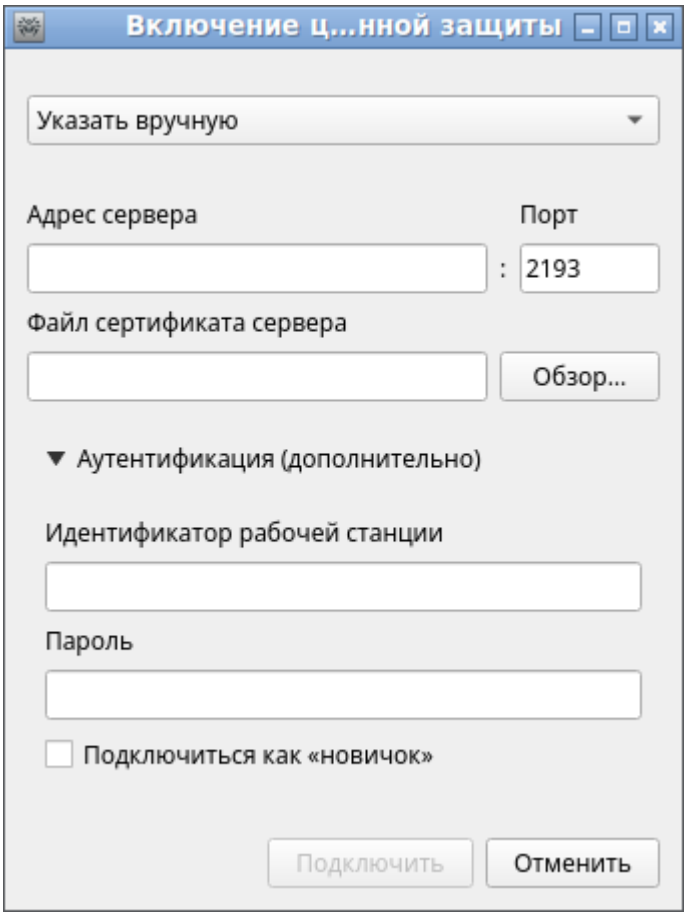


Рисунок 50. Подключение к серверу централизованной защиты

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

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

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.



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 Desktop Security Suite к серверу централизованной защиты, он будет работать под управлением сервера до тех пор, пока вы его не переведете в автономный режим. Подключение к серверу будет происходить автоматически каждый раз при запуске операционной системы (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 Desktop Security Suite 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 Desktop Security Suite. 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 Desktop Security Suite. В противном случае просмотр сообщений недоступен и выпадающий список **Максимальное время хранения сообщений от сервера** не отображается на странице настроек режима защиты.

8.1.9.9. Настройка использования Dr.Web Cloud

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

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

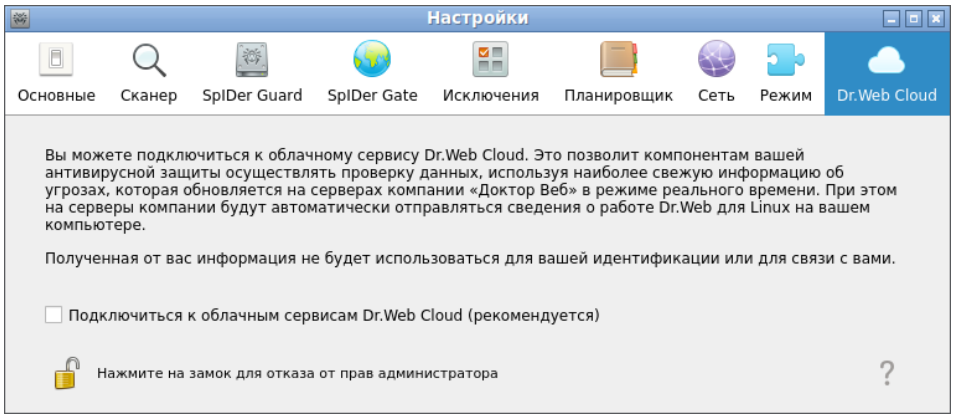


Рисунок 51. Управление сервисом Dr.Web Cloud

Чтобы разрешить или запретить Dr.Web Desktop Security Suite использовать сервис Dr.Web Cloud, установите или сбросьте соответствующий флажок.

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

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

8.1.10. Дополнительно

8.1.10.1. Аргументы командной строки

Чтобы запустить графический интерфейс управления Dr.Web Desktop Security Suite из командной строки, выполните команду:

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

где *<путь>* — путь, подлежащий проверке. Вы можете указать список путей, разделенных пробелами.

Параметры командной строки	
Параметр	**Описание**
`--version`	Назначение: Вывести на экран консоли или эмулятора терминала информацию о версии графического интерфейса. Краткий вариант: `-v` Аргументы: Нет
`--help`	Назначение: Вывести на экран консоли или эмулятора терминала краткую справку по имеющимся параметрам командной строки графического интерфейса. Краткий вариант: `-h` Аргументы: Нет
`--Autonomous`	Назначение: Запустить графический интерфейс в режиме автономного экземпляра. Краткий вариант: `-a` Аргументы: Нет
`--ExpressScan`	Назначение: Запустить графический интерфейс и сразу начать быструю проверку. Краткий вариант: Нет. Аргументы: Нет
`--FullScan`	Назначение: Запустить графический интерфейс и сразу начать полную проверку. Краткий вариант: Нет. Аргументы: Нет
`--CustomScan`	Назначение: Запустить графический интерфейс и открыть страницу выбора объектов, подлежащих проверке. Краткий вариант: Нет. Аргументы: Нет

Пример:

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

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

8.1.10.2. Запуск автономного экземпляра

Dr.Web Desktop Security Suite поддерживает работу в особом режиме — режиме *автономного экземпляра*.

Если запустить графический интерфейс управления Dr.Web Desktop Security Suite в режиме автономного экземпляра, то он будет работать с отдельным комплектом сервисных компонентов (работающим в фоне *демоном управления конфигурацией* Dr.Web Desktop Security Suite (`drweb-configd`), Сканером и используемым им антивирусным ядром), запущенным специально для поддержки работоспособности запущенного экземпляра программы.

Особенности функционирования графического интерфейса управления Dr.Web Desktop Security Suite в режиме автономного экземпляра:

- Для запуска графического интерфейса управления Dr.Web Desktop Security Suite в режиме автономного экземпляра 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 Desktop Security Suite подключен к серверу централизованной защиты, автономный экземпляр *не сообщает* серверу централизованной защиты об угрозах, обнаруженных при запуске в режиме автономного экземпляра.
- Все вспомогательные компоненты, обслуживающие работу автономного экземпляра 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 запущенным автономным экземпляром в каталоге временных файлов (указанном в системной переменной окружения `TMPDIR`).
- Автономно запущенный экземпляр 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.
- Число одновременно работающих автономных экземпляров графического интерфейса управления не ограничено.
- При завершении работы автономно запущенного экземпляра графического интерфейса также завершает работу и комплект обслуживающих ее сервисных компонентов.

8.2. Работа из командной строки

Чтобы управлять работой Dr.Web Desktop Security Suite из командной строки, используйте утилиту `drweb-ctl` компонента Dr.Web Ctl, принципы работы и примеры использования которой подробно описаны в соответствующих разделах.

9. Компоненты Dr.Web Desktop Security Suite

В разделе перечислены компоненты, входящие в состав Dr.Web Desktop Security Suite. Для каждого компонента указаны его назначение, принципы функционирования, а также параметры, которые он хранит в файле конфигурации.

9.1. Dr.Web ConfigD

Демон управления конфигурацией Dr.Web ConfigD — это центральный управляющий компонент Dr.Web Desktop Security Suite. Он обеспечивает централизованное хранение настроек для всех компонентов Dr.Web Desktop Security Suite, управляет активностью всех компонентов и организует доверительный обмен данными между ними.

Dr.Web ConfigD выполняет следующие функции:

- запуск и остановка компонентов Dr.Web Desktop Security Suite в зависимости от настроек;
- автоматический перезапуск компонентов в случае сбоев;
- запуск компонентов по запросу от других компонентов;
- оповещение компонентов об изменении настроек;
- предоставление возможности централизованного управления конфигурационными параметрами;
- предоставление компонентам информации из используемого ключевого файла;
- получение лицензионной информации от компонентов;
- получение новой лицензионной информации от специализированных компонентов;
- оповещение запущенных компонентов об изменении лицензионной информации.

9.1.1. Принципы работы

Демон управления конфигурацией Dr.Web ConfigD всегда запускается с правами суперпользователя (*root*). Он запускает остальные компоненты Dr.Web Desktop Security Suite и связывается с ними через предварительно открытый сокет. Демон управления конфигурацией принимает подключения от прочих компонентов Dr.Web Desktop Security Suite через информационный сокет (доступен публично) и административный сокет (доступен только компонентам, запущенным с правами суперпользователя). Демон загружает параметры конфигурации и лицензионные данные из файлов или обеспечивает их получение от используемого сервера централизованной защиты через агент Dr.Web ES Agent, а также подстановку корректных значений по умолчанию для параметров конфигурации. К моменту старта любого компонента или отсылки ему сигнала SIGHUP демон управления конфигурацией всегда имеет целостный непротиворечивый набор настроек всех компонентов Dr.Web Desktop Security Suite.

При получении сигнала SIGHUP Dr.Web ConfigD перечитывает параметры конфигурации и данные из лицензионного ключевого файла. В случае необходимости демон также рассылает компонентам уведомления, чтобы они перечитали собственные параметры конфигурации.

При получении сигнала SIGTERM Dr.Web ConfigD сначала завершает работу всех компонентов, а потом сам завершает работу. Dr.Web ConfigD обеспечивает удаление всех временных файлов компонентов после того, как они завершат работу.

Принципы взаимодействия с другими компонентами

1. При запуске все компоненты получают от Dr.Web ConfigD параметры конфигурации и лицензионную информацию. В дальнейшей работе компоненты используют только эти полученные настройки.
2. Dr.Web ConfigD обеспечивает сбор сообщений от всех запущенных под его управлением компонентов в единый журнал. Dr.Web ConfigD собирает все сообщения, выводимые компонентами в *stderr*, и помещает в общий журнал Dr.Web Desktop Security Suite с отметкой, у какого компонента и в какой момент произошла ошибка.
3. Все управляемые компоненты завершают работу с определенным кодом. Если код завершения отличен от `101`, `102` и `103`, компонент будет перезапущен, а соответствующее сообщение из *stderr* будет зафиксировано в журнале Dr.Web Desktop Security Suite.
   - Завершение работы с кодом 101 означает, что компонент не может функционировать с предоставленной лицензией. Компонент будет перезапущен только при изменении параметров лицензии.
   - Завершение работы с кодом 102 означает, что он не может функционировать с текущими параметрами конфигурации. Dr.Web ConfigD предпримет попытку перезапустить компонент, когда будет изменены какие-либо параметры конфигурации.
   - Завершение работы с кодом `103` происходит в результате длительного отсутствия обращений к компонентам, запускаемым Dr.Web ConfigD по требованию (Dr.Web Scanning Engine и Dr.Web File Checker). Период, по истечении которого компонент завершает работу с кодом `103`, указывается в настройках соответствующего компонента (параметр `IdleTimeLimit`).
   - Если новые значения параметров конфигурации, полученные компонентом от Dr.Web ConfigD, не могут быть применены «на лету», компонент завершает работу с кодом `0`, чтобы Dr.Web ConfigD перезапустил его.
   - Если компонент не может подключиться к Dr.Web ConfigD или происходит ошибка протокола взаимодействия, компонент отправляет соответствующее сообщение в *stderr* и завершает работу с кодом `1`.

4. Организован обмен сигналами.
   - Чтобы компонент применил измененные параметры конфигурации, Dr.Web ConfigD отправляет ему сигнал SIGHUP.
   - Чтобы компонент завершил работу, Dr.Web ConfigD отправляет ему сигнал SIGTERM. Компонент должен завершить работу в течение 30 секунд после получения сигнала.
   - Если компонент не завершает работу в течение положенных 30 секунд, Dr.Web ConfigD отправляет ему сигнал SIGKILL для принудительного завершения работы.

9.1.2. Аргументы командной строки

Чтобы запустить демон управления конфигурацией Dr.Web ConfigD из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-configd [<параметры>]
```

Dr.Web ConfigD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет
`--config`	Назначение: Использовать при работе указанный конфигурационный файл. Краткий вариант: `-c` Аргументы: <*путь к файлу*> — путь к используемому конфигурационному файлу.
`--daemonize`	Назначение: Запустить компонент в режиме демона, т. е. без доступа к терминалу. Краткий вариант: `-d` Аргументы: Нет
`--pid-file`	Назначение: Использовать при работе указанный PID-файл. Краткий вариант: `-p` Аргументы: <*путь к файлу*> — путь к файлу, в котором следует сохранить идентификатор процесса (PID).

Пример:

```
$ /opt/drweb.com/bin/drweb-configd -d -c /etc/opt/drweb.com/drweb.ini
```

Приведенная команда запустит Dr.Web ConfigD в режиме демона, заставив его использовать конфигурационный файл `/etc/opt/drweb.com/drweb.ini`.

Замечания о запуске

Для обеспечения работоспособности Dr.Web Desktop Security Suite компонент должен быть запущен в режиме демона. В штатном режиме Dr.Web ConfigD запускается при старте операционной системы, для чего он оснащен скриптом управления с именем `drweb-configd`, размещенным в системном каталоге (`/etc/init.d`). Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки (запускается командой `drweb-ctl`).

> Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-configd`.

9.1.3. Параметры конфигурации

Демон управления конфигурацией Dr.Web ConfigD использует параметры, указанные в секции `[Root]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента Dr.Web ConfigD. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала демона управления конфигурацией, а также метод ведения журнала для тех компонентов, у которых не указан свой собственный метод ведения журнала. > При начальной загрузке, пока конфигурационный файл еще не прочитан, демон управления конфигурацией будет использовать следующие значения этого параметра: > • в режиме демона (если был запущен с параметром `-d`) — `SYSLOG:Daemon`; > • в ином случае — `Stderr`. > Если компонент работает в фоновом режиме (запущен с параметром командной строки `-d`), значение `Stderr` *не может* быть использовано для данного параметра. Значение по умолчанию: `SYSLOG:Daemon`

Параметр	Описание
`PublicSocketPath` *{путь к файлу}*	Путь к сокету, используемому для взаимодействия всех компонентов Dr.Web Desktop Security Suite. Значение по умолчанию: `/var/run/.com.drweb.public`
`AdminSocketPath` *{путь к файлу}*	Путь к сокету, используемому для взаимодействия компонентов Dr.Web Desktop Security Suite, обладающих повышенными (административными) привилегиями. Значение по умолчанию: `/var/run/.com.drweb.admin`
`DebugIpc` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC (взаимодействие демона управления конфигурацией с другими компонентами). Значение по умолчанию: `No`
`UseCloud` *{логический}*	Использовать или не использовать сервис Dr.Web Cloud для получения сведений о вредоносности файлов и URL. Значение по умолчанию: `No`
`UseMesh` *{логический}*	Использовать или не использовать для проверки компонент Dr.Web MeshD. Если этот параметр выключен, для проверки вместо Dr.Web MeshD используется Dr.Web Scanning Engine. Возможные значения: • `On`, `Yes`, `True` — использовать Dr.Web MeshD; • `Off`, `No`, `False` — не использовать Dr.Web MeshD. Если компонент Dr.Web MeshD не установлен, то вне зависимости от указанного значения будет использоваться компонент Dr.Web Scanning Engine. Если ни один из компонентов не установлен, то проверка завершается с ошибкой x119. Значение по умолчанию: `No`
`UseVxcube` *{логический}*	Использовать или не использовать Dr.Web vxCube при проверке почтовых вложений в режиме внешнего фильтра, подключенного к MTA. Значение по умолчанию: `No`
`KeyPath` *{путь к файлу}*	Путь к ключевому файлу (лицензионному или демонстрационному). Значение по умолчанию: `/etc/opt/drweb.com/drweb32.key`
`CoreEnginePath` *{путь к файлу}*	Путь к динамической библиотеке антивирусного ядра Dr.Web Virus-Finding Engine. Значение по умолчанию: `/var/opt/drweb.com/lib/drweb32.dll`
`VirusBaseDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы вирусных баз. Значение по умолчанию: `/var/opt/drweb.com/bases`

Параметр	Описание
`DwsDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы автоматически обновляемой базы категорий веб-ресурсов. Значение по умолчанию: `/var/opt/drweb.com/dws`
`VersionDir` *{путь к каталогу}*	Путь к каталогу, в котором хранится информация о текущих версиях используемых компонентов Dr.Web Desktop Security Suite. Значение по умолчанию: `/var/opt/drweb.com/version`
`AntispamDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы, используемые антиспам-библиотекой. Значение по умолчанию: `/var/opt/drweb.com/antispam`
`CacheDir` *{путь к каталогу}*	Путь к каталогу кеша (используется как для кеша обновлений, так и для кеша проверенных файлов). Значение по умолчанию: `/var/opt/drweb.com/cache`
`TempDir` *{путь к каталогу}*	Путь к каталогу для хранения временных файлов. Значение по умолчанию: *Путь, извлеченный из системной переменной окружения* `TMPDIR`, `TMP`, `TEMP` или `TEMPDIR` (переменные перебираются в указанном порядке). Если ни одна из них не обнаружена, то используется `/tmp`.
`RunDir` *{путь к каталогу}*	Путь к каталогу, в котором находятся PID-файлы запущенных компонентов и сокеты, используемые для взаимодействия компонентов Dr.Web Desktop Security Suite. Значение по умолчанию: `/var/run`
`VarLibDir` *{путь к каталогу}*	Путь к каталогу библиотек, используемых компонентами Dr.Web Desktop Security Suite. Значение по умолчанию: `/var/opt/drweb.com/lib`
`AdminGroup` *{имя группы | GID}*	Группа пользователей, обладающих административными правами в рамках Dr.Web Desktop Security Suite. Данные пользователи, наряду с суперпользователем (пользователем *root*), могут повышать привилегии компонентов Dr.Web Desktop Security Suite до привилегий суперпользователя. Значение по умолчанию: *Определяется автоматически* в момент установки Dr.Web Desktop Security Suite
`TrustedGroup` *{имя группы | GID}*	Группа пользователей, являющихся доверенными. Параметр используется в работе компонента проверки сетевого трафика SpIDer Gate. Сетевой трафик таких пользователей пропускается SpIDer Gate без проверки. Значение по умолчанию: `drweb`
`VersionNotification` *{логический}*	Уведомлять или не уведомлять пользователя о наличии обновлений для текущей установленной версии Dr.Web Desktop Security Suite.

Параметр	Описание
	Значение по умолчанию: `Yes`
`DefaultLogLevel` *{уровень подробности}*	Уровень подробности ведения журнала *для всех компонентов* Dr.Web Desktop Security Suite по умолчанию. Используется, если в конфигурации какого-либо из компонентов не указан свой уровень подробности ведения журнала. Значение по умолчанию: `Notice`
`VxcubeApiAddress` *{строка}*	Доменное имя (FQDN) или IP-адрес узла, на котором находится сервер API Dr.Web vxCube. Значение по умолчанию: *(не задано)*
`VxcubeApiKey` *{строка}*	Ключ API Dr.Web vxCube. Значение по умолчанию: *(не задано)*
`VxcubeProxyUrl` *{адрес подключения}*	Адрес прокси-сервера, который используется для подключения к Dr.Web vxCube. Поддерживаются только HTTP-прокси без авторизации. Возможные значения: <*адрес подключения*> — параметры подключения к прокси-серверу в формате `http://`<*хост*>`:`<*порт*>, где: • <*хост*> — адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN); • <*порт*> — используемый порт. Значение по умолчанию: *(не задано)*

9.2. Dr.Web Ctl

В этом разделе

- Общие сведения
- Удаленная проверка узлов

Общие сведения

Имеется возможность управлять работой Dr.Web Desktop Security Suite из командной строки. 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);

- запуск обновления антивирусных компонентов (вирусных баз, антивирусного ядра, и прочих, в зависимости от поставки);
- просмотр и изменение параметров конфигурации Dr.Web Desktop Security Suite;
- просмотр состояния компонентов Dr.Web Desktop Security Suite и статистики обнаруженных угроз;
- просмотр карантина и управление его содержимым (через компонент Dr.Web File Checker);
- подключение к серверу централизованной защиты или отключение от него.

Чтобы команды управления, вводимые пользователем, имели эффект, должен быть запущен демон управления конфигурацией Dr.Web ConfigD (по умолчанию он автоматически запускается при старте операционной системы).



Для выполнения некоторых управляющих команд требуются полномочия суперпользователя.

Для получения полномочий суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Утилита `drweb-ctl` поддерживает стандартное автодополнение команд управления Dr.Web Desktop Security Suite, 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.

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 Ж. Описание известных ошибок.

Удаленная проверка узлов

Dr.Web Desktop Security Suite 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`).

9.2.1. Формат вызова из командной строки

Утилита управления работой Dr.Web Desktop Security Suite имеет следующий формат вызова:

```
$ drweb-ctl [<общие опции> | <команда> [<аргумент>] [<опции команды>]]
```

где:

- *<общие опции>* — опции, которые могут быть использованы при запуске без указания команды или для любой из команды. Не являются обязательными для запуска.
- *<команда>* — команда, которая должна быть выполнена Dr.Web Desktop Security Suite (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. Зависят от команды. У некоторых команд опции отсутствуют.

9.2.2. 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`

9.2.3. Команды

В этом разделе

- Команды антивирусной проверки
- Команды управления угрозами и карантином
- Команды управления конфигурацией
- Расширенные команды
  - Команды управления обновлением и работой в режиме централизованной защиты
  - Информационные команды

9.2.3.1. Команды антивирусной проверки

Доступны следующие команды антивирусной проверки файловой системы:

Команда	Описание
`scan <путь>`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker указанного файла или каталога. **Аргументы** *<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`.

Команда	Описание
	Опции `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. ⚠ Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`, также о них не будет сообщено серверу централизованной защиты, если Dr.Web Desktop Security Suite работает под его управлением. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--FollowSymlinks` — автоматически разрешать символические ссылки. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`.

Команда	Описание
	`--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <*число*> — 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: *(не задано)*. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--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. `--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.

Команда	Описание
	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`). `--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).

Команда	Описание
`bootscan` *<устройство>* | `ALL`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker загрузочной записи на указанных дисковых устройствах. Проверяются как записи MBR, так и записи VBR. **Аргументы** *<устройство>* — путь к блочному файлу дискового устройства, загрузочная запись на котором подлежит проверке. Может быть указано несколько дисковых устройств через пробел. Обязательный аргумент. Если вместо файла устройства указано `ALL`, будут проверены все загрузочные записи на всех доступных дисковых устройствах. **Опции** `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. ⚠ Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`, также о них не будет сообщено серверу централизованной защиты, если Dr.Web Desktop Security Suite работает под его управлением. `--Report` *<тип>* — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` *<интервал времени>* — тайм-аут на проверку одного файла в миллисекундах. 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

Команда	Описание
`procscan`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker 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 автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. ⚠ Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`, также о них не будет сообщено серверу централизованной защиты, если Dr.Web Desktop Security Suite работает под его управлением. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`.

Команда	Описание
	`--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--Exclude` <*путь*> — путь, исключаемый 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. `--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`. 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`.

Команда	Описание
	`--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 Desktop Security Suite.
`memscan --Cure` <*логическое значение*>	**Назначение**: Инициировать проверку процессов. В отличие от команды `procscan`, проверка осуществляется только в оперативной памяти. **Аргументы**: Нет. **Опции** `--Cure` <*логическое значение*> — лечить угрозу при ее обнаружении. Обязательный параметр. Возможные значения: • `On`, `Yes`, `True` — лечить угрозу при ее обнаружении; • `Off`, `No`, `False` — не лечить угрозу при ее обнаружении. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного процесса в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `-d [--Debug]` — вывести на экран расширенные диагностические сообщения во время выполнения указанной команды.
`netscan [`<*путь*>`]`	**Назначение**: Инициировать распределенную проверку указанного файла или каталога через агент сетевой проверки данных Dr.Web Network Checker. Если настроенные соединения с другими узлами, на которых имеется продукт Dr.Web для Unix, поддерживающий функцию распределенной проверки, отсутствуют, то будет произведена проверка с использованием сканирующего ядра, доступного локально (аналогично команде `scan`). **Аргументы** <*путь*> — путь к файлу или каталогу, который нужно проверить.

Команда	Описание
	Если этот аргумент опущен, то производится сканирование данных, поступающих через входной поток stdin. **Опции** `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого

Команда	Описание
	параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio <степень>` — максимально допустимая степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract <число>` — 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: *(не задано)*. `--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`
`rawscan <путь>`	**Назначение**: Инициировать «сырую» проверку указанного файла или каталога с использованием сканирующего ядра Dr.Web Scanning Engine напрямую, без использования компонента проверки файлов Dr.Web File Checker. ⚠ Угрозы, обнаруженные при «сыром» сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`. Рекомендуется использовать эту команду только для отладки функционирования Dr.Web Scanning Engine. Команда имеет следующую особенность: она выводит заключение «cured» (вылечен), если нейтрализована, по меньшей мере, *одна* из угроз, обнаруженных в файле (не обязательно *все* из них). Таким образом, *не рекомендуется* использовать эту команду, если требуется надежное сканирование файлов. Вместо этого для проверки файлов и каталогов рекомендуется использовать команду `scan`.

Команда	Описание
	Аргументы <*путь*> — путь к файлу или каталогу, который нужно проверить. **Опции** `--ScanEngine` <*путь*> — путь к Unix-сокету сканирующего ядра Dr.Web Scanning Engine. Если не указан, то для проверки будет запущен автономный экземпляр сканирующего ядра (будет завершен после окончания проверки). `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.

Команда	Описание
	Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <*число*> — 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: *(не задано)*. `--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`. `--ListCleanItem` — включить вывод списка чистых файлов при проверке контейнера. `--ShellTrace` — включить вывод дополнительной отладочной информации при проверке файла. `--Output` <*путь к файлу*> — дублировать вывод команды в указанный файл
`remotescan` <*узел*> <*путь*>	**Назначение**: Инициировать проверку указанного файла или каталога на указанном удаленном узле, подключившись к нему через *SSH* или *Telnet*.

Команда	Описание
	 Угрозы, обнаруженные при удаленном сканировании, не будут нейтрализованы, более того, они не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`. Вы можете использовать эту команду только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров, ТВ-приставок и прочих «умных» устройств вы можете воспользоваться механизмом обновления прошивки, а для вычислительных машин — выполнив подключение к ним (в том числе — в удаленном терминальном режиме) и произведя соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустив антивирусное ПО, установленное на них. **Аргументы** • *<узел>* — IP-адрес или доменное имя узла, к которому необходимо подключиться для проверки. • *<путь>* — путь к файлу или каталогу, который нужно проверить (должен быть абсолютным). **Опции** `-l [--Login]` *<имя>* — логин (имя пользователя) для авторизации на удаленном узле через 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.  Команда `remotescan` предназначена для сканирования маршрутизаторов SOHO (Small Office / Home Office). Ключ в формате, используемом по умолчанию утилитой `ssh-keygen`, не поддерживается. Для проверки удаленного узла по SSH требуется ключ в формате PEM, который можно сгенерировать командой: `$ ssh-keygen -t rsa -m PEM -f rsa_pem`

Команда	Описание
	`-m [--Method]` <*SSH*|*Telnet*> — метод (протокол) подключения к удаленному узлу. Если метод не указан, будет использован SSH. `-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). `--UseChannels` <*число*> — число каналов передачи данных. Значение по умолчанию: `5`. `--Password` <*пароль*> — пароль для аутентификации указанного пользователя через выбранный протокол.  Пароль передается в открытом виде. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены.

Команда	Описание
	Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <*число*> — 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: *(не задано)*. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Exclude` <*путь*> — путь, исключаемый 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. `--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.

Команда	Описание
	`--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. `--ForceInteractive` — использовать интерактивную сессию SSH (только для метода подключения SSH). *Необязательная опция.*
`mailquarantine`	**Назначение**: Задать настройки служебного компонента управления очередями писем Dr.Web Mail Quarantine. **Аргументы**: Нет. **Опции** `--Show` — показать указанную очередь сообщений. Требует указания опции `--Queue`. Используйте вызов: `$ drweb-ctl mailquarantine --Queue <очередь> --Show` `--Stat` — показать статистику всех очередей сообщений; `--Flush` — поставить отложенные сообщения из указанной очереди в очередь для немедленной обработки. Требует указания опции `--Queue`. Используйте вызов: `$ drweb-ctl mailquarantine --Queue <очередь> --Flush` `--CheckHealth` — проверить согласованность в базе данных сообщений; `--FixHealth` — исправить ошибки согласованности в базе данных сообщений; `-q [--Queue] <очередь>` — указать очередь сообщений, над которой будут производиться операции. Возможные значения: • `SmtpFresh` — сообщения, ожидающие проверки в режиме SMTP; • `SmtpAccepted` — сообщения, проверенные и принятые в режиме SMTP; • `BccFresh` — сообщения, ожидающие проверки в режиме BCC; • `BccAccepted` — сообщения, проверенные и принятые в режиме BCC. `-l [--Limit] <число>` — максимальное количество отображаемых сообщений из выбранной очереди.

Команда	Описание
	`-d [--Debug]` — вывести на экран расширенные диагностические сообщения во время выполнения указанной команды. Не имеет смысла без указания команды. Используйте вызов: `$ drweb-ctl mailquarantine <команда> -d` **Примеры** 1. Чтобы показать электронные сообщения, ожидающие проверки в режиме SMTP, выполните команду: `$ drweb-ctl mailquarantine -q smtpfresh --show` Примерный результат выполнения команды: `ID: 78541` `Sender:` `Recipients: buy@drweb.com` `Deferred: until 2025-Feb-26 12:32:01` `ID: 78534` `Sender:` `Recipients: pr@drweb.com` `Deferred: until 2025-Feb-26 12:37:02` 2. Чтобы переместить сообщения, ожидающие проверки в режиме BCC, в очередь для немедленной обработки, выполните команду: `$ drweb-ctl mailquarantine -q bccfresh --flush` Примерный результат выполнения команды: `Flushed 2 entries`

9.2.3.2. 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 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 «Доктор Веб»);

Команда	Описание
	• 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]` — ожидать поступления новых сообщений об угрозах и выводить их сразу при поступлении (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `--Cure <`*список угроз*`>` — выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Quarantine <`*список угроз*`>` — выполнить перемещение в карантин перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Delete <`*список угроз*`>` — выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Ignore <`*список угроз*`>` — игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить 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. `--Directory <`*список каталогов*`>` — выводить только те угрозы, которые были обнаружены в файлах в каталогах из *<списка каталогов>*. Если эта опция указана совместно с любой из опций-действий, она игнорируется.
`quarantine [<`*действие*`> <`*объект*`>]`	**Назначение**: Применить действие к указанному объекту, находящемуся в карантине.

Команда	Описание
	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 «Доктор Веб»). **Аргументы**: Нет. **Опции** `--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]` — ожидать поступления новых сообщений об угрозах и выводить их сразу при поступлении (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-a [--Autonomous]` — запустить автономный экземпляр компонента проверки файлов Dr.Web File Checker для выполнения заданного действия с карантином, завершив работу компонента после окончания действия. Эта опция может быть применена совместно с любой из опций, указанных ниже. `--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).

Команда	Описание
	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 автономного экземпляра, т. е. с опцией `-a` (`--Autonomous`), но без опции `--Discovery`, то это равносильно вызову: `quarantine --Autonomous --Discovery` `--Delete` <*объект*> — удалить указанный объект, помещенный в карантин. Удаление объекта, помещенного в карантин — необратимая операция. `--Restore` <*объект*> — восстановить указанный объект из карантина в исходное место. Для выполнения этого действия может потребоваться, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). Восстановить файл из карантина можно, даже если он инфицирован. `--Cure` <*объект*> — попытаться вылечить указанный объект в карантине. Даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина воспользуйтесь опцией восстановления `--Restore`. `--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 путь, так и относительный (относительно текущего каталога). 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`

Команда	Описание
	восстанавливает из карантина все имеющиеся в нем объекты, помещая их в подкаталог `test`, находящийся в текущем каталоге, из которого запущена команда `drweb-ctl`. Если для варианта `--Restore All` указана дополнительная опция `--TargetPath`, то она 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 по классификации компании «Доктор Веб»
`%{threat_type}`	Тип угрозы («known virus» и т. д.) по классификации компании «Доктор Веб»
`%{size}`	Размер исходного файла
`%{origin}`	Полное имя исходного файла с путем
`%{path}`	Синоним `%{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 Desktop Security Suite, обработавшего угрозу
`%{event}`	Последнее событие, связанное с угрозой: • `FOUND` — угроза была обнаружена; • `CURE` — угроза была вылечена; • `QUARANTINE` — файл с угрозой был перемещен в карантин; • `DELETE` — файл с угрозой был удален; • `IGNORE` — угроза была проигнорирована; • `RECAPTURED` — угроза была обнаружена 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>
}
...
```

9.2.3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
`cfset` <*секция*>`.`<*параметр*> <*значение*>	**Назначение**: Изменить активное значение указанного параметра текущей конфигурации Dr.Web Desktop Security Suite. **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. 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 разделе Приложение Г. Конфигурационный файл Dr.Web Desktop Security Suite, а также 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

Команда	Описание
	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 секций, описывающих индивидуальные параметры , применение опции `-r` приводит к замене значения параметра в индивидуальной секции на значение, указанное у соответствующего «родительского» параметра в секции настроек компонента. Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`cfshow [<`*секция*`>[.<`*параметр*`>]]`	**Назначение**: Вывести на экран параметры текущей конфигурации Dr.Web Desktop Security Suite. Для вывода параметров по умолчанию используется формат <*секция*>.<*параметр*> = <*значение*>. Секции и параметры не установленных компонентов по умолчанию не выводятся. **Аргументы** • <*секция*> — имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла. • <*параметр*> — имя выводимого параметра. Необязательный аргумент. Если не указан, выводятся все параметры указанной секции, в противном случае выводится только этот параметр. Если указан без имени секции, то выводятся все вхождения этого параметра во все секции конфигурационного файла.

Команда	Описание
	Опции `--Uncut` — вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. Если не указано, то 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 файла `.ini`: 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**: Перезагрузить конфигурацию Dr.Web Desktop Security Suite. При этом демон управления конфигурацией Dr.Web ConfigD выполняет следующие действия: • перечитывает конфигурацию и рассылает ее изменения всем компонентам Dr.Web Desktop Security Suite; • переоткрывает журнал Dr.Web Desktop Security Suite; • запускает компоненты, использующие вирусные базы (включая антивирусное ядро); • пытается запустить компоненты, работа которых была нештатно завершена. **Аргументы**: Нет. **Опции**: Нет

9.2.3.4. Расширенные команды

В этом разделе

- Команды управления обновлением и работой в режиме централизованной защиты
- Информационные команды

9.2.3.4.1. 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, антивирусного ядра и прочих, в зависимости от поставки) с серверов обновлений компании «Доктор Веб», прервать уже запущенный процесс обновления или откатить результаты последнего обновления, восстановив предыдущие версии обновленных файлов. Команда не имеет эффекта, если Dr.Web Desktop Security Suite работает под управлением сервера централизованной защиты. **Аргументы**: Нет. **Опции** `--Stop` — прервать уже идущий процесс обновления. `--Rollback` — откатить последнее обновление и восстановить последние сохраненные копии обновленных файлов. `--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.
`esconnect` <*сервер*>`[:`<*порт*>`]`	**Назначение**: Подключить Dr.Web Desktop Security Suite к указанному серверу централизованной защиты. 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.

