



# Dr.WEB

для Интернет-шлюзов UNIX

## Руководство администратора



© «Доктор Веб», 2018. Все права защищены

Материалы, приведенные в данном документе, являются собственностью «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 «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 «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 для Интернет-шлюзов UNIX**

**Версия 11.0**

**Руководство администратора**

**07.09.2018**

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

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

Веб-сайт: <https://www.drweb.com/>

Телефон: +7 (495) 789-45-87

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

## **«Доктор Веб»**

«Доктор Веб» – российский разработчик средств информационной безопасности.

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

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

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

**Мы благодарны пользователям за поддержку решений семейства Dr.Web!**



## Содержание

<b>Условные обозначения и сокращения</b>	<b>8</b>
<b>Введение</b>	<b>9</b>
<b>О продукте</b>	<b>10</b>
Основные функции	10
Структура программного комплекса	13
Каталоги карантина	18
Полномочия для работы с файлами	19
Режимы работы	20
<b>Системные требования</b>	<b>25</b>
<b>Лицензирование</b>	<b>29</b>
<b>Установка и удаление продукта</b>	<b>30</b>
<b>Установка продукта</b>	<b>31</b>
Установка универсального пакета	32
Установка в режиме командной строки	34
Установка из репозитория	35
<b>Обновление продукта</b>	<b>38</b>
Получение текущих обновлений	38
Переход на новую версию	39
<b>Удаление продукта</b>	<b>42</b>
Удаление универсального пакета	42
Удаление в режиме командной строки	43
Удаление продукта, установленного из репозитория	43
<b>Дополнительно</b>	<b>46</b>
Пакеты и файлы продукта	46
Выборочные установка и удаление компонентов	49
<b>Настройка подсистем безопасности</b>	<b>55</b>
Настройка политик безопасности SELinux	56
Настройка разрешений PARSEC (Astra Linux)	59
<b>Начало работы</b>	<b>61</b>
Регистрация и активация продукта	61
Проверка работоспособности продукта	64
Интеграция с прокси-сервером Squid	66
Защита локального веб-сервера	70



<b>Краткие инструкции</b>	<b>72</b>
<b>Компоненты программного комплекса</b>	<b>76</b>
<b>Dr.Web ConfigD</b>	<b>76</b>
Принципы работы	76
Аргументы командной строки	78
Параметры конфигурации	79
<b>Dr.Web Ctl</b>	<b>83</b>
Формат вызова из командной строки	85
Примеры использования	109
Параметры конфигурации	113
<b>Веб-интерфейс управления Dr.Web</b>	<b>114</b>
Управление компонентами	115
Управление угрозами	116
Управление настройками	118
Управление централизованной защитой	123
Проверка локальных файлов	125
<b>Dr.Web ICAPD</b>	<b>129</b>
Принципы работы	129
Аргументы командной строки	132
Параметры конфигурации	133
Интеграция с прокси-сервером HTTP Squid	148
<b>SpIDer Gate</b>	<b>149</b>
Принципы работы	150
Аргументы командной строки	152
Параметры конфигурации	152
<b>Dr.Web Firewall для Linux</b>	<b>155</b>
Принципы работы	155
Аргументы командной строки	155
Параметры конфигурации	156
<b>Dr.Web ClamD</b>	<b>177</b>
Принципы работы	177
Аргументы командной строки	178
Параметры конфигурации	179
Интеграция с внешними приложениями	184
<b>Dr.Web File Checker</b>	<b>187</b>
Принципы работы	187



Аргументы командной строки	188
Параметры конфигурации	189
<b>Dr.Web Network Checker</b>	<b>192</b>
Принципы работы	192
Аргументы командной строки	194
Параметры конфигурации	195
<b>Dr.Web Scanning Engine</b>	<b>200</b>
Принципы работы	200
Аргументы командной строки	202
Параметры конфигурации	205
<b>Dr.Web Updater</b>	<b>207</b>
Принципы работы	207
Аргументы командной строки	208
Параметры конфигурации	209
<b>Dr.Web ES Agent</b>	<b>215</b>
Принципы работы	215
Аргументы командной строки	217
Параметры конфигурации	217
<b>Dr.Web HTTPD</b>	<b>220</b>
Принципы работы	220
Аргументы командной строки	222
Параметры конфигурации	223
<b>Dr.Web SNMPD</b>	<b>226</b>
Принципы работы	226
Аргументы командной строки	228
Параметры конфигурации	229
Интеграция с системами мониторинга	232
Dr.Web SNMP MIB	242
<b>Dr.Web CloudD</b>	<b>277</b>
Принципы работы	277
Аргументы командной строки	278
Параметры конфигурации	278
<b>Dr.Web LookupD</b>	<b>280</b>
Принципы работы	280
Аргументы командной строки	282
Параметры конфигурации	282