Команда	Описание
	`--Login` <*ID*> — логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты. `--Password` <*пароль*> — пароль для подключения к серверу централизованной защиты. `--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). `--Group` <*ID*> — идентификатор группы на сервере, в которую следует поместить рабочую станцию при подключении. Указывается только совместно с опцией `--Password`. `--Rate` <*ID*> — идентификатор тарифной группы, которую следует применить к рабочей станции при ее включении в группу на сервере централизованной защиты. Указывается только совместно с опцией `--Group`. `--CfgFile` <*путь*> — подключиться к серверу централизованной защиты, используя конфигурационный файл с настройками соединения.  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 Desktop Security Suite от сервера централизованной защиты и перевести его в автономный режим работы.  Команда не имеет эффекта, если Dr.Web Desktop Security Suite уже работает в автономном режиме. **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`.

9.2.3.4.2. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	**Назначение**: Вывести на экран информацию о работающих компонентах Dr.Web Desktop Security Suite. Для каждого запущенного компонента выводится следующая информация: • внутреннее имя; • идентификатор процесса GNU/Linux (PID); • состояние (запущен, остановлен и т. п.); • код ошибки, если работа компонента завершена вследствие ошибки; • дополнительная информация (опционально); Для демона управления конфигурацией (`drweb-configd`) в качестве дополнительной информации выводятся: • перечень установленных компонентов — *Installed*; • перечень компонентов, запуск которых должен быть обеспечен демоном — *Should run*. **Аргументы**: Нет. **Опции** `-f [--Follow]` — ожидать поступления новых сообщений об изменении состояния модулей и выводить их на экран сразу при поступлении (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 записей об угрозах; • 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 записей об угрозах в каждом файле

Команда	Описание
`certificate`	**Назначение**: Вывести на экран содержимое доверенного сертификата Dr.Web, который используется Dr.Web Desktop Security Suite для доступа к защищенным соединениям с целью их проверки, если эта проверка включена в настройках. Чтобы сохранить сертификат в файл <*cert_name*>`.pem`, выполните команду: `$ drweb-ctl certificate > <cert_name>.pem` **Аргументы**: Нет. **Опции**: Нет
`events`	**Назначение**: Просмотреть события Dr.Web Desktop Security Suite. Кроме этого, команда позволяет выполнить управление событиями (отметка как «прочитанные», удаление). **Аргументы**: Нет. **Опции** `--Report` <*тип*> — тип отчета о событиях. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. `-f [--Follow]` — ожидать поступления новых событий и выводить их на экран сразу при поступлении (нажатие CTRL+C прерывает ожидание). `--ShowSeen` — показать также и уже прочитанные события; `-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` — неожиданное завершение работы какого-либо компонента. Для вывода событий всех типов используйте `All`.

Команда	Описание
	`--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 Desktop Security Suite в виде страницы HTML (тело страницы выводится в указанный файл). **Аргументы** <*тип*> — тип событий, для которых формируется отчет (указывается один тип). Возможные значения см. в описании опции `--Types` команды `events`. 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.

Команда	Описание
`idpass <идентификатор>`	**Назначение**: Вывести на экран пароль, который был сгенерирован компонентом проверки сообщений электронной почты Dr.Web MailD для почтового сообщения с указанным идентификатором и использован для защиты вложенного архива с угрозами, вырезанными из письма (т. е. если в настройках компонента параметр `RepackPassword` был установлен в значение `HMAC(<secret>)`). **Аргументы** *<идентификатор>* — идентификатор сообщения электронной почты. **Опции** `-s [--Secret] <secret>` — секретное слово, использованное для генерации пароля архива. Если секретное слово не указано при вызове команды, будет использовано текущее секретное слово *<secret>*, указанное в настройках Dr.Web MailD. Если при этом параметр `RepackPassword` отсутствует или установлен в значение, отличное от `HMAC(<secret>)`, команда вернет ошибку. Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (обычно пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`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 автономного 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.

Команда	Описание
	Опции `--GetDemo` — запросить демонстрационный ключ сроком на месяц и получить его, 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). `--NetworkTimeout` <*интервал времени*> — тайм-аут в миллисекундах на сетевые операции при использовании команды `license`. Используется для продолжения активации в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то активация будет продолжена. Если указан `0`, то тайм-аута нет. Значение по умолчанию: `0`. `--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. раздел Лицензирование. Для регистрации серийного номера и для получения демонстрационного периода требуется наличие подключения к интернету.
`log`	**Назначение**: Вывести в консоль (поток *stdout*) последние записи журнала Dr.Web Desktop Security Suite (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 пробел. Если параметр не указан, выводятся

Команда	Описание
	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`. `-f [--Follow]` — ожидать поступления новых записей в журнал и выводить их на экран сразу при поступлении (нажатие CTRL+C прерывает ожидание).  Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (обычно пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`stat`	**Назначение**: Вывести на экран статистику работы компонентов, обрабатывающих файлы, либо агента сетевой проверки данных Dr.Web Network Checker (нажатие CTRL+C или Q прерывает отображение статистики). В статистике отображается: • имя компонента, инициировавшего проверку файлов; • PID компонента; • усредненное количество файлов, обрабатываемых в секунду за последнюю минуту, 5 минут, 15 минут; • процент использования кеша проверенных файлов; • среднее количество ошибок проверки в секунду. Для агента распределенной проверки на экран выводится: • перечень локальных клиентов, инициировавших сканирование; • перечень удаленных узлов, которым переданы файлы на сканирование; • перечень удаленных узлов, от которых получены файлы на сканирование. Для локальных клиентов агента распределенной проверки указывается имя и PID, а для удаленных — адрес и порт узла. Для каждого клиента, как локального, так и удаленного выводится: • среднее за секунду количество проверенных файлов; • среднее за секунду количество переданных и полученных байт; • среднее за секунду количество ошибок. **Аргументы**: Нет.

Команда	Описание
	Опции `-n [--Netcheck]` — вывести на экран статистику работы агента сетевой проверки данных

9.2.4. Примеры использования

В этом разделе

- Проверка объектов
  - Простые команды проверки
  - Проверка файлов, отобранных по критериям
  - Проверка дополнительных объектов
- Управление конфигурацией
- Управление угрозами
- Пример работы в режиме автономного экземпляра
- Обновление без подключения к интернету

Проверка объектов

Простые команды проверки

1. Выполнить проверку каталога `/home` с параметрами по умолчанию:

```
$ drweb-ctl scan /home
```

2. Выполнить проверку списка путей к файлам, перечисленным 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
```

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 1 мая 2017 года:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

Проверка дополнительных объектов

Проверка объектов каталога `/tmp` на удаленном узле *192.168.0.1* при подключении к нему через SSH как пользователь *user* с паролем *passw*:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

Управление конфигурацией

1. Вывести на экран информацию о запущенных компонентах Dr.Web Desktop Security Suite:

```
$ drweb-ctl appinfo
```

2. Вывести на экран все параметры из секции `[Root]`:

```
$ drweb-ctl cfshow Root
```

3. Задать значение `No` для параметра `Start` в секции `[LinuxSpider]` (это приведет к остановке работы монитора файловой системы SplDer Guard):

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

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 Desktop Security Suite:

```
$ drweb-ctl update
```

5. Выполнить перезагрузку конфигурации для компонентов Dr.Web Desktop Security Suite:

```
# drweb-ctl reload
```

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 Desktop Security Suite 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 Desktop Security Suite к серверу централизованной защиты, используя файл настроек подключения `install.cfg`:

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

8. Отключить Dr.Web Desktop Security Suite от сервера централизованной защиты:

```
# drweb-ctl esdisconnect
```

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 Desktop Security Suite:

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

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
```

5. Сгенерировать пароль для защищенного архива в почтовом сообщении с идентификатором `12345`, при условии, что для этого письма использовался метод генерации паролей *HMAC*, а актуальное секретное слово указано в настройках компонента Dr.Web MailD:

```
# drweb-ctl idpass 12345
```

Пример работы в режиме автономного экземпляра

Проверить файлы и обработать карантин в режиме автономного экземпляра:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=QUARANTINE
$ drweb-ctl quarantine -a --Delete All
```

Первая команда проверит файлы в каталоге `/home/user` в режиме автономного экземпляра, и файлы, содержащие известные угрозы, будут помещены в карантин. Вторая команда обработает содержимое карантина (также в режиме автономного экземпляра) и удалит все содержащиеся в нем объекты.

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.

Чтобы получить обновления

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
```

9.2.5. Параметры конфигурации

Утилита управления из командной строки Dr.Web Ctl не имеет собственной секции параметров в объединенном конфигурационном файле Dr.Web Desktop Security Suite. Утилита использует параметры, указанные в секции `[Root]`.

9.3. SpIDer Guard



Компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Монитор файловой системы SpIDer Guard предназначен для мониторинга файловой активности на томах файловой системы операционных систем GNU/Linux. Компонент работает в режиме резидентного монитора и отслеживает основные события файловой системы, связанные с изменением файлов (их создание, открытие, закрытие). При перехвате этих событий монитор проверяет, был ли изменен файл, и в этом случае формирует для компонента проверки файлов Dr.Web File Checker задание на проверку содержимого измененного файла сканирующим ядром Dr.Web Scanning Engine.

Кроме того, монитор файловой системы SpIDer Guard отслеживает попытки запуска исполняемых файлов. Если программа, содержащаяся в исполняемом файле, по результатам проверки будет признана вредоносной, все процессы, запущенные из этого файла, будут принудительно завершены.

9.3.1. Принципы работы

В этом разделе

- Общие сведения
- Определение областей файловой системы, подлежащих наблюдению
- Режим усиленного мониторинга файлов

Общие сведения

Монитор файловой системы SpIDer Guard работает в пользовательском пространстве (*user mode*), используя для контроля событий файловой системы системный механизм fanotify или специальный *загружаемый модуль ядра* Linux (*LKM — Loadable Kernel Module*), разработанный компанией «Доктор Веб». В настройках рекомендуется использовать *автоматический режим* (`Auto`), который позволит компоненту при старте определить и использовать наилучший режим работы, поскольку не все версии ядра Linux поддерживают механизм fanotify, использующийся монитором. Если компонент не может использовать указанный в настройках режим интеграции, он завершается сразу после старта. Если указан автоматический режим, то компонент попытается использовать сначала fanotify, а затем модуль ядра LKM. Если не получится использовать ни один из этих режимов, компонент завершит работу.

Для ряда ОС модуль ядра поставляется совместно с SplDer Guard уже в скомпилированном виде. Если для ОС, в которой используется SplDer Guard, модуль ядра не поставляется в скомпилированном виде, используйте исходный код модуля, предоставляемый компанией «Доктор Веб» для сборки и установки модуля ядра вручную (инструкция по сборке приведена в разделе Приложение Е. Сборка модуля ядра для SplDer Guard).

При обнаружении новых или измененных файлов монитор отправляет задание на их проверку компоненту проверки файлов Dr.Web File Checker, который, в свою очередь, инициирует их проверку сканирующим ядром Dr.Web Scanning Engine. При работе через системный механизм fanotify монитор может блокировать доступ к файлам (всех типов или только к исполняемым файлам — PE, ELF, скриптам с преамбулой `#!`), которые еще не проверены, до момента окончания их проверки (см. ниже).

SplDer Guard автоматически распознает моменты монтирования и отмонтирования новых томов файловой системы (например, на накопителях USB-flash и CD/DVD, массивы RAID и т. п.) и корректирует список наблюдаемых областей по мере необходимости.

Определение областей файловой системы, подлежащих наблюдению

Для оптимизации проверки файловой системы, монитор файловой системы SplDer Guard контролирует обращение только к тем файлам, которые находятся в областях файловой системы, указанных в конфигурации. Каждая такая область определяется как путь к некоторому каталогу дерева файловой системы и называется *защищаемым пространством (protected space)*. Совокупность всех защищаемых пространств образует в файловой системе единую *область наблюдения*, контролируемую монитором. Помимо области наблюдения, в настройках компонента можно задать также совокупность каталогов файловой системы, которые требуется исключить из мониторинга (*область исключения*). Если в настройках компонента не указано ни одного защищаемого пространства, область наблюдения охватывает собой все дерево каталогов файловой системы. Таким образом, наблюдению подвергаются только те файлы, пути к которым принадлежат области наблюдения, но не принадлежат области исключения.

Использование исключений бывает необходимо, например, если некоторые файлы часто изменяются, что порождает их постоянную перепроверку и тем самым нагружает систему. Если точно известно, что частое изменение файлов в некотором каталоге не является следствием вредоносной активности, а следствием работы некоторой доверенной программы, то можно добавить путь к этому каталогу, или изменяемым файлам в нем, в список исключений. В этом случае монитор файловой системы SplDer Guard не будет реагировать на изменения этих файлов, даже если они принадлежат области наблюдения. Кроме того, имеется возможность указать и саму программу,

работающую с файлами, в списке доверенных программ (параметр конфигурации `ExcludedProc`), тогда файловые операции, производимые этой программой, также не будут приводить к проверкам файлов, даже если эти файлы находятся в области наблюдения. Аналогично, при необходимости, можно запретить мониторинг и проверку файлов, находящихся в других файловых системах, примонтированных к локальной файловой системе (например, примонтированные через CIFS каталоги с внешних файловых серверов). Для указания файловых систем, файлы на которых не должны проверяться, используется параметр `ExcludedFilesystem`.

Защищаемые пространства, как части области наблюдения с указанными для них параметрами проверки, задаются в настройках компонента как именованные секции, содержащие в своем имени произвольный уникальный идентификатор, присвоенный защищаемому пространству. Каждая секция, описывающая пространство, содержит параметр `Path`, определяющий путь в файловой системе, хранящий каталоги этого защищаемого пространства (т. е. фрагмент дерева файловой системы, находящийся под наблюдением в рамках данного пространства), а также параметр `ExcludedPath`, определяющий локальную (т. е. относительно `Path`) область исключения внутри защищаемого пространства. Параметр `ExcludedPath` может содержать в себе стандартные файловые маски (т. е. содержать символы `*` и `?`). Кроме локальных областей исключения, в настройках может быть задана и глобальная область исключения, при помощи параметра `ExcludedPath`, указанного вне секций, описывающих защищаемые пространства. Все каталоги, попавшие в эту область, в том числе и каталоги защищаемых пространств, будут исключены из проверки. К каждому защищаемому пространству применяется только глобальная и собственная области исключения: если одно пространство вложено в другое, то к вложенному пространству не применяются настройки исключения, указанные для включающего его защищаемого пространства. Кроме того, в настройках каждого защищаемого пространства имеется логический параметр `Enable`, определяющий, включено или нет наблюдение за файлами, находящимися в области наблюдения данного пространства. Если этот параметр установлен в значение `No`, то содержимое данного пространства не контролируется монитором. Кроме того, защищаемое пространство не контролируется монитором, если параметр `Path` имеет пустое значение.



Если у всех защищаемых пространств, указанных в настройках монитора, наблюдение отключено, или их пути не заданы, то SplDer Guard работает вхолостую, поскольку ни один файл дерева файловой системы не будет находиться под наблюдением. Если необходимо контролировать всю файловую систему как единое защищаемое пространство, следует удалить из настроек все именованные секции защищаемых пространств.

Рассмотрим пример настроек областей наблюдения и исключения. Пусть в настройках компонента заданы следующие параметры:

```
[LinuxSpider]
ExcludedPath = /directory1/tmp
...

[LinuxSpider.Space.space1]
```

```
Path = /directory1
ExcludedPath = "*.tmp"
...

[LinuxSpider.Space.space2]
Path = /directory1/directory2
...

[LinuxSpider.Space.space3]
Path = /directory3
Enable = No
...
```

Это означает, что под наблюдением находятся файлы, расположенные в каталоге `/directory1`, и его подкаталогах, за исключением каталога `/directory1/tmp`. Кроме того, исключаются из наблюдения файлы, чье полное имя соответствует маске `/directory1/*.tmp` (это не касается вложенной области `/directory1/directory2`, на которую данная маска не распространяется, не смотря на то, что эта область вложена в защищаемое пространство *space1*). Файлы, находящиеся в каталоге `/directory3`, не контролируются.

Режим усиленного мониторинга файлов

SpIDer Guard может использовать три режима мониторинга:

- *Обычный* (установлен по умолчанию) — отслеживаются операции доступа 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. SpIDer Guard блокирует запрошенную операцию доступа к исполняемому файлу до тех пор, пока не станут известны результаты его проверки на наличие угроз.

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

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

Dr.Web File Checker 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.

Для настройки режима мониторинга измените значение параметра `BlockBeforeScan` в настройках компонента.

9.3.2. Аргументы командной строки

Чтобы запустить компонент SpIDer Guard из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-spider [<параметры>]
```

SpIDer Guard допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-spider --help
```

Данная команда выведет на экран краткую справку компонента SpIDer Guard.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при загрузке операционной системы. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-spider`.

9.3.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Настройка индивидуальных параметров мониторинга защищаемых пространств

Компонент использует параметры конфигурации, заданные в секции `[LinuxSpider]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-spider`
`Start` *{логический}*	Компонент запускается демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: Зависит от того, в составе какого продукта Dr.Web работает компонент.
`[*] ExcludedPath` *{путь к файлу или каталогу}*	Путь к объекту, который должен быть пропущен при мониторинге файловых операций. Допускается указание пути как к отдельному файлу, так и к каталогу в целом. Если указан каталог, то будут исключены из наблюдения все файлы и подкаталоги (включая вложенные) этого каталога. Допускается использовать файловые маски (содержащие символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`).

Параметр	Описание
	Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список файл `/etc/file1` и каталог `/usr/bin`. • Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset LinuxSpider.ExcludedPath -a /etc/file1` `# drweb-ctl cfset LinuxSpider.ExcludedPath -a /usr/bin` • Добавление значений в файл конфигурации. ○ Два значения в одной строке: `[LinuxSpider]` `ExcludedPath = "/etc/file1", "/usr/bin"` ○ Две строки (по одному значению в строке): `[LinuxSpider]` `ExcludedPath = /etc/file1` `ExcludedPath = /usr/bin` Чтобы изменения вступили в силу, перезагрузите конфигурацию Dr.Web Desktop Security Suite с помощью команды: `# drweb-ctl reload` Нет смысла указывать здесь пути к символическим ссылкам, поскольку при проверке файла всегда анализируется прямой путь к нему. Значение по умолчанию: `/proc, /sys`
`Mode` *{LKM | FANOTIFY | AUTO}*	Режим работы SplDer Guard. Возможные значения: • `LKM` — работа через LKM-модуль Dr.Web, установленный в ядро операционной системы (*LKM — Loadable Kernel Module*); • `FANOTIFY` — работа через системный механизм *fanotify*; • `AUTO` — автоматическое определение оптимального режима работы.

Параметр	Описание
	 Изменять значения этого параметра следует производить с крайней осторожностью, поскольку ядра Linux в разной мере поддерживают тот и другой режим работы. Настоятельно рекомендуется оставлять этот параметр в значении `AUTO`, чтобы при запуске был выбран оптимальный режим интеграции с диспетчером файловой системы. При этом компонент сначала пытается использовать режим `FANOTIFY`, потом, в случае неудачи, — `LKM`. Если не удалось использовать ни один из режимов, работа компонента завершается. При необходимости вы можете собрать LKM-модуль Dr.Web из исходного кода и установить его в систему, следуя инструкции в разделе Приложение E. Сборка модуля ядра для SplDer Guard. Значение по умолчанию: `AUTO`
`ExcludedProc` *{путь к файлу или список путей}*	Список процессов, файловая активность которых не контролируется. Если файловая операция была совершена любым из процессов, указанных в значении параметра, то измененный или созданный файл не будет проверяться. Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Допускается использовать файловые маски (содержащие символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`). Пример: Добавить в список процессы `wget` и `curl`. • Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/wget` `# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/curl` • Добавление значений в файл конфигурации.

Параметр	Описание
	○ Два значения в одной строке: `[LinuxSpider]` `ExcludedProc = "/usr/bin/wget",` `"/usr/bin/curl"` ○ Две строки (по одному значению в строке): `[LinuxSpider]` `ExcludedProc = /usr/bin/wget` `ExcludedProc = /usr/bin/curl` Чтобы изменения вступили в силу, перезагрузите конфигурацию Dr.Web Desktop Security Suite с помощью команды: `# drweb-ctl reload` Значение по умолчанию: *(не задано)*
`BlockBeforeScan` *{Off | Executables | All}*	Блокировать файлы при обращении к ним до проверки монитором (усиленный или «параноидальный» режим мониторинга). Допустимые значения: • `Off` — не блокировать доступ к файлам, даже если они не проверены. • `Executables` — блокировать доступ к исполняемым файлам (форматов PE и ELF и скриптов, содержащих преамбулу `#!`), не проверенным монитором. • `All` — блокировать доступ ко всем файлам, не проверенным монитором. Файлы блокируются только в режиме `FANOTIFY`. Значение по умолчанию: `Off`
`ExcludedFilesystem` *{имя файловой системы}*	Файловая система, доступ к файлам которой контролироваться не будет. Данная функция доступна только в режиме `FANOTIFY`. Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список файловые системы `cifs` и `nfs`.

Параметр	Описание
	• Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a cifs` `# drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a nfs` • Добавление значений в файл конфигурации. ○ Два значения в одной строке: `[LinuxSpider]` `ExcludedFilesystem = "cifs", "nfs"` ○ Две строки (по одному значению в строке): `[LinuxSpider]` `ExcludedFilesystem = cifs` `ExcludedFilesystem = nfs` Чтобы изменения вступили в силу, перезагрузите конфигурацию Dr.Web Desktop Security Suite с помощью команды: `# drweb-ctl reload` Значение по умолчанию: `cifs`
`[*] OnKnownVirus` *{действие}*	Действие при обнаружении в проверяемом файле известной угрозы (вируса и т. д.). Допустимые значения: `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `CURE`
`[*] OnIncurable` *{действие}*	Действие в случае невозможности излечения угрозы. Допустимые значения: `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnSuspicious` *{действие}*	Действие при обнаружении в проверяемом с помощью эвристического анализа файле неизвестной угрозы (или подозрения на угрозу). Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnAdware` *{действие}*	Действие при обнаружении в проверяемом файле рекламной программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnDialers` *{действие}*	Действие при обнаружении в проверяемом файле программы автоматического дозвона.

Параметр	Описание
	Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnJokes` *{действие}*	Действие при обнаружении в проверяемом файле программы-шутки. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`[*] OnRiskware` *{действие}*	Действие при обнаружении в проверяемом файле потенциально опасной программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`[*] OnHacktools` *{действие}*	Действие при обнаружении в проверяемом файле в проверяемом файле хакерской программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`[*] ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `30s`
`[*] HeuristicAnalysis` *{On | Off}*	Использовать или не использовать эвристический анализ для поиска возможных неизвестных угроз. Эвристический анализ повышает надежность проверки, но увеличивает ее длительность. Действие на срабатывание эвристического анализатора задается параметром `OnSuspicious`. Допустимые значения: • `On` — использовать эвристический анализ при проверке. • `Off` — не использовать эвристический анализ. Значение по умолчанию: `On`
`[*] PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает

Параметр	Описание
	предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[*] ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `0`
`[*] MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `0`
`[*] ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (например, страницы HTML, файлы `.jar` и т. п.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[*] MaxCompressionRatio` *{целое число}*	Максимально допустимая степень сжатия проверяемых объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`

Параметр	Описание
`DebugAccess` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о доступе к файлам. Значение по умолчанию: `No`

Настройка индивидуальных параметров мониторинга защищаемых пространств

Для каждого защищаемого пространства файловой системы в конфигурационном файле, наряду с секцией `[LinuxSpider]`, хранящей все параметры работы монитора, задается отдельная секция, определяющая путь к наблюдаемой области файловой системы и параметры ее мониторинга. Каждая индивидуальная секция защищаемого пространства должна иметь имя вида `[LinuxSpider.Space.`<*имя пространства*>`]`, где <*имя пространства*> — уникальный идентификатор защищаемого пространства.

Индивидуальная секция пространства должна включать в себя следующие параметры, отсутствующие в общей секции `[LinuxSpider]`:

Параметр	Описание
`Path` *{путь к каталогу}*	Определяет путь к каталогу, хранящему файлы, которые должны находиться под наблюдением (включая вложенные каталоги). По умолчанию данный параметр имеет пустое значение, поэтому при добавлении защищаемого пространства к области наблюдения обязательно следует задать данный параметр. Значение по умолчанию: *(не задано)*
`Enable` *{логический}*	Содержимое защищаемого пространства, расположенное внутри пути `Path`, должно находиться под наблюдением монитора. Установка данного параметра в `No` предписывает монитору исключить содержимое данного защищаемого пространства из объединенной области наблюдения. Значение по умолчанию: `Yes`



Если у всех защищаемых пространств, указанных в настройках монитора, наблюдение отключено, или их пути не заданы, то SplDer Guard работает вхолостую, поскольку ни один файл дерева файловой системы не будет находиться под наблюдением. Если необходимо контролировать всю файловую систему как единое защищаемое пространство, следует удалить из настроек все именованные секции защищаемых пространств.

Кроме указанных выше, индивидуальные секции защищаемых пространств могут включать в себя список параметров из общей секции настроек компонента, отмеченных обозначением `[*]` в таблице выше, и переопределяющих параметр, заданный для защищаемого пространства (например, действие при обнаружении угрозы, максимальную глубину проверки архивов и т. п.). Если для защищаемого пространства не указан какой-либо из параметров, то мониторинг файлов в этом пространстве регулируется значениями соответствующих параметров из секции `[LinuxSpider]`.

Чтобы добавить новую секцию параметров для защищаемого пространства с тегом *<имя пространства>* при помощи утилиты управления Dr.Web Ctl (запускается командой `drweb-ctl`), выполните команду:

```
# drweb-ctl cfset LinuxSpider.Space -a <имя пространства>
```

Пример:

```
# drweb-ctl cfset LinuxSpider.Space -a Space1
# drweb-ctl cfset LinuxSpider.Space.Space1.Path /home/user1
```

Первая команда добавит в файл конфигурации секцию `[LinuxSpider.Space.Space1]`, а вторая задаст для нее значение параметра `Path`, указав путь к наблюдаемой области файловой системы. Все прочие параметры в данной секции будут совпадать со значениями параметров из общей секции `[LinuxSpider]`.

9.4. Dr.Web MailD

Компонент Dr.Web MailD предназначен для непосредственной проверки сообщений электронной почты, поиска в них вредоносного содержимого (не только вложений, но и ссылок на вредоносные или нежелательные сайты), а также анализа сообщений на наличие признаков спама и соответствие их критериям безопасности, заданных администратором системы электронной почты (проверка тела и заголовков сообщений при помощи указанных администратором регулярных выражений).



При большой интенсивности проверки сообщений электронной почты возможно возникновение проблем с проверкой сообщений из-за исчерпания компонентом Dr.Web Network Checker числа доступных файловых дескрипторов. В этом случае необходимо увеличить величину лимита на число файловых дескрипторов, доступных Dr.Web Desktop Security Suite.

9.4.1. Принципы работы

Компонент может осуществлять защиту электронной почты путем организации *прокси*, выполняющего проверку сообщений электронной почты, передаваемых по протоколу SMTP, POP3 или IMAP4, прозрачно для серверов электронной почты. Для организации данного способа проверки используются компоненты SpIDer Gate и Dr.Web Firewall для Linux. В силу того, что эти компоненты работают только в среде GNU/Linux, этот способ доступен только для этого семейства операционных систем.

Компонент использует правила обработки, определенные в настройках компонента Dr.Web Firewall для Linux.

Для проверки URL, содержащихся в сообщениях электронной почты, используются те же автоматически обновляемые базы категорий веб-ресурсов, которые используются компонентом SpIDer Gate. Для обращения к облачному сервису Dr.Web Cloud используется компонент Dr.Web CloudD (использование облачного сервиса задается в основных настройках Dr.Web Desktop Security Suite, и при необходимости может быть отключено). Для проверки передаваемых данных Dr.Web MailD использует агента сетевой проверки данных Dr.Web Network Checker, который, в свою очередь, инициирует их проверку сканирующим ядром Dr.Web Scanning Engine.

Проверка почтовых вложений на наличие вредоносного кода выполняется непосредственно компонентом Dr.Web MailD.

Для анализа сообщений на наличие признаков спама Dr.Web MailD использует специальный компонент Dr.Web Anti-Spam.



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

9.4.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web MailD из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-maild [<параметры>]
```

Dr.Web MailD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет

Параметр	Описание
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-maild --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web MailD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при поступлении от других компонентов Dr.Web Desktop Security Suite заявок на проверку сообщений электронной почты. Для управления параметрами работы компонента, а также для проверки сообщений электронной почты по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Чтобы запустить утилиту Dr.Web Ctl, используйте команду `drweb-ctl`.

Чтобы получить справку о компоненте из командной строки, выполните команду `man 1 drweb-maild`.

9.4.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[MailD]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента.

Параметр	Описание
	Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-maild`
`FixedSocketPath` *{путь к файлу}*	Путь к файлу Unix-сокета фиксированного экземпляра компонента. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр компонента, доступный клиентам через этот сокет.  Убедитесь, что каталогу с файлом сокета назначены следующие права доступа: `drwxr-xr-x` Чтобы просмотреть права доступа, выполните команду: `$ ls -ld <путь к каталогу>` Значение по умолчанию: *(не задано)*
`TemplatesDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы шаблонов почтовых сообщений, возвращаемых пользователю при блокировке. Значение по умолчанию: `/var/opt/drweb.com/templates/maild`
`ReportLanguages` *{строка}*	Языки, используемые для генерации служебных сообщений (например, сообщений, возвращаемых пользователю при блокировании сообщений электронной почты). Каждый язык идентифицируется двухбуквенным обозначением (`en`, `ru` и т. п.). Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список языки `ru` и `de`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке: `[MailD]` `ReportLanguages = "ru", "de"`

Параметр	Описание
	• Две строки (по одному значению в строке): `[MailD]` `ReportLanguages = ru` `ReportLanguages = de` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset MailD.ReportLanguages -a ru` `# drweb-ctl cfset MailD.ReportLanguages -a de` Значение по умолчанию: `en`
`RepackPassword` *{None | Plain(<password>) | HMAC(<secret>)}*	Способ формирования пароля для архивов с вредоносными объектами, помещаемых в сообщения, доставляемые получателям: • `None` — архивы не будут защищены паролем (не рекомендуется); • `Plain(<password>)` — все архивы будут защищены одним и тем же паролем *<password>*; • `HMAC(<secret>)` — для каждого архива будет сгенерирован уникальный пароль на основании пары (*<secret>*, *<идентификатор сообщения>*). Чтобы восстановить пароль, которым защищен архив, по идентификатору сообщения и известному секрету, выполните команду `drweb-ctl idpass`. ⚠ По умолчанию для данного параметра задано значение `None`, которое рекомендуется изменить в процессе настройки Dr.Web Desktop Security Suite. Значение по умолчанию: `None`
`TemplateContacts` *{строка}*	Контактные данные администратора Dr.Web Desktop Security Suite для вставки в сообщения об угрозах (используется в шаблонах сообщений). Контактная информация будет добавлена в перепакованное сообщение только в том случае, если к нему будет прикреплен защищенный паролем архив с угрозами или иными нежелательными объектами, вырезанными из исходного сообщения. Если, согласно текущему значению параметра `RepackPassword` (см. ниже), прикрепляемые архивы не защищаются паролем, то контактная информация не добавляется в измененное сообщение. Значение по умолчанию: *(не задано)*

Параметр	Описание
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`DnsResolverConfPath` *{путь к файлу}*	Путь к файлу настроек DNS (DNS resolver). Значение по умолчанию: `/etc/resolv.conf`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Значение параметра `IdleTimeLimit` игнорируется (компонент не завершает свою работу по истечении максимального времени простоя), если задано значение какого-либо из параметров: `FixedSocketPath`, `MilterSocket`, `SpamdSocket`, `RspamdHttpSocket`, `RspamdSocket`, `SmtpSocket`, `BccSocket`. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `10m`
`SpoolDir` *{путь к каталогу}*	Каталог для временного хранения проверяемых писем. Значение по умолчанию: `/tmp/com.drweb.maild`
`Hostname` *{строка}*	Имя узла (FQDN) отправителя. Будет фигурировать в строке приветствия HELO/EHLO, полученной от SMTP-клиента, и как значение по умолчанию для `srvname` в заголовке `Authentication-Results`. Значение по умолчанию: *текущее имя хоста*
`CaPath` *{путь к файлу или каталогу}*	Путь к каталогу или файлу с перечнем доверенных корневых сертификатов. Значение по умолчанию: *путь к системному перечню доверенных сертификатов*. Зависит от дистрибутива GNU/Linux. • Для Astra Linux, Debian, Linux Mint, SUSE Linux и Ubuntu обычно используется путь `/etc/ssl/certs/`. • Для CentOS и Fedora — путь `/etc/pki/tls/certs/ca-bundle.crt`.

Параметр	Описание
	• Для других дистрибутивов путь может быть определен с помощью команды `openssl version -d`. • Если эта команда недоступна или дистрибутив ОС опознать не удалось, используется значение `/etc/ssl/certs/`
`WarnOfUnknownDomain` *{логический}*	Добавлять в тело письма предупреждение о том, что домен отправителя не включен в список защищенных доменов (см. параметр `ProtectedDomains`) и необходимо соблюдать меры предосторожности. Текст предупреждения задается параметром `ExternalDomainWarning`. Возможные значения: • `On`, `Yes`, `True` — добавлять предупреждение; • `Off`, `No`, `False` — не добавлять предупреждение. Значение по умолчанию: `No`
`ProtectedDomains` *{строка}*	Список доменов, защищенных продуктами Dr.Web. Если домен отправителя не входит в этот список, то в тело письма будет добавлено предупреждение о том, что необходимо соблюдать меры предосторожности (см. параметры `WarnOfUnknownDomain` и `ExternalDomainWarning`). Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список домены `drweb.com` и `drweb.ru`. 1. Добавление значений в файл конфигурации. • Несколько значений в одной строке: `[MailD]` `ProtectedDomains = "localhost", "drweb.com", "drweb.ru"` • По одному значению в строке: `[MailD]` `ProtectedDomains = localhost` `ProtectedDomains = drweb.com` `ProtectedDomains = drweb.ru` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset MailD.ProtectedDomains -a drweb.com` `# drweb-ctl cfset MailD.ProtectedDomains -a drweb.ru` Значение по умолчанию: `localhost`
`ExternalDomainWarning` *{кодировка; текст предупреждения}*	Текст предупреждения о том, что необходимо соблюдать меры предосторожности, который будет добавлен в тело

Параметр	Описание
	письма, если домен отправителя не включен в список защищенных доменов (см. параметр `ProtectedDomains`), а параметр `WarnOfUnknownDomain` имеет значение `Yes`. При обработке письма название кодировки определяется полем `charset` заголовка письма. Список названий кодировок, соответствующих стандарту RFC2047, доступен по ссылке. Если не удалось определить кодировку, то будет использовано значение `default`. Текст предупреждения в этом случае рекомендуется составлять, используя латинский алфавит. Если задано несколько значений с одинаковой кодировкой, то для такой кодировки будет использован текст, указанный в последнем таком значении. Пример: Добавить текст предупреждения для кодировки KOI8-R (также известной как `csKOI8R`). 1. Добавление значений в файл конфигурации, по одному значению в строке: `[MailD]` `ExternalDomainWarning = "{""default"", ""Attention: The message was sent from an external domain. It is not recommended to follow links, open attachments, or provide confidential information.""}"` `ExternalDomainWarning = "{""utf-8"", ""Внимание: письмо отправлено с внешнего домена. Не рекомендуется переходить по ссылкам, открывать вложения или предоставлять конфиденциальную информацию.""}"` `ExternalDomainWarning = "{""KOI8-R"", ""External domain warning""}"` `ExternalDomainWarning = "{""csKOI8R"", ""External domain warning""}"` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset -a MailD.ExternalDomainWarning '{"KOI8-R", "External domain warning"}'` `# drweb-ctl cfset -a MailD.ExternalDomainWarning '{"csKOI8R", "External domain warning"}'` Значения по умолчанию: `{"default", "Attention: The message was sent from an external domain. It is not recommended to follow links, open attachments, or provide confidential information."}` `{"utf-8", "Внимание: письмо отправлено с внешнего домена. Не рекомендуется переходить по ссылкам, открывать вложения или предоставлять конфиденциальную информацию."}`
`ScanTimeout`	Тайм-аут на проверку одного сообщения.

Параметр	Описание
{интервал времени}	Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `3m`
`HeuristicAnalysis` *{логический}*	Использовать или не использовать эвристический анализ для поиска возможных неизвестных угроз при проверке сообщения, инициированной по запросу Dr.Web MailD. Эвристический анализ повышает надежность проверки, но увеличивает ее длительность. Возможные значения: • `On`, `Yes`, `True` — использовать эвристический анализ; • `Off`, `No`, `False` — не использовать эвристический анализ. Значение по умолчанию: `On`
`PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.

Параметр	Описание
	Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности при проверке других типов объектов с вложениями (например, страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MaxCompressionRatio` *{целое число}*	Максимально допустимая степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке сообщения, инициированной по запросу Dr.Web MailD. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`
`MaxSizeToExtract` *{размер}*	Ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. По умолчанию никаких ограничений на размер файлов в архивах нет. Значение этого параметра указывается как число с суффиксом (`b`, `kb`, `mb`, `gb`). Если суффикс не указан, число интерпретируется как размер в байтах. Если установлено значение `0`, файлы в архивах проверяться не будут. Значение по умолчанию: `None`
`MilterDebugIpc` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (`LogLevel = Debug`) сообщения протокола *Milter*. Возможные значения: • `On`, `Yes`, `True` — сохранять в журнале; • `Off`, `No`, `False` — не сохранять в журнале. Значение по умолчанию: `No`
`MilterTraceContent` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (`LogLevel = Debug`) тело сообщений электронной почты, полученных на проверку через интерфейс *Milter*. Возможные значения:

Параметр	Описание
	• `On`, `Yes`, `True` — сохранять в журнале; • `Off`, `No`, `False` — не сохранять в журнале. Значение по умолчанию: `No`
`MilterSocket` *{путь к файлу | IP-адрес:порт}*	Сокет для подключения к MTA как *Milter*-фильтр сообщений электронной почты (на этот сокет MTA будет выполнять подключение при использовании Dr.Web MailD в качестве соответствующего фильтра). Допускается использование Unix-сокета или сетевого сокета. Правила обработки сообщений, поступающих на проверку через *Milter*, задаются параметром `MilterHook` (см. ниже). Значение по умолчанию: *(не задано)*
`MilterHook` *{путь к файлу | функция Lua}*	Код скрипта на языке Lua для обработки почтовых сообщений, полученных через интерфейс *Milter*, либо путь к файлу этого скрипта. Если указан недоступный файл, то при загрузке компонента будет выдана ошибка. Значение по умолчанию: `local dw = require "drweb"` `local dwcfg = require "drweb.config"` `function milter_hook(ctx)` `  -- Отклонить сообщение, если оно похоже на спам` `  if ctx.message.spam.score >= 100 then` `    dw.notice("Spam score: " .. ctx.message.spam.score)` `    return {action = "reject"}` `  else` `    -- Добавить заголовки X-Drweb-Spam с отчетом о спаме` `    ctx.modifier.add_header_field("X-DrWeb-SpamScore", ctx.message.spam.score)` `    ctx.modifier.add_header_field("X-DrWeb-SpamState", ctx.message.spam.type)` `    ctx.modifier.add_header_field("X-DrWeb-SpamDetail", ctx.message.spam.reason)` `    ctx.modifier.add_header_field("X-DrWeb-SpamVersion", ctx.message.spam.version)` `  end` `  -- Проверить письмо на наличие угроз и, если они имеются, перепаковать его` `  for threat, path in ctx.message.threats{category = {"known_virus", "virus_modification", "unknown_virus", "adware", "dialer"}} do` `    ctx.modifier.repack()` `    dw.notice(threat.name .. " found in " .. (ctx.message.part_at(path).name or path))` `  end`

Параметр	Описание
	<pre>-- Перепаковать, если найден нежелательный URL for url in ctx.message.urls{category = {"infection_source", "not_recommended", "owners_notice"}} do ctx.modifier.repack() dw.notice("URL found: " .. url .. "(" .. url.categories[1] .. ")") end -- Добавить заголовок X-AntiVirus ctx.modifier.add_header_field("X-AntiVirus", "Checked by Dr.Web [MailD version: " .. dwcfg.maild.version .. "]") -- Принять письмо со всеми запланированными преобразованиями return {action = 'accept'} end</pre>
`SpamdDebugIpc` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (`LogLevel = Debug`) сообщения протокола *Spamd*. Возможные значения: • `On`, `Yes`, `True` — сохранять в журнале; • `Off`, `No`, `False` — не сохранять в журнале. Значение по умолчанию: `No`
`SpamdSocket` *{путь к файлу | IP-адрес:порт}*	Сокет для подключения к MTA как *Spamd*-фильтр сообщений электронной почты (на этот сокет MTA будет выполнять подключение при использовании Dr.Web MailD в качестве соответствующего фильтра). Допускается использование Unix-сокета или сетевого сокета. Правила обработки сообщений, поступающих на проверку через *Spamd*, задаются параметром `SpamdReportHook` (см. ниже). Значение по умолчанию: *(не задано)*
`SpamdReportHook` *{путь к файлу | функция Lua}*	Код скрипта на языке Lua для обработки сообщений электронной почты, полученных через интерфейс *Spamd*, либо путь к файлу, содержащему этот скрипт. Если указан недоступный файл, то при загрузке компонента будет выдана ошибка. Значение по умолчанию: <pre>local dw = require "drweb" function spamd_report_hook(ctx) local score = 0 local report = ""</pre>

Параметр	Описание
	<pre>-- Прибавить 1000 баллов за каждую угрозу в сообщении for threat, path in ctx.message.threats{category = {"known_virus", "virus_modification", "unknown_virus", "adware", "dialer"}} do score = score + 1000 report = report .. "Threat found: " .. threat.name .. "\n" dw.notice(threat.name .. " found in " .. (ctx.message.part_at(path).name or path)) end -- Прибавить 100 баллов за каждый нежелательный URL в сообщении for url in ctx.message.urls{category = {"infection_source", "not_recommended", "owners_notice"}} do score = score + 100 report = report .. "Url found: " .. url .. "\n" dw.notice("URL found: " .. url .. "(" .. url.categories[1] .. ")") end -- Добавить спам-рейтинг score = score + ctx.message.spam.score report = report .. "Spam score: " .. ctx.message.spam.score .. "\n" if ctx.message.spam.score >= 100 then dw.notice("Spam score: " .. ctx.message.spam.score) end -- Вернуть результат проверки return { score = score, threshold = 100, report = report } end</pre>
`RspamdDebugIpc` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (`LogLevel = Debug`) сообщения протокола *Rspamd*. Возможные значения: • `On`, `Yes`, `True` — сохранять в журнале; • `Off`, `No`, `False` — не сохранять в журнале. Значение по умолчанию: `No`
`RspamdHttpSocket` *{путь к файлу | IP-адрес:порт}*	Сокет для подключения к MTA в качестве *Rspamd*-фильтра сообщений электронной почты (на этот сокет MTA будет выполнять подключение при использовании Dr.Web MailD в качестве соответствующего фильтра, с использованием HTTP-варианта протокола *Rspamd*). Допускается использование Unix-сокета или сетевого сокета.

Параметр	Описание
	Правила обработки сообщений, поступающих через *Rspamd*, задаются параметром `RspamdHook` (см. ниже). Значение по умолчанию: *(не задано)*
`RspamdSocket` *{путь к файлу | IP-адрес:порт}*	Сокет для подключения к MTA в качестве *Rspamd*-фильтра сообщений электронной почты (на этот сокет MTA будет выполнять подключение при использовании Dr.Web MailD в качестве соответствующего фильтра, с использованием *legacy*-варианта протокола *Rspamd*). Допускается использование Unix-сокета или сетевого сокета. Значение по умолчанию: *(не задано)*
`RspamdHook` *{путь к файлу | функция Lua}*	Код скрипта на языке Lua для обработки сообщений электронной почты, полученных через интерфейс *Rspamd*, либо путь к файлу, содержащему этот скрипт. Если указан недоступный файл, то при загрузке компонента будет выдана ошибка. Значение по умолчанию: `local dw = require "drweb"` `function rspamd_hook(ctx)` `  local score = 0` `  local symbols = {}` `  -- Прибавить 1000 баллов за каждую угрозу в сообщении` `  for threat, path in ctx.message.threats{category = {"known_virus", "virus_modification", "unknown_virus", "adware", "dialer"}} do` `  score = score + 1000` `  table.insert(symbols, {name = threat.name, score = 1000})` `  dw.notice(threat.name .. " found in " .. (ctx.message.part_at(path).name or path))` `  end` `  -- Прибавить 100 баллов за каждый нежелательный URL в сообщении` `  for url in ctx.message.urls{category = {"infection_source", "not_recommended", "owners_notice"}} do` `  score = score + 100` `  table.insert(symbols, {name = "URL " .. url, score = 100})` `  dw.notice("URL found: " .. url .. "(" .. url.categories[1] .. ")")` `  end` `  -- Добавить спам-рейтинг` `  score = score + ctx.message.spam.score` `  table.insert(symbols, {name = "Spam score", score = ctx.message.spam.score})`

Параметр	Описание
	`if ctx.message.spam.score >= 100 then dw.notice("Spam score: " .. ctx.message.spam.score) end -- Вернуть результат проверки return { score = score, threshold = 100, symbols = symbols } end`
`SpfCheckTimeout` *{интервал времени}*	Максимальное общее время, отведенное на проверку SPF. Значение по умолчанию: `20s`
`SpfVoidLimit` *{целое число}*	Максимально допустимое число пустых ответов во время проверки SPF. Значение по умолчанию: `2`
`SmtpDebugIpc` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) SMTP-команды в режиме SMTP. Возможные значения: • `On`, `Yes`, `True` — сохранять в журнале; • `Off`, `No`, `False` — не сохранять в журнале. Значение по умолчанию: `No`
`SmtpTraceContent` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) содержимое почтовых сообщений в режиме SMTP. Возможные значения: • `On`, `Yes`, `True` — сохранять в журнале; • `Off`, `No`, `False` — не сохранять в журнале. Значение по умолчанию: `No`
`SmtpRetryInterval` *{интервал времени}*	Тайм-аут на повторную попытку проверки или отправки сообщения в случае ошибки при работе в режиме SMTP. Допустимые значения: от 1 секунды (`1s`) до 1 дня (`1d`). Значение по умолчанию: `5m`
`SmtpRequireTls` *{Always | IfSupported | Never}*	Политика работы с расширением STARTTLS протокола SMTP в режиме SMTP.

Параметр	Описание
	Допустимые значения: • `Always` — всегда использовать защищенное соединение; прерывать соединение, если сервер не поддерживает его защиту. • `IfSupported` — если сервер поддерживает защищенное соединение, то предпочитать его; в ином случае отправлять сообщения по незащищенным каналам. • `Never` — не использовать защищенное соединение. Значение по умолчанию: `Always`
`SmtpSslCertificate` *{путь к файлу сертификата}*	Путь к файлу сертификата для подключения MTA к Dr.Web MailD, работающему в качестве внешнего фильтра сообщений электронной почты в режиме SMTP или BCC. Значение по умолчанию: *(не задано)*
`SmtpSslKey` *{путь к файлу закрытого ключа}*	Путь к файлу закрытого ключа для подключения MTA к Dr.Web MailD, работающему в качестве внешнего фильтра сообщений электронной почты в режиме SMTP или BCC. Значение по умолчанию: *(не задано)*
`SmtpTimeout` *{интервал времени}*	Максимальное время хранения сообщения в очереди (в минутах), в течение которого должна быть выполнена проверка при работе Dr.Web MailD в режиме SMTP. Если в течение указанного времени проверка не завершилась успешно, то будет выполнено действие, указанное в параметре `SmtpTimeoutAction`. Если указано нулевое значение, проверка выполняется немедленно после помещения сообщения в очередь или после очередной неудачной попытки проверки. Если значение данного параметра превышает значение параметра `SmtpRetryInterval`, то в течение указанного времени будут предприняты две попытки проверки. Допустимые значения: `0`, либо от 1 минуты (`1m`) до 1 недели (`1w`). Значение по умолчанию: `1h`
`SmtpTimeoutAction` *{Accept|Discard}*	Действие, которое выполняется по истечении интервала времени, указанного в параметре `SmtpTimeout`. Допустимые значения: • `Accept` — принять (разрешить MTA отправить сообщение получателю); • `Discard` — отбросить сообщение, не уведомляя отправителя. Значение по умолчанию: `Accept`

Параметр	Описание
`SmtpSocket` *{путь к файлу | IP-адрес:порт}*	Сокет для подключения к MTA в качестве фильтра сообщений электронной почты в режиме SMTP (MTA будет подключаться через этот сокет при использовании Dr.Web MailD в качестве внешнего фильтра). Допускается использование Unix-сокета или сетевого сокета. Сервер, подключающийся через данный сокет, использует сертификат, путь к файлу которого задается параметром `SmtpSslCertificate`, и закрытый ключ, путь к файлу которого задается параметром `SmtpSslKey`. Значение по умолчанию: *(не задано)*
`SmtpSenderRelay` *{путь к файлу | IP-адрес:порт}*	Сокет для подключения Dr.Web MailD к MTA для отправки прошедших проверку сообщений в режиме SMTP (Dr.Web MailD, используемый в качестве внешнего фильтра, будет подключаться к MTA через этот сокет). Допускается использование Unix-сокета или сетевого сокета. Значение по умолчанию: *(не задано)*
`SmtpHook` *{путь к файлу | функция Lua}*	Код скрипта на языке Lua для обработки сообщений электронной почты, полученных на проверку в режиме SMTP, либо путь к файлу, содержащему этот скрипт. Если в секции `[Root]` конфигурационного файла установлено значение параметра `UseVxcube=Yes`, в Lua-скрипт по умолчанию добавляется операция проверки файлов почтовых вложений с помощью Dr.Web vxCube. Значение по умолчанию: `local dw = require "drweb"` `function smtp_hook(ctx)` `  -- Отклонить сообщение, если оно похоже на спам` `  if ctx.message.spam.score >= 100 then` `  dw.notice("Spam score: " .. ctx.message.spam.score)` `  return {action = "discard"}` `  else` `  -- Добавить заголовки X-Drweb-Spam с отчетом о спаме` `  ctx.modifier.add_header_field("X-DrWeb-SpamScore", ctx.message.spam.score)` `  ctx.modifier.add_header_field("X-DrWeb-SpamState", ctx.message.spam.type)` `  ctx.modifier.add_header_field("X-DrWeb-SpamDetail", ctx.message.spam.reason)` `  ctx.modifier.add_header_field("X-DrWeb-SpamVersion", ctx.message.spam.version)` `  end` `  -- Проверить письмо на наличие угроз и, если они имеются, перепаковать его`

Параметр	Описание
	`` threat_categories = {"known_virus", "virus_modification", "unknown_virus", "adware", "dialer"} if ctx.message.has_threat({category = threat_categories}) then for threat, path in ctx.message.threats({category = threat_categories}) do dw.notice(threat.name .. " found in " .. (ctx.message.part_at(path).name or path)) end ctx.modifier.repack() return {action = "accept"} end -- Перепаковать, если найден нежелательный URL url_categories = {"infection_source", "not_recommended", "owners_notice"} if ctx.message.has_url({category = url_categories}) then for url in ctx.message.urls({category = url_categories}) do dw.notice("URL found: " .. url .. " (" .. url.categories[1] .. ")") end ctx.modifier.repack() return {action = "accept"} end -- Принять письмо со всеми запланированными преобразованиями return {action = 'accept'} end ```
`BccSocket` *{путь к файлу | IP-адрес:порт}*	Сокет для подключения к MTA в качестве фильтра сообщений электронной почты в режиме BCC (MTA будет подключаться через этот сокет при использовании Dr.Web MailD в качестве внешнего фильтра). Допускается использование Unix-сокета или сетевого сокета. Сервер, подключающийся через данный сокет, использует сертификат, путь к файлу которого задается параметром `SmtpSslCertificate`, и закрытый ключ, путь к файлу которого задается параметром `SmtpSslKey`. Значение по умолчанию: *(не задано)*
`BccReporterAddress` *{строка}*	Адрес электронной почты, с которого будут отправляться отчеты Dr.Web MailD по итогам проверки вложений почтовых сообщений в режиме BCC. Значение по умолчанию: *(не задано)*
`BccReporterPassword` *{None | Plain(<пароль>)}*	Пароль от почтового ящика, с которого будут отправляться отчеты Dr.Web MailD по итогам проверки вложений почтовых сообщений в режиме BCC.

Параметр	Описание
	Возможные значения: • `None` — ящик не защищен паролем; • `Plain(<`*`пароль`*`>)` — ящик защищен указанным паролем. Значение по умолчанию: `None`
`BccReportRecipientAddress` *{строка}*	Адрес электронной почты, на который будут отправляться отчеты Dr.Web MailD по итогам проверки вложений почтовых сообщений в режиме BCC. Значение по умолчанию: *(не задано)*
`BccSmtpServer` *{строка}*	Адрес MTA для отправки почтовых сообщений в режимах SMTP и BCC. Допускается использование домена, IP-адреса или Unix-сокета. Значение по умолчанию: *(не задано)*
`BccTimeout`	Максимальное время хранения сообщения в очереди (в минутах), в течение которого должна быть выполнена проверка при работе Dr.Web MailD в режиме BCC. Если в течение указанного времени проверка не завершилась успешно, то будет выполнено действие `Discard`. Если указано нулевое значение, проверка выполняется немедленно после помещения сообщения в очередь или после очередной неудачной попытки проверки. Если значение данного параметра превышает значение параметра `SmtpRetryInterval`, то в течение указанного времени будут предприняты две попытки проверки. Допустимые значения: `0`, либо от 1 минуты (`1m`) до 1 недели (`1w`). Значение по умолчанию: `1h`
`VxcubePlatforms` *{платформа, ... | All}*	Список платформ ОС для выполнения файлов почтовых вложений при использовании Dr.Web vxCube в качестве инструмента проверки почтовых сообщений в режиме внешнего фильтра (SMTP или BCC). Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Допустимые значения: • <*платформа*> — значение поля `os_code` (название ОС с указанием разрядности) из API-вызова `platforms` в Dr.Web vxCube (подробнее см. Руководство пользователя Dr.Web vxCube, раздел Platform); • `All` — все доступные платформы.

Параметр	Описание
	Значение по умолчанию: `All`
`VxcubeFileFormats` *{формат, ... | All}*	Список форматов файлов почтовых вложений, которые будут отправляться на анализ при использовании Dr.Web vxCube в качестве инструмента проверки почтовых сообщений в режиме внешнего фильтра (SMTP или BCC). Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Допустимые значения: • *<формат>* — значение поля `name` (буквенное обозначение формата) из API-вызова `formats` в Dr.Web vxCube (подробнее см. Руководство пользователя Dr.Web vxCube, раздел Format); • `All` — все доступные форматы. Значение по умолчанию: `All`
`VxcubeSampleRunTime` *{интервал времени}*	Время выполнения файла почтового вложения, отправленного на анализ в Dr.Web vxCube при использовании его в качестве инструмента проверки почтовых сообщений в режиме внешнего фильтра (SMTP или BCC). Значение по умолчанию: `1m`

9.5. Dr.Web Anti-Spam

Компонент Dr.Web Anti-Spam предназначен для непосредственной проверки сообщений электронной почты на наличие признаков спама. Этот компонент используется компонентом проверки сообщений электронной почты Dr.Web MailD. В зависимости от поставки, компонент Dr.Web Anti-Spam может отсутствовать в составе решения Dr.Web Desktop Security Suite (в этом случае Dr.Web MailD не выполняет анализ сообщений электронной почты на наличие признаков спама).



Компонент не поддерживается для архитектур ARM64, E2K и IBM POWER (ppc64el).

9.5.1. Принципы работы

Анализ сообщений, полученных от Dr.Web MailD (или иного внешнего приложения), на наличие признаков спама производится с использованием антиспам-библиотеки и

компонента Dr.Web Anti-Spam. Анализ сообщений производится автономно без обращения к внешним источникам информации о спаме. Данное решение обеспечивает высокую скорость обработки писем и постоянное улучшение качества анализа сообщений благодаря динамическому обновлению базы правил спам-классификации сообщений (обновление производится автоматически посредством компонента обновления Dr.Web Updater).

Вы можете создать свой собственный компонент (внешнее приложение), использующий Dr.Web Anti-Spam для проверки почтовых сообщений на спам. Для этого компонент Dr.Web Anti-Spam предоставляет специализированный API, основанный на технологии Google Protobuf. Для получения описания API Dr.Web Anti-Spam, а также примеров кода клиентского приложения, использующего Dr.Web Anti-Spam, обратитесь в отдел по работе с партнерами компании «Доктор Веб».

В Dr.Web Desktop Security Suite для архитектур ARM64, E2K и IBM POWER (ppc64el) компонент Dr.Web Anti-Spam отсутствует.

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 сохраните каждое такое сообщение в отдельный файл с расширением `.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*.

9.5.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Anti-Spam из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-ase [<параметры>]
```

Dr.Web Anti-Spam допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-ase --help
```

Эта команда выведет на экран краткую справку компонента Dr.Web Anti-Spam.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD и контролируется компонентом Dr.Web MailD при проверке сообщений электронной почты на спам. При этом, если в настройках компонента Dr.Web Anti-Spam задано значение параметра `FixedSocket`, то один экземпляр Dr.Web Anti-Spam будет автоматически запущен компонентом Dr.Web ConfigD и постоянно доступен клиентам через указанный Unix-сокет. Для управления параметрами работы компонента, а также для проверки почтовых объектов по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки (запускается командой `drweb-ctl`).



Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-ase`.

9.5.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[Antispam]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-ase`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Если установлено значение параметра `FixedSocket`, то настройка игнорируется (компонент не завершает свою работу по истечении максимального времени простоя). Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`FixedSocket` *{путь к файлу}*	Путь к файлу сокета фиксированной копии компонента. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр компонента, доступный клиентам через этот сокет.

Параметр	Описание
	 Убедитесь, что каталогу с файлом сокета назначены следующие права доступа: `drwxr-xr-x` Чтобы просмотреть права доступа, выполните команду: `$ ls -ld <путь к каталогу>` Значение по умолчанию: *(не задано)*
`FullCheck` *{логический}*	Выполнять или не выполнять полную проверку сообщения на наличие признаков спама. Если `No`, то проверка будет остановлена, как только число баллов спама превысит величину, указанную в параметре `FastCheckStopThreshold`. Значение по умолчанию: `Yes`
`AllowCyrillicText` *{логический}*	Добавлять или не добавлять баллы в спам-рейтинг, если сообщение содержит текст на кириллице. Если параметр имеет значение `No`, то за наличие текста на кириллице начисляются дополнительные баллы спама. Значение по умолчанию: `Yes`
`AllowCjkText` *{логический}*	Добавлять или не добавлять баллы в спам-рейтинг, если сообщение содержит текст на китайском, корейском, японском языках. Если параметр имеет значение `No`, то за наличие текста на этих языках начисляются дополнительные баллы спама. Значение по умолчанию: `Yes`
`CheckCommercialEmails` *{логический}*	Исключать из проверки коммерческие сообщения (рекламные рассылки, уведомления об акциях и распродажах и т. п.). Если `No`, то такие сообщения классифицируются как спам. Значение по умолчанию: `No`
`CheckSuspiciousEmails` *{логический}*	Исключать из проверки подозрительные сообщения (например, содержащие предложения денежных переводов). Если `No`, то такие сообщения классифицируются как спам. Значение по умолчанию: `No`
`CheckCommunityEmails` *{логический}*	Исключать из проверки сообщения от социальных сетей. Если `No`, то такие сообщения классифицируются как спам. Значение по умолчанию: `No`
`CheckTransactionalEmails` *{логический}*	Исключать из проверки сообщения о транзакциях (регистрация, покупка товара или услуги и т. п.). Если `No`, то такие сообщения классифицируются как спам. Значение по умолчанию: `No`

Параметр	Описание
`DetectSpamType` *{логический}*	Отключать проверку на тип спама (мошенничество, аферы). Если `No`, то такие сообщения классифицируются как спам. Значение по умолчанию: `No`
`FastCheckStopThreshold` *{целое число}*	Предельное число баллов спама, по достижении которого проверка сообщения останавливается, если параметр `FullCheck` имеет значение `No`. Значение по умолчанию: `300`

9.6. Dr.Web Mail Quarantine

Менеджер очереди почтовых сообщений Dr.Web Mail Quarantine предназначен для хранения писем и их метаинформации на жестком диске во время проверки писем.

Dr.Web Mail Quarantine используется компонентом Dr.Web MailD при работе в режимах SMTP и BCC. Dr.Web Mail Quarantine обеспечивает сохранение очереди сообщений и бесперебойное протекание процессов проверки и переотправки сообщений в случае ошибок компонента Dr.Web MailD или потери соединения с MTA.

9.6.1. Принципы работы

Компонент Dr.Web Mail Quarantine обеспечивает выполнение двух основных задач:

- Сохранение очереди писем и информации о них на жестком диске на время проверки писем компонентом Dr.Web MailD. Письма хранятся как файлы, а информация о них сохраняется в реляционной базе данных SQLite. Хранение писем необходимо для работы режимах SMTP и BCC.
- Повторное направление письма в компонент Dr.Web MailD через определенный таймаут в случае возникновения ошибки в процессе обработки письма (например, если не получилось осуществить переотправку письма). С помощью компонента обеспечивается бесперебойная передача обработанного письма в MTA.

9.6.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Mail Quarantine из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-mail-quarantine [<параметры>]
```

Dr.Web Mail Quarantine допускает использование следующих параметров:

Параметр	Описание

`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-mail-quarantine --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Mail Quarantine.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-mail-quarantine`.

9.6.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[MailQuarantine]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log`	Метод ведения журнала компонента.

Параметр	Описание
{тип журнала}	Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-mail-quarantine`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`SpoolDir` *{путь к каталогу}*	Каталог в локальной файловой системе, используемый для временного хранения писем и метаданных. Значение по умолчанию: `/var/opt/drweb.com/lib/mail-quarantine`

9.7. SpIDer Gate



Данный компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Компонент проверки сетевого трафика и URL SpIDer Gate предназначен для проверки данных, загружаемых на локальный узел из сети или передаваемых в сеть с локального узла, на наличие угроз и предотвращения соединения с узлами сети, внесенными в нежелательные категории веб-ресурсов и в черные списки, формируемые системным администратором самостоятельно.

Вы можете указать в настройках компонента, протоколы каких типов следует проверять. Компонент содержит в себе анализатор типа протокола, используемого для передачи данных по проверяемому соединению. Если установлено, что протокол является почтовым, для анализа данных и поиска угроз используется компонент проверки сообщений электронной почты Dr.Web MailD.

Для проверки принадлежности URL той или иной категории (в рамках проверки соединений, использующих протокол HTTP/HTTPS) компонент использует как базу категорий веб-ресурсов, регулярно обновляемую с серверов обновлений компании «Доктор Веб», так и опрашивает облачный сервис Dr.Web Cloud. Компания «Доктор Веб» поддерживает следующие категории веб-ресурсов:

- *InfectionSource* — сайты, содержащие вредоносное ПО («источники распространения угроз»).
- *NotRecommended* — сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению.
- *AdultContent* — сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.
- *Violence* — сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
- *Weapons* — сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
- *Gambling* — сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.
- *Drugs* — сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
- *ObsceneLanguage* — сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
- *Chats* — сайты для обмена сообщениями в режиме реального времени.
- *Terrorism* — сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.

- *FreeEmail* — сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика.
- *SocialNetworks* — социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств.
- *DueToCopyrightNotice* — сайты, ссылки на которые указаны правообладателями произведений, защищенных авторскими правами (кинофильмы, музыкальные произведения и т. д.).
- *OnlineGames* — сайты, на которых размещены игры, использующие постоянное соединение с интернетом.
- *Anonymizers* — сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам.
- *CryptocurrencyMiningPool* — сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют.
- *Jobs* — сайты, предназначенные для поиска вакансий.

Системный администратор может определять, доступ к узлам каких категорий является нежелательным. Дополнительно пользователь может формировать собственные черные списки узлов, доступ к которым будет блокироваться, а также белые списки узлов, доступ к которым будет разрешаться, даже если они относятся к нежелательным категориям. Для URL, информация о которых отсутствует в локальных черных списках и базе категорий веб-ресурсов, компонент может отправлять запросы в облачный сервис Dr.Web Cloud с целью проверки, не имеется ли информации об их вредоносности, полученной от других продуктов Dr.Web в режиме реального времени.



Один и тот же сайт может принадлежать нескольким категориям одновременно. Доступ к такому сайту будет заблокирован, если он принадлежит хотя бы одной из категорий, доступ к которой нежелателен.

Даже если сайт включен в белый список, то отправляемые и загружаемые с него данные все равно проверяются на наличие угроз.

В случае большой интенсивности проверки файлов, передаваемых по протоколу HTTP, возможно возникновение проблем с проверкой из-за исчерпания компонентом Dr.Web Network Checker числа доступных файловых дескрипторов. В этом случае необходимо увеличить лимит на число файловых дескрипторов, доступных Dr.Web Desktop Security Suite.

9.7.1. Принципы работы

Компонент SpIDer Gate выполняет контроль сетевых соединений, устанавливаемых пользовательскими приложениями. Компонент проверяет, находится ли узел, с которым клиентское приложение собирается установить соединение, в любой из категорий веб-ресурсов, отмеченной в настройках как нежелательная для посещения. Кроме этого компонент может отправлять запросы на проверку URL в облачный сервис Dr.Web

Cloud. Если URL обнаружен в какой-либо из нежелательных категорий (в том числе сервисом Dr.Web Cloud) или в черном списке, сформированным системным администратором, то соединение разрывается, а пользователю (если соединение устанавливалось по протоколу HTTP/HTTPS) возвращается HTML-страница с сообщением о запрете соединения, сформированная SpIDer Gate на основании шаблона, поставляемого совместно с компонентом. Данная страница содержит сообщение о невозможности доступа к запрошенному ресурсу и описание причины отказа. Аналогичная страница формируется и возвращается клиенту в случае, если в передаваемых данных SpIDer Gate обнаружит угрозу, подлежащую блокировке. Если соединение использует протокол, отличный от HTTP(S), то компонент выполняет только проверку того, разрешено ли установление соединения с данным узлом. Если протокол является почтовым (SMTP, POP3 или IMAP), для анализа данных и поиска угроз используется компонент проверки сообщений электронной почты Dr.Web MailD. Этот компонент самостоятельно разбирает сообщения электронной почты, извлекая вложенные файлы и URL. При этом компонент использует параметры блокировки, общие с компонентом SpIDer Gate.

Перенаправление соединений, устанавливаемых клиентскими приложениями с удаленными серверами, осуществляется прозрачно для клиентских приложений сервисным компонентом Dr.Web Firewall для Linux, выполняющим динамическое управление правилами NetFilter, системного компонента Linux.

Для регулярного автоматического обновления базы категорий веб-ресурсов с серверов компании «Доктор Веб» используется тот же компонент Dr.Web Updater, который обновляет вирусные базы для сканирующего ядра Dr.Web Scanning Engine. Для обращения к облачному сервису Dr.Web Cloud используется компонент Dr.Web CloudD (использование облачного сервиса задается в основных настройках Dr.Web Desktop Security Suite и при необходимости может быть отключено). Для проверки передаваемых данных SpIDer Gate использует агента сетевой проверки данных Dr.Web Network Checker, который, в свою очередь, инициирует их проверку сканирующим ядром Dr.Web Scanning Engine.

9.7.2. Аргументы командной строки

Чтобы запустить компонент SpIDer Gate из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-gated [<параметры>]
```

SpIDer Gate допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет

`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-gated --help
```

Данная команда выведет на экран краткую справку компонента SpIDer Gate.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-gated`.

9.7.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[GateD]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-gated`

Параметр	Описание
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`TemplatesDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы шаблонов HTML-страниц уведомлений о блокировке веб-ресурсов. Значение по умолчанию: `/var/opt/drweb.com/templates/gated`
`CaPath` *{путь}*	Путь к каталогу или файлу с перечнем доверенных корневых сертификатов. Значение по умолчанию: *Путь к системному перечню доверенных сертификатов*. Зависит от дистрибутива GNU/Linux. • Для Astra Linux, Debian, Linux Mint, SUSE Linux и Ubuntu это обычно путь `/etc/ssl/certs/`. • Для CentOS и Fedora — `/etc/pki/tls/certs/ca-bundle.crt`. • Для других дистрибутивов путь может быть определен с помощью команды `openssl version -d`. • Если команда недоступна или дистрибутив ОС опознать не удалось, используется значение `/etc/ssl/certs/`.



Изменения, внесенные в настройки проверки соединений, не влияют на проверку соединений, которые уже были установлены приложениями до внесения изменений.

Другие параметры настройки проверки трафика, включая правила проверки, задаются в настройках сервисного компонента Dr.Web Firewall для Linux.

9.8. Dr.Web Firewall для Linux



Данный компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Для корректной работы компонента 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.

Компонент Dr.Web Firewall для Linux является вспомогательным и играет роль менеджера соединений для SplDer Gate. Dr.Web Firewall для Linux обеспечивает прохождение устанавливаемых соединений через SplDer Gate для проверки передаваемого трафика.

9.8.1. Принципы работы

В этом разделе

- Общие сведения
- Механизм перехвата соединений
  - Действия в правилах iptables и nftables
  - Метки пакетов и соединений
  - Маршруты и политики маршрутизации (ip rule, ip route)
  - Правила NetFilter (iptables)
  - Правила NetFilter (nftables)
- Порядок перехвата соединений

Общие сведения

Компонент Dr.Web Firewall для Linux обеспечивает корректную работу компонента SplDer Gate, анализируя правила маршрутизации, заданные для NetFilter (системного компонента Linux), и модифицируя их таким образом, чтобы устанавливаемые соединения перенаправлялись на SplDer Gate, который выступает в качестве промежуточного звена (прокси) между клиентским приложением и удаленным сервером.

Dr.Web Firewall для Linux может отдельно управлять правилами перенаправления исходящих и входящих, а также транзитных соединений. Для тонкой настройки правил пропуска или перенаправления соединений компонент может использовать как правила, внедренные в настройки, так и скрипт проверки, написанный на языке Lua.

Dr.Web Firewall для Linux поддерживает настройку Netfilter с помощью интерфейсов `nftables` и `iptables` (последний используется для совместимости).



Чтобы получить более подробную информацию об интерфейсах для подсистемы Netfilter, выполните команды `$ man iptables` и `$ man nftables`.

Механизм перехвата соединений

Для перехвата соединений Dr.Web Firewall для Linux использует таблицы маршрутизации, указанные в базе данных политик маршрутизации, а также интерфейс *nf_conntrack* системного компонента NetFilter. Перехваченные соединения и передающиеся по ним пакеты с целью правильной маршрутизации помечаются битовыми метками, которые позволяют Dr.Web Firewall для Linux принимать правильные решения о перенаправлении соединений и обработке передающихся пакетов на различных этапах прохождения ими цепочек в NetFilter.



Чтобы получить более подробную информацию об управлении политиками маршрутизации, выполните команды `$ man ip`, `$ man ip route` и `$ man ip rule`.

Действия в правилах iptables и nftables

Dr.Web Firewall для Linux использует следующие действия в правилах `iptables` и `nftables`:

- *MARK* — присвоить пакету указанную числовую метку.
- *TPROXY* — установить изначальный адрес назначения соединения и перенаправить пакет из цепочки *PREROUTING* NetFilter на указанный сетевой сокет (<*IP-адрес*>:<*порт*>), не меняя содержимое пакета.
- *NFQUEUE* — передать пакет из сетевого стека ядра на проверку процессу, работающему вне пространства ядра. Dr.Web Firewall для Linux подключается к очереди *NFQUEUE* с заданным номером через специальный *Netlink*-сокет и получает пакеты, по которым необходимо вынести вердикты по дальнейшей обработке (Dr.Web Firewall для Linux обязан сообщить NetFilter один из следующих вердиктов: *DROP*, *ACCEPT*, *REPEAT*).