<b>Приложения</b>	<b>289</b>
<b>Приложение А. Виды компьютерных угроз</b>	<b>289</b>
<b>Приложение Б. Устранение компьютерных угроз</b>	<b>294</b>
<b>Приложение В. Техническая поддержка</b>	<b>297</b>
<b>Приложение Г. Конфигурационный файл программного комплекса</b>	<b>298</b>
Структура файла	299
Типы параметров	300
Правила проверки трафика	303
<b>Приложение Д. Генерация сертификатов SSL</b>	<b>324</b>
<b>Приложение Е. Описание известных ошибок</b>	<b>327</b>
<b>Приложение Ж. Список сокращений</b>	<b>380</b>
<b>Предметный указатель</b>	<b>382</b>



## 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.
<i>Антивирусная сеть</i>	Новый термин или акцент на термине в описаниях.
<code>&lt;IP-address&gt;</code>	Поля для замены функциональных названий фактическими значениями.
<b>Сохранить</b>	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
<code>/home/user</code>	Наименования файлов и каталогов, фрагменты программного кода.
<a href="#">Приложение А</a>	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.



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

- \$ – для исполнения команды достаточно обычных прав пользователя.
- # – для исполнения команды требуются права суперпользователя (обычно – *root*). Для повышения прав можно использовать команды **su** и **sudo**.

Перечень сокращений приведен в разделе [Приложение Ж. Список сокращений](#).





## Введение

Благодарим вас за приобретение программного продукта Dr.Web для Интернет-шлюзов UNIX. Он позволит вам обеспечить надежную защиту вашего сервера и пользователей предоставляемых им услуг от распространения компьютерных угроз всех возможных типов, используя наиболее современные технологии обнаружения и обезвреживания угроз.

Данное руководство предназначено для помощи администраторам серверов, работающих под управлением операционных систем семейства **GNU/Linux**, а также других UNIX-подобных ОС, таких как **Solaris** и **FreeBSD**, в установке и использовании продукта Dr.Web для Интернет-шлюзов UNIX версии 11.0.

## Соглашение о путях к файлам продукта

Dr.Web для Интернет-шлюзов UNIX предназначен для функционирования в среде различных типов операционных систем семейства **UNIX**. При этом пути, используемые для размещения компонентов и служебных файлов продукта, зависят от операционной системы. В документе используются следующие условные обозначения:

- *<opt\_dir>* – каталог, используемый для размещения основных файлов, включая исполняемые файлы и библиотеки.
- *<etc\_dir>* – каталог, используемый для размещения конфигурационного и ключевого файлов продукта.
- *<var\_dir>* – каталог, используемый для размещения вспомогательных и временных файлов продукта.

Реальные пути, соответствующие введенным обозначениям в разных операционных системах, приведены в таблице ниже.

Тип ОС	Условное обозначение	Реальный путь
<b>GNU/Linux, Solaris</b>	<i>&lt;opt_dir&gt;</i>	/opt/drweb.com
	<i>&lt;etc_dir&gt;</i>	/etc/opt/drweb.com
	<i>&lt;var_dir&gt;</i>	/var/opt/drweb.com
<b>FreeBSD</b>	<i>&lt;opt_dir&gt;</i>	/usr/local/libexec/drweb.com
	<i>&lt;etc_dir&gt;</i>	/usr/local/etc/drweb.com
	<i>&lt;var_dir&gt;</i>	/var/drweb.com

Для экономии места в примерах условные обозначения будут раскрываться в пути, характерные для ОС **GNU/Linux**. В тех местах документа, где это возможно, будут приводиться примеры реальных путей для всех типов ОС.



## О продукте

Dr.Web для Интернет-шлюзов UNIX создан для защиты Интернет-шлюзов, работающих под управлением ОС семейства UNIX (**GNU/Linux, Solaris и FreeBSD**) от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения через них угроз, разработанных для различных платформ.