Действие *CONNMARK* (присвоить соединению указанную числовую метку) поддерживается в `iptables`, но не поддерживается в `nftables`. В правилах `nftables` следует использовать выражения `ct mark` или `ct mark set`.

Метки пакетов и соединений

Для пометки пакетов Dr.Web Firewall для Linux использует следующие три бита (из доступных 32 бит) в метках пакетов и в метке соединения:

- Бит `LDM` (*Local Delivery Mark*) — признак локального соединения. Пакеты, в метке которых установлен этот бит, с помощью установленных правил маршрутизации направляются на локальный хост.
- Бит `CPM` (*Client Packets Mark*) — признак соединения между клиентом (инициатором соединения) и прокси, т. е. Dr.Web Firewall для Linux.
- Бит `SPM` (*Server Packets Mark*) — признак соединения между прокси, т. е. Dr.Web Firewall для Linux, и сервером (приемником соединения).

Биты `LDM`, `CPM` и `SPM` могут быть любыми *разными* битами, которые не используются для пометки пакетов другими приложениями, выполняющими маршрутизацию соединений. При настройках по умолчанию Dr.Web Firewall для Linux выбирает подходящие (не используемые другими приложениями) биты автоматически.

Маршруты и политики маршрутизации (ip rule, ip route)

Для корректной работы Dr.Web Firewall для Linux (в любом режиме проверки соединений) в системе должна быть настроена политика маршрутизации `ip rule`, использующая таблицу маршрутов с номером 100:

```
from all fwmark <LDM>/<LDM> lookup 100
```

В эту таблицу должен быть добавлен маршрут следующего вида:

```
local default dev lo scope host
```

Данная политика маршрутизации гарантирует, что пакеты, в метке которых установлен бит `LDM`, всегда направляются на локальный узел.



Здесь и далее выражение <*XXX*> для бита `XXX` представляет собой шестнадцатеричное (*hexadecimal*) число, равное 2^N, где *N* — порядковый номер бита `XXX` в метке пакета. Например, если в качестве бита `LDM` выбран самый младший (нулевой) бит метки пакета, то <*LDM*> = 2^0 = *0x1*.

Правила NetFilter (iptables)

При использовании `iptables` для корректной работы Dr.Web Firewall для Linux (в любом режиме проверки соединений) в таблицах `nat` и `mangle` соответствующих цепочек подсистемы NetFilter должны присутствовать следующие шесть правил (представлены в формате вывода команды `# iptables-save`):

```
*nat
-A POSTROUTING -o lo -m comment --comment drweb-firewall -m mark --mark <LDM>/<LDM> -j
ACCEPT
*mangle
-A PREROUTING -m comment --comment drweb-firewall -m mark --mark 0x0/<CPM+SPM> -m
connmark --mark <SPM>/<CPM+SPM> -j MARK --set-xmark <LDM>/<LDM>
-A PREROUTING -p tcp -m comment --comment drweb-firewall -m mark ! --mark
<CPM+SPM>/<CPM+SPM> -m connmark --mark <CPM>/<CPM+SPM> -j TPROXY --on-port <порт>
--on-ip <IP-адрес> --tproxy-mark <LDM>/<LDM>
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark <CPM>/<CPM+SPM> -j
CONNMARK --set-xmark <CPM>/0xffffffff
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark <SPM>/<CPM+SPM> -j
CONNMARK --set-xmark <SPM>/0xffffffff
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark 0x0/<CPM+SPM> -m connmark
! --mark 0x0/<CPM+SPM> -j MARK --set-xmark <LDM>/<LDM>
```



В описании ниже этим правилам присвоены порядковые номера 1–6 (в том порядке, в котором они здесь перечислены). Выражение <*X*+*Y*> обозначает число, равное побитовому «*ИЛИ*» (сумме) соответствующих чисел *X* и *Y*.

Параметры <*IP-адрес*> и <*порт*> в правиле № 3 указывают на сетевой сокет, на котором Dr.Web Firewall для Linux контролирует перехваченные соединения.

Кроме того, при включении в настройках Dr.Web Firewall для Linux режима перехвата соединений (исходящих, входящих и транзитных), в таблицах `mangle` соответствующих цепочек (*OUTPUT*, *INPUT*, *FORWARD*) должны присутствовать следующие дополнительные правила (по одному для каждого из режимов):

- Для перехвата исходящих соединений (*OUTPUT*):

  ```
  -A OUTPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags SYN,ACK SYN -m
  mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <ONum> --queue-bypass
  ```

- Для перехвата входящих соединений (*INPUT*):

  ```
  -A INPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags SYN,ACK SYN -m
  mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <INum> --queue-bypass
  ```

- Для перехвата транзитных соединений (*FORWARD*):

  ```
  -A FORWARD -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags SYN,ACK SYN -
  m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <FNum> --queue-bypass
  ```



В описании ниже этим правилам присвоены порядковые номера 7, 8 и 9 (в том порядке, в котором они здесь перечислены).

Здесь <*ONum*>, <*INum*> и <*FNum*> — номера очередей в *NFQUEUE*, в которых Dr.Web Firewall для Linux ожидает появления пакетов, сигнализирующих об установке соединений соответствующих направлений (это пакеты с установленным флагом `SYN`, но со снятым флагом `ACK`).

Правила NetFilter (nftables)

При использовании `nftables` для корректной работы Dr.Web Firewall для Linux (в любом режиме проверки соединений) в таблице `drweb-firewall` подсистемы NetFilter должны присутствовать следующие шесть правил (представлены в формате вывода команды `# nft list ruleset`, вывод будет отличаться на разных ОС):

```
table ip drweb-firewall {
	chain prerouting {
		type filter hook prerouting priority mangle; policy accept;
		meta mark & <CPM+SPM> == 0x0 ct mark & <CPM+SPM> == <SPM> meta mark set
meta mark | <LDM> counter packets 0 bytes 0 comment "drweb-firewall"
		meta l4proto tcp meta mark & <CPM+SPM> != <CPM+SPM> ct mark & <CPM+SPM>
== <CPM> tproxy to <IP-адрес>:<порт> meta mark set meta mark | <LDM> counter packets 0
bytes 0 accept comment "drweb-firewall"
	}

	chain output {
		type route hook output priority mangle; policy accept;
		meta l4proto tcp @th,104,8 & 0x12 == <CPM> meta mark & <CPM+SPM> == 0x0
counter packets 0 bytes 0 queue flags bypass to 0 comment "drweb-firewall"
		meta mark & <CPM+SPM> == <CPM> ct mark set ct mark & <CPM> | <CPM>
counter packets 0 bytes 0 comment "drweb-firewall"
		meta mark & <CPM+SPM> == <SPM> ct mark set ct mark & <SPM> | <SPM>
counter packets 0 bytes 0 comment "drweb-firewall"
		meta mark & <CPM+SPM> == 0x0 ct mark & <CPM+SPM> != 0x0 meta mark set
meta mark | <LDM> counter packets 0 bytes 0 comment "drweb-firewall"
	}

	chain input {
		type filter hook input priority mangle; policy accept;
	}

	chain forward {
		type filter hook forward priority mangle; policy accept;
	}
}
```

Выражение <*X*+*Y*> обозначает число, равное побитовому «ИЛИ» (сумме) соответствующих чисел *X* и *Y*.

Параметры <*IP-адрес*> и <*порт*> указывают на сетевой сокет, на котором Dr.Web Firewall для Linux контролирует перехваченные соединения.

При включении в настройках Dr.Web Firewall для Linux режима перехвата соединений (исходящих, входящих и транзитных), в таблице `drweb-firewall` соответствующих цепочек (*OUTPUT*, *INPUT*, *FORWARD*) должны присутствовать следующие правила (по одному для каждого из режимов):

- Для перехвата исходящих соединений (*OUTPUT*):

```
meta l4proto tcp @th,104,8 & 0x12 == <CPM> meta mark & <CPM+SPM> == 0x0 counter
packets 0 bytes 0 queue flags bypass to 0 comment "drweb-firewall"
```

- Для перехвата входящих соединений (*INPUT*):

```
meta l4proto tcp @th,104,8 & 0x12 == <CPM> meta mark & <CPM+SPM> == 0x0 counter
packets 0 bytes 0 queue flags bypass to 1 comment "drweb-firewall"
```

- Для перехвата транзитных соединений (*FORWARD*):

```
meta l4proto tcp @th,104,8 & 0x12 == <CPM> meta mark & <CPM+SPM> == 0x0 counter
packets 0 bytes 0 queue flags bypass to 2 comment "drweb-firewall"
```

Порядок перехвата соединений

Согласно любому из правил `iptables` № 7, 8 и 9, пакеты, сигнализирующие о начале нового сетевого соединения соответствующего направления, если они не помечены одновременно битами `CPM` и `SPM`, помещаются NetFilter в соответствующие очереди *NFQUEUE*, откуда они будут прочитаны Dr.Web Firewall для Linux через интерфейс *nf_conntrack*. Правила № 4 и 5 отмечают само соединение как перехватываемое, т. е. в метке соединения устанавливается бит, указывающий направление соединения. Номер этого бита в метке соединения совпадает с номером бита в метке пакета. В результате этого пакеты, посылаемые по этому соединению, благодаря правилам № 2, 3 и 6, будут получены Dr.Web Firewall для Linux. Правило № 1 добавляется в начало цепочки *POSTROUTING* таблицы `nat`, чтобы в случае настроенного NAT не транслировать адреса для маркированных пакетов, так как это нарушит логику перехвата и обработки соединений Dr.Web Firewall для Linux.

При появлении пакета в одной из очередей *NFQUEUE* Dr.Web Firewall для Linux выполняет базовую проверку правильности пакета на тот случай, если в NetFilter установлены неверные правила. Далее Dr.Web Firewall для Linux пытается соединиться с сервером от своего имени с сокета, имеющего метку `PSC`. При этом сработает правило № 5. Правило локальной доставки № 6 не сработает, поскольку на пакете стоит метка `SPM`, а это правило действует только для пакетов с меткой *<CPM+SPM>*.

- *Если соединиться с сервером не удалось*, Dr.Web Firewall для Linux формирует для клиента пакет с установленным битом `RST`, заменяя в пакете пару *<IP-адрес>:<порт>* на адрес сетевого сокета запрашиваемого сервера. В *NFQUEUE* при этом отправляется вердикт *DROP*. На сокете, с которого будет оправлен пакет с битом `RST`, установлена метка *<CPM+SPM>*, так что ни одно из указанных выше правил не сработает, и этот пакет будет доставлен клиенту по обычным правилам маршрутизации.
- *Если соединение с удаленным сервером удалось установить*, Dr.Web Firewall для Linux копирует перехваченный SYN-пакет и повторно отправляет его с сокета, имеющего

метку <*LDM*+*CPM*>, чтобы отправленный пакет был перенаправлен на локальный сетевой сокет. Благодаря установленному биту `LDM`, в процессе выбора выходного интерфейса, согласно заданным правилам маршрутизации, отправленный пакет попадет на интерфейс *loopback*, откуда попадет в цепочку NetFilter *PREROUTING*, где для него сработает правило № 3. Таким образом, отправленный пакет в неизменном виде будет перенаправлен на сетевой сокет Dr.Web Firewall для Linux. Данный прием позволяет Dr.Web Firewall для Linux сохранить полную адресную четверку для соединения (IP-адрес и порт отправителя пакета, IP-адрес и порт получателя пакета).

Для сетевого сокета, на котором Dr.Web Firewall для Linux принимает перехватываемые соединения согласно правилу № 3, установлена опция `IP_TRANSPARENT` и метка <*LDM*+*CPM*>, благодаря чему пакеты, отправляемые Dr.Web Firewall для Linux с этого сокета, не попадут в очереди *NFQUEUE*. При подключении клиента производится поиск парного сокета по сохраненной адресной четверке (IP-адрес и порт отправителя, IP-адрес и порт получателя). После того, как соединение с клиентом и с сервером установлено, к соединению применяется процедура проверки, заданная в виде процедуры на языке Lua, а также правила проверки, заданные в настройках Dr.Web Firewall для Linux. Если проверки пройдены успешно и соединение не подлежит разрыву, то сопоставленная пара сокетов, соединяющая клиентскую и серверную сторону установленного соединения, передается компоненту SpIDer Gate для анализа передаваемых по соединению данных. Дальнейшее взаимодействие клиента и сервера производится через посредника, роль которого играет SpIDer Gate. Кроме пары сокетов, ассоциированных с клиентской и серверной стороной соединения, SpIDer Gate получает от Dr.Web Firewall для Linux параметры и правила проверки установленного соединения.

Упрощенно схема работы Dr.Web Firewall для Linux показана на рисунке ниже.

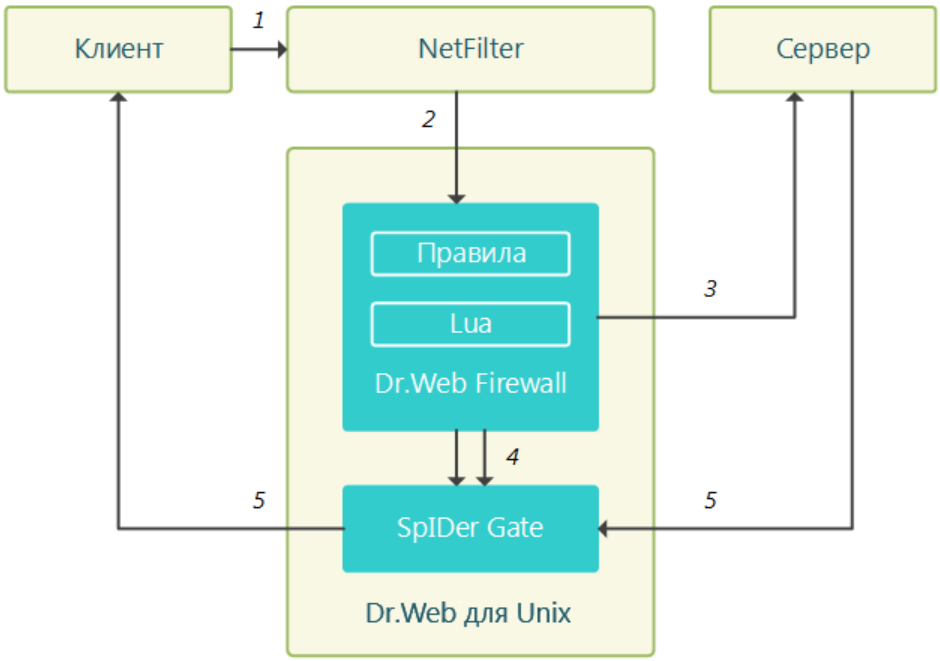


Рисунок 52. Схема работы Dr.Web Firewall для Linux

Цифрами обозначены следующие этапы обработки соединения:

1. Попытка клиента установить соединение с сервером.
2. Перенаправление NetFilter устанавливаемого соединения в Dr.Web Firewall для Linux согласно правилам маршрутизации.
3. Попытка Dr.Web Firewall для Linux установить соединение с сервером от имени клиента и проверка соединения.
4. Передача пары сокетов, ассоциированных с клиентской и серверной сторонами соединения, SpIDer Gate для обслуживания соединения, а также параметров и правил его проверки.
5. Обмен данными между сервером и клиентом через SpIDer Gate в роли посредника.

Для правильной работы компонента Dr.Web Firewall для Linux необходимо наличие указанных правил в таблицах маршрутизации с правильными номерами битов пометки, очередей *NFQUEUE* и адресом сетевого сокета для перехвата соединений. При настройках по умолчанию компонент выполняет надлежащую настройку правил автоматически. Если автоматическая настройка соединений компонентом отключена в его настройках, необходимо обеспечить наличие необходимых правил вручную при начале работы компонента.

9.8.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Firewall для Linux из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-firewall [<параметры>]
```

Dr.Web Firewall для Linux допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-firewall --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Firewall для Linux.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-firewall`.

9.8.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Правила проверки трафика и блокировки доступа

- Просмотр и редактирование правил
- Просмотр правил с помощью команды drweb-ctl cfshow
- Редактирование правил с помощью команды drweb-ctl cfset
- Набор правил по умолчанию
- Примеры правил проверки трафика и блокировки доступа

Компонент использует параметры конфигурации, заданные в секции `[LinuxFirewall]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-firewall`
`AutoconfigureIptables` *{Yes | No}*	Включить или отключить режим настройки правил для системного компонента NetFilter через интерфейс `iptables`. Допустимые значения: • `Yes` — автоматически настраивать правила для NetFilter при запуске компонента и удалять их при завершении работы компонента (*рекомендуется*). • `No` — не настраивать правила автоматически. Правила должны быть добавлены администратором вручную перед запуском компонента и удалены, когда он завершит работу.

Параметр	Описание
	 Если автоматическая настройка правил для `iptables` не разрешена, необходимо обеспечить наличие необходимых правил `iptables` к моменту начала работы компонента. Значение по умолчанию: `Yes`
`AutoconfigureRouting` *{Yes | No}*	Режим настройки правил и политик маршрутизации `ip route` и `ip rule`. Допустимые значения: • `Yes` — автоматически настраивать правила и политики маршрутизации `ip route` и `ip rule` при запуске компонента и удалять их при завершении работы компонента (*рекомендуется*). • `No` — не настраивать правила автоматически. Правила должны быть добавлены администратором вручную перед запуском компонента и удалены, когда он завершит работу.  Если автоматическая настройка правил и политик маршрутизации не разрешена, необходимо обеспечить наличие необходимых правил `ip route` и `ip rule` к моменту начала работы компонента. Значение по умолчанию: `Yes`
`LocalDeliveryMark` *{целое число | Auto}*	Метка <*LDM*> для пакетов, перенаправляемых на сетевой сокет Dr.Web Firewall для Linux (определяется параметром `TproxyListenAddress`, см. ниже) для перехвата соединения. Допустимые значения: • <*целое число*> — метка <*LDM*>, присваиваемая пакетам. Численно равна 2^N, где N — номер бита `LDM` в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически (*рекомендуется*).

Параметр	Описание
	 При назначении числа <*LDM*> вручную убедитесь, что соответствующий бит в метке пакетов не используется никакими другими приложениями, управляющими маршрутизацией соединений и пакетов (в том числе, через NetFilter). Если указано недопустимое значение, запуск компонента завершится ошибкой. Указанное число <*LDM*> должно использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No` и/или `AutoconfigureRouting = No`. Значение по умолчанию: `Auto`
`ClientPacketsMark` *{целое число | Auto}*	Метка <*CPM*>, которой помечаются пакеты, следующие между клиентом (инициатором соединения) и Dr.Web Firewall для Linux. Допустимые значения: • <*целое число*> — метка <*CPM*>, присваиваемая пакетам. Численно равна 2^N, где N — номер бита `CPM` в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически (*рекомендуется*).

Параметр	Описание
	 При назначении числа <*CPM*> вручную необходимо убедиться, что соответствующий бит в метке пакетов не используется никакими другими приложениями, управляющими маршрутизацией соединений и пакетов (в том числе, через NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число <*CPM*> должно использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`
`ServerPacketsMark` *{целое число | Auto}*	Метка <*SPM*>, которой помечаются пакеты, следующие между Dr.Web Firewall для Linux и сервером (приемником соединения). Допустимые значения: • <*целое число*> — метка <*SPM*>, присваиваемая пакетам. Численно равна 2^N, где N — номер бита `SPM` в пакете, $0 \leq N \leq 31$. • `Auto` —разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически (*рекомендуется*).

Параметр	Описание
	 При назначении числа <*SPM*> вручную необходимо убедиться, что соответствующий бит в метке пакетов не используется никакими другими приложениями, управляющими маршрутизацией соединений и пакетов (в том числе, через NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число <*SPM*> должно использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No` и/или `AutoconfigureRouting = No`. Значение по умолчанию: `Auto`
`TproxyListenAddress` *{сетевой сокет}*	Сетевой сокет (<*IP-адрес*>:<*порт*>), на котором Dr.Web Firewall для Linux принимает перехваченные соединения. Если задан нулевой порт, то сокет выбирается системой автоматически.  Необходимо убедиться, что соответствующий сокет не используется никакими другими приложениями. Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанные IP-адрес и порт должны использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `127.0.0.1:0`
`OutputDivertEnable` *{Yes | No}*	Включить или отключить режим перехвата исходящих соединений (т. е. соединений, инициированных приложениями на локальном узле).

Параметр	Описание
	Допустимые значения: • `Yes` — перехватывать и обрабатывать исходящие соединения; • `No` — не перехватывать и не обрабатывать исходящие соединения.  Данная настройка добавляет или удаляет правило маршрутизации № 5, которое необходимо добавлять или удалять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `No`
`OutputDivertNfqueueNumber` *{целое число | Auto}*	Номер очереди *NFQUEUE*, из которой Dr.Web Firewall для Linux будет извлекать SYN-пакеты, инициирующие исходящие соединения. Допустимые значения: • *<целое число>* — номер очереди *<ONum>* для отслеживания SYN-пакетов перехватываемых исходящих соединений в *NFQUEUE*; • `Auto` —разрешить Dr.Web Firewall для Linux выбрать подходящий номер очереди автоматически (*рекомендуется*).  При назначении числа *<ONum>* вручную необходимо убедиться, что соответствующая очередь не используется никакими другими приложениями, контролирующими соединения и пакеты (в том числе через правила NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число *<ONum>* должно использоваться в правиле маршрутизации № 5, которое необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`

Параметр	Описание
`OutputDivertConnectTransparently` *{Yes | No}*	Включить или отключить режим эмуляции подключения к получателю (серверу) с IP-адреса отправителя перехваченного пакета (клиента) для исходящих соединений. Допустимые значения: • `Yes` — при перехвате соединения подключаться к серверу не со своего адреса, а с адреса клиента, который запросил соединение; • `No` — подключаться к серверу с адреса Dr.Web Firewall для Linux. Поскольку в режиме перехвата исходящих соединений адреса клиента и Dr.Web Firewall для Linux чаще всего совпадают, значение по умолчанию — `No`. Значение по умолчанию: `No`
`OutputDivertMark` *{целое число | Auto | None}*	Метка, которой помечаются пакеты в режиме перехвата исходящих соединений при использовании подсистемы мандатного доступа PARSEC. Допустимые значения: • *<целое число>* — метка, присваиваемая пакетам. Численно равна 2^N, где N — номер бита метки в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически. • `None` — не устанавливать метку. Значение по умолчанию: `None`
`InputDivertEnable` *{Yes | No}*	Включить или отключить режим перехвата входящих соединений (т. е. соединений, инициированных приложениями на удаленном узле, с приложениями, работающими на локальном узле). Допустимые значения: • `Yes` — перехватывать и обрабатывать входящие соединения; • `No` — не перехватывать и не обрабатывать входящие соединения.

Параметр	Описание
	 Данная настройка добавляет или удаляет правило маршрутизации № 7, которое необходимо добавлять или удалять вручную, если `AutoconfigureIptables = No`. Если указано недопустимое значение, то запуск компонента завершится ошибкой. Значение по умолчанию: `No`
`InputDivertNfqueueNumber` *{целое число | Auto}*	Номер очереди *NFQUEUE*, из которой Dr.Web Firewall для Linux будет извлекать SYN-пакеты, инициирующие входящие соединения. Допустимые значения: • *<целое число>* — номер очереди *<INum>* для отслеживания SYN-пакетов перехватываемых входящих соединений в *NFQUEUE*; • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий номер очереди автоматически (*рекомендуется*).  При назначении числа *<INum>* вручную необходимо убедиться, что соответствующая очередь не используется никакими другими приложениями, управляющими контролем соединений и пакетов (в том числе через правила NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число *<INum>* должно использоваться в правиле маршрутизации № 7, которое необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`
`InputDivertConnectTransparently` *{Yes | No}*	Включить или отключить режим эмуляции подключения к получателю (серверу) с IP-адреса отправителя перехваченного пакета (клиента) для входящих соединений.

Параметр	Описание
	Допустимые значения: • `Yes` — при перехвате соединения подключаться к серверу не со своего адреса, а с адреса клиента, который запросил соединение; • `No` — подключаться к серверу с адреса Dr.Web Firewall для Linux. В режиме перехвата входящих соединений весь трафик проходит через Dr.Web Firewall для Linux и можно безопасно подключиться к серверу с фиктивного адреса клиента, поэтому значение по умолчанию — `Yes`. Значение по умолчанию: `Yes`
`InputDivertMark` *{целое число | Auto | None}*	Метка, которой помечаются пакеты в режиме перехвата входящих соединений при использовании подсистемы мандатного доступа PARSEC. Допустимые значения: • *<целое число>* — метка, присваиваемая пакетам. Численно равна 2^N, где N — номер бита метки в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически. • `None` — не устанавливать метку. Значение по умолчанию: `None`
`ForwardDivertEnable` *{Yes | No}*	Включить или отключить режим перехвата транзитных соединений (т. е. соединений, инициированных приложениями на одном удаленном узле, с приложениями, работающими на другом удаленном узле). Допустимые значения: • `Yes` — перехватывать и обрабатывать транзитные соединения; • `No` — не перехватывать и не обрабатывать транзитные соединения. ⚠ Данная настройка добавляет или удаляет правило маршрутизации № 8, которое необходимо добавлять или удалять вручную, если `AutoconfigureIptables = No`.

Параметр	Описание
	Значение по умолчанию: `No`
`ForwardDivertNfqueueNumber` *{целое число | Auto}*	Номер очереди *NFQUEUE*, из которой Dr.Web Firewall для Linux будет извлекать SYN-пакеты, инициирующие транзитные соединения. Допустимые значения: • *<целое число>* — номер очереди *<FNum>* для отслеживания SYN-пакетов перехватываемых транзитных соединений в *NFQUEUE*; • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий номер очереди автоматически (*рекомендуется*). ⚠ При назначении числа *<FNum>* вручную необходимо убедиться, что соответствующая очередь не используется никакими другими приложениями, управляющими контролем соединений и пакетов (в том числе через правила NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число *<FNum>* должно использоваться в правиле маршрутизации № 8, которое необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`
`ForwardDivertConnectTransparently` *{Yes | No}*	Включить или отключить режим эмуляции подключения к получателю (серверу) с IP-адреса отправителя перехваченного пакета (клиента) для транзитных соединений. Допустимые значения: • `Yes` — при перехвате соединения подключаться к серверу не со своего адреса, а с адреса клиента, который запросил соединение; • `No` — подключаться к серверу с адреса Dr.Web Firewall для Linux. Поскольку в режиме перехвата транзитных соединений нет гарантии, что весь трафик проходит через один и тот же узел (маршрутизатор), на

Параметр	Описание
	котором установлен Dr.Web Firewall для Linux, для корректной работы значение по умолчанию — `No`. Если конфигурация сети гарантирует, что все защищаемые приложения используют один и тот же маршрутизатор, параметр можно установить в `Yes`, и в этом случае при подключении к серверам Dr.Web Firewall для Linux всегда будет эмулировать подключение с адреса клиента. Значение по умолчанию: `No`
`ForwardDivertMark` *{целое число | Auto | None}*	Метка, которой помечаются пакеты в режиме перехвата транзитных соединений при использовании подсистемы мандатного доступа PARSEC. Допустимые значения: • *<целое число>* — метка, присваиваемая пакетам. Численно равна 2^N, где N — номер бита метки в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически. • `None` — не устанавливать метку. Значение по умолчанию: `None`
`Whitelist` *{список доменов}*	Белый список доменов (домены, подключение к которым разрешено, даже если они относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет разрешен и ко всем поддоменам доменов, указанных в этом списке). Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения параметра объединяются в единый список). Пример: Добавить в список домены `example.com` и `example.net`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке: `[LinuxFirewall]` `Whitelist = "example.com", "example.net"` • Две строки (по одному значению в строке): `[LinuxFirewall]` `Whitelist = example.com` `Whitelist = example.net`

Параметр	Описание
	2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset LinuxFirewall.Whitelist -a example.com` `# drweb-ctl cfset LinuxFirewall.Whitelist -a example.net`  Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах проверки, заданных для Dr.Web Firewall для Linux. В перечне правил, заданных по умолчанию (см. ниже), гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет обеспечен, даже если там будут находиться домены из блокируемых категорий веб-ресурсов, но только если производится запрос к узлу с использованием протокола HTTP. Кроме этого, условия правил по умолчанию гарантируют, что данные, загружаемые с доменов из белого списка, *будут проверяться на наличие угроз* (так как данные возвращаются в ответе, и переменная `direction` имеет значение `response`). Значение по умолчанию: *(не задано)*
`Blacklist` *{список доменов}*	Черный список доменов (домены, подключение к которым запрещено, даже если они не относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет запрещен и ко всем поддоменам доменов, указанных в этом списке). Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения параметра объединяются в единый список). Пример: Добавить в список домены `example.com` и `example.net`. 1. Добавление значений в файл конфигурации.

Параметр	Описание
	• Два значения в одной строке: `[LinuxFirewall]` `Blacklist = "example.com", "example.net"` • Две строки (по одному значению в строке): `[LinuxFirewall]` `Blacklist = example.com` `Blacklist = example.net` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset LinuxFirewall.Blacklist -a example.com` `# drweb-ctl cfset LinuxFirewall.Blacklist -a example.net` ⚠ Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах проверки, заданных для Dr.Web Firewall для Linux. Условия правил, заданных по умолчанию (см. ниже), гарантируют, что доступ к доменам (и их поддоменам) из данного списка по протоколу HTTP будет запрещен всегда. Если домен добавлен одновременно в список `Whitelist` и список `Blacklist`, то правила, заданные по умолчанию, гарантируют, что доступ пользователей к домену по протоколу HTTP будет заблокирован. --- Сайты из черного списка не будут блокироваться, если отключена проверка исходящего трафика (убедитесь, что параметр `OutputDivertEnable` имеет значение `Yes`, `On` или `True`). Если эти сайты используют протокол HTTPS, также установите параметр `UnwrapSsl` в значение `Yes`, `On` или `True`. Значение по умолчанию: *(не задано)*

Параметр	Описание
`InspectHttp` *{On | Off}*	Проверять данные, передаваемые по протоколу HTTP. Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`InspectPop3` *{On | Off}*	Проверять данные, передаваемые по протоколу POP3 (используется компонент Dr.Web MailD). Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`InspectImap` *{On | Off}*	Проверять данные, передаваемые по протоколу IMAP (используется компонент Dr.Web MailD). Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`InspectSmtp` *{On | Off}*	Проверять данные, передаваемые по протоколу SMTP (используется компонент Dr.Web MailD). Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`InspectFtp` *{On | Off}*	Проверять данные, передаваемые по протоколу FTP. Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`ExcludedProc` *{путь к файлу}*	Белый список процессов (процессы, сетевая активность которых не контролируется). Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения параметра объединяются в единый список). Пример: Добавить в список процессы `wget` и `curl`. 1. Добавление значений в файл конфигурации.

Параметр	Описание
	• Два значения в одной строке: `[LinuxFirewall]` `ExcludedProc = "/usr/bin/wget", "/usr/bin/curl"` • Две строки (по одному значению в строке): `[LinuxFirewall]` `ExcludedProc = /usr/bin/wget` `ExcludedProc = /usr/bin/curl` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset LinuxFirewall.ExcludedProc -a /usr/bin/wget` `# drweb-ctl cfset LinuxFirewall.ExcludedProc -a /usr/bin/curl` ⚠ Реальное использование списка процессов, указанного в данном параметре, зависит от того, *как* он используется в правилах проверки, заданных для Dr.Web Firewall для Linux. В перечне правил, заданных по умолчанию, гарантируется, что трафик всех процессов, указанных в этом списке пропускается *без какой-либо проверки*. Значение по умолчанию: *(не задано)*
`UnwrapSsl` *{логический}*	Проверять или не проверять зашифрованный трафик, передаваемый через SSL.

Параметр	Описание
	 В текущей реализации значение данной переменной не оказывает никакого влияния на проверку защищенного трафика. Для реального управления проверкой нужно создать правило, в котором содержится действие `SET Unwrap_SSL = true/false`. Если значение параметра изменять с помощью команды `cfset` утилиты `drweb-ctl`, то зависимые правила будут перестраиваться автоматически. Значение по умолчанию: `No`
`BlockUnchecked` *{логический}*	Блокировать получение и передачу данных, если они не могут быть проверены.  Значение этого параметра влияет на обработку правил, в которых невозможно определить истинность или ложность условия вследствие ошибки: в случае `No` правило будет пропущено как не сработавшее, а в случае `Yes` будет выполнено действие `BLOCK as BlackList`. Значение по умолчанию: `No`
`BlockInfectionSource` *{логический}*	Блокировать попытки подключения к сайтам, содержащим вредоносное ПО (входящим в категорию *InfectionSource*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockNotRecommended` *{логический}*	Блокировать попытки подключения к нерекомендуемым сайтам (входящим в категорию *NotRecommended*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockAdultContent` *{логический}*	Блокировать попытки подключения к сайтам, содержащим материалы для взрослых (входящим в категорию *AdultContent*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockViolence` *{логический}*	Блокировать попытки подключения к сайтам, содержащим сцены насилия (входящим в категорию *Violence*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockWeapons` *{логический}*	Блокировать попытки подключения к сайтам, посвященным оружию (входящим в категорию *Weapons*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockGambling` *{логический}*	Блокировать попытки подключения к сайтам, посвященным азартным играм и играм на деньги (входящим в категорию *Gambling*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`

Параметр	Описание
`BlockDrugs` *{логический}*	Блокировать попытки подключения к сайтам, посвященным наркотикам (входящим в категорию *Drugs*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockObsceneLanguage` *{логический}*	Блокировать попытки подключения к сайтам, содержащим нецензурную лексику (входящим в категорию *ObsceneLanguage*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockChats` *{логический}*	Блокировать попытки подключения к сайтам чатов (входящим в категорию *Chats*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockTerrorism` *{логический}*	Блокировать попытки подключения к сайтам, посвященным терроризму (входящим в категорию *Terrorism*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockFreeEmail` *{логический}*	Блокировать попытки подключения к сайтам бесплатных почтовых служб (входящим в категорию *FreeEmail*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match`

Параметр	Описание
	Значение по умолчанию: `No`
`BlockSocialNetworks` *{логический}*	Блокировать попытки подключения к сайтам социальных сетей (входящим в категорию *SocialNetworks*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockDueToCopyrightNotice` *{логический}*	Блокировать попытки подключения к сайтам, ссылки на которые были добавлены по обращению правообладателей (входящим в категорию *DueToCopyrightNotice*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockOnlineGames` *{логический}*	Блокировать попытки подключения к сайтам онлайн-игр (входящим в категорию *OnlineGames*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockAnonymizers` *{логический}*	Блокировать попытки подключения к сайтам анонимайзеров (входящим в категорию *Anonymizers*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockCryptocurrencyMiningPools` *{логический}*	Блокировать попытки подключения к сайтам, объединяющим пользователей с целью добычи (майнинга) криптовалют (входящим в категорию *CryptocurrencyMiningPool*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockJobs` *{логический}*	Блокировать попытки подключения к сайтам, предназначенным для поиска вакансий (входящим в категорию *Jobs*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockKnownVirus` *{логический}*	Блокировать получение и передачу данных, если они содержат известную угрозу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockSuspicious` *{логический}*	Блокировать получение и передачу данных, если они содержат неизвестную угрозу, обнаруженную эвристическим анализатором. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockAdware` *{логический}*	Блокировать получение и передачу данных, если они содержат рекламную программу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockDialers` *{логический}*	Блокировать получение и передачу данных, если они содержат программу дозвона.

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockJokes` *{логический}*	Блокировать получение и передачу данных, если они содержат программу-шутку. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`BlockRiskware` *{логический}*	Блокировать получение и передачу данных, если они содержат потенциально опасную программу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`BlockHacktools` *{логический}*	Блокировать получение и передачу данных, если они содержат программу взлома. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла по запросу SplDer Gate. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `30s`
`HeuristicAnalysis` *{On | Off}*	Использовать или не использовать эвристический анализ для поиска возможных неизвестных угроз при проверке файла, инициированной по запросу SplDer Gate. Использование эвристического анализа повышает надежность проверки, но увеличивает ее длительность.

Параметр	Описание
	Действие при срабатывании эвристического анализатора задается параметром `BlockSuspicious`. Допустимые значения: • `On` — использовать эвристический анализ при проверке; • `Off` — не использовать эвристический анализ. Значение по умолчанию: `On`
`PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение 0 указывает, что вложенные объекты не проверяются.

Параметр	Описание
	Значение по умолчанию: `8`
`ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (страниц HTML, файлов `.jar` и др.). Задает уровень в иерархии вложенности, после которого объекты внутри объектов будут пропускаться при проверке файла, инициированной по запросу SpIDer Gate. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MaxCompressionRatio` *{целое число}*	Максимально допустимая степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке файла, инициированной по запросу SpIDer Gate. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`
`InterceptHook` *{путь к файлу | функция Lua}*	Скрипт обработки соединений на языке Lua, либо путь к файлу, хранящему этот скрипт. Если указанный файл недоступен, то при загрузке компонента будет выдана ошибка. Значение по умолчанию: `local dwl = require 'drweb.lookup'` `function intercept_hook(ctx)` `  -- do not check if group == Root.TrustedGroup` `  if ctx.divert == "output" and ctx.group == "drweb"` `  then` `  return "pass"` `  end` `  -- do not check connections from privileged ports` `  -- except FTP active mode` `  if ctx.src.port >= 0 and ctx.src.port <= 1024` `  and ctx.src.port ~= 20` `  then` `  return "pass"` `  end`

Параметр	Описание
	`return "check"` `end`
`XtablesLockPath` *{путь к файлу}*	Путь к файлу блокировки таблиц `iptables` (NetFilter). Если значение параметра не указано, проверяются пути `/run/xtables.lock` и `/var/run/xtables.lock`. Если файл блокировок не обнаружен по указанному пути или путям по умолчанию, запуск компонента завершится ошибкой. Значение по умолчанию: *(не задано)*



Изменения, внесенные в настройки проверки соединений, не влияют на проверку соединений, которые уже были установлены приложениями до внесения изменений. Если необходимо применить их для уже запущенных приложений, необходимо заставить их разорвать и повторно установить сетевое соединение, например, путем перезапуска этих приложений.

Правила проверки трафика и блокировки доступа

В дополнение к параметрам, перечисленным выше, в секции присутствует 11 *наборов правил* `RuleSet*` (`RuleSet0`, ..., `RuleSet10`), непосредственно управляющих проверкой трафика и блокировкой доступа пользователей к веб-ресурсам, а также загрузкой контента из интернета. Для некоторых значений в условиях (например, диапазоны IP-адресов, перечни категорий сайтов, черные и белые списки сайтов и т. п.) предусмотрена подстановка значений, загружаемых из текстовых файлов, а также извлеченных из внешних источников данных через LDAP. При обработке соединений все правила проверяются в порядке сверху вниз единым списком до момента нахождения сработавшего правила, содержащего финальную резолюцию. Пропуски в списке правил, если встречаются, игнорируются.

Просмотр и редактирование правил

Для удобства редактирования списка правил, по умолчанию в списке оставлены «пустоты», т. е. наборы `RuleSet<i>`, не содержащие правил (где `<i>` — номер набора `RuleSet`).



Вы *не можете* добавить элементы списка, отличные от уже имеющихся `RuleSet<i>`, но можете добавить или удалить любое правило в любом элементе `RuleSet<i>`.

Просматривать и редактировать правила можно любым из следующих способов:

- путем просмотра и изменения файла конфигурации в любом текстовом редакторе (помните, что в этом файле сохраняются только те параметры, значения которых отличаются от значений по умолчанию);
- через интерфейс командной строки Dr.Web Ctl (команды `drweb-ctl cfshow` и `drweb-ctl cfset`).



Если вы редактировали правила, внося изменения в файл конфигурации, для применения внесенных изменений перезапустите Dr.Web Desktop Security Suite. Для этого выполните команду `drweb-ctl reload`.

Просмотр правил с помощью команды drweb-ctl cfshow

Для просмотра содержимого набора правил `LinuxFirewall.RuleSet1` выполните команду:

```
# drweb-ctl cfshow LinuxFirewall.RuleSet1
```

Редактирование правил с помощью команды drweb-ctl cfset

Здесь и далее <*правило*> — текст правила.

- Замена всех правил в наборе правил `LinuxFirewall.RuleSet1` на новое правило:

```
# drweb-ctl cfset LinuxFirewall.RuleSet1 '<правило>'
```

- Добавление еще одного правила в набор правил `LinuxFirewall.RuleSet1`:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 '<правило>'
```

- Удаление конкретного правила из набора правил `LinuxFirewall.RuleSet1`:

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 '<правило>'
```

- Возврат набора правил `LinuxFirewall.RuleSet1` к состоянию по умолчанию:

```
# drweb-ctl cfset -r LinuxFirewall.RuleSet1
```

При использовании утилиты `drweb-ctl` для редактирования правил заключайте строку добавляемого правила <*правило*> в одинарные или двойные кавычки, а внутренние кавычки, если они встречаются в правиле, экранируйте символом обратной косой черты `\`.

Важно помнить следующие особенности хранения правил в переменных конфигурации `RuleSet`<*i*>:

- При добавлении безусловных правил условная часть и двоеточие могут быть опущены, однако такие правила всегда сохраняются в списке правил в виде строки '`:` <*действие*>'.

- При добавлении правил, содержащих несколько действий (правила вида '*<условие>* : *<действие 1>*, *<действие 2>*'), такие правила будут преобразованы в цепочку элементарных правил '*<условие>* : *<действие 1>*' и '*<условие>* : *<действие 2>*'.
- Так как в записи правил не предусмотрено дизъюнкции (логическое «ИЛИ») условий в условной части, для реализации логического «ИЛИ» запишите цепочку правил, в условии каждого из которых будет указано условие-дизъюнкт.

Чтобы добавить в набор правил `LinuxFirewall.RuleSet1` правило безусловного пропуска (действие `PASS`), выполните команду:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'PASS'
```

Чтобы удалить это правило из указанного набора правил, выполните команду:

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 ' : PASS'
```

Чтобы добавить в набор правил `LinuxFirewall.RuleSet1` правило, изменяющее для соединений, следующих с неразрешенных адресов, путь к стандартным шаблонам и выполняющее блокировку, выполните команду:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'src_ip not in file("/etc/trusted_ip") : set
http_template_dir = "mytemplates", BLOCK'
```

Эта команда добавит *два правила* в указанный набор правил, поэтому, чтобы удалить их, выполните две команды:

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in file("/etc/trusted_ip") : set
http_template_dir = "mytemplates"'
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in file("/etc/trusted_ip") :
BLOCK'
```

Чтобы добавить в набор правил `LinuxFirewall.RuleSet1` правило вида «Осуществить блокировку, если обнаружен вредоносный объект типа *KnownVirus* или URL из категории *Terrorism*», необходимо добавить в этот набор сразу два правила:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'threat_category in (KnownVirus) : BLOCK as
_match'
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'url_category in (Terrorism) : BLOCK as
_match'
```

Для их удаления также потребуется две команды, как в примере выше.

Набор правил по умолчанию

По умолчанию задан следующий набор правил, управляющих блокировкой:

```
RuleSet0 =
RuleSet1 = divert output : set HttpTemplatesDir = "output"
RuleSet1 = divert output : set MailTemplatesDir = "firewall"
RuleSet1 = divert input : set HttpTemplatesDir = "input"
RuleSet1 = divert input : set MailTemplatesDir = "server"
RuleSet1 = proc in "LinuxFirewall.ExcludedProc" : PASS
RuleSet1 =  : set Unwrap_SSL = false
```

```
RuleSet2 =
RuleSet3 =
RuleSet4 =
RuleSet5 = protocol in (Http), direction request, url_host in "LinuxFirewall.Blacklist"
: BLOCK as BlackList
RuleSet5 = protocol in (Http), direction request, url_host in "LinuxFirewall.Whitelist"
: PASS
RuleSet6 =
RuleSet7 = protocol in (Http), direction request, url_category in
"LinuxFirewall.BlockCategory" : BLOCK as _match
RuleSet8 =
RuleSet9 = protocol in (Http), divert input, direction request, threat_category in
"LinuxFirewall.BlockThreat" : BLOCK as _match
RuleSet9 = protocol in (Http), direction response, threat_category in
"LinuxFirewall.BlockThreat" : BLOCK as _match
RuleSet9 = protocol in (Smtp), threat_category in "LinuxFirewall.BlockThreat" : REJECT
RuleSet9 = protocol in (Smtp), url_category in "LinuxFirewall.BlockCategory" : REJECT
RuleSet9 = protocol in (Smtp), total_spam_score gt 0.80 : REJECT
RuleSet9 = protocol in (Pop3, Imap), threat_category in "LinuxFirewall.BlockThreat" :
REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), url_category in "LinuxFirewall.BlockCategory" :
REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), total_spam_score gt 0.80 : REPACK as _match
RuleSet10 =
```

Первое правило указывает, что если соединение устанавливается процессом, указанным в параметре `ExcludedProc` (см. выше), то соединение пропускается без проверки каких-либо дополнительных условий. Следующее правило (срабатывает безусловно) запрещает проверку защищенных соединений. Это правило, как и все следующие ниже, будет анализироваться только если соединение не связано с исключаемым процессом. Кроме того, поскольку все последующие правила зависят от определения типа протокола, то, если запрещено проверять защищенные соединения, а соединение защищенное, в этом случае все они не сработают из-за невозможности определить истинность условий.

Следующие пять правил регламентируют обработку исходящих HTTP-соединений:

1. Если узел, с которым устанавливается соединение, включен в черный список, соединение блокируется, а дальнейшие проверки не производятся.
2. Если узел находится в белом списке, соединение пропускается, дальнейшие проверки не производятся.
3. Если URL, к которому обращается клиент, относится к категории нежелательных для посещения веб-ресурсов, то соединение блокируется, а дальнейшие проверки не производятся.
4. Если ответ, поступивший от удаленного узла по HTTP, содержит угрозу, относящуюся к категориям, которые следует блокировать, то соединение блокируется, а дальнейшие проверки не производятся.
5. Если данные, передаваемые с локального узла на удаленный сервер, содержат угрозу, относящуюся к категориям, которые следует блокировать, то соединение блокируется, а дальнейшие проверки не производятся.

Эти пять правил будут работать только в том случае, если параметр `InspectHttp` имеет значение `On`. В противном случае ни одно из них не сработает.

Следующие шесть правил, указанных в `RuleSet9`, регламентируют проверку данных, передаваемых по протоколам электронной почты (SMTP, POP3 или IMAP), и срабатывают в следующих случаях:

- сообщение содержит вложения;
- сообщение содержит URL из категорий, подлежащих блокировке;
- сообщение оценено как спам с индексом не менее 0,8.

При этом к письмам, передаваемым по протоколу SMTP, применяется действие, блокирующее передачу письма (т. е. его отправку или прием), а для протоколов IMAP и POP3 производится обработка письма, заключающаяся в удалении из него вредоносного содержимого («перепаковка»).



Если компонент проверки сообщений электронной почты на наличие признаков спама Dr.Web Anti-Spam не установлен, то проверка писем на наличие признаков спама не производится. В этом случае правила, содержащие проверку порога спама (переменную `total_spam_score`), отсутствуют.

Правила проверки электронной почты будут работать только в том случае, если соответствующие параметры `Inspect`<*EmailProtocol*> имеют значение `On`. В противном случае ни одно из правил не сработает.

Для непосредственной проверки передаваемого письма на предмет наличия в нем вредоносных вложений, а также для анализа на признаки спама должен быть установлен дополнительный компонент проверки электронной почты — Dr.Web MailD. Если он не установлен, передаваемые сообщения будут блокироваться по причине ошибки *«Невозможно проверить»*. Чтобы разрешить прохождение писем, которые невозможно проверить, установите параметр `BlockUnchecked` в значение `No` (см. выше). Кроме того, при отсутствии компонента проверки электронной почты рекомендуется установить значение `No` для параметров `InspectSmtp`, `InspectPop3` и `InspectImap`.

Примеры правил проверки трафика и блокировки доступа

1. Разрешить для пользователей с диапазоном IP-адресов *10.10.0.0–10.10.0.254* доступ по протоколу HTTP к сайтам любых категорий, кроме категории *Chats*:

```
protocol in (HTTP), src_ip in (10.10.0.0/24), url_category not in (Chats) : PASS
```

Если правило:

```
protocol in (HTTP), url_host in "LinuxFirewall.Blacklist" : BLOCK as
BlackList
```

разместить в списке правил выше (т. е. раньше) указанного правила, то доступ к доменам из черного списка, т. е. доменам, перечисленным в параметре `LinuxFirewall.Blacklist`, будет блокироваться и для пользователей с диапазоном IP-адресов *10.10.0.0–10.10.0.254*. А если это правило разместить ниже (т. е. позже), то пользователям с диапазоном IP-адресов *10.10.0.0–10.10.0.254* будут доступны также и сайты из черного списка.

Так как резолюция `PASS` является конечной, более никакие правила не проверяются, следовательно, проверка загружаемых данных на наличие угроз производиться также не будет.

Чтобы разрешить пользователям с диапазоном IP-адресов *10.10.0.0–10.10.0.254* доступ к сайтам любых категорий, кроме категории *Chats*, если они не находятся в черном списке, но при этом не разрешать загрузку угроз, используйте следующее правило:

```
protocol in (HTTP), url_category not in (Chats), url_host not in
"LinuxFirewall.Blacklist", threat_category not in "LinuxFirewall.BlockCategory" :
PASS
```

2. Не выполнять проверку содержимого *загружаемых из интернета* видеофайлов (т. е. данных с типом MIME `video/*`, где `*` соответствует любому типу MIME-класса `video`):

```
direction response, content_type in ("video/*") : PASS
```

Выгружаемые с локального компьютера файлы (в том числе и с типом MIME `video/*`) будут проверяться, так как они передаются *в запросах, а не ответах*, т. е. для них переменная `direction` имеет значение `request`.

9.9. Dr.Web File Checker

Компонент проверки файлов Dr.Web File Checker предназначен для проверки файлов и каталогов файловой системы. Он используется другими компонентами Dr.Web Desktop Security Suite для проверки объектов файловой системы. Кроме этого, компонент ведет постоянно хранимый реестр всех угроз, обнаруженных в файловой системе, и выполняет функцию менеджера карантина, управляя содержимым каталогов, в которых располагаются изолированные файлы.

9.9.1. Принципы работы

Компонент Dr.Web File Checker запускается с правами суперпользователя (пользователя *root*) и используется для сканирования объектов файловой системы (файлы, каталоги и загрузочные записи).

Dr.Web File Checker индексирует все проверенные файлы и каталоги и сохраняет данные о проверенных объектах в специальном кеше, чтобы не выполнять повторную проверку объектов, которые уже были проверены ранее и не изменялись с момента последней проверки (в этом случае, если заявка о проверке такого объекта поступает повторно, возвращается результат его предыдущей проверки, извлеченный из кеша).

При поступлении запросов на проверку объектов файловой системы от других компонентов Dr.Web File Checker проверяет, требуется ли проверка запрошенного объекта, и если да, то формирует задание на проверку его содержимого для сканирующего ядра Dr.Web Scanning Engine. Если проверенный объект содержит угрозу, то Dr.Web File Checker заносит его в реестр обнаруженных угроз и применяет к нему нейтрализующее действие (лечение, удаление или перемещение в карантин), если это действие задано клиентским компонентом, инициировавшим проверку, в качестве реакции на угрозу. В качестве инициаторов проверки могут выступать различные компоненты Dr.Web Desktop Security Suite.

В процессе проверки запрошенных объектов файловой системы компонент проверки файлов формирует и отправляет компоненту-клиенту, запросившему проверку, отчеты о результатах проверки и предпринятых действиях по нейтрализации угроз, если они были обнаружены.

Помимо стандартного метода проверки файлов, для внутренних нужд поддерживаются специальные методы проверки файлов:

- *Метод «flow»* — метод потоковой проверки файлов. Компонент, использующий этот метод, один раз инициализирует параметры проверки и обезвреживания угроз, и далее эти параметры будут применяться ко всему потоку заявок на проверку файлов, поступающих от этого компонента. Этот метод проверки используется монитором SpIDer Guard.
- *Метод «proxy»* — метод проверки файлов, заключающийся в том, что компонент проверки файлов выполняет только проверку файлов на наличие угроз, не применяя к

ним никаких действий, в том числе не выполняя регистрацию обнаруженных угроз (эти действия целиком возлагаются на компонент, инициировавший проверку). Этот метод проверки используется .

В процессе своей работы компонент проверки файлов не только ведет реестр угроз и управляет карантином, но и собирает общую статистику проверки файлов, усредняя количество файлов, проверенных в течение секунды за последнюю минуту, последние 5 минут, последние 15 минут.

9.9.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web File Checker из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-filecheck [<параметры>]
```

Dr.Web File Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-filecheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web File Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при поступлении от других компонентов Dr.Web Desktop Security Suite заявок на проверку объектов файловой системы. Для управления параметрами работы компонента, а также для проверки файлов по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для проверки произвольного файла или каталога компонентом Dr.Web File Checker используйте команду `scan` утилиты Dr.Web Ctl:

```
$ drweb-ctl scan <путь к файлу или каталогу>
```

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-filecheck`.

9.9.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[FileCheck]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

Эта секция хранит следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-filecheck`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`DebugClientIpc` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC. Значение по умолчанию: `No`
`DebugScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения, поступающие в процессе проверки файлов.

Параметр	Описание
	Значение по умолчанию: `No`
`DebugFlowScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«flow»*. Метод *«flow»* обычно используется монитором SpIDer Guard. Значение по умолчанию: `No`
`DebugProxyScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«proxy»*. Метод *«proxy»* обычно используется . Значение по умолчанию: `No`
`DebugCache` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о состоянии кеша проверенных файлов. Значение по умолчанию: `No`
`MaxCacheSize` *{размер}*	Максимальный разрешенный размер кеша для хранения информации о проверенных файлах. Если указано `0`, то кеширование отключено. Значение по умолчанию: `50mb`
`RescanInterval` *{интервал времени}*	Длительность интервала, в течение которого не производится повторная проверка содержимого файлов, информация о предыдущей проверке которых имеется в кеше (период актуальности кешированной информации). Допустимые значения: от 0 секунд (`0s`) до 1 минуты (`1m`). Если указан интервал менее `1s`, то задержка отсутствует, файл будет проверяться при любом запросе. Значение по умолчанию: `1s`

9.10. Dr.Web Network Checker

Компонент сетевой проверки данных Dr.Web Network Checker предназначен для проверки в сканирующем ядре данных, полученных через сеть, а также для организации распределенной проверки файлов на наличие угроз. Он позволяет организовать соединение между набором узлов сети с установленным на них Dr.Web Desktop Security Suite с целью приема и передачи данных (например, содержимого файлов) между узлами сети для проверки этих данных. При взаимодействии узлов компонент организует автоматическое распределение задач на проверку данных (передавая и получая их по сети) на все доступные узлы сети, с которыми настроено соединение, обеспечивая балансировку их нагрузки, вызванной проверкой отправленных данных. Если соединения с удаленными узлами не настроены, компонент передает все полученные данные на проверку локальному сканирующему ядру Dr.Web Scanning Engine.



Данный компонент всегда используется для проверки данных, полученных через сетевые соединения, поэтому, если он отсутствует или недоступен, будет нарушена работоспособность компонентов, отправляющих данные на проверку через сетевое соединение (SplDer Gate, Dr.Web MailD).

Данный компонент не предназначен для организации распределенной проверки файлов, расположенных в локальной файловой системе, так как не может заменить компонент проверки файлов Dr.Web File Checker. Для организации распределенной проверки локальных файлов используйте компонент Dr.Web MeshD.

В случае большой интенсивности проверки данных, передаваемых через сеть, возможно возникновение проблем с проверкой из-за исчерпания числа доступных файловых дескрипторов. В этом случае необходимо увеличить лимит на число файловых дескрипторов, доступных Dr.Web Desktop Security Suite.

Обмен проверяемыми данными может производиться как по открытому каналу, так и по защищенному, с использованием SSL/TLS. При использовании защищенного соединения необходимо обеспечить узлы, обменивающиеся файлами, корректными сертификатами и ключами SSL. Для генерации ключей и сертификатов можно воспользоваться утилитой `openssl`. Пример использования утилиты `openssl` для генерации сертификатов и закрытых ключей приведен в разделе Приложение Д. Генерация сертификатов SSL.

9.10.1. Принципы работы

Компонент позволяет передать данные, не представленные в виде файлов в локальной файловой системе, на сканирование в сканирующее ядро Dr.Web Scanning Engine, расположенное на локальном или удаленном узле. С такими данными работают компоненты, отправляющие данные на проверку через сетевое соединение (SplDer Gate, Dr.Web MailD).



Эти компоненты всегда используют Dr.Web Network Checker (даже расположенный на локальном узле) для передачи файлов на проверку сканирующему ядру Dr.Web Scanning Engine. Поэтому, если Dr.Web Network Checker недоступен, эти компоненты *не смогут корректно функционировать*.

Кроме этого, Dr.Web Network Checker позволяет организовать соединение Dr.Web Desktop Security Suite с заданным набором узлов в сети с установленным на них Dr.Web Desktop Security Suite (или любым другим решением Dr.Web для Unix версии не ниже 10.1) для организации распределенной проверки на наличие данных, не представленных в виде файлов в локальной файловой системе. За счет этого компонент позволять создать и настроить *сканирующий кластер*, представляющий собой набор узлов сети, обменивающихся данными для проверки (на каждом узле должен быть запущен свой экземпляр агента распределенной проверки Dr.Web Network Checker). На каждом узле сети, включенном в сканирующий кластер, Dr.Web Network Checker выполняет автоматическое распределение задач на проверку данных, передавая их по сети на все доступные узлы, с которыми настроено соединение. При этом осуществляется балансировка нагрузки на узлы, вызванной проверкой данных, в зависимости от количества ресурсов, доступных на удаленных узлах. В качестве индикатора количества ресурсов, доступных для нагрузки, выступает количество дочерних сканирующих процессов, порожденных сканирующим ядром Dr.Web Scanning Engine на узле, включенном в кластер. Также оцениваются длины очередей файлов, дожидающихся проверки на каждом используемом узле.

При этом любой узел сети, включенный в сканирующий кластер, может выступать как в роли клиента сканирования, передающего данные на удаленную проверку, так и в роли сервера сканирования, принимающего с указанных узлов сети данные для проверки. При необходимости агент распределенной проверки можно настроить таким образом, чтобы узел выступал только в качестве сервера сканирования или только в качестве клиента сканирования.

Данные, принятые по сети для проверки, сохраняются в локальную файловую системы в виде временных файлов и передаются на проверку сканирующему ядру Dr.Web Scanning Engine, либо, в случае его недоступности или большой нагруженности, на другой узел сканирующего кластера.

Имеющийся в настройках компонента параметр `InternalOnly` позволяет управлять режимом работы Dr.Web Network Checker, определяя, используется ли он для включения Dr.Web Desktop Security Suite в сканирующий кластер или только для обеспечения внутренних нужд компонентов, работающих локально в составе Dr.Web Desktop Security Suite.

Вы можете создать свой собственный компонент (внешнее приложение), использующий Dr.Web Network Checker для проверки файлов. Для этого компонент Dr.Web Network Checker предоставляет специализированный API, основанный на технологии Google Protobuf. Описание API Dr.Web Network Checker, а также примеры кода клиентского приложения, использующего Dr.Web Network Checker, поставляются в составе пакета `drweb-netcheck`.

9.10.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Network Checker из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-netcheck [<параметры>]
```

Dr.Web Network Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-netcheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Network Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости (обычно при старте операционной системы). При этом, если в настройках компонента задано значение параметра `FixedSocket`, а параметр `InternalOnly` установлен в значение `No`, то компонент будет запущен демоном управления конфигурацией и постоянно доступен клиентам через Unix-сокет. Для управления параметрами работы компонента, а также для запуска сетевого сканирования (при наличии настроенного соединения с другими узлами сети) используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки. Если соединение с другими узлами сети не

настроено, вместо сетевого сканирования будет запущено обычное сканирование на стороне локального сканирующего ядра.



Чтобы запустить утилиту Dr.Web Ctl, используйте команду `drweb-ctl`.

Чтобы проверить произвольный файл или каталог компонентом Dr.Web Network Checker, используйте команду `netscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```

Чтобы получить справку о компоненте из командной строки, выполните команду `man 1 drweb-netcheck`.

9.10.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[NetCheck]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-netcheck`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска.

Параметр	Описание
	Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает работу. Если задано значение параметра `LoadBalanceAllowFrom` или `FixedSocket`, то настройка игнорируется (компонент не завершает свою работу по истечении максимального времени простоя). Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`FixedSocket` *{путь к файлу | адрес}*	Сокет фиксированного экземпляра агента Dr.Web Network Checker. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр агента распределенной проверки файлов, доступный клиентам через этот сокет. Возможные значения: • *<путь к файлу>* — путь к файлу локального Unix-сокета; • *<адрес>* — сетевой сокет в виде пары *<IP-адрес>*:*<порт>*. Убедитесь, что каталогу с файлом сокета назначены следующие права доступа: `drwxr-xr-x` Чтобы просмотреть права доступа, выполните команду: `$ ls -ld <путь к каталогу>` Значение по умолчанию: *(не задано)*
`InternalOnly` *{логический}*	Режим работы компонента. Если задано значение `Yes`, то компонент используется только для внутренних нужд компонентов Dr.Web Desktop Security Suite, но не обслуживает сканирующий кластер или внешние (по отношению к Dr.Web Desktop Security Suite) клиентские приложения вне зависимости от

Параметр	Описание
	настроек `LoadBalance*` и заданного значения параметра `FixedSocket`. Значение по умолчанию: `No`
`LoadBalanceUseSsl` *{логический}*	Использовать или не использовать SSL/TLS для соединения с другими узлами. Возможные значения: • `Yes` — использовать SSL/TLS; • `No` — не использовать SSL/TLS. Если этот параметр установлен в `Yes`, то для данного узла и для всех узлов, с которыми он взаимодействует, должны быть обязательно заданы соответствующие друг другу сертификат и закрытый ключ (параметры `LoadBalanceSslCertificate` и `LoadBalanceSslKey`). Значение по умолчанию: `No`
`LoadBalanceSslCertificate` *{путь к файлу}*	Путь к файлу сертификата SSL, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS. Файл сертификата и файл закрытого ключа (определяется параметром `LoadBalanceSslKey`) должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`LoadBalanceSslKey` *{путь к файлу}*	Путь к файлу закрытого ключа, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS. Файл сертификата (определяется параметром `LoadBalanceSslCertificate`) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`LoadBalanceSslCa` *{путь}*	Путь к каталогу или файлу, в котором располагается перечень доверенных корневых сертификатов. Среди данных сертификатов должен находиться сертификат, удостоверяющий подлинность сертификатов, используемых агентами внутри сканирующего кластера при обмене данными через SSL/TLS.

Параметр	Описание
	Если значение параметра не задано, то Dr.Web Network Checker, работающий на данном узле, не проверяет подлинность сертификатов взаимодействующих агентов, однако они, в зависимости от заданных для них настроек, могут проверять подлинность сертификата, используемого агентом, работающим на данном узле. Значение по умолчанию: *(не задано)*
`LoadBalanceServerSocket` *{адрес}*	Сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web Network Checker на данном узле для получения файлов на проверку от удаленных узлов (при работе в качестве сервера сетевого сканирования). Значение по умолчанию: *(не задано)*
`LoadBalanceAllowFrom` *{IP-адрес}*	IP-адрес удаленного узла сети, от которого Dr.Web Network Checker на данном узле может принимать файлы на проверку (как сервер сетевого сканирования). Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список адреса узлов 192.168.0.1 и 10.20.30.45. 1. Добавление значений в файл конфигурации. • Два значения в одной строке: `[NetCheck]` `LoadBalanceAllowFrom = "192.168.0.1", "10.20.30.45"` • Две строки (по одному значению в строке): `[NetCheck]` `LoadBalanceAllowFrom = 192.168.0.1` `LoadBalanceAllowFrom = 10.20.30.45` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 192.168.0.1` `# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 10.20.30.45` Если параметр пуст, то удаленные файлы на проверку не принимаются (узел не работает в режиме сервера). Значение по умолчанию: *(не задано)*
`LoadBalanceSourceAddress` *{IP-адрес}*	IP-адрес сетевого интерфейса, используемого Dr.Web Network Checker на данном узле для передачи файлов на

Параметр	Описание
	удаленную проверку, если узел работает как клиент сетевого сканирования, и если на узле доступно несколько сетевых интерфейсов. Если указать пустое значение, то используемый сетевой интерфейс будет автоматически выбран ядром ОС. Значение по умолчанию: *(не задано)*
`LoadBalanceTo` *{адрес}*	Сокет (IP-адрес и порт) удаленного узла, на который Dr.Web Network Checker на данном узле может отправлять файлы на удаленную проверку (как клиент сетевого сканирования). Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678. 1. Добавление значений в файл конфигурации. • Два значения в одной строке: `[NetCheck]` `LoadBalanceTo = "192.168.0.1:1234", "10.20.30.45:5678"` • Две строки (по одному значению в строке): `[NetCheck]` `LoadBalanceTo = 192.168.0.1:1234` `LoadBalanceTo = 10.20.30.45:5678` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset NetCheck.LoadBalanceTo -a 192.168.0.1:1234` `# drweb-ctl cfset NetCheck.LoadBalanceTo -a 10.20.30.45:5678` Если параметр пуст, то локальные файлы не передаются на удаленную проверку (узел не работает в режиме клиента сетевого сканирования). Значение по умолчанию: *(не задано)*
`LoadBalanceStatusInterval` *{интервал времени}*	Интервал времени между рассылками данным узлом информации о своей загруженности для всех агентов распределенной проверки, перечисленных в параметре `LoadBalanceAllowFrom`. Значение по умолчанию: `1s`

Параметр	Описание
`SpoolDir` *{путь к каталогу}*	Каталог в локальной файловой системе, используемый для хранения файлов, принятых Dr.Web Network Checker по сети от клиентов сканирования для проверки. Значение по умолчанию: `/tmp/com.drweb.ncheck`
`LocalScanPreference` *{дробное число}*	Относительный вес (предпочтительность) узла при выборе места для проверки файла (локального или принятого по сети). Если в некоторый момент времени вес локального узла больше суммарного веса всех доступных узлов-серверов сканирования, файл будет оставлен агентом для локальной проверки. Минимальное значение: `1`. Значение по умолчанию: `1`
`LoadBalanceSslCrl` *{путь}*	Путь к каталогу или файлу с перечнем отозванных сертификатов. Если значение параметра не задано, то Dr.Web Network Checker, работающий на данном узле, не проверяет сертификаты взаимодействующих агентов на актуальность, однако они, в зависимости от заданных для них настроек, могут проверять актуальность сертификата, используемого агентом, работающим на данном узле. Значение по умолчанию: *(не задано)*

9.11. Dr.Web Scanning Engine

Сканирующее ядро Dr.Web Scanning Engine предназначено для поиска вирусов и других вредоносных объектов в файлах и загрузочных записях (*MBR — Master Boot Record*, *VBR — Volume Boot Record*) дисковых устройств. Компонент выполняет загрузку в память и запуск антивирусного ядра Dr.Web Virus-Finding Engine и вирусных баз Dr.Web, используемых им для поиска угроз.

Сканирующее ядро работает в режиме демона, в качестве сервиса, принимающего от других компонентов Dr.Web Desktop Security Suite запросы на проверку объектов файловой системы на наличие угроз (это компоненты Dr.Web File Checker и Dr.Web Network Checker и, возможно, Dr.Web MeshD). При отсутствии или недоступности компонентов Dr.Web Scanning Engine и Dr.Web Virus-Finding Engine антивирусные проверки на данном узле не производятся (за исключением случаев, когда в составе Dr.Web Desktop Security Suite присутствует компонент Dr.Web MeshD, в настройках которого задано соединение с узлами локального облака, предоставляющими услугу сканирующего ядра).

9.11.1. Принципы работы

Компонент Dr.Web Scanning Engine, работающий в режиме демона, принимает от других компонентов Dr.Web Desktop Security Suite запросы на проверку объектов файловой системы (файлов, загрузочных записей на дисках) на наличие внедренных угроз, формирует очереди задач на проверку объектов и выполняет проверку запрошенных объектов, используя антивирусное ядро Dr.Web Virus-Finding Engine. Если в проверенном объекте обнаружена угроза, и в задании на проверку стоит указание выполнять лечение, сканирующее ядро пытается выполнять лечение, если это действие может быть применено к проверенному объекту.

Сканирующее ядро, антивирусное ядро Dr.Web Virus-Finding Engine и вирусные базы образуют атомарный комплекс и не могут быть разделены. Сканирующее ядро осуществляет загрузку вирусных баз и обеспечивает среду для функционирования кросс-платформенного антивирусного ядра Dr.Web Virus-Finding Engine. Обновление вирусных баз и антивирусного ядра производится компонентом обновлений Dr.Web Updater, входящим в состав Dr.Web Desktop Security Suite, но не являющимся частью сканирующего ядра. Компонент обновлений запускается демоном управления конфигурацией Dr.Web ConfigD периодически или принудительно в ответ на поступившую команду пользователя. Кроме того, если Dr.Web Desktop Security Suite функционирует в режиме централизованной защиты, то функции обновления вирусных баз и антивирусного ядра берет на себя агент централизованной защиты Dr.Web ES Agent, который взаимодействует с сервером централизованной защиты и получает обновления от него.

Dr.Web Scanning Engine может работать как под контролем демона управления конфигурацией Dr.Web ConfigD, так и автономно. В первом случае демон обеспечивает

запуск ядра и своевременное обновление вирусных баз, используемых ядром. Во втором случае запуск ядра и обновление вирусных баз возлагаются на использующее его внешнее приложение. Компоненты Dr.Web Desktop Security Suite, выполняющие запросы к сканирующему ядру на предмет проверки файлов, используют тот же программный интерфейс, что и внешние приложения.

Вы можете создать свой собственный компонент (внешнее приложение), использующий Dr.Web Scanning Engine для проверки файлов. Для этого компонент Dr.Web Scanning Engine предоставляет специализированный API, основанный на технологии Google Protobuf. Для получения описания API Dr.Web Scanning Engine, а также примеров кода клиентского приложения, использующего Dr.Web Scanning Engine, обратитесь в отдел по работе с партнерами компании «Доктор Веб».

Поступающие задачи на сканирование автоматически распределяются по трем очередям, имеющим различный приоритет (высокий, нормальный и низкий). Очередь, в которую будет помещена задача, определяется исходя из того, какой компонент ее сформировал. Например, задачи, поступающие от мониторов файловых систем, помещаются в очереди высокого приоритета, поскольку при мониторинге важна скорость реакции на действия с объектами файловой системы. Сканирующее ядро ведет статистику своего использования, фиксируя количество поступивших задач на сканирование, а также длины очередей. В качестве показателя средней нагрузки сканирующее ядро определяет среднюю длину очередей в секунду. Этот показатель усредняется для последней минуты, последних 5 минут и последних 15 минут.

Антивирусное ядро Dr.Web Virus-Finding Engine поддерживает как сигнатурный анализ (поиск известных угроз на основе сигнатур, содержащихся в вирусных базах), так и различные технологии эвристического и поведенческого анализа, предназначенные для распознавания потенциальной опасности объекта на основе анализа последовательности содержащихся в нем машинных инструкций и других признаков исполняемого кода.

Эвристический анализатор не гарантирует достоверного распознавания угроз и может допускать следующие ошибки:

- *Ошибки первого рода* — это ложные срабатывания анализатора, когда в качестве вредоносного отмечается безопасный объект.
- *Ошибки второго рода* — это ошибочное признание вредоносного объекта безопасным.

Поэтому угрозы, обнаруженные эвристическим анализатором, отнесены в особую категорию «Подозрительные» (*Suspicious*).

Рекомендуется выполнять перемещение подозрительных объектов в карантин с тем, чтобы в дальнейшем, после обновления вирусных баз, проверить их методами сигнатурного анализа. Для предотвращения ошибок второго рода рекомендуется поддерживать вирусные базы в актуальном состоянии.

Антивирусное ядро Dr.Web Virus-Finding Engine позволяет осуществлять проверку как незапакованных, так и запакованных файлов и объектов, содержащихся в различных контейнерах, таких как архивы, сообщения электронной почты и т. д.

9.11.2. Аргументы командной строки

Чтобы запустить сканирующее ядро Dr.Web Scanning Engine из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-se <сокет> [<параметры>]
```

где обязательный аргумент *<сокет>* указывает адрес сокета, используемого Dr.Web Scanning Engine для обслуживания запросов клиентских компонентов. Может задаваться только в виде пути к файлу (сокет Unix).

Dr.Web Scanning Engine допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет
Дополнительные параметры запуска (совпадают с параметрами из конфигурационного файла и замещают их при необходимости):	
`--CoreEnginePath`	Назначение: Путь к файлу библиотеки антивирусного ядра Dr.Web Virus-Finding Engine. Краткий вариант: Нет. Аргументы: *<путь к файлу>* — полный путь к файлу используемой библиотеки.
`--VirusBaseDir`	Назначение: Путь к каталогу, содержащему файлы вирусных баз. Краткий вариант: Нет. Аргументы: *<путь к каталогу>* — полный путь к каталогу вирусных баз.
`--TempDir`	Назначение: Путь к каталогу временных файлов. Краткий вариант: Нет. Аргументы: *<путь к каталогу>* — полный путь к каталогу временных файлов.
`--KeyPath`	Назначение: Путь к используемому ключевому файлу. Краткий вариант: Нет.

	Аргументы: <*путь к файлу*> — полный путь к ключевому файлу.
`--MaxForks`	Назначение: Максимальное разрешенное число дочерних процессов, которые Dr.Web Scanning Engine может породить в процессе проверки. Краткий вариант: Нет. Аргументы: <*число*> — максимальное разрешенное число дочерних процессов.
`--WatchdogInterval`	Назначение: Периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность дочерних процессов, занимающихся проверкой содержимого файлов, для остановки зависших при проверке. Краткий вариант: Нет. Аргументы: <*интервал времени*> — периодичность проверки дочерних процессов.
`--AbortForkOnTimeout`	Назначение: Завершить процессы сканирования при тайм-ауте, послав им сигнал SIGABRT. Краткий вариант: Нет. Аргументы: Нет
`--ShellTrace`	Назначение: Отслеживание оболочки (вывод в журнал расширенной информации о проверке файлов ядром Dr.Web Virus-Finding Engine). Краткий вариант: Нет. Аргументы: Нет
`--LogLevel`	Назначение: Уровень подробности ведения журнала ядром Dr.Web Scanning Engine в процессе работы. Краткий вариант: Нет. Аргументы: <*уровень подробности*>. Возможные значения: • `DEBUG` — самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация. • `INFO` — выводятся все сообщения. • `NOTICE` — выводятся сообщения об ошибках, предупреждения, уведомления. • `WARNING` — выводятся сообщения об ошибках и предупреждения. • `ERROR` — выводятся только сообщения об ошибках.
`--Log`	Назначение: Способ ведения журнала сообщений компонента. Краткий вариант: Нет. Аргументы: <*тип журнала*>. Возможные значения: • `Stderr[:ShowTimestamp]` — сообщения будут выводиться в стандартный поток ошибок *stderr*. Опция `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени.

	• `Syslog[:<facility>]` — сообщения будут передаваться системной службе журналирования `syslog`. Дополнительная метка *<facility>* используется для указания типа журнала, в котором `syslog` будет сохранять сообщения. Возможные значения: ○ `DAEMON` — сообщения демонов; ○ `USER` — сообщения пользовательских процессов; ○ `MAIL` — сообщения почтовых программ; ○ `LOCAL0` — сообщения локальных процессов 0; ... ○ `LOCAL7` — сообщения локальных процессов 7. • *<path>* — путь к файлу, в который будут сохраняться сообщения журнала. Примеры: `--Log /var/opt/drweb.com/log/se.log` `--Log Stderr:ShowTimestamp` `--Log Syslog:DAEMON`
`--ForkMemoryLimit`	Назначение: Максимальный объем оперативной памяти, выделяемый для работы экземпляра сканирующего ядра. Краткий вариант: Нет. Аргументы: *<размер в байтах>* — максимальный объем оперативной памяти. Допустимые значения: от 1073741824 байт (1 Гб) до 4294967296 байт (4 Гб). Значение по умолчанию: `4294967296` (4 Гб) ⚠ Этот параметр не задействуется в 32-разрядных дистрибутивах продукта.
`--EngineDallocLimit`	Назначение: Максимальный объем оперативной памяти, выделяемый для хранения временных файлов. Краткий вариант: Нет. Аргументы: *<размер в байтах>* — максимальный объем оперативной памяти. Допустимые значения: от 52428800 байт (50 Мб) до 1073741824 байт (1 Гб). Значение по умолчанию: `524288000` (500 Мб) ⚠ Настоятельно не рекомендуется менять значение по умолчанию для этого параметра, если вы не уверены, что это действительно необходимо.

Пример:

```
$ /opt/drweb.com/bin/drweb-se /tmp/drweb.ipc/.se --MaxForks=5
```

Данная команда запустит экземпляр сканирующего ядра Dr.Web Scanning Engine, заставив его создать Unix-сокет `/tmp/drweb.ipc/.se` для взаимодействия с клиентскими компонентами и порождать не более 5 сканирующих дочерних процессов при проверке файлов.

Замечания о запуске

При необходимости может быть запущено произвольное количество экземпляров сканирующего ядра Dr.Web Scanning Engine, предоставляющих сервис по проверке файлов на наличие угроз клиентским приложениям (не обязательно только компонентам Dr.Web Desktop Security Suite). При этом, если в конфигурации компонента задано значение параметра `FixedSocketPath`, то один экземпляр сканирующего ядра всегда будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD и доступен клиентам через Unix-сокет. Экземпляры сканирующего ядра, запускаемые непосредственно из командной строки, будут работать в автономном режиме, без подключения к демону управления конфигурацией, даже если он запущен. Для управления параметрами работы компонента, а также для проверки файлов по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для сканирования произвольного файла или каталога компонентом Dr.Web Scanning Engine используйте команду `rawscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl rawscan <путь к каталогу или файлу>
```

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-se`.

9.11.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ScanEngine]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

Эта секция хранит следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента.

Параметр	Описание
	Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-se`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Если задано значение параметра `FixedSocketPath`, то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя). Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `1h`
`FixedSocketPath` *{путь к файлу}*	Путь к файлу Unix-сокета фиксированного экземпляра сканирующего ядра Dr.Web Scanning Engine. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр сканирующего ядра, доступный клиентам через этот сокет. ⚠ Убедитесь, что каталогу с файлом сокета назначены следующие права доступа: `drwxr-xr-x` Чтобы просмотреть права доступа, выполните команду: `$ ls -ld <путь к каталогу>` Значение по умолчанию: *(не задано)*
`MaxForks` *{целое число}*	Максимальное разрешенное количество экземпляров дочерних сканирующих процессов, порождаемых сканирующим ядром Dr.Web Scanning Engine, которые могут быть запущены одновременно. Значение по умолчанию: *Автоматически определяется при старте* как удвоенное число доступных процессорных ядер, или `4`, если полученное число меньше 4.

Параметр	Описание
`ForkMemoryLimit` *{целое число}*	Максимальный объем оперативной памяти, выделяемый для работы экземпляра сканирующего ядра. Значение указывается как целое число с суффиксом (*b, kb, mb, gb*). Если суффикс не указан, то значение интерпретируется как размер в байтах. Допустимые значения: от 1 гигабайта (`1GB`) до 4 гигабайт (`4GB`). Значение по умолчанию: `4GB` ⚠ Этот параметр не задействуется в 32-разрядных дистрибутивах Dr.Web Desktop Security Suite.
`EngineDallocLimit` *{целое число}*	Максимальный объем оперативной памяти, выделяемый для хранения временных файлов. Если указанное значение меньше размера временного файла, то он будет создан на устройстве хранения, что замедлит работу Dr.Web Desktop Security Suite. Значение указывается как целое число с суффиксом (*b, kb, mb, gb*). Если суффикс не указан, то значение интерпретируется как размер в байтах. Допустимые значения: от 50 мегабайт (`50MB`) до 1 гигабайта (`1GB`). Значение по умолчанию: `500MB` ⚠ Настоятельно не рекомендуется менять значение по умолчанию для этого параметра, если вы не уверены, что это действительно необходимо.
`WatchdogInterval` *{интервал времени}*	Периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность порожденных им дочерних сканирующих процессов для обнаружения зависаний при проверке («сторожевой таймер»). Значение по умолчанию: `15s`
`BufferedIo` *{логическое значение}*	Использовать или не использовать буферизованный ввод-вывод при проверке файлов. Использование буферизованного ввода-вывода в ОС семейства GNU/Linux может увеличить скорость проверки файлов, расположенных на медленных дисковых устройствах. Возможные значения: • `On`, `Yes`, `True` — использовать буферизованный ввод-вывод; • `Off`, `No`, `False` — не использовать буферизованный ввод-вывод. Значение по умолчанию: `Off`

Параметр	Описание
`AbortForkOnTimeout` *{логическое значение}*	Завершать или не завершать процессы сканирования при тайм-ауте, послав им сигнал SIGABRT. Возможные значения: • `On`, `Yes`, `True` — завершать процессы сканирования при тайм-ауте; • `Off`, `No`, `False` — не завершать процессы сканирования при тайм-ауте. Значение по умолчанию: `Off`

9.12. Dr.Web Updater

Компонент обновлений Dr.Web Updater предназначен для получения обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine с серверов обновлений компании «Доктор Веб».

Если Dr.Web Desktop Security Suite работает в режиме централизованной защиты, то в качестве источника обновлений используется сервер централизованной защиты, причем все обновления получаются с сервера через Dr.Web ES Agent, а Dr.Web Updater для загрузки обновлений не используется.

9.12.1. Принципы работы

Компонент подключается к серверам обновлений компании «Доктор Веб» для проверки наличия и загрузки обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine, базы категорий веб-ресурсов, а также компонента проверки писем на спам. Списки серверов, образующих доступную зону обновлений, хранятся в специальном файле, который подписан с целью невозможности его модификации. При подключении к серверам обновлений через прокси-сервер поддерживается только базовая и дайджест-аутентификация.

Если Dr.Web Desktop Security Suite не подключен к серверу централизованной защиты или подключен к нему в мобильном режиме, то Dr.Web Updater автоматически запускается демоном управления конфигурацией Dr.Web ConfigD с периодичностью, указанной в настройках. Также компонент может быть запущен Dr.Web ConfigD в ответ на поступившую команду пользователя (внеочередное обновление).

При наличии на серверах обновлений доступных обновлений, они загружаются в каталог `/var/opt/drweb.com/cache/`, после чего размещаются в рабочих каталогах Dr.Web Desktop Security Suite.

По умолчанию все обновления загружаются с зоны обновления, общей для всех продуктов Dr.Web. Перечень используемых по умолчанию серверов, входящих в зону обновления, указывается в файлах, находящихся в каталогах, указанных в параметрах `*DrlDir`, сгруппированных по типу выполняемого обновления: для вирусных баз и антивирусного ядра, для базы категорий веб-ресурсов, для компонента проверки писем на спам). При необходимости по запросу клиента может быть создана особая зона обновления (для каждого вида обновления), список серверов которой указывается в отдельном файле (по умолчанию с именем `update.drl`). Этот файл находится в каталоге, указанном в соответствующем параметре `*CustomDrlDir`. В этом случае компонент обновлений будет загружать обновления только с этих серверов, не используя серверы из зоны по умолчанию.

Для отказа от использования особой зоны обновления достаточно очистить значение соответствующего параметра `*CustomDrlDir` в настройках компонента.

Содержимое файлов списков серверов подписано для невозможности их модификации. Если вам необходимо создать особый перечень серверов обновления, обратитесь в техническую поддержку.

Компонент может выполнять сохранение резервных копий обновляемых файлов для последующего отката обновлений по команде пользователя. Место сохранения резервных копий и глубина хранимой истории обновлений задаются в настройках компонента. Откат обновлений выполняется через утилиту управления Dr.Web Desktop Security Suite из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`).

9.12.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Updater из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-update [<параметры>]
```

Dr.Web Updater допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-update --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Updater.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается демоном управления конфигурацией Dr.Web ConfigD автоматически, по мере необходимости. Для управления параметрами работы компонента, а также для обновления вирусных баз и антивирусного ядра по требованию пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-update`.

9.12.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[Update]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, то используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-update`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Компонент запускается при очередном обновлении по расписанию. По окончании обновления ждет указанный интервал времени, и, если новых запросов не поступает, то завершает свою работу до следующей попытки обновления. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать

Параметр	Описание
	постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `10m`
`Start` *{логический}*	Запускать или не запускать компонент при загрузке Dr.Web Desktop Security Suite. Этот параметр имеет приоритет над параметром `DwsUpdateEnabled`. Допустимые значения: • `Yes` — запускать компонент при загрузке Dr.Web Desktop Security Suite; • `No` — не запускать компонент при загрузке Dr.Web Desktop Security Suite. Значение по умолчанию: `Yes`
`UpdateInterval` *{интервал времени}*	Частота проверки наличия обновлений на серверах обновления Dr.Web, т. е. период времени, который должен пройти от предыдущей успешной попытки подключения к серверам обновления (автоматического или инициированного пользователем) до следующей попытки выполнить обновление. Значение по умолчанию: `30m`
`NetworkTimeout` *{интервал времени}*	Тайм-аут на сетевые операции компонента при выполнении обновлений с серверов Dr.Web. Используется для ожидания продолжения обновления в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то обновление будет продолжено. Не имеет смысла указывать величину тайм-аута более `75s`, т. к. за это время соединение закроется по тайм-ауту TCP. Минимальное значение: `5s`. Значение по умолчанию: `60s`
`RetryInterval` *{интервал времени}*	Частота повторных попыток выполнить обновление с серверов обновления, если очередная попытка выполнить обновление завершилось неудачей. Допустимые значения: от 1 минуты (`1m`) до 30 минут (`30m`). Значение по умолчанию: `3m`
`MaxRetries` *{целое число}*	Количество повторных попыток выполнить обновление с серверов обновления Dr.Web (предпринимаемых через промежутки времени, указанные в параметре

Параметр	Описание
	`RetryInterval`), если предыдущая попытка обновления закончилась неудачей. Если значение параметра — `0`, то повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени, указанный в параметре `UpdateInterval`). Значение по умолчанию: `3`
`UseHttps` *{Always | ResListOnly | Never}*	Использовать или не использовать протокол HTTPS при скачивании обновлений. Допустимые значения: • `Always` — всегда использовать протокол HTTPS при скачивании обновлений. • `ResListOnly` — использовать протокол HTTPS только при скачивании файла `.lst` со списком файлов обновления. Сами файлы обновления будут скачиваться по протоколу HTTP. • `Never` — всегда использовать протокол HTTP при скачивании обновлений. Значение по умолчанию: `ResListOnly`
`Proxy` *{строка подключения}*	Параметры подключения к прокси-серверу, который используется компонентом обновлений Dr.Web Updater для подключения к серверам обновлений Dr.Web (например, если непосредственное подключение к внешним серверам запрещено политиками безопасности сети). Если значение параметра не задано, то прокси-сервер не используется. Возможные значения: <*строка подключения*> — строка подключения к прокси-серверу. Имеет следующий формат (URL): `[`<*протокол*>`://][`<*пользователь*>`:`<*пароль*>`@]` <*хост*>`:`<*порт*> где: • <*протокол*> — тип используемого протокола (в текущей версии доступен только `http`); • <*пользователь*> — имя пользователя для подключения к прокси-серверу; • <*пароль*> — пароль для подключения к прокси-серверу; • <*хост*> — адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN); • <*порт*> — используемый порт.

Параметр	Описание
	Части URL <*протокол*> и <*пользователь*>:<*пароль*> могут отсутствовать. Адрес прокси-сервера <*хост*>:<*порт*> является обязательным. Если имя пользователя или пароль содержат символы `@`, `%` или `:`, то их следует заменить на соответствующие HEX-коды: `%40`, `%25` и `%3A` соответственно. Примеры: 1. В файле конфигурации: • Подключение к прокси-серверу на узле `proxyhost.company.org` на порт `123`: `Proxy = proxyhost.company.org:123` • Подключение к прокси-серверу на узле `10.26.127.0` на порт `3336`, используя протокол HTTP, от имени пользователя `legaluser` с паролем `passw`: `Proxy = http://legaluser:passw@10.26.127.0:3336` • Подключение к прокси-серверу на узле `10.26.127.0` на порт `3336` от имени пользователя `user@company.com` с паролем `passw%123`: `Proxy = user%40company.com:passw%25123%3A@10.26.127.0:3336` 2. Задание тех же самых значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset Update.Proxy proxyhost.company.org:123` `# drweb-ctl cfset Update.Proxy http://legaluser:passw@10.26.127.0:3336` `# drweb-ctl cfset Update.Proxy user%40company.com:passw%25123%3A@10.26.127.0:3336` Значение по умолчанию: *(не задано)*
`ExcludedFiles` *{имя файла}*	Имя файла, который не будет обновляться компонентом обновлений Dr.Web Updater. Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список файлы `123.vdb` и `456.dws`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке: `[Update]` `ExcludedFiles = "123.vdb", "456.dws"`

Параметр	Описание
	• Две строки (по одному значению в строке): `[Update]` `ExcludedFiles = 123.vdb` `ExcludedFiles = 456.dws` 2. Добавление значений с помощью команды `drweb-ctl cfset`: `# drweb-ctl cfset Update.ExcludedFiles -a 123.vdb` `# drweb-ctl cfset Update.ExcludedFiles -a 456.dws` Значение по умолчанию: `drweb32.lst`
`BaseUpdateEnabled` *{логический}*	Разрешить или запретить обновление вирусных баз и антивирусного ядра. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`BaseDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам из стандартной зоны обновления, используемым для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: `/var/opt/drweb.com/drl/bases`
`BaseCustomDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам особой («клиентской») зоны обновления, используемым для обновления вирусных баз и антивирусного ядра. Если в каталоге, на который указывает параметр, имеется непустой подписанный файл списка серверов (файл `.drl`), то обновление ведется только с этих серверов, а серверы основной зоны (см. выше) не используются для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: `/var/opt/drweb.com/custom-drl/bases`
`VersionUpdateEnabled` *{логический}*	Разрешить или запретить обновление версий компонентов Dr.Web Desktop Security Suite. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`VersionDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам, используемым для обновления версий компонентов Dr.Web Desktop Security Suite.

Параметр	Описание
	Значение по умолчанию: `/var/opt/drweb.com/drl/version`
`DwsUpdateEnabled` *{логический}*	Разрешить или запретить обновление базы категорий веб-ресурсов. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`DwsDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам стандартной зоны обновления, используемым для обновления базы категорий веб-ресурсов. Значение по умолчанию: `/var/opt/drweb.com/drl/dws`
`DwsCustomDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам особой («клиентской») зоны обновления, используемым для обновления базы категорий веб-ресурсов. Если в каталоге, на который указывает параметр, имеется непустой подписанный файл списка серверов (файл `.drl`), то обновление ведется только с этих серверов, а серверы основной зоны (см. выше) не используются для обновления базы категорий веб-ресурсов. Значение по умолчанию: `/var/opt/drweb.com/custom-drl/dws`
`AntispamUpdateEnabled` *{логический}*	Разрешить или запретить обновление библиотеки проверки писем на спам. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`AntispamDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам стандартной зоны обновления, используемым для обновления библиотеки проверки писем на спам. Значение по умолчанию: `/var/opt/drweb.com/drl/antispam`
`AntispamCustomDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам особой («клиентской») зоны обновления, используемым для обновления библиотеки проверки писем на спам.

Параметр	Описание
	Если в каталоге, на который указывает параметр, имеется непустой подписанный файл списка серверов (файл `.drl`), то обновление ведется только с этих серверов, а серверы основной зоны (см. выше) не используются для обновления библиотеки проверки писем на спам. Значение по умолчанию: `/var/opt/drweb.com/custom-drl/antispam`
`BackupDir` *{путь к каталогу}*	Путь к каталогу, в который сохраняются старые версии обновляемых файлов для возможности отката обновлений. При каждом обновлении сохраняются резервные копии только обновленных файлов. Значение по умолчанию: `/var/opt/drweb.com/backup`
`MaxBackups` *{целое число}*	Максимальное количество сохраняемых предыдущих версий обновляемых файлов. При превышении этой величины самая старая копия удаляется при очередном обновлении. Если значение параметра — `0`, то предыдущие версии файлов для восстановления не сохраняются. Значение по умолчанию: `0`

9.13. Dr.Web ES Agent

Агент централизованной защиты Dr.Web ES Agent предназначен для подключения Dr.Web Desktop Security Suite к серверу централизованной защиты.

Когда Dr.Web Desktop Security Suite подключен к серверу централизованной защиты, Dr.Web ES Agent синхронизирует лицензионный ключевой файл с ключами, хранящимися на сервере централизованной защиты. Кроме того, Dr.Web ES Agent передает на сервер централизованной защиты, к которому он подключен, статистику инцидентов, связанных с вредоносным ПО, перечень запущенных компонентов и их состояние.

Также Dr.Web ES Agent выполняет обновление вирусных баз Dr.Web Desktop Security Suite непосредственно с подключенного сервера централизованной защиты, минуя компонент обновления Dr.Web Updater.

9.13.1. Принципы работы

Компонент Dr.Web ES Agent осуществляет подключение к серверу централизованной защиты, который позволяет администратору сети реализовать на всем пространстве сети единую политику безопасности, в частности, настроить на всех рабочих станциях и серверах сети одинаковые стратегии проверки файлов и других объектов файловой системы и реакции на обнаруженные угрозы. Кроме того, сервер централизованной защиты выполняет в рамках защищаемой сети функции внутреннего сервера обновлений, играя роль хранилища актуальных вирусных баз (обновление в этом случае производится через Dr.Web ES Agent, Dr.Web Updater не используется).

При подключении Dr.Web ES Agent к серверу централизованной защиты агент обеспечивает прием от сервера актуальной версии настроек программных компонентов и лицензионного ключевого файла, которые он передает демону управления конфигурацией Dr.Web ConfigD для применения к управляемым компонентам. Кроме того, он может принимать от сервера централизованной защиты задания на проверку объектов файловой системы на рабочей станции (в том числе по расписанию).

Dr.Web ES Agent собирает и отправляет на сервер, к которому он подключен, статистику обнаружения различных угроз и примененных действий.

Для подключения Dr.Web ES Agent к серверу централизованной защиты требуется иметь пароль и идентификатор узла («рабочей станции» в терминах сервера централизованной защиты), а также файл публичного ключа шифрования, используемого сервером для подтверждения его подлинности. Вместо идентификатора станции можно указать при подключении идентификатор основной и тарифной групп, в которые станцию необходимо включить на сервере. Требуемые идентификаторы и файл публичного ключа можно получить у администратора, управляющего антивирусной защитой сети через сервер централизованной защиты.

Кроме того, к серверу централизованной защиты можно подключить защищаемый узел («рабочую станцию») в режиме «новичок», если данная возможность разрешена сервером централизованной защиты. В этом случае после того, как администратор подтвердит заявку на подключение станции, сервер централизованной защиты автоматически сгенерирует для узла новые идентификатор и пароль и отправит их агенту для использования при последующих подключениях.

9.13.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web ES Agent из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-esagent [<параметры>]
```

Dr.Web ES Agent допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-esagent --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web ES Agent.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически, при старте операционной системы, демоном управления конфигурацией Dr.Web ConfigD. Для управления параметрами работы компонента, а также для подключения Dr.Web Desktop Security Suite к серверу централизованной защиты используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-esagent`.

9.13.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ESAgent]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-esagent`
`MobileMode` *{On | Off | Auto}*	Использовать или не использовать мобильный режим Dr.Web Desktop Security Suite при подключении к серверу централизованной защиты. Допустимые значения: • `On` — использовать мобильный режим, если он разрешен сервером централизованной защиты (устанавливать обновления с серверов обновлений компании «Доктор Веб» с помощью Dr.Web Updater); • `Off` — не использовать мобильный режим, оставаться в режиме централизованной защиты (всегда получать обновления только с сервера централизованной защиты); • `Auto` — использовать мобильный режим, если он разрешен сервером централизованной защиты, а обновления устанавливать как с серверов обновлений компании «Доктор Веб» с помощью Dr.Web Updater, так и с сервера централизованной защиты, в зависимости от того, какое соединение доступно и качество какого соединения лучше. Поведение данного параметра зависит от разрешений на сервере: если мобильный режим на используемом сервере не разрешен, то параметр не имеет никакого эффекта. Значение по умолчанию: `Auto`
`Discovery` *{On | Off}*	Разрешить или запретить агенту принимать *discovery*-запросы от инспектора сети, встроенного в сервер централизованной защиты (*discovery*-запросы используются инспектором для проверки структуры и состояния антивирусной сети).

Параметр	Описание
	Допустимые значения: • `On` — разрешать агенту принимать и обрабатывать *discovery*-запросы; • `Off` — запретить агенту принимать и обрабатывать *discovery*-запросы.  Данный параметр имеет приоритет над настройками сервера централизованной защиты: если указано значение `Off`, агент не будет принимать discovery-запросы, даже если эта функция включена на сервере. Значение по умолчанию: `On`
`UpdatePlatform` *{название платформы}*	Обозначение платформы, для которой агент будет получать с сервера централизованной защиты обновления для антивирусного ядра. Допустимые значения: • для GNU/Linux: `unix-linux-32`, `unix-linux-64-engine64`, `unix-linux-aarch64`, `unix-linux-e2k`, `unix-linux-e2k-engine64`, `unix-linux-mips`, `unix-linux-ppc64le`; • для FreeBSD: `unix-freebsd-32`, `unix-freebsd-64-engine64`; • для Darwin: `unix-darwin-32`, `unix-darwin-64-engine64`, `unix-darwin-aarch64`.  Настоятельно не рекомендуется изменять значение параметра, если вы не уверены, что это действительно необходимо. Значение по умолчанию: *Зависит от используемой платформы*
`DebugIpc` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC (взаимодействие Dr.Web ES Agent и демона управления конфигурацией Dr.Web ConfigD). Значение по умолчанию: `No`
`DebugConfig` *{логический}*	Добавлять или не добавлять в журнал информацию о настройках, полученных от сервера централизованной защиты. Значение по умолчанию: `No`
`SrvMsgAutoremove` *{целое число}*	Срок хранения сообщений. По завершении указанного срока сообщения удаляются из базы. Допустимые значения: от 1 недели (`1w`) до 365 дней (`365d`). Значение параметра указывается в виде целого числа с суффиксом `s`, `m`, `h`, `d`, `w`. Значение по умолчанию: `1w`

9.14. Dr.Web MeshD

Компонент Dr.Web MeshD представляет собой агент, включающий узел с установленным Dr.Web Desktop Security Suite в «локальное облако», объединяющее узлы, на которых установлены продукты Dr.Web для Unix. Данное облако позволяет одним узлам облака получить доступ к сканирующему ядру других, другими словами, воспользоваться услугой по проверке файлов.

Для объединения узлов с установленными продуктами Dr.Web для Unix в составе каждого узла должен присутствовать компонент Dr.Web MeshD, обеспечивающий включение этого узла в облако. Полномочия узла в рамках облака и возможности облака, используемые узлом, гибко регулируются настройками компонента Dr.Web MeshD.

Обмен данными с другими узлами облака производится по защищенному каналу SSH.

9.14.1. Принципы работы

В этом разделе

- Типы подключений
- Режимы работы
- Услуги
  - Удаленное сканирование файлов (Engine)
  - Передача файлов на проверку (File)
  - Проверка URL (Url)

Dr.Web MeshD играет роль посредника, обеспечивающего взаимодействие между узлом, на котором установлен Dr.Web Desktop Security Suite, и другими узлами облака.

Типы подключений

При работе Dr.Web MeshD использует подключения следующих типов:

- *Клиентские (сервисные)* используются Dr.Web MeshD для подключения к нему других узлов облака, которые являются клиентами услуг, предоставляемых данным узлом.

  Компоненты Dr.Web Desktop Security Suite, работающие на узле и использующие услуги, предоставленные облаком, подключаются к Dr.Web MeshD, работающий на этом же узле, через локальный Unix-сокет. Клиентское подключение при этом не используется.

- *Партнерские (одноранговые)* используются Dr.Web MeshD для взаимодействия с равноправными (в рамках некоторой услуги) узлами-партнерами облака. Обычно подобные горизонтальные связи используются для масштабирования и

распределения нагрузки при взаимодействии с облаком, а также синхронизации состояния узлов облака.

- *Восходящие* используются Dr.Web MeshD для подключения данного узла в роли клиента к узлам облака, предоставляющим услуги (например, передача файлов на проверку и т. д.).

Использование подключений всех трех типов настраивается для разных услуг облака независимо друг от друга. При этом один и тот же узел может быть настроен как сервер для обслуживания клиентских запросов в рамках одной услуги (например, проверки URL) и как клиент — в рамках другой услуги (например, удаленного сканирования файлов).

В рамках облака узлы осуществляют взаимодействие по защищенному протоколу SSH, т. е. все стороны в рамках каждого межузлового взаимодействия всегда взаимно аутентифицированы. Для аутентификации используются узловые ключи (*host keys*) согласно RFC 4251. Клиентское подключение от локального компонента всегда считается доверенным.

Режимы работы

Dr.Web MeshD может работать как в режиме демона, так и запускаться по запросам от других компонентов Dr.Web Desktop Security Suite, расположенных на локальном узле. Если Dr.Web MeshD настроен на обслуживание клиентских подключений (параметр `ListenAddress` не пуст) и активирована возможность оказания хотя бы одной из услуг, Dr.Web MeshD запускается как демон и ждет подключения со стороны клиентов.

Если Dr.Web MeshD не настроен на обслуживание клиентских подключений (параметр `ListenAddress` пуст) и запросы к нему отсутствуют в течение периода времени, указанного в параметре `IdleTimeLimit`, работа компонента автоматически завершается.

Услуги

Удаленное сканирование файлов (Engine)

Данная услуга позволяет использовать Dr.Web Scanning Engine для проверки удаленных файлов: узлы, работающие в роли клиентов, отправляют файлы на проверку на серверный узел, а серверные узлы предоставляют услугу по проверке файлов, отправленных клиентскими узлами. Типовые настройки клиента следующие:

```
…
[MeshD]
EngineChannel = On
EngineUplink = <адрес сервера>
ListenAddress =
…
```

На узле, выполняющем роль локального сервера сканирования, заданы следующие настройки:

```
EngineChannel = On
EngineUplink =
ListenAddress = <адрес>:<порт>
```

Здесь *<адрес сервера>* в восходящем соединении клиента должен указывать на те *<адрес>* и *<порт>*, которые используются серверным узлом для организации клиентских подключений.

Передача файлов на проверку (File)

Данная функциональность не используется (функция удаленного сканирования оказывается в рамках услуги *Engine*).

Проверка URL (Url)

Данная услуга предназначена для проверки URL на принадлежность к потенциально опасным и нежелательным категориям: узлы, выступающие в роли клиентов, отправляют URL для проверки на серверный узел. Типовые настройки клиента следующие:

```
…
[MeshD]
UrlChannel = On
UrlUplink = <адрес сервера>
ListenAddress =
…
```

На узле, выступающем в качестве сервера для проверки URL, заданы следующие настройки:

```
UrlChannel = On
UrlUplink =
ListenAddress = <адрес>:<порт>
```

Здесь *<адрес сервера>* в восходящем соединении клиента должен указывать на те *<адрес>* и *<порт>*, которые используются серверным узлом для организации клиентских подключений.

9.14.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web MeshD из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-meshd [<параметры>]
```

Dr.Web MeshD допускает использование следующих параметров:

Параметр	Описание

`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-meshd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web MeshD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-meshd`.

9.14.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[MeshD]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`

Параметр	Описание
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-meshd`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`DebugSsh` *{логический}*	Сохранять или не сохранять в журнале сообщения протокола SSH (используется для передачи сообщений и данных), полученных и отправленных компонентом Dr.Web MeshD, работающим на данном узле, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`ListenAddress` *<IP-адрес>:<порт>*	Сетевой сокет (адрес и порт) клиентского подключения, на котором компонент ожидает поступления соединений от узлов облака, являющихся клиентами услуг, предоставляемых данным узлом облака. Чтобы компонент мог прослушивать интерфейс IPv6 и определять клиентские узлы облака по IPv6, параметр должен быть обязательно установлен. Если значение не задано, то компонент не принимает запросы от клиентов. Значение по умолчанию: `0.0.0.0:7090`, если установлен пакет `drweb-scanning-server`, в противном случае значение не задано
`DnsResolverConfPath` *{путь к файлу}*	Путь к файлу настроек DNS. Значение по умолчанию: `/etc/resolv.conf`
`DiscoveryResponderPort` *{номер порта}*	Порт, на котором вышестоящий узел MeshD отвечает по протоколу UDP на запросы клиентов. Механизм *discovery* работает только если задан параметр `ListenAddress`. Значение по умолчанию: `18008`
`FileChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге обмена файлами. Если этот параметр установлен в значение `On`, то компонент Dr.Web MeshD будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD.

Параметр	Описание
	Значение по умолчанию: `On`
`FileUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, принимающего на проверку файлы с этого узла. Возможные значения: • *значение не указано* — сервер для этой услуги не задан, и Dr.Web MeshD не будет ни к кому подключаться. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*. Если *<домен>* не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`FileDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги обмена файлами, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`EngineChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге предоставления сканирующего ядра. Если этот параметр установлен в значение `On`, то компонент Dr.Web MeshD будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD. Значение по умолчанию: `On`
`EngineUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, предоставляющего услуги сканирующего ядра для данного узла. Возможные значения: • *значение не указано* — сервер для этой услуги не задан, и Dr.Web MeshD не будет ни к кому подключаться. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*. Если *<домен>* не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним.

Параметр	Описание
	• `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`EngineDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги сканирования, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`UrlChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге проверки URL. Значение по умолчанию: `On`
`UrlUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, проверяющего URL для данного узла. Возможные значения: • *значение не указано* — сервер проверки URL не задан. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*. Если *<домен>* не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`UrlDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги проверки URL, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`



В текущей версии Dr.Web Desktop Security Suite услуга передачи файлов на проверку *File* не используется. Вместо нее следует использовать услугу сканирующего ядра *Engine*.

9.15. Dr.Web URL Checker

Dr.Web URL Checker — вспомогательный компонент, предназначенный для проверки ссылок на вредоносные и нежелательные веб-ресурсы.

Dr.Web URL Checker используется следующими компонентами:

- Dr.Web MeshD,
- SplDer Gate,
- Dr.Web MailD

9.15.1. Принципы работы

Компонент Dr.Web URL Checker предназначен для проверки URL на принадлежность к нежелательным или потенциально опасным категориям.

Проверка выполняется либо с помощью специализированных баз ссылок, либо с помощью сервиса Dr.Web CloudD. Чтобы использовать сервис Dr.Web CloudD, выполните команду:

```
# drweb-ctl cfset Root.UseCloud Yes
```

Компонент Dr.Web URL Checker не может быть запущен пользователем. Он запускается демоном управления конфигурацией Dr.Web ConfigD по запросу от других компонентов.

9.15.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web URL Checker из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-urlcheck [<параметры>]
```

Dr.Web URL Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-urlcheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web URL Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-urlcheck`.