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 и мобильных устройств, работающих под управлением распространенных операционных систем, от угроз, предназначенных для различных платформ. В настоящее время, наряду с Dr.Web для Интернет-шлюзов UNIX, в компании «Доктор Веб» разработаны также и другие антивирусные решения как для операционных систем семейства **UNIX (GNU/Linux, Solaris и FreeBSD)**, так и для ОС **IBM OS/2, Novell NetWare, macOS и Windows**. Кроме того, разработаны антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением ОС **Andorid, Symbian, BlackBerry и Windows Mobile**.

Компоненты продукта Dr.Web для Интернет-шлюзов UNIX постоянно обновляются, а вирусные базы, базы категорий веб-ресурсов и базы правил спам-фильтрации сообщений электронной почты регулярно дополняются новыми сигнатурами угроз, что обеспечивает актуальный уровень защищенности серверов, рабочих станций и мобильных устройств пользователей, а также используемых ими программ и данных. 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 (данная функция доступна не во всех продуктах).

## Основные функции

Основные функции продукта Dr.Web для Интернет-шлюзов UNIX:

1. **Поиск и обезвреживание угроз.** Производится поиск как непосредственно вредоносных программ всех возможных типов (различные вирусы, включая вирусы, инфицирующие почтовые файлы и загрузочные записи дисков, троянские программы, почтовые черви и т.п.), так и нежелательных программ (рекламные программы, программы-шутки, программы автоматического дозвона). Подробнее о видах угроз см. [Приложение А. Виды компьютерных угроз](#).

Для обнаружения угроз используются:

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



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

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

При проверке файловой системы по запросу пользователя имеется возможность как полной проверки всех объектов файловой системы, доступных пользователю, так и выборочной проверки только указанных объектов (отдельных каталогов или файлов, соответствующих указанным критериям). 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. В системах, реализующих мандатную модель доступа к файлами с набором различных уровней доступа, сканирование файлов, недоступных на текущем уровне доступа, может производиться в специальном режиме [автономной копии](#).

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

Утилита управления из командной строки [Dr.Web Ctl](#), входящая в состав продукта, позволяет также выполнять проверку на наличие угроз файловых систем удаленных узлов сети, предоставляющих удаленный терминальный доступ через SSH.



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

2. **Анализ данных, передаваемых в сеть Интернет.** Отслеживаются и проверяются как запросы пользователей (т.е. попытки подключиться к веб-серверу и загрузить на него некоторый файл), так и непосредственно данные, направляемые веб-серверами в ответ на запросы пользователей. Для анализа запросов и возвращаемых данных, продукт подключается по протоколу ICAP как внешний фильтр к прокси-серверу, обрабатывающему HTTP-соединения пользователей локальной сети. Кроме того, при помощи компонента SpIDer Gate можно реализовать функции барьера, предотвращающего прием и передачу инфицированных файлов публичным веб-сервером организации (*данная возможность доступна только в ОС GNU/Linux*). Для



ограничения доступа к нежелательным веб-сайтам используются как автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, поставляемая вместе с Dr.Web для Интернет-шлюзов UNIX, так и черные и белые списки, ведущиеся системным администратором вручную. Также производится обращение к сервису Dr.Web Cloud для проверки наличия информации, не отмечен ли веб-ресурс, к которому пытается обратиться пользователь, как вредоносный, другими антивирусными продуктами Dr.Web.



Обратите внимание, что продукт *не предназначен* для проверки трафика, следующего через узел транзитом. Он предназначен только для интеграции с локально установленным прокси-сервером HTTP (таким, как **Squid**) или веб-сервером.

3. **Надежная изоляция инфицированных или подозрительных объектов**, обнаруженных в файловой системе сервера, 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.  
*Угрозы, обнаруженные компонентом [Dr.Web ICAPD](#) в сообщениях протокола HTTP, не перемещаются в карантин на Интернет-шлюзе. Вместо этого блокируется их загрузка и передача получателю, о чем он информируется путем отправки ему специальной HTML-страницы с сообщением о блокировке.*
4. **Автоматическое обновление** антивирусного ядра, содержимого вирусных баз, базы категорий веб-ресурсов для поддержания высокого уровня надежности защиты от вредоносных программ.
5. **Сбор статистики** проверок и вирусных инцидентов; ведение журнала обнаруженных угроз. Отправка уведомлений об обнаруженных угрозах по SNMP внешним системам мониторинга и серверу централизованной защиты, если программный комплекс работает в режиме [централизованной защиты](#).
6. **Обеспечение работы под управлением сервера централизованной защиты** (такого, как Dr.Web Enterprise Server или в рамках сервиса Dr.Web AV-Desk) для применения на сервере [единых политик безопасности](#), принятых в некоторой сети, в состав которой он входит. Это может быть как сеть некоторого предприятия (корпоративная сеть) или частная сеть VPN, так и сеть, организованная провайдером каких-либо услуг, например, доступа к сети Интернет.



## Структура программного комплекса



Продукт Dr.Web для Интернет-шлюзов UNIX представляет собой программный комплекс, состоящий из набора компонентов, каждый из которых выполняет свой набор функций. Перечень компонентов, входящих в Dr.Web для Интернет-шлюзов UNIX, перечислен в таблице ниже.

Компонент	Описание
Dr.Web ConfigD	<p>Демон управления конфигурацией комплекса Dr.Web для Интернет-шлюзов UNIX. Решает следующие задачи:</p> <ul style="list-style-type: none"><li>• Управляет активностью (запуск и остановка) других компонентов программного комплекса в зависимости от настроек. Производит перезапуск компонентов, завершивших работу в результате сбоя. Осуществляет запуск одних компонентов комплекса по требованию других. Информировать компоненты продукта об изменении состава запущенных компонентов.</li><li>• Хранит и предоставляет всем компонентам информацию об имеющихся лицензионных ключах и настройках. Принимает изменённые настройки и ключи от уполномоченных компонентов Dr.Web для Интернет-шлюзов UNIX. Оповещает компоненты при изменении лицензионных ключей и настроек.</li></ul>
	<p>Исполняемый файл компонента: <b>drweb-configd</b></p> <p>Внутреннее наименование, выводимое в журнал: <i>ConfigD</i></p>
Dr.Web Virus-Finding Engine	<p>Антивирусное ядро. Является основным компонентом антивирусной защиты. Реализует <a href="#">алгоритмы поиска</a> и распознавания <a href="#">вирусов и вредоносных программ</a>, а также анализа подозрительного поведения (используя сигнатурный и эвристический анализ).</p> <p>Используется всеми компонентами Dr.Web для Интернет-шлюзов UNIX через Dr.Web Scanning Engine.</p>
	<p>Исполняемый файл компонента: <b>drweb32.dll</b></p> <p>Внутреннее наименование, выводимое в журнал: <i>CoreEngine</i></p>
Dr.Web Scanning Engine	<p>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 по запросам от других компонентов Dr.Web для Интернет-шлюзов UNIX. Организует очередь файлов, ожидающих проверки. Выполняет лечение тех угроз, для которых данное действие применимо. Может работать как под управлением демона Dr.Web ConfigD, так и в автономном режиме.</p>



Компонент	Описание
	<p>Используется всеми компонентами Dr.Web для Интернет-шлюзов UNIX для антивирусной проверки.</p> <hr/> <p>Исполняемый файл компонента: <b>drweb-se</b></p> <p>Внутреннее наименование, выводимое в журнал: <i>ScanEngine</i></p>
Вирусные базы Dr.Web	<p>Автоматически обновляемая база данных сигнатур вирусов и прочих угроз, а также алгоритмов распознавания и нейтрализации вредоносного программного обеспечения.</p> <p>Используется антивирусным ядром Dr.Web Virus-Finding Engine и поставляется совместно с ним.</p>
Базы категорий веб-ресурсов	<p>Автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, и используемая для блокирования доступа к нежелательным сайтам.</p> <p>Используется компонентами, проверяющими сетевую активность пользователей и приложений, такими как SpIDer Gate, Dr.Web ICAPD, Dr.Web MailD.</p>
Dr.Web File Checker	<p>Компонент проверки объектов файловой системы и менеджер карантина. Принимает от других компонентов Dr.Web для Интернет-шлюзов UNIX задания на проверку файлов. 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 и перемещение их в карантин и восстановление из карантина, управляет <a href="#">каталогами карантина</a>. Организует и содержит в актуальном состоянии кэш, хранящий информацию о ранее проверенных файлах для уменьшения частоты повторных проверок файлов.</p> <p>Используется компонентами, проверяющими объекты файловой системы.</p> <hr/> <p>Исполняемый файл компонента: <b>drweb-filecheck</b></p> <p>Внутреннее наименование, выводимое в журнал: <i>FileCheck</i></p>
Dr.Web ICAPD	<p>ICAP-сервер, выполняющий анализ запросов и трафика, проходящего через прокси-серверы HTTP (такие как <b>Squid</b>). Предотвращает передачу инфицированных файлов и доступ к узлам сети, внесенными как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором. При запрете доступа к внешним серверам и при обнаружении угроз в передаваемых данных предписывает прокси-серверу вернуть клиенту специальную страницу ответа, содержащую сообщение о невозможности доступа к запрошенному ресурсу или загрузки инфицированного файла.</p>



Компонент	Описание
	<p>Исполняемый файл компонента: <b>drweb-icapd</b></p> <p>Внутреннее наименование, выводимое в журнал: ICAPD</p>
Dr.Web ES Agent	<p>Агент централизованной защиты. Обеспечивает работу программного комплекса в централизованном и мобильном <u>режимах</u>. Обеспечивает связь с сервером централизованной защиты, получает от него <u>лицензионный</u> ключевой файл, обновления вирусных баз и антивирусного ядра. Передает на сервер информацию о составе и состоянии компонентов программного комплекса Dr.Web для Интернет-шлюзов UNIX и накопленную статистику вирусных инцидентов.</p> <p>Исполняемый файл компонента: <b>drweb-esagent</b></p> <p>Внутреннее наименование, выводимое в журнал: ESAgent</p>
SpIDer Gate	<p>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 системным администратором.</p> <div> Поставляется только в составе дистрибутивов, предназначенных для ОС семейства <b>GNU/Linux</b>.</div> <p>Исполняемый файл компонента: <b>drweb-gated</b></p> <p>Внутреннее наименование, выводимое в журнал: Gated</p>
Dr.Web Firewall для Linux	<p>Менеджер сетевых соединений. Используется SpIDer Gate и обеспечивает прохождение через него соединений, устанавливаемых приложениями, работающими на узле, для проверки передаваемого через них трафика.</p> <div> Поставляется только в составе дистрибутивов, предназначенных для ОС семейства <b>GNU/Linux</b>.</div> <p>Исполняемый файл компонента: <b>drweb-firewall</b></p> <p>Внутреннее наименование, выводимое в журнал: LinuxFirewall</p>
Dr.Web Network Checker	<p>Агент сетевой проверки данных. Используется для передачи на проверку в сканирующее ядро данных, отправленных компонентами программного комплекса через сеть (это такие компоненты, как Dr.Web ClamD, SpIDer Gate, Dr.Web ICAPD).</p>





Компонент	Описание
	<p>Кроме этого, позволяет программному комплексу Dr.Web для Интернет-шлюзов UNIX организовывать распределенную проверку файлов: принимать на проверку файлы с удаленных узлов сети и передавать локальные файлы на проверку на удаленные узлы сети. Для приема и передачи файлов на удаленных узлах также должен функционировать антивирусный продукт Dr.Web для операционных систем семейства UNIX. В режиме распределенной проверки агент позволяет автоматически распределять интенсивность антивирусного сканирования по доступным узлам, снижая нагрузку на узлы с большим объемом проверки (например, выполняющих роль почтовых или файловых серверов и Интернет-шлюзов).</p> <p>Для обеспечения безопасности при передаче файлов по сети использует SSL.</p> <p>Исполняемый файл компонента: <b>drweb-netcheck</b></p> <p>Внутреннее наименование, выводимое в журнал: NetCheck</p>
Dr.Web HTTPD	<p>Веб-сервер управления компонентами Dr.Web для Интернет-шлюзов UNIX. Предоставляет веб-интерфейс управления (должен быть установлен дополнительно), а также служебный интерфейс для работы модуля расширения браузеров Dr.Web Link Checker (может быть установлен дополнительно). Веб-интерфейс может быть открыт в браузере на локальном или удаленном узле сети. Наличие веб-интерфейса управления позволяет продукту не использовать сторонние веб-серверы (такие, например, как <b>Apache HTTP Server</b>) и утилиты удаленного администрирования наподобие <b>Webmin</b>.</p> <p>Для обеспечения безопасности при подключении к веб-интерфейсу управления использует протокол HTTPS.</p> <p>Исполняемый файл компонента: <b>drweb-httpd</b></p> <p>Внутреннее наименование, выводимое в журнал: HTTPD</p>
Dr.Web Ctl	<p>Утилита, обеспечивающая интерфейс управления Dr.Web для Интернет-шлюзов UNIX из командной строки операционной системы.</p> <p>Позволяет осуществлять запуск проверки файлов, просматривать содержимое карантина и управлять им, запускать обновление вирусных баз, подключать программный комплекс к серверу централизованной защиты и отключаться от него, просматривать и изменять значения параметров конфигурации программного комплекса.</p> <p>Исполняемый файл компонента: <b>drweb-ctl</b></p> <p>Внутреннее наименование, выводимое в журнал: Ctl</p>

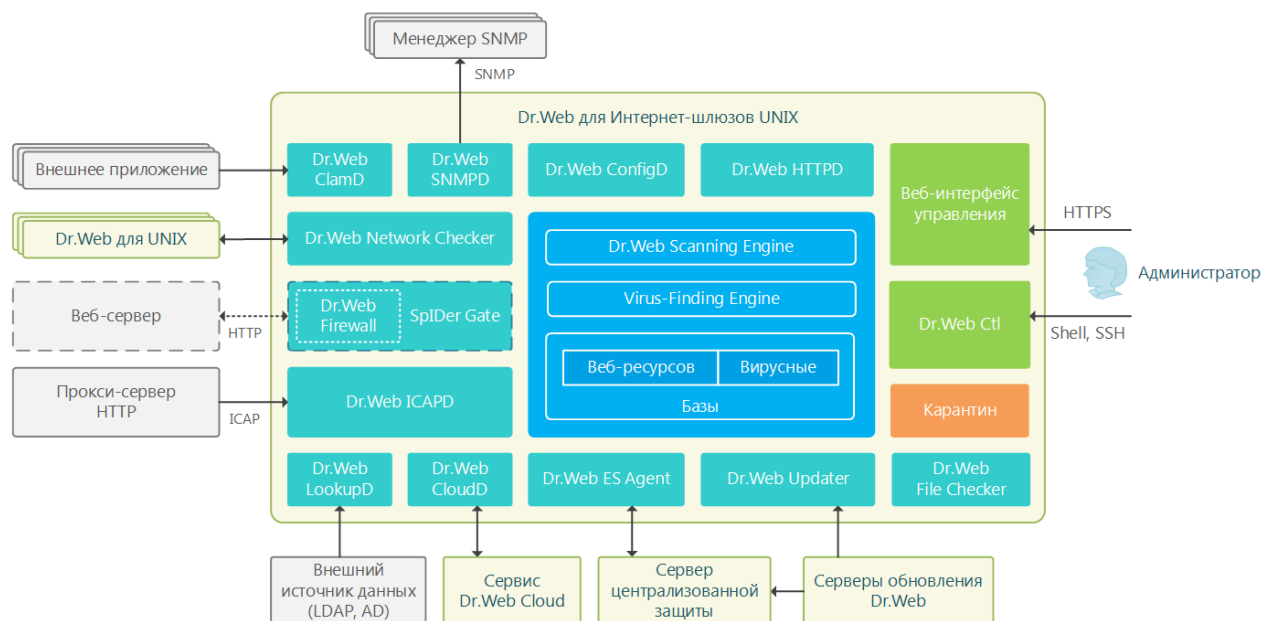




Компонент	Описание
Dr.Web Updater	<p>Компонент обновления. Отвечает за загрузку с серверов обновлений компании «Доктор Веб» обновлений для вирусных баз и баз категорий веб-ресурсов, антивирусного ядра.</p> <p>Обновления могут загружаться как автоматически, по расписанию, так и непосредственно по команде пользователя (через утилиту Dr.Web Ctl или через веб-интерфейс управления).</p> <hr/> <p>Исполняемый файл компонента: <b>drweb-update</b></p> <p>Внутреннее наименование, выводимое в журнал: Update</p>
Dr.Web SNMPD	<p>Представляет собой SNMP-агент. Предназначен для интеграции программного комплекса Dr.Web для Интернет-шлюзов UNIX с внешними системами мониторинга посредством протокола SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов комплекса, а также собирать статистику обнаружения и нейтрализации угроз. Поддерживает протоколы SNMP v2c и v3.</p> <hr/> <p>Исполняемый файл компонента: <b>drweb-snmpd</b></p> <p>Внутреннее наименование, выводимое в журнал: SNMPD</p>
Dr.Web ClamD	<p>Компонент, эмулирующий интерфейс антивирусного демона <b>clamd</b>, являющегося компонентом антивирусного продукта <b>ClamAV®</b>. Позволяет прозрачно использовать для антивирусной проверки продукт Dr.Web для Интернет-шлюзов UNIX любым приложениям, которые могут использовать антивирусный продукт <b>ClamAV®</b>.</p> <hr/> <p>Исполняемый файл компонента: <b>drweb-clamd</b></p> <p>Внутреннее наименование, выводимое в журнал: ClamD</p>
Dr.Web CloudD	<p>Компонент, отправляющий 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.</p> <hr/> <p>Исполняемый файл компонента: <b>drweb-cloudd</b></p> <p>Внутреннее наименование, выводимое в журнал: CloudD</p>
Dr.Web LookupD	<p>Компонент, осуществляющий выборку данных из хранилищ данных (служб каталогов), таких как <b>Active Directory</b>, при помощи протокола LDAP, для использования их в правилах проверки сетевого трафика пользователей.</p> <hr/> <p>Исполняемый файл компонента: <b>drweb-lookupd</b></p> <p>Внутреннее наименование, выводимое в журнал: LookupD</p>



На рисунке ниже показана структура программного комплекса Dr.Web для Интернет-шлюзов UNIX и его взаимодействия с внешними приложениями.



## Каталоги карантина

Карантин продукта Dr.Web для Интернет-шлюзов UNIX версии 11.0 представляет собой систему каталогов, предназначенных для надежной изоляции файлов, содержащих выявленные угрозы, которые в данный момент не могут быть обезврежены по каким-либо причинам. Например, обнаруженная угроза может быть неизлечимой, потому что еще неизвестна Dr.Web для Интернет-шлюзов UNIX (например, она была обнаружена эвристическим анализатором, а в вирусных базах ее сигнатура, а следовательно – и метод лечения, отсутствует), или при попытке ее лечения возникают ошибки. Кроме того, файл может быть перемещен в карантин непосредственно по желанию пользователя, в случае если он выбрал соответствующее действие в списке обнаруженных угроз или указал его как реакцию на угрозы определенного типа.

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

Каталоги карантина размещаются:

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



Каталоги карантина Dr.Web всегда имеют имя `.com.drweb.quarantine` и создаются по мере необходимости, в тот момент, когда к какой-либо угрозе применяется [действие](#) «В карантин», т.е. до тех пор, пока угроз не обнаружено, каталоги карантина не создаются. При этом всегда создается только тот каталог карантина, который требуется для изоляции файла. Для определения, в какой из каталогов требуется изолировать файл, используется имя владельца файла. Если при движении к корню файловой системы / от каталога, содержащего файл, достигается домашний каталог владельца, файл изолируется в каталог карантина, находящийся в нем. В противном случае файл будет изолирован в каталог карантина, созданный в корне тома, содержащего файл (корневой каталог тома необязательно совпадет с корнем файловой системы). Таким образом, любой инфицированный файл, помещаемый в карантин, всегда остается на том томе, на котором он был обнаружен. Это обеспечивает корректную работу карантина при наличии в системе съемных накопителей и других томов, которые могут монтироваться в файловую систему операционной системы периодически и в различные точки.

Пользователь может управлять содержимым карантина из командной строки, используя утилиту [Dr.Web Ctl](#), или через [веб-интерфейс управления](#) (если он установлен). При этом всегда обрабатывается консолидированный карантин, объединяющий в себе все каталоги с изолированными объектами, доступные в данный момент.



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 для Интернет-шлюзов UNIX могут использовать карантин для изоляции угроз. Например, его не использует компонент Dr.Web ClamD, а также компоненты Dr.Web ICAPD и Dr.Web MailD (могут не входить в состав используемого вами продукта).

## Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз Dr.Web для Интернет-шлюзов UNIX (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 архива  (Отображение только элементов, которые содержат ошибку или угрозу)	Без ограничений. Специальных полномочий не требуется.



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

Для запуска утилиты управления из командной строки [Dr.Web Ctl](#) с правами суперпользователя (*root*) вы можете воспользоваться командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.



Обратите внимание, что сканирующее ядро Dr.Web Scanning Engine не может работать с файлами, размер которых больше 4 Гбайт (при попытке проверки таких файлов будет выдаваться ошибка «Файл слишком большой»).

## Режимы работы

Антивирусное решение Dr.Web для Интернет-шлюзов UNIX может работать как в одиночном 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 для Интернет-шлюзов UNIX.

- В *одиночном режиме (standalone mode)* защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационный и