9.15.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[Urlcheck]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-urlcheck`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `None`, если установлен пакет `drweb-scanning-server`, и `10m` в противном случае
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`.

Параметр	Описание
	Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`

9.16. Dr.Web CloudD

В этом разделе

- Принципы работы
- Работа с сервисом Dr.Web Cloud
- Аргументы командной строки
- Параметры конфигурации

Принципы работы

Компонент Dr.Web CloudD предназначен для обращения к облачному сервису Dr.Web Cloud компании «Доктор Веб». Сервис Dr.Web Cloud собирает от всех антивирусных продуктов Dr.Web свежую информацию об обнаруженных угрозах, что позволяет:

- нейтрализовать новейшие угрозы, описание которых еще не внесено в вирусные базы;
- оградить пользователей от посещения нежелательных сайтов, описание которых еще не внесено в базы категорий веб-ресурсов;
- снизить вероятность ложных срабатываний сканирующего ядра Dr.Web Scanning Engine.

Если компонент включен, то он будет периодически отправлять облачному сервису Dr.Web Cloud статистику обнаружения инфицированных файлов.



Все данные, отправляемые компонентом на серверы компании «Доктор Веб», являются обезличенными и не позволяют идентифицировать пользователя.

При установке Dr.Web Desktop Security Suite в графическом режиме посредством универсального пакета `.run` флажок **Я хочу подключиться к облачным сервисам Dr.Web Cloud** установлен по умолчанию. Если его не снять, то компонент Dr.Web CloudD будет включен. При установке Dr.Web Desktop Security Suite из репозитория компонент Dr.Web CloudD по умолчанию выключен.

Облачный сервис Dr.Web Cloud используется как дополнительный эшелон защиты при проверке файловых систем, сетевого трафика и URL. Если компонент Dr.Web CloudD включен, то он задействуется при всех операциях проверки файловых систем.

Работа с сервисом Dr.Web Cloud

Подключение Dr.Web Desktop Security Suite к сервису Dr.Web Cloud происходит автоматически при включении компонента Dr.Web CloudD.

Вы можете включить или отключить компонент Dr.Web CloudD с помощью:

- графического интерфейса Dr.Web Desktop Security Suite;
- утилиты Dr.Web Ctl;
- редактирования конфигурационного файла вручную.

Включение или отключение с помощью графического интерфейса Dr.Web Desktop Security Suite

1. Откройте окно **Dr.Web для Linux** и нажмите  для перехода к настройкам.
2. Перейдите на вкладку **Dr.Web Cloud**.
3. Переведите Dr.Web Desktop Security Suite в режим администратора.
4. Чтобы включить компонент Dr.Web CloudD и подключиться к сервису Dr.Web Cloud, установите флажок **Подключиться к облачным сервисам Dr.Web Cloud (рекомендуется)**, в противном случае снимите этот флажок.

Подробнее про настройку сервиса Dr.Web Cloud в графическом режиме.

Включение или отключение с помощью утилиты Dr.Web Ctl

Чтобы включить Dr.Web CloudD, выполните команду:

```
# drweb-ctl cfset Root.UseCloud Yes
```

Чтобы отключить этот компонент, выполните команду:

```
# drweb-ctl cfset Root.UseCloud No
```

Включение или отключение путем редактирования конфигурационного файла вручную



Вы должны быть уверены в корректности изменений, вносимых в конфигурационный файл.

1. Откройте конфигурационный файл `/etc/opt/drweb.com/drweb.ini` для GNU/Linux в предпочитаемом вами текстовом редакторе с правами администратора. Чтобы получить права администратора, используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.
2. Если в конфигурационном файле отсутствует секция `[Root]`, то перейдите в конец файла и добавьте с новой строки:
   - Для включения компонента и подключения к сервису:

   ```
   [Root]
   UseCloud = Yes
   ```

   - Для выключения компонента и отключения от сервиса:

```
[Root]
UseCloud = No
```

Если конфигурационный файл уже включает секцию `[Root]`:

- Если параметр `UseCloud` отсутствует, добавьте его, указав `UseCloud = Yes` для подключения к сервису или `UseCloud = No` для отключения от него.
- Если параметр `UseCloud` уже указан в секции `[Root]`, то измените его значение на `Yes` для подключения к сервису или на `No` для отключения от него.

3. Перезагрузите конфигурацию Dr.Web Desktop Security Suite, выполнив команду:

```
# drweb-ctl reload
```

для применения внесенных изменений.

Компонент Dr.Web CloudD запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.

> Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-cloudd`.

Аргументы командной строки

Чтобы показать справочную информацию о компоненте Dr.Web CloudD, выполните команду:

```
$ /opt/drweb.com/bin/drweb-cloudd [<параметры>]
```

`drweb-cloudd` принимает следующие параметры:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-cloudd --help
```

Эта команда выведет на экран краткую справку о компоненте Dr.Web CloudD.

Параметры конфигурации

Компонент Dr.Web CloudD использует параметры конфигурации, заданные в секции `[CloudD]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

Чтобы изменить значение какого-либо параметра Dr.Web CloudD, выполните команду:

```
# drweb-ctl cfset CloudD.<параметр> <значение>
```

В секции `[CloudD]` представлены следующие параметры:

Параметр	Допустимые значения	Описание
`LogLevel`	*Debug, Info, Notice, Warning или Error*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log`	*Auto, Syslog[:<Daemon, User, Mail или Local0..7>] или <путь к файлу>*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath`	*путь к файлу*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-cloudd`
`RunAsUser`	*<UID> или <имя пользователя>*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit`	*интервал времени*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет

Параметр	Допустимые значения	Описание
		работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `1h`
`FixedSocketPath`	*путь к файлу*	Путь к файлу Unix-сокета фиксированного экземпляра компонента. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр компонента, доступный клиентам через этот сокет. ⚠ Убедитесь, что каталогу с файлом сокета назначены следующие права доступа: `drwxr-xr-x` Чтобы просмотреть права доступа, выполните команду: `$ ls -ld <путь к каталогу>` Значение по умолчанию: *(не задано)*
`PersistentCache`	*On, Yes, True, Off, No или False*	Включать или нет сохранение на диск кеша ответов, получаемых от Dr.Web Cloud. Значение по умолчанию: `Off`
`DebugSdk`	*On, Yes, True, Off, No или False*	Включать или нет в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения от Dr.Web Cloud. Значение по умолчанию: `No`

9.17. Dr.Web StatD

Компонент Dr.Web StatD предназначен для накопления статистики событий, возникающих в процессе работы компонентов Dr.Web Desktop Security Suite. Полученные события регистрируются в постоянном хранилище и могут быть получены по запросу.

9.17.1. Принципы работы

Компонент Dr.Web StatD обеспечивает накопление и постоянное хранение событий, поступающих от компонентов Dr.Web Desktop Security Suite в процессе работы. Регистрируются события следующих типов:

- неожиданное завершение работы компонента;
- обнаружение угрозы в сообщении электронной почты.

Просмотр событий и управление ими обеспечивается командой `events` утилиты Dr.Web Ctl.

9.17.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web StatD из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-statd [<параметры>]
```

Dr.Web StatD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-statd --help
```

Эта команда выведет на экран краткую справку компонента Dr.Web StatD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Desktop Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-statd`.

9.17.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[StatD]` объединенного конфигурационного файла Dr.Web Desktop Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-statd`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на

Параметр	Описание
	числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`MaxEventStoreSize` *{размер}*	Максимальный разрешенный размер базы событий. Задается в `mb`, например: `MaxEventStoreSize = 100mb`. Минимальное значение: `50mb`. Значение по умолчанию: `1GB`

10. Приложения

10.1. Приложение А. Виды компьютерных угроз

В этом разделе

- Компьютерные вирусы
- Компьютерные черви
- Троянские программы
- Программы взлома
- Рекламные программы
- Программы-шутки
- Программы дозвона
- Потенциально опасные программы
- Подозрительные объекты

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. Значительное число вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы классифицируются по типам 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 скриптов (например, служебные файлы операционной системы). Они также могут инфицировать файлы других типов, которые поддерживают исполнение скриптов, и могут распространяться, например, посредством уязвимых веб-приложений.
- *Загрузочные вирусы* инфицируют загрузочные секторы дисков и разделов, а также главные загрузочные секторы 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 механизмами защиты от обнаружения, которые 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 таких вирусов 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 (например, низкоуровневый типа языка ассемблера или высокоуровневый типа языка Go) и по инфицируемым ими операционным системам.

Компьютерные черви

Как и вирусы, программы типа *«компьютерный червь»* способны создавать свои копии, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего во вложениях сообщений электронной почты или через интернет) и рассылает свои функциональные копии на другие компьютеры. Черви используют действия пользователя, либо распространяются автоматически.

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

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

В компании «Доктор Веб» червей классифицируют 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 системы мгновенного обмена сообщениями (ICQ, IM, IRC и т. д.).

Троянские программы

Вредоносные программы этого типа не способны к саморепликации. Троянские программы выдают себя за одну из популярных 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 выполняться другими типами угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- *Бэкдоры* — это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы.
- *Руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, каталоги, 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 ядра системы, 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 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 злоумышленниками 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 относиться к любому типу компьютерных угроз (возможно, даже неизвестному для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать

в карантин, а также отправлять на анализ специалистам антивирусной лаборатории «Доктор Веб».

10.2. Приложение Б. Устранение компьютерных угроз

В этом разделе

- Методы обнаружения угроз
  - Сигнатурный анализ
  - Origins Tracing™
  - Эмуляция исполнения
  - Эвристический анализ
  - Облачные технологии обнаружения угроз
- Действия с угрозами

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

Методы обнаружения угроз

Сигнатурный анализ

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

Origins Tracing™

Это уникальная технология Dr.Web, которая позволяет определять новые и модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы инфицирования 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 о характерных признаках как вредоносного, так и безопасного исполняемого кода, статистическая значимость которых подтверждена опытным путем. Каждый признак кода имеет определенный *вес* (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует технологию FLY-CODE™ — универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке запакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, запакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому

объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

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 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 действие для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий. В скобках указан параметр, обозначающий соответствующее действие и используемый в объединенном конфигурационном файле и командах утилиты Dr.Web Ctl.

- **Сообщать** (`REPORT`) — уведомить о наличии угрозы, но ничего не делать с инфицированным объектом.
- **Лечить** (`CURE`) — попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое.



Это действие применимо не ко всем видам угроз.

- **В карантин** (`QUARANTINE`) — переместить инфицированный объект (если он допускает эту операцию) в специальный каталог карантина с целью его изоляции.
- **Удалить** (`DELETE`) — 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.

К почтовым сообщениям при их проверке компонентом Dr.Web MailD могут быть применены действия:

- **Пропустить** (`PASS`) — пропустить обнаруженную угрозу, не предпринимая никаких действий.
- **Отбросить** (`DISCARD`) — принять письмо, но не доставлять его получателю.
- **Отклонить** (`REJECT`) — отклонить письмо и не допустить его доставку получателю.
- **Вернуть временную ошибку** (`TEMPFAIL`) — вместо передачи письма вернуть отправителю или получателю письма сообщение об ошибке.
- **Перепаковать** (`REPACK`) — перед доставкой письма получателю модифицировать его, переместив угрозы в карантин, представляющий собой архив, прикрепляемый к письму, а также добавить в письмо уведомление об обнаружении угроз.
- **Добавить заголовок** (`ADD_HEADER`) — при передаче письма получателю добавить к нему указанный заголовок.
- **Изменить заголовок** (`CHANGE_HEADER`) — при передаче письма получателю изменить значение указанного заголовка.

10.3. Приложение B. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

1. Ознакомьтесь с последними версиями описаний и руководств.
2. Прочитайте раздел часто задаваемых вопросов.
3. Посетите форумы компании «Доктор Веб».

Если после этого не удалось решить проблему, заполните веб-форму в соответствующей секции раздела официального сайта, чтобы связаться со службой технической поддержки компании «Доктор Веб».

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы

можете найти на официальном сайте.

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 Desktop Security Suite.

Для сбора информации для службы технической поддержки введите команду:

```
# /opt/drweb.com/bin/support-report.sh <путь к файлу>
```

где *<путь к файлу>* — путь к архиву в формате `.tgz`, в котором будет сохранена отладочная информация о продукте и системном окружении, например, `/tmp/report.tgz`. Уже имеющиеся файлы не перезаписываются. Если путь не указан, то архив будет сохранен в каталоге суперпользователя, запустившего утилиту (например, `/root`), и будет называться следующим образом:

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

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



Утилиту для сбора информации для службы технической поддержки необходимо запускать с правами суперпользователя (*root*). Для получения прав суперпользователя используйте команду смены пользователя `su` или команду 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 «Доктор Веб»;
- содержимое журналов:
  - журналы Dr.Web Desktop Security Suite (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 команд `df`, `ip a` (`ifconfig -a`), `ldconfig -p`, `iptables-save`, `nft export xml`.
- информация о настройках и конфигурации Dr.Web Desktop Security Suite:
  - перечень загруженных вирусных баз (`drweb-ctl baseinfo -l`);
  - перечень файлов из каталогов Dr.Web Desktop Security Suite и их MD5-хеши;
  - версия и MD5-хеш файла антивирусного ядра Dr.Web Virus-Finding Engine;
  - информация о пользователе и разрешениях, извлеченная из ключевого файла, если

Dr.Web Desktop Security Suite работает не в режиме централизованной защиты.

10.4. Приложение Г. Конфигурационный файл Dr.Web Desktop Security Suite

Параметрами конфигурации всех компонентов Dr.Web Desktop Security Suite управляет координирующий демон управления конфигурацией Dr.Web ConfigD. Измененные параметры конфигурации всех компонентов хранятся в едином файле `drweb.ini`, который по умолчанию располагается в каталоге `/etc/opt/drweb.com/`.



В текстовом файле конфигурации хранятся значения только тех параметров, установленные значения которых не совпадают со значением по умолчанию. Если параметр отсутствует в файле конфигурации, то это означает, что он имеет значение по умолчанию.

Чтобы просмотреть перечень всех параметров, доступных для изменения, включая те, которые отсутствуют в конфигурационном файле, так как имеют значения по умолчанию, выполните команду:

```
$ drweb-ctl cfshow
```

Изменить значение любого параметра можно двумя способами:

- Выполнив команду:

```
# drweb-ctl cfset <секция>.<параметр> <новое значение>
```



Для выполнения этой команды утилита управления Dr.Web Ctl должна запускаться от имени суперпользователя (пользователя *root*). Для получения прав суперпользователя используйте команду `su` или `sudo`.

Синтаксис команд `cfshow` и `cfset` утилиты Dr.Web Ctl (модуль `drweb-ctl`) подробнее описан в разделе Dr.Web Ctl.

- Задав этот параметр в конфигурационном файле (отредактировав файл в любом текстовом редакторе) и перезапустив конфигурацию Dr.Web Desktop Security Suite для применения внесенных в файл изменений с помощью команды:

```
# drweb-ctl reload
```

10.4.1. Структура файла

Конфигурационный файл сформирован в соответствии с правилами, приведенными ниже.

- Содержимое файла разбито на последовательность именованных секций. Возможные имена секций жестко заданы и не могут быть произвольными. Имя секции указывается в квадратных скобках и совпадает с именем компонента Dr.Web Desktop Security Suite, использующего параметры из этой секции (за исключением секции

`[Root]`, в которой хранятся параметры демона управления конфигурацией Dr.Web ConfigD).

- Символы `;` или `#` в начале строк конфигурационного файла обозначают комментарий. Такие строки пропускаются компонентами Dr.Web Desktop Security Suite при чтении параметров из конфигурационного файла.
- В одной строке файла содержится только один параметр:

  ```
  <имя параметра> = <значение>
  ```

- Возможные имена параметров жестко заданы и не могут быть произвольными.
- Все имена секций и параметров регистронезависимы. Значения параметров, за исключением имен каталогов и файлов в путях (для Unix-подобных ОС), также регистронезависимы.
- Значения параметров в конфигурационном файле должны быть заключены в кавычки в том случае, если они содержат пробелы.
- Некоторые параметры могут иметь несколько значений, в этом случае значения параметра разделяются запятой или значение параметра задается несколько раз в разных строках конфигурационного файла. При перечислении значений параметра через запятую пробелы между значением и запятой, если встречаются, игнорируются. Если пробел является частью значения параметра, все значение заключается в кавычки.

  Параметру можно присвоить несколько значений:

  - перечислив их через запятую:

    ```
    Parameter = "Value1", "Value2","Value 3"
    ```

  - в виде последовательности строк:

    ```
    Parameter = Value2
    Parameter = Value1
    Parameter = "Value 3"
    ```

  Порядок значений параметра также несущественен.



Пути к файлам всегда заключаются в кавычки, если они перечисляются через запятую, например:

```
ExcludedPaths = "/etc/file1", "/etc/file2"
```

Описание секций конфигурационного файла приведено в описании использующих его компонентов Dr.Web Desktop Security Suite.

10.4.2. Типы параметров

Параметры конфигурации могут принадлежать к следующим типам:

1. *Адрес* — адрес сетевого соединения в виде пары *<IPv4-адрес>:<порт>* или *<IPv6-адрес>:<порт>*. Значение IPv6-адреса указывается в квадратных скобках. В некоторых случаях порт может быть опущен (в каждом случае это указывается в описании параметра).

2. *Логический* — параметр-флаг, принимающий значения `On`, `Yes`, `True` (параметр включен) и `Off`, `No`, `False` (параметр выключен).
3. *Целое число* — неотрицательное целое число.
4. *Дробное число* — в качестве значения параметра может быть указано неотрицательное число, содержащее дробную часть.
5. *Интервал времени* — в качестве значения параметра указывается длина временного интервала, состоящего из целого неотрицательного числа и буквы-суффикса, указывающего заданную единицу измерения. Могут быть использованы суффиксы, задающие единицы измерения:
   - `w` — недели (`1w` = `7d`);
   - `d` — сутки (`1d` = `24h`);
   - `h` — часы (`1h` = `60m`);
   - `m` — минуты (`1m` = `60s`);
   - `s` или без суффикса — секунды.

   Для временного интервала, заданного в секундах, можно указать миллисекунды после точки (не более трех знаков, например, `0.5s` — 500 миллисекунд). В записи одного временного интервала можно использовать совокупность интервалов, измеренных в различных единицах, в этом случае он будет образовываться их суммой (в реальности в параметрах конфигурации всегда сохраняется количество миллисекунд, образующих указанный временной интервал).

   В общем виде любой интервал времени может быть представлен выражением N_1wN_2dN_3hN_4mN_5[.N_6]s, где N_1, ..., N_6 — число соответствующих единиц времени, включенных в данный интервал. Например, год (как 365 суток) можно представить следующим образом (все записи эквивалентны): `365d`, `52w1d`, `52w24h`, `51w7d24h`, `51w7d23h60m`, `8760h`, `525600m`, `31536000s`.

   Примеры задания интервала длиной в 30 минут, 2 секунды, 500 миллисекунд:

   - в файле конфигурации:

   ```
   UpdateInterval = 30m2.5s
   ```

   - с помощью команды `drweb-ctl cfset`:

   ```
   # drweb-ctl cfset Update.UpdateInterval 1802.5s
   ```

   - задание через параметр командной строки (например, для сканирующего ядра):

   ```
   # /opt/drweb.com/bin/drweb-se <сокет> --WatchdogInterval 1802.5
   ```

6. *Размер* — в качестве значения параметра указывается размер какого-либо объекта (файла, буфера, кеша и т. п.), состоящий из целого неотрицательного числа и суффикса, указывающего заданную единицу измерения. Могут быть использованы суффиксы, задающие единицы размера:
   - `GB` — гигабайты (`1GB` = `1024MB`);
   - `MB` — мегабайты (`1MB` = `1024KB`);

- `KB` — килобайты (`1KB` = `1024B`);
- `B` — байты.

Если суффикс опущен, считается, что размер задан в байтах. В записи одного размера можно использовать совокупность размеров, измеренных в различных единицах, в этом случае он будет образовываться их суммой (фактически, в параметрах конфигурации размер всегда сохраняется в байтах).

7. *Путь к каталогу (файлу)* — в качестве значения параметра выступает строка, представляющая собой допустимый путь к каталогу (файлу).



Путь к файлу должен заканчиваться именем файла.



В Unix-подобных операционных системах имена каталогов и файлов регистрозависимы. Если это не оговорено непосредственно в описании параметра, в качестве пути нельзя использовать маски, содержащие специальные символы (`?`, `*`).

8. *Уровень подробности* — параметр задает уровень подробности записи в журнал для компонента Dr.Web Desktop Security Suite. Возможные значения:
   - `Debug` — самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация.
   - `Info` — выводятся все сообщения.
   - `Notice` — выводятся сообщения об ошибках, предупреждения, уведомления.
   - `Warning` — выводятся сообщения об ошибках и предупреждения.
   - `Error` — выводятся только сообщения об ошибках.
9. *Тип журнала* — параметр определяет способ ведения журнала компонентом Dr.Web Desktop Security Suite. Возможные значения:
   - `Stderr[:ShowTimestamp]` — сообщения будут выводиться в стандартный поток ошибок *stderr*. Данное значение может быть использовано *только* в настройках демона управления конфигурацией. При этом, если он работает в фоновом режиме («*daemonized*»), т. е. запущен с указанием параметра `-d`, это значение *не может* быть использовано, поскольку компоненты, работающие в фоновом режиме, не имеют доступа к потокам ввода/вывода терминала). Дополнительный параметр `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени.
   - `Auto` — сообщения для сохранения в журнал передаются демону управления конфигурацией Dr.Web ConfigD, который сохраняет их в единое место в соответствии с собственными настройками (параметр `Log` в секции `[Root]`). Данное значение определено для всех компонентов, *кроме демона управления конфигурацией*, и используется как значение по умолчанию.
   - `Syslog[:<facility>]` — сообщения будут передаваться компонентом системной службе журналирования `syslog`.

- Дополнительная метка <*facility*> используется для указания типа журнала, в котором `syslog` будет сохранять сообщения. Возможные значения:
  - `Daemon` — сообщения демонов,
  - `User` — сообщения пользовательских процессов,
  - `Mail` — сообщения почтовых программ,
  - `Local0` — сообщения локальных процессов 0,
  - ...
  - `Local7` — сообщения локальных процессов 7.
- <*путь к файлу*> — сообщения будут сохраняться компонентом непосредственно в указанный файл журнала.

Примеры задания параметра:

- в файле конфигурации:

```
Log = Stderr:ShowTimestamp
```

- с помощью команды `drweb-ctl cfset`:

```
# drweb-ctl cfset Root.Log /tmp/log
```

- задание через параметр командной строки (например, для сканирующего ядра):

```
# /opt/drweb.com/bin/drweb-se <сокет> --Log Syslog:DAEMON
```

10. *Действие* — действие компонента Dr.Web Desktop Security Suite при обнаружении угроз определенного типа или при возникновении какого-либо другого события. Возможные значения:
    - **Сообщать** (`REPORT`) — только сформировать уведомление об угрозе, не предпринимая никаких других действий;
    - **Лечить** (`CURE`) — попытаться выполнить лечение (удалить из тела файла только вредоносное содержимое);
    - **В карантин** (`QUARANTINE`) — переместить инфицированный файл в карантин;
    - **Удалить** (`DELETE`) — удалить инфицированный файл.



Некоторые из действий могут быть неприменимы в некоторых случаях (например, для события «Ошибка сканирования» неприменимо действие `CURE`). Перечень разрешенных действий всегда указывается в описании каждого параметра, имеющего тип *действие*.

Прочие типы параметров и их возможные значения указаны непосредственно в описании параметров конфигурации.

10.5. Приложение Д. Генерация сертификатов SSL

Для компонентов Dr.Web Desktop Security Suite, использующих для обмена данными защищенный канал передачи данных SSL/TLS и основанные на нем прикладные протоколы, такие как HTTPS, LDAPS, SMTPS и т. п., необходимо обеспечить наличие закрытых ключей SSL и соответствующих им сертификатов. Для некоторых компонентов ключи и сертификаты генерируются автоматически, а для других они должны быть предоставлены пользователем Dr.Web Desktop Security Suite. Все компоненты используют сертификаты, представленные в формате PEM.

Для генерации закрытых ключей и сертификатов, используемых для соединений через SSL/TLS, в том числе для удостоверяющих сертификатов центра сертификации (ЦС) и для подписанных сертификатов, можно использовать утилиту командной строки `openssl` (входит в состав криптографического пакета OpenSSL).

Рассмотрим последовательность действий, необходимых для создания закрытого ключа и соответствующего ему сертификата SSL, а также сертификата SSL, подписанного удостоверяющим сертификатом ЦС.

Чтобы сгенерировать закрытый ключ SSL и сертификат

1. Для генерации закрытого ключа (алгоритм RSA, длина ключа — 2048 бит) выполните команду:

   ```
   $ openssl genrsa -out keyfile.key 2048
   ```

   Если требуется защитить ключ паролем, дополнительно используйте опцию `-des3`. Сгенерированный ключ находится в файле `keyfile.key` в текущем каталоге.

   Для просмотра сгенерированного ключа выполните команду:

   ```
   $ openssl rsa -noout -text -in keyfile.key
   ```

2. Для генерации сертификата на указанный срок на основании имеющегося закрытого ключа (в данном примере — на 365 суток) выполните команду:

   ```
   $ openssl req -new -x509 -days 365 -key keyfile.key -out certificate.crt
   ```

   Эта команда запросит данные, идентифицирующие сертифицируемый объект (такие как имя, организация и т. п.). Сгенерированный сертификат будет помещен в файл `certificate.crt`.

   Для проверки содержимого сгенерированного сертификата выполните команду:

   ```
   $ openssl x509 -noout -text -in certificate.crt
   ```

Чтобы зарегистрировать сертификат в качестве доверенного сертификата ЦС

1. Переместите или скопируйте файл сертификата в системный каталог доверенных сертификатов (в Debian или Ubuntu — `/etc/ssl/certs`).

2. Создайте в каталоге доверенных сертификатов символическую ссылку на сертификат, именем которой будет являться хеш сертификата.
3. Переиндексируйте содержимое системного каталога сертификатов.

Приведенный ниже пример выполняет все эти три действия. Предполагается, что текущим каталогом является системный каталог доверенных сертификатов `/etc/ssl/certs`, а сертификат, который регистрируется в качестве доверенного, располагается в файле `/home/user/ca.crt`:

```
# cp /home/user/ca.crt .
# ln -s ca.crt `openssl x509 -hash -noout -in ca.crt`.0
# c_rehash /etc/ssl/certs
```

Чтобы создать подписанный сертификат

1. Сгенерируйте файл-запрос на подписание сертификата *(Certificate Signing Request — CSR)* на основании имеющегося закрытого ключа. Если ключа нет, сгенерируйте его.

   Запрос на подписание создается командой:

   ```
   $ openssl req -new -key keyfile.key -out request.csr
   ```

   Эта команда, так же как и команда создания сертификата, запрашивает данные, идентифицирующие сертифицируемый объект. Здесь `keyfile.key` — имеющийся файл закрытого ключа. Полученный запрос будет сохранен в файл `request.csr`.

   Для проверки результата создания запроса выполните команду:

   ```
   $ openssl req -noout -text -in request.csr
   ```

2. Для создания подписанного сертификата на основании запроса и имеющегося сертификата ЦС выполните команду:

   ```
   $ openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set_serial 01 -in request.csr
   -out sigcert.crt
   ```

   Для создания подписанного сертификата нужно иметь три файла: файл корневого сертификата `ca.crt` и его закрытый ключ `ca.key` (в качестве `ca.crt` и `ca.key` можно использовать сертификат `certificate.crt` и ключ `keyfile.key`, тогда полученный сертификат будет самоподписанными), а также файл запроса на подписание сертификата `request.csr`. Созданный подписанный сертификат будет сохранен в файл `sigcert.crt`.

   Для проверки результата выполните команду:

   ```
   $ openssl x509 -noout -text -in sigcert.crt
   ```

Повторите процедуру создания ключа и сертификата (или подписанного сертификата, в зависимости от необходимости) столько раз, сколько уникальных сертификатов вам требуется. Например, с точки зрения соображений безопасности, каждый агент распределенной проверки файлов Dr.Web Network Checker, входящий в сканирующий кластер, должен иметь собственную пару ключ/сертификат.

Преобразование подписанного сертификата

Некоторые браузеры или почтовые клиенты могут потребовать преобразования подписанного сертификата, используемого для удостоверения личности, в формат PKCS12.

Указанное преобразование выполняется командой:

```
# openssl pkcs12 -export -in sigcert.crt -out sigcert.pfx -inkey keyfile.key
```

Здесь sigcert.crt — имеющийся файл подписанного сертификата, а keyfile.key — файл соответствующего ему закрытого ключа. Полученный преобразованный сертификат будет сохранен в файл sigcert.pfx.

10.6. Приложение E. Сборка модуля ядра для SpIDer Guard

В этом разделе

- Общие сведения
- Инструкция по сборке модуля ядра
- Возможные ошибки сборки

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 файлы исходного кода загружаемого модуля ядра, чтобы его можно было собрать вручную.

LKM-модуль, используемый SpIDer Guard, предназначен для работы с ядрами Linux версий 2.6.* и новее.

Для архитектур ARM64, E2K и IBM POWER (ppc64el) работа с LKM не поддерживается.

Архив с исходным кодом загружаемого модуля ядра располагается в каталоге основных файлов Dr.Web Desktop Security Suite (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 Desktop Security Suite. Если нет, то 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 исходного кода требуются права суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя при сборке используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Инструкция по сборке модуля ядра

1. Распакуйте архив с исходным кодом 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.

   Для записи в каталог, содержащий архив, необходимы права суперпользователя.

2. Перейдите в созданный каталог с исходным кодом и выполните команду:

   ```
   # make
   ```

   В случае возникновения ошибок на этапе `make`, устраните их и выполните компиляцию повторно.

3. После успешного окончания этапа `make` выполните команды:

   ```
   # make install
   # depmod
   ```

4. После успешной сборки модуля ядра и его регистрации в системе, выполните дополнительно настройку SplDer Guard, указав ему режим работы с модулем ядра, выполнив команду:

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

   Также допускается установка значения `AUTO` вместо значения `LKM`. В этом случае SplDer Guard будет пробовать использовать не только модуль ядра, но и системный механизм fanotify. Для получения дополнительной информации выполните команду:

   ```
   $ man 1 drweb-spider
   ```

Возможные ошибки сборки

На этапе выполнения сборки *make* могут возникать ошибки. В этом случае проверьте следующее:

- Для успешной сборки требуется наличие интерпретатора 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 с файлами исходного кода ядра. В этом случае используйте команду `make` с параметром `KDIR=<путь к исходному коду ядра>`. Обычно он размещается в каталоге `/usr/src/kernels/<версия ядра>`.

Версия ядра, выдаваемая командой `uname -r`, может не совпадать с именем каталога *<версия ядра>*.

10.7. Приложение Ж. Описание известных ошибок

В этом разделе

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

Если у вас возникла ошибка, описание которой отсутствует в данном разделе, обратитесь в техническую поддержку. Будьте готовы сообщить код ошибки и описать обстоятельства ее возникновения.

Рекомендации по идентификации ошибок

- Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.
- Для облегчения идентификации ошибки рекомендуется настроить вывод журнала в отдельный файл и разрешить вывод расширенной отладочной информации. Для этого выполните команды:

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Для возврата настроек ведения журнала по умолчанию выполните команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Коды ошибок

Сообщение об ошибке: *Error on monitor channel (Ошибка связи с монитором)*

Код ошибки: `x1`

Внутреннее обозначение ошибки: `EC_MONITOR_IPC_ERROR`

Описание: Ошибка связи одного или нескольких компонентов с демоном управления конфигурацией Dr.Web ConfigD.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Перезапустите демон управления конфигурацией:

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

2. Убедитесь, что в системе установлен, настроен и корректно функционирует механизм аутентификации PAM. При необходимости 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 Desktop Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```
4. Если демон управления конфигурацией запустить не удается, попробуйте переустановить пакет `drweb-configd`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Operation is already in progress (Операция уже выполняется)*

Код ошибки: `x2`

Внутреннее обозначение ошибки: `EC_ALREADY_IN_PROGRESS`

Описание: Запрошенная операция уже выполняется.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Подождите завершения операции и при необходимости повторите требуемое действие позже.

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

Сообщение об ошибке: *Operation is in pending state (Операция ожидает выполнения)*

Код ошибки: `x3`

Внутреннее обозначение ошибки: `EC_IN_PENDING_STATE`

Описание: Запрошенная операция ожидает выполнения (возможно, в текущий момент устанавливается сетевое соединение или происходит загрузка и инициализация какого-либо компонента, требующая продолжительного времени).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно

просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Подождите начала выполнения операции и при необходимости повторите требуемое действие позже.

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

Сообщение об ошибке: *Interrupted by user (Прервано пользователем)*

Код ошибки: `x4`

Внутреннее обозначение ошибки: `EC_INTERRUPTED_BY_USER`

Описание: Действие было прервано пользователем (возможно, оно выполнялось слишком долго).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие позже.

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

Сообщение об ошибке: *Operation canceled (Операция отменена)*

Код ошибки: `x5`

Внутреннее обозначение ошибки: `EC_CANCELED`

Описание: Действие было отменено.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие.

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

Сообщение об ошибке: *IPC connection terminated (Соединение IPC разорвано)*

Код ошибки: `x6`

Внутреннее обозначение ошибки: `EC_LINK_DISCONNECTED`

Описание: IPC-соединение с одним из компонентов Dr.Web Desktop Security Suite разорвано (возможно, компонент завершил свою работу из-за простоя или по команде пользователя).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Если операция не была завершена, повторите ее позже. В противном случае разрыв соединения не является ошибкой.

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

Сообщение об ошибке: *Invalid IPC message size (Недопустимый размер сообщения IPC)*

Код ошибки: `x7`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_SIZE`

Описание: В процессе обмена данными между компонентами получено сообщение недопустимого размера.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Desktop Security Suite:

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

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

Сообщение об ошибке: *Invalid IPC message format (Недопустимый формат сообщения IPC)*

Код ошибки: `x8`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_FORMAT`

Описание: В процессе обмена данными между компонентами получено сообщение недопустимого формата.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Desktop Security Suite:

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

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

Сообщение об ошибке: *Not ready (Не готов)*

Код ошибки: `x9`

Внутреннее обозначение ошибки: `EC_NOT_READY`

Описание: Требуемое действие не может быть выполнено, потому что запрошенный компонент или устройство еще не инициализированы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие позже.

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

Сообщение об ошибке: *Component is not installed (Компонент не установлен)*

Код ошибки: `x10`

Внутреннее обозначение ошибки: `EC_NOT_INSTALLED`

Описание: Компонент, необходимый для выполнения требуемой функции, не установлен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Установите или переустановите требуемый компонент. Если неизвестно, какой именно компонент необходим, попробуйте это выяснить, ознакомившись с содержимым журнала.
2. Если установка или переустановка требуемого компонента не помогла, попробуйте переустановить Dr.Web Desktop Security Suite.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Unexpected IPC message (Неожиданное сообщение IPC)*

Код ошибки: `x11`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_MESSAGE`

Описание: В процессе обмена данными между компонентами получено недопустимое сообщение.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Desktop Security Suite, выполнив команду:

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

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

Сообщение об ошибке: *IPC protocol violation (Нарушение протокола IPC)*

Код ошибки: `x12`

Внутреннее обозначение ошибки: `EC_PROTOCOL_VIOLATION`

Описание: В процессе обмена данными между компонентами произошло нарушение протокола.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Desktop Security Suite, выполнив команду:

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

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

Сообщение об ошибке: *Subsystem state is unknown (Неизвестное состояние подсистемы)*

Код ошибки: `x13`

Внутреннее обозначение ошибки: `EC_UNKNOWN_STATE`

Описание: Подсистема Dr.Web Desktop Security Suite, необходимая для выполнения операции, находится в неизвестном состоянии.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web Desktop Security Suite, выполнив команду:

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

   после чего повторите операцию.

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

Сообщение об ошибке: *Path must be absolute (Путь должен быть абсолютным)*

Код ошибки: x20

Внутреннее обозначение ошибки: EC_NOT_ABSOLUTE_PATH

Описание: Указан относительный путь к файлу или каталогу вместо абсолютного.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Замените относительный путь к файлу или каталогу на абсолютный и повторите операцию.

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

Сообщение об ошибке: *Not enough memory (Недостаточно памяти для завершения операции)*

Код ошибки: x21

Внутреннее обозначение ошибки: EC_NO_MEMORY

Описание: Недостаточно памяти для выполнения операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Попробуйте увеличить объем памяти, доступной процессам Dr.Web Desktop Security Suite (например, изменив лимиты при помощи команды `ulimit`), перезапустить Dr.Web Desktop Security Suite и повторить операцию.

В некоторых случаях системный сервис `systemd` может игнорировать заданные изменения лимита. В этом случае отредактируйте (или создайте, при его отсутствии) файл `/etc/systemd/system/drweb-configd.service.d/limits.conf`, указав в нем измененное значение лимита, например:

```
[Service]
LimitDATA=32767
```

С перечнем доступных лимитов `systemd` можно ознакомиться, выполнив команду `man systemd.exec`.

Для перезапуска Dr.Web Desktop Security Suite выполните команду:

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

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

Сообщение об ошибке: *IO error (Ошибка ввода-вывода)*

Код ошибки: x22

Внутреннее обозначение ошибки: EC_IO_ERROR

Описание: Произошла ошибка ввода/вывода (например, дисковое устройство еще не инициализировано или раздел файловой системы более не доступен).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обеспечьте доступность требуемого устройства ввода/вывода или раздела файловой системы и повторите операцию.

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

Сообщение об ошибке: *No such file or directory (Нет такого файла или каталога)*

Код ошибки: `x23`

Внутреннее обозначение ошибки: `EC_NO_SUCH_ENTRY`

Описание: Попытка обращения к несуществующему файлу или каталогу.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного пути. При необходимости исправьте путь и повторите операцию.

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

Сообщение об ошибке: *Permission denied (Доступ запрещен)*

Код ошибки: `x24`

Внутреннее обозначение ошибки: `EC_PERMISSION_DENIED`

Описание: Недостаточно прав для доступа к указанному файлу или каталогу.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного пути и наличие необходимых прав у компонента. Если доступ к объекту запрещен, измените права доступа к нему или повысьте права компонента и повторите операцию.

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

Сообщение об ошибке: *Not a directory (Не каталог)*

Код ошибки: x25

Внутреннее обозначение ошибки: EC_NOT_A_DIRECTORY

Описание: Указанный объект файловой системы не является каталогом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность пути к объекту. Исправьте путь и повторите операцию.

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

Сообщение об ошибке: *Data file corrupted (Файл данных поврежден)*

Код ошибки: x26

Внутреннее обозначение ошибки: EC_DATA_CORRUPTED

Описание: Запрашиваемые данные повреждены.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web Desktop Security Suite:

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

   после чего повторите операцию.

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

Сообщение об ошибке: *File already exists (Файл уже существует)*

Код ошибки: x27

Внутреннее обозначение ошибки: EC_FILE_EXISTS

Описание: Файл с указанным именем уже существует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность написания имени файла. При необходимости исправьте его и повторите операцию.

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

Сообщение об ошибке: *Read-only file system (Файловая система только для чтения)*

Код ошибки: `x28`

Внутреннее обозначение ошибки: `EC_READ_ONLY_FS`

Описание: Файловая система доступна только для чтения.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность пути к объекту. Исправьте путь так, чтобы он указывал на раздел файловой системы, доступный для записи, и повторите операцию.

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

Сообщение об ошибке: *Network error (Ошибка сети)*

Код ошибки: `x29`

Внутреннее обозначение ошибки: `EC_NETWORK_ERROR`

Описание: Ошибка сети (возможно, внезапно перестал отвечать удаленный узел или не удается установить соединение).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

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

Сообщение об ошибке: *Not a drive (Не дисковое устройство)*

Код ошибки: `x30`

Внутреннее обозначение ошибки: `EC_NOT_A_DRIVE`

Описание: Производится попытка обращения к устройству ввода/вывода, которое не является дисковым устройством.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

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 и сообщите код ошибки.

Сообщение об ошибке: *Unexpected EOF (Неожиданный конец файла)*

Код ошибки: `x31`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_EOF`

Описание: При чтении данных неожиданно был достигнут конец файла.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

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 и сообщите код ошибки.

Сообщение об ошибке: *File was changed (Файл был изменен)*

Код ошибки: `x32`

Внутреннее обозначение ошибки: `EC_FILE_WAS_CHANGED`

Описание: Проверяемый файл был изменен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите операцию сканирования.

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

Сообщение об ошибке: *Not a regular file (Объект не является файлом)*

Код ошибки: `x33`

Внутреннее обозначение ошибки: `EC_NOT_A_REGULAR_FILE`

Описание: Запрашиваемый объект файловой системы не является регулярным файлом (он может быть каталогом, сокетом или другим объектом).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с

содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

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 и сообщите код ошибки.

Сообщение об ошибке: *Name already in use (Имя уже используется)*

Код ошибки: `x34`

Внутреннее обозначение ошибки: `EC_NAME_ALREADY_IN_USE`

Описание: Объект с указанным именем уже существует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

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

Сообщение об ошибке: *Host is offline (Хост отключен)*

Код ошибки: `x35`

Внутреннее обозначение ошибки: `EC_HOST_OFFLINE`

Описание: Удаленный узел недоступен по сети.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность требуемого узла сети. При необходимости исправьте адрес узла сети и повторите операцию.

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

Сообщение об ошибке: *Resource limit reached (Достигнут предел использования ресурса)*

Код ошибки: `x36`

Внутреннее обозначение ошибки: `EC_LIMIT_REACHED`

Описание: Достигнут предел использования ресурса.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность требуемого ресурса. При необходимости увеличьте лимит на использование ресурса и повторите операцию.

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

Сообщение об ошибке: *Mounting points are different (Различные точки монтирования)*

Код ошибки: `x37`

Внутреннее обозначение ошибки: `EC_CROSS_DEVICE_LINK`

Описание: Восстановление файла предполагает перемещение между двумя точками монтирования.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Выберите другой путь для восстановления файла и повторите операцию.

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

Сообщение об ошибке: *Unpacking error (Ошибка распаковки)*

Код ошибки: `x38`

Внутреннее обозначение ошибки: `EC_UNPACKING_ERROR`

Описание: Не удалось распаковать архив (возможно, он защищен паролем или поврежден).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

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 и сообщите код ошибки.

Сообщение об ошибке: *Virus base corrupted (Вирусная база повреждена)*

Код ошибки: `x40`

Внутреннее обозначение ошибки: `EC_BASE_CORRUPTED`

Описание: Вирусные базы повреждены.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации). Вы можете воспользоваться утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

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

Сообщение об ошибке: *Non-supported virus database version (Неподдерживаемая версия вирусных баз)*

Код ошибки: `x41`

Внутреннее обозначение ошибки: `EC_OLD_BASE_VERSION`

Описание: Вирусные базы предназначены для старой версии программы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации). Вы можете воспользоваться утилитой 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: выполните команду:

```
$ drweb-ctl update
```

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

Сообщение об ошибке: *Empty virus database (Вирусная база пуста)*

Код ошибки: `x42`

Внутреннее обозначение ошибки: `EC_EMPTY_BASE`

Описание: Вирусная база пуста.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации). Вы можете воспользоваться утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

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

Сообщение об ошибке: *Object cannot be cured (Объект не может быть вылечен)*

Код ошибки: `x43`

Внутреннее обозначение ошибки: `EC_CAN_NOT_BE_CURED`

Описание: Действие **Лечить** было применено к неизлечимому объекту.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Выберите действие, допустимое для данного объекта, и повторите операцию.

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

Сообщение об ошибке: *Non-supported virus database combination (Неподдерживаемая комбинация вирусных баз)*

Код ошибки: `x44`

Внутреннее обозначение ошибки: `EC_INVALID_BASE_SET`

Описание: Несовместимые вирусные базы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации). Вы можете воспользоваться утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

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

Сообщение об ошибке: *Scan limit reached (Достигнут предел проверки)*

Код ошибки: `x45`

Внутреннее обозначение ошибки: `EC_SCAN_LIMIT_REACHED`

Описание: При сканировании объекта превышены заданные ограничения (например, на величину распакованного файла, на глубину уровней вложенности и т. п.).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Измените ограничения для сканирования объектов (в настройках соответствующего компонента) 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 и сообщите код ошибки.

Сообщение об ошибке: *Authentication failed (Неверные учетные данные пользователя)*

Код ошибки: `x47`

Внутреннее обозначение ошибки: `EC_AUTH_FAILED`

Описание: Попытка пройти аутентификацию с неверными учетными данными пользователя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

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

Сообщение об ошибке: *Authorization failed (Пользователь не имеет требуемых прав)*

Код ошибки: `x48`

Внутреннее обозначение ошибки: `EC_NOT_AUTHORIZED`

Описание: Текущий пользователь не имеет прав на выполнение требуемой операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите попытку авторизации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

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

Сообщение об ошибке: *Access token is invalid (Недопустимый токен доступа)*

Код ошибки: `x49`

Внутреннее обозначение ошибки: `EC_INVALID_TOKEN`

Описание: Компонент Dr.Web Desktop Security Suite предъявил некорректный токен авторизации при попытке выполнения операции, требующей повышенные права.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Пройдите аутентификацию, указав правильные учетные данные пользователя, имеющего необходимые полномочия, и повторите операцию.

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

Сообщение об ошибке: *Invalid argument (Недопустимый аргумент)*

Код ошибки: `x60`

Внутреннее обозначение ошибки: `EC_INVALID_ARGUMENT`

Описание: Команда не может быть выполнена, так как указан недопустимый аргумент.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность написания и формат команды.
2. Повторите требуемое действие, указав допустимый аргумент.

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

Сообщение об ошибке: *Invalid operation (Недопустимая операция)*

Код ошибки: `x61`

Внутреннее обозначение ошибки: `EC_INVALID_OPERATION`

Описание: Совершена попытка выполнить недопустимую команду.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие, указав допустимую команду.

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

Сообщение об ошибке: *Superuser privileges required (Требуются полномочия суперпользователя)*

Код ошибки: `x62`

Внутреннее обозначение ошибки: `EC_ROOT_ONLY`

Описание: Для выполнения требуемого действия требуются полномочия суперпользователя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повысьте свои права до суперпользователя и повторите требуемое действие. Для повышения прав можно воспользоваться командой `su` или `sudo`.

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

Сообщение об ошибке: *Not allowed in centralized protection mode (Не разрешено в режиме централизованной защиты)*

Код ошибки: `x63`

Внутреннее обозначение ошибки: `EC_STANDALONE_MODE_ONLY`

Описание: Требуемое действие можно выполнить только при работе Dr.Web Desktop Security Suite в автономном режиме.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Переведите Dr.Web Desktop Security Suite в автономный режим и повторите операцию снова.

Для перевода Dr.Web Desktop Security Suite в автономный режим выполните команду:

```
# drweb-ctl esdisconnect
```

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

Сообщение об ошибке: *Non-supported OS (Неподдерживаемая ОС)*

Код ошибки: `x64`

Внутреннее обозначение ошибки: `EC_NON_SUPPORTED_OS`

Описание: Операционная система, установленная на узле, не поддерживается Dr.Web Desktop Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Установите операционную систему из списка, указанного в системных требованиях.

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

Сообщение об ошибке: *Feature not implemented (Функция не реализована)*

Код ошибки: `x65`

Внутреннее обозначение ошибки: `EC_UNKNOWN_OPTION`

Описание: Запрашиваемые функции компонента отсутствуют в текущей версии.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с

содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Попробуйте сбросить настройки Dr.Web Desktop Security Suite в значения по умолчанию.

Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

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

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

Сообщение об ошибке: *Unknown option (Неизвестный параметр)*

Код ошибки: `x66`

Внутреннее обозначение ошибки: `EC_UNKNOWN_OPTION`

Описание: Файл конфигурации содержит параметры, неизвестные или не поддерживаемые в текущей версии Dr.Web Desktop Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` в любом текстовом редакторе, удалите строку, содержащую недопустимый параметр, сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

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

2. Если это не поможет, попробуйте сбросить настройки Dr.Web Desktop Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

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

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

Сообщение об ошибке: *Unknown section (Неизвестная секция)*

Код ошибки: `x67`

Внутреннее обозначение ошибки: `EC_UNKNOWN_SECTION`

Описание: Файл конфигурации содержит секции, неизвестные или не поддерживаемые в текущей версии Dr.Web Desktop Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

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

2. Если это не поможет, попробуйте сбросить настройки Dr.Web Desktop Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

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

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

Сообщение об ошибке: *Invalid option value (Недопустимое значение параметра)*

Код ошибки: `x68`

Внутреннее обозначение ошибки: `EC_INVALID_OPTION_VALUE`

Описание: Для одного или нескольких параметров в файле конфигурации указано недопустимое значение.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра 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 можно 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 демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

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

3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web Desktop Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

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

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

Сообщение об ошибке: *Invalid state (Недопустимое состояние)*

Код ошибки: `x69`

Внутреннее обозначение ошибки: `EC_INVALID_STATE`

Описание: Недопустимое состояние компонента или Dr.Web Desktop Security Suite в целом для выполнения запрошенной операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие через некоторое время.
2. При повторении ошибки перезапустите Dr.Web Desktop Security Suite, выполнив команду:

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

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

Сообщение об ошибке: *Only one value allowed (Разрешено только одно значение)*

Код ошибки: `x70`

Внутреннее обозначение ошибки: `EC_NOT_LIST_OPTION`

Описание: В файле конфигурации для параметра, который может иметь только одно значение, задано значение в виде списка.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра 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 можно 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 демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

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

3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web Desktop Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

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

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

Сообщение об ошибке: *Record not found (Запись не найдена)*

Код ошибки: `x80`

Внутреннее обозначение ошибки: `EC_RECORD_NOT_FOUND`

Описание: Информация о найденной угрозе отсутствует (возможно, угроза уже была обработана другим компонентом).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

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

Сообщение об ошибке: *Record is in process now (Запись обрабатывается в данный момент)*

Код ошибки: `x81`

Внутреннее обозначение ошибки: `EC_RECORD_BUSY`

Описание: Угроза уже обрабатывается другим компонентом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

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

Сообщение об ошибке: *File has already been quarantined (Файл уже находится в карантине)*

Код ошибки: `x82`

Внутреннее обозначение ошибки: `EC_QUARANTINED_FILE`

Описание: Файл уже находится в карантине. Возможно, угроза уже была обработана другим компонентом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

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

Сообщение об ошибке: *Update zone is not provided by cloud (Зона обновления в облаке недоступна)*

Код ошибки: `x83`

Внутреннее обозначение ошибки: `EC_NO_ZONE_IN_CLOUD`

Описание: Попытка обновления с помощью Dr.Web Cloud завершилась неудачей.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие через некоторое время.

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

Сообщение об ошибке: *Update zone is not provided on disk (Зона обновления на диске недоступна)*

Код ошибки: `x84`

Внутреннее обозначение ошибки: `EC_NO_ZONE_ON_DISK`

Описание: Попытка обновления вирусных баз в режиме оффлайн завершилась неудачей.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Убедитесь, что путь к устройству, с которого производится обновление, указан верно.
2. Убедитесь, что пользователь, от имени которого выполняется обновление, обладает правами на чтение каталога с обновлениями.

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

Сообщение об ошибке: *Cannot backup before update (Не удалось сохранить резервную копию перед обновлением)*

Код ошибки: `x89`

Внутреннее обозначение ошибки: `EC_BACKUP_FAILED`

Описание: Перед началом загрузки обновлений с сервера обновлений не удалось сохранить резервную копию подлежащих обновлению файлов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 воспользуйтесь утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

3. Если ошибка повторяется, проверьте, что пользователь, от имени которого исполняется компонент, 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 повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Invalid DRL file (Недопустимый DRL-файл)*

Код ошибки: `x90`

Внутреннее обозначение ошибки: `EC_BAD_DRL_FILE`

Описание: Нарушена структура одного из файлов со списками серверов обновлений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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). Воспользуйтесь утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду (<**DrlDir*> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значения 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

3. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Invalid LST file (Недопустимый LST-файл)*

Код ошибки: `x91`

Внутреннее обозначение ошибки: `EC_BAD_LST_FILE`

Описание: Нарушена структура файла с перечнем обновляемых вирусных баз.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Обновите вирусные базы повторно через некоторое время: выполните команду:

   ```
   $ drweb-ctl update
   ```

2. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Invalid compressed file (Недопустимый сжатый файл)*

Код ошибки: `x92`

Внутреннее обозначение ошибки: `EC_BAD_LZMA_FILE`

Описание: Нарушена структура загруженного файла с обновлениями.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите вирусные базы повторно через некоторое время: выполните команду:

```
$ drweb-ctl update
```

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

Сообщение об ошибке: *Proxy authentication error (Ошибка аутентификации на прокси-сервере)*

Код ошибки: `x93`

Внутреннее обозначение ошибки: `EC_PROXY_AUTH_ERROR`

Описание: Не удалось подключиться к серверам обновлений через прокси-сервер, указанный в настройках.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность параметров подключения к прокси-серверу (задаются в параметре с именем `Proxy` в секции `[Update]` файла конфигурации).
   - Воспользуйтесь утилитой 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: выполните команду:

```
$ drweb-ctl update
```

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

Сообщение об ошибке: *No update servers available (Нет доступных серверов обновлений)*

Код ошибки: `x94`

Внутреннее обозначение ошибки: `EC_NO_UPDATE_SERVERS`

Описание: Не удалось подключиться ни к одному из серверов обновлений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 (задаются в параметре с именем `Proxy` в секции `[Update]` файла конфигурации).
   - Воспользуйтесь утилитой 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.

   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).

- Воспользуйтесь утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

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

Сообщение об ошибке: *Invalid key file format (Недопустимый формат ключевого файла)*

Код ошибки: `x95`

Внутреннее обозначение ошибки: `EC_BAD_KEY_FORMAT`

Описание: Нарушен формат ключевого файла.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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. Воспользуйтесь утилитой 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. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

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

Сообщение об ошибке: *License is already expired (Срок действия лицензии истек)*

Код ошибки: `x96`

Внутреннее обозначение ошибки: `EC_EXPIRED_KEY`

Описание: Срок действия лицензии истек.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

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

Сообщение об ошибке: *Network operation timed out (Истек тайм-аут сетевой операции)*

Код ошибки: `x97`

Внутреннее обозначение ошибки: `EC_NETWORK_TIMEDOUT`

Описание: Истекло время ожидания сетевого соединения (возможно, внезапно перестал отвечать удаленный узел или не удается установить требуемое соединение).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

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

Сообщение об ошибке: *Invalid checksum (Недопустимая контрольная сумма)*

Код ошибки: `x98`

Внутреннее обозначение ошибки: `EC_BAD_CHECKSUM`

Описание: Неверная контрольная сумма загруженного файла с обновлениями.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите вирусные базы повторно через некоторое время: выполните команду:

```
$ drweb-ctl update
```

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

Сообщение об ошибке: *Invalid trial license (Недопустимый демонстрационный ключевой файл)*

Код ошибки: `x99`

Внутреннее обозначение ошибки: `EC_BAD_TRIAL_KEY`

Описание: Демонстрационный ключевой файл недействителен (например, он был получен для другого компьютера).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

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

Сообщение об ошибке: *Blocked license key (Лицензионный ключевой файл заблокирован)*

Код ошибки: `x100`

Внутреннее обозначение ошибки: `EC_BLOCKED_LICENSE`

Описание: Текущая лицензия заблокирована (возможно, нарушены условия лицензионного соглашения на использование Dr.Web Desktop Security Suite).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

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

Сообщение об ошибке: *Invalid license (Недопустимая лицензия)*

Код ошибки: `x101`

Внутреннее обозначение ошибки: `EC_BAD_LICENSE`

Описание: Используемая лицензия предназначена для другого программного продукта или не содержит необходимых разрешений для работы компонентов Dr.Web Desktop Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

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

Сообщение об ошибке: *Invalid configuration (Недопустимая конфигурация)*

Код ошибки: `x102`

Внутреннее обозначение ошибки: `EC_BAD_CONFIG`

Описание: Компонент Dr.Web Desktop Security Suite не может функционировать из-за неправильных настроек конфигурации.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Если ошибка вызвана компонентом SpIDer Guard, то, вероятнее 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).
   - Воспользуйтесь утилитой 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.

   > ⚠ Работа компонента SpIDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список поддерживаемых (см. раздел Системные требования и совместимость).

3. Если ошибка вызвана компонентом Dr.Web Firewall для Linux, то, вероятнее всего, наблюдается конфликт с другим брандмауэром. Например, известно, что Dr.Web Firewall для Linux конфликтует с брандмауэром FirewallD в ОС Fedora, CentOS, Red Hat Enterprise Linux (при

каждом перезапуске FirewallD портит правила маршрутизации трафика, задаваемые Dr.Web Firewall для Linux).

Для устранения ошибки перезагрузите Dr.Web Desktop Security Suite, выполнив команду:

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

или команду:

```
# drweb-ctl reload
```



Если не запретить работу FirewallD, указанная ошибка Dr.Web Firewall для Linux 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 сбросьте его настройки 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, сбросьте настройки Dr.Web Desktop Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

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

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

Сообщение об ошибке: *Invalid executable file (Недопустимый исполняемый файл)*

Код ошибки: `x104`

Внутреннее обозначение ошибки: `EC_BAD_EXECUTABLE`

Описание: Невозможно запустить компонент. Исполняемый файл поврежден или путь к нему указан неверно.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 Desktop Security Suite (параметр `ExePath` в секции компонента), выполнив команду (замените *<секция компонента>* на название соответствующей секции файла конфигурации):

   ```
   $ drweb-ctl cfshow <секция компонента>.ExePath
   ```

3. Сбросьте 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, переустановите пакет соответствующего компонента.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Core engine is not available (Ядро Virus-Finding Engine недоступно)*

Код ошибки: `x105`

Внутреннее обозначение ошибки: `EC_NO_CORE_ENGINE`

Описание: Файл антивирусного ядра Dr.Web Virus-Finding Engine отсутствует или недоступен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к файлу антивирусного ядра `drweb32.dll` и при необходимости исправьте его (параметр `CoreEnginePath` в секции `[Root]` файла конфигурации).

   - Воспользуйтесь утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

3. Если путь правильный и ошибка повторяется после обновления вирусных баз, переустановите пакет `drweb-bases`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *No virus databases (Вирусные базы отсутствуют)*

Код ошибки: `x106`

Внутреннее обозначение ошибки: `EC_NO_VIRUS_BASES`

Описание: Вирусные базы отсутствуют.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации). Вы можете воспользоваться утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

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

Сообщение об ошибке: *Process terminated by signal (Процесс завершен по сигналу)*

Код ошибки: `x107`

Внутреннее обозначение ошибки: `EC_APP_TERMINATED`

Описание: Компонент завершил работу (возможно, из-за простоя или вследствие команды пользователя).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 Desktop Security Suite в значения по умолчанию.

Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

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

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

Сообщение об ошибке: *Unexpected process termination (Непредвиденное завершение процесса)*

Код ошибки: `x108`

Внутреннее обозначение ошибки: `EC_APP_CRASHED`

Описание: Компонент неожиданно завершил работу по причине сбоя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите выполнявшуюся операцию.
2. Если компонент постоянно аварийно завершает свою работу, сбросьте 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, сбросьте настройки Dr.Web Desktop Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```
4. Если ошибка повторяется после сброса настроек Dr.Web Desktop Security Suite, переустановите пакет компонента.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Incompatible software detected (Обнаружено несовместимое ПО)*

Код ошибки: `x109`

Внутреннее обозначение ошибки: `EC_INCOMPATIBLE`

Описание: Один или несколько компонентов Dr.Web Desktop Security Suite не могут функционировать корректно. В системе обнаружено программное обеспечение, препятствующее их работе.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Если ошибка вызвана компонентом SpIDer Gate, то проблема может быть связана с наличием программного обеспечения, формирующего для системного брандмауэра NetFilter правила, которые препятствуют корректной работе SpIDer Gate — например, Shorewall или SuseFirewall2 (в ОС SUSE Linux). Такие приложения периодически выполняют проверку целостности заданной ими системы правил и перезаписывают их.

   Настройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе SpIDer Gate. Если сделать это не удается, отключите конфликтующее 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 следующие строки:

```
## 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 для параметра `FW_LO_NOTRACK` значение `no`:

```
FW_LO_NOTRACK="no"
```

   4) Перезапустите SuseFirewall2:

```
# rcSuSEfirewall2 restart
```

   > ⚠ Если в настройках SuseFirewall2 параметр `FW_LO_NOTRACK` отсутствует, для устранения конфликта остановите это приложение и запретите его запуск при последующих загрузках ОС.

   После изменения настроек или отключения конфликтующего приложения перезапустите SpIDer Gate.

2. Если ошибка вызвана другим компонентом, то отключите или перенастройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Invalid anti-spam library (Недопустимая антиспам-библиотека)*

Код ошибки: `x110`

Внутреннее обозначение ошибки: `EC_BAD_ANTISPAM_LIB`

Описание: Отсутствует, недоступен или поврежден файл антиспам-библиотеки, необходимой для проверки электронной почты.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к файлу библиотеки и при необходимости исправьте его (параметр `AntispamCorePath` в секции `[Root]` файла конфигурации).
   - Воспользуйтесь утилитой 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: выполните команду:

   ```
   $ drweb-ctl update
   ```

3. Если путь правильный и ошибка повторяется после обновления вирусных баз, переустановите пакет `drweb-maild`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *No web resource databases (Базы категорий веб-ресурсов отсутствуют)*

Код ошибки: `x112`

Внутреннее обозначение ошибки: `EC_NO_DWS_BASES`

Описание: Отсутствуют базы категорий веб-ресурсов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу базы категорий веб-ресурсов и при необходимости исправьте его (параметр `DwsDir` в секции `[Root]` файла конфигурации).

   - Воспользуйтесь утилитой 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 базы категорий веб-ресурсов:

   - выполните команду:

   ```
   $ drweb-ctl update
   ```

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

Сообщение об ошибке: *Kernel module is not available (Недоступен модуль ядра Linux для SplDer Guard)*

Код ошибки: `x113`

Внутреннее обозначение ошибки: `EC_NO_KERNEL_MODULE`

Описание: Модуль ядра Linux, необходимый для работы SplDer Guard, отсутствует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте установленный режим работы компонента и при необходимости исправьте его, указав значение *Auto* (параметр `Mode` в секции `[LinuxSpider]` файла конфигурации).

   - Воспользуйтесь утилитой 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.

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

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

Сообщение об ошибке: *MeshD is not available (Компонент MeshD недоступен)*

Код ошибки: `x114`

Внутреннее обозначение ошибки: `EC_NO_MESHD`

Описание: Отсутствует компонент Dr.Web MeshD (требуется для распределения нагрузки при проверке файлов).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-meshd` и при необходимости исправьте его (параметр `ExePath` в секции `[MeshD]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow MeshD.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset MeshD.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset MeshD.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web MeshD в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-meshd`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *UrlCheck is not available (Компонент UrlCheck недоступен)*

Код ошибки: `x116`

Внутреннее обозначение ошибки: `EC_NO_URL_CHECK`

Описание: Отсутствует компонент Dr.Web URL Checker (требуется для проверки URL на принадлежность к запрещенным или потенциально опасным категориям).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-urlcheck` и при необходимости исправьте его (параметр `ExePath` в секции `[URLCheck]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow URLCheck.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset URLCheck.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset URLCheck.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web URL Checker в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-urlcheck`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *GateD is not available (SplDer Gate недоступен)*

Код ошибки: `x117`

Внутреннее обозначение ошибки: `EC_NO_GATED`

Описание: Отсутствует компонент SplDer Gate (требуется для проверки сетевых соединений).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-gated`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *MailD is not available (Компонент MailD недоступен)*

Код ошибки: `x118`

Внутреннее обозначение ошибки: `EC_NO_MAILD`

Описание: Отсутствует компонент Dr.Web MailD (требуется для проверки электронной почты).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-maild`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *ScanEngine is not available (Scanning Engine недоступен)*

Код ошибки: `x119`

Внутреннее обозначение ошибки: `EC_NO_SCAN_ENGINE`

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

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 Desktop Security Suite 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 Dr.Web Scanning Engine в конфигурации, или если предыдущие шаги не помогли, установите или переустановите пакет `drweb-se`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *FileCheck is not available (File Checker недоступен)*

Код ошибки: `x120`

Внутреннее обозначение ошибки: `EC_NO_FILE_CHECK`

Описание: Компонент Dr.Web File Checker отсутствует или не может быть запущен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 Dr.Web File Checker в конфигурации, или если предыдущие шаги не помогли, установите или переустановите пакет `drweb-filecheck`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *ESAgent is not available (ES Agent недоступен)*

Код ошибки: `x121`

Внутреннее обозначение ошибки: `EC_NO_ESAGENT`

Описание: Отсутствует компонент Dr.Web ES Agent, необходимый для подключения к серверу централизованной защиты.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 Dr.Web ES Agent в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-esagent`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Firewall is not available (Компонент Firewall для Linux недоступен)*

Код ошибки: x122

Внутреннее обозначение ошибки: EC_NO_FIREWALL

Описание: Отсутствует компонент Dr.Web Firewall для Linux, необходимый для проверки сетевых соединений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-firewall`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *NetCheck is not available (Network Checker недоступен)*

Код ошибки: x123

Внутреннее обозначение ошибки: EC_NO_NETCHECK

Описание: Отсутствует компонент Dr.Web Network Checker, необходимый для проверки файлов по сети.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 Dr.Web Network Checker в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-netcheck`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *CloudD is not available (Компонент CloudD недоступен)*

Код ошибки: `x124`

Внутреннее обозначение ошибки: `EC_NO_CLOUDD`

Описание: Отсутствует компонент Dr.Web CloudD, необходимый для обращения к облаку Dr.Web Cloud.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

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 утилитой 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 Dr.Web CloudD в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-cloudd`.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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

Сообщение об ошибке: *Unexpected error (Непредвиденная ошибка)*

Код ошибки: `x125`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_ERROR`

Описание: Возникла непредвиденная ошибка в работе одного или нескольких компонентов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Desktop Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl`). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Desktop Security Suite, выполнив команду:

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

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

Ошибки без кода

Симптомы: После установки модуля ядра SpIDer Guard работа операционной системы аварийно завершается с ошибкой ядра «*Kernel panic*».

Описание: Работа модуля ядра SpIDer Guard невозможна в среде исполнения ядра ОС (например, ОС работает в среде гипервизора Xen).

Устранение ошибки

1. Отмените загрузку модуля ядра SpIDer Guard (модуль ядра имеет имя `drweb`), добавив в загрузчике GNU GRUB строку:

   ```
   drweb.blacklist=yes
   ```

   в строку параметров загрузки ядра ОС.
2. После загрузки ОС удалите модуль `drweb.ko` из каталога дополнительных модулей `/lib/modules/`uname -r`/extra`.
3. Установите для SpIDer 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 SpIDer 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: Такие компоненты, как SpIDer Gate, Dr.Web MailD, не проверяют сообщения; в журнале Dr.Web Desktop Security Suite наблюдаются сообщения `Too many open files`.

Описание: В связи большой загрузкой по проверке данных компонент Dr.Web Network Checker исчерпал лимит на число доступных файловых дескрипторов.

Устранение ошибки

1. Увеличьте лимит на число открытых файловых дескрипторов, доступных приложению, используя команду `ulimit -n` (по умолчанию лимит на число дескрипторов для Dr.Web Desktop Security Suite составляет 16384).

   В некоторых случаях системный сервис `systemd` может игнорировать заданные изменения лимита.

   В этом случае отредактируйте (или создайте, при его отсутствии) файл `/etc/systemd/system/drweb-configd.service.d/limits.conf`, указав в нем измененное значение лимита:

   ```
   [Service]
   LimitNOFILE=16384
   ```

   С перечнем доступных лимитов `systemd` можно ознакомиться, выполнив команду `man systemd.exec`.

2. После изменения лимита перезапустите Dr.Web Desktop Security Suite, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы: Главное окно Dr.Web Desktop Security Suite неактивно, индикатор в области уведомлений рабочего стола отображается с символом критической ошибки, а выпадающее меню индикатора содержит только один неактивный пункт — **Запуск**.

Описание: Dr.Web Desktop Security Suite не может запуститься, поскольку демон управления конфигурацией Dr.Web ConfigD недоступен.

Устранение ошибки

1. Выполните команду:

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

   для перезапуска Dr.Web ConfigD и Dr.Web Desktop Security Suite в целом.

2. Если эта команда вернет ошибку или не даст никакого эффекта, выполните отдельную установку пакета `drweb-configd`.

   Это также может означать, что в системе для аутентификации пользователей не используется PAM. Если это так, то установите и настройте его, поскольку без PAM корректная работа Dr.Web Desktop Security Suite невозможна.

3. Если и после этого ошибка повторится, удалите Dr.Web Desktop Security Suite целиком, после

чего установите его повторно.

Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы

1. Индикатор в области уведомлений рабочего стола не отображается после входа в систему.
2. Попытка выполнить команду запуска графического интерфейса:

   ```
   $ drweb-gui
   ```

   приводит к запуску главного окна Dr.Web Desktop Security Suite.

Описание: Возможно, данная ошибка связана с отсутствием в 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*).

   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 Desktop Security Suite целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web Desktop Security Suite и его компонентов см. в разделах Установка Dr.Web Desktop Security Suite и Удаление Dr.Web Desktop Security Suite.

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 SplDer Gate.
2. Если SplDer Gate требуется оставить выключенным, удалите некорректные правила NetFilter (`iptables`), выполнив команду:

```
# iptables-save | grep -v "comment --comment --comment" | iptables-restore
```



Вызов команд `iptables-save` и `iptables-restore` требует наличия прав суперпользователя. Для получения прав суперпользователя можно воспользоваться командой `su` или `sudo`.

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, можно включить ручной режим перенаправления соединений для SplDer Gate, задавая требуемые правила вручную при помощи утилиты `iptables` (не рекомендуется).
- Дополнительные сведения см. в справке `man`: `drweb-firewall(1)`, `drweb-gated(1)`, `iptables(8)`.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы: Двойной щелчок по значку файла или каталога в графическом файловом менеджере вместо его открытия запускает проверку в Dr.Web Desktop Security Suite.

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

Устранение ошибки

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



Для редактирования системного файла ассоциаций вам потребуются полномочия суперпользователя (обычно пользователя *root*). При необходимости используйте команду `su` или `sudo`.

3. Найдите в файле секцию `[Default Applications]`, а в ней строки ассоциаций вида <*MIME-*

mun>=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, вызываемой командой man: xdg-mime(1), xdg-open(1), xdg-settings(1).

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

10.8. Приложение 3. Список сокращений

В данном руководстве следующие сокращения использованы без расшифровки:

Обозначение	Расшифровка
AD	Microsoft Active Directory
FQDN	Fully Qualified Domain Name
GID	Group ID (системный идентификатор группы пользователей)
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
IMA/EVM	Integrity Measurement Architecture and Extended Verification Module (подсистема ядра Linux, позволяющая осуществлять контроль целостности файловой системы)
IP	Internet Protocol
LKM	Loadable Kernel Module (загружаемый модуль ядра)
MBR	Master Boot Record
PID	Process ID (системный идентификатор процесса)
PAM	Pluggable Authentication Modules
RPM	Red Hat Package Manager (формат пакетов)
SP	Service Pack
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User ID (системный идентификатор пользователя)
URI	Uniform Resource Identifier

Обозначение	Расшифровка
URL	Uniform Resource Locator
VBR	Volume Boot Record
ОС	Операционная система

© «Доктор Веб», 2026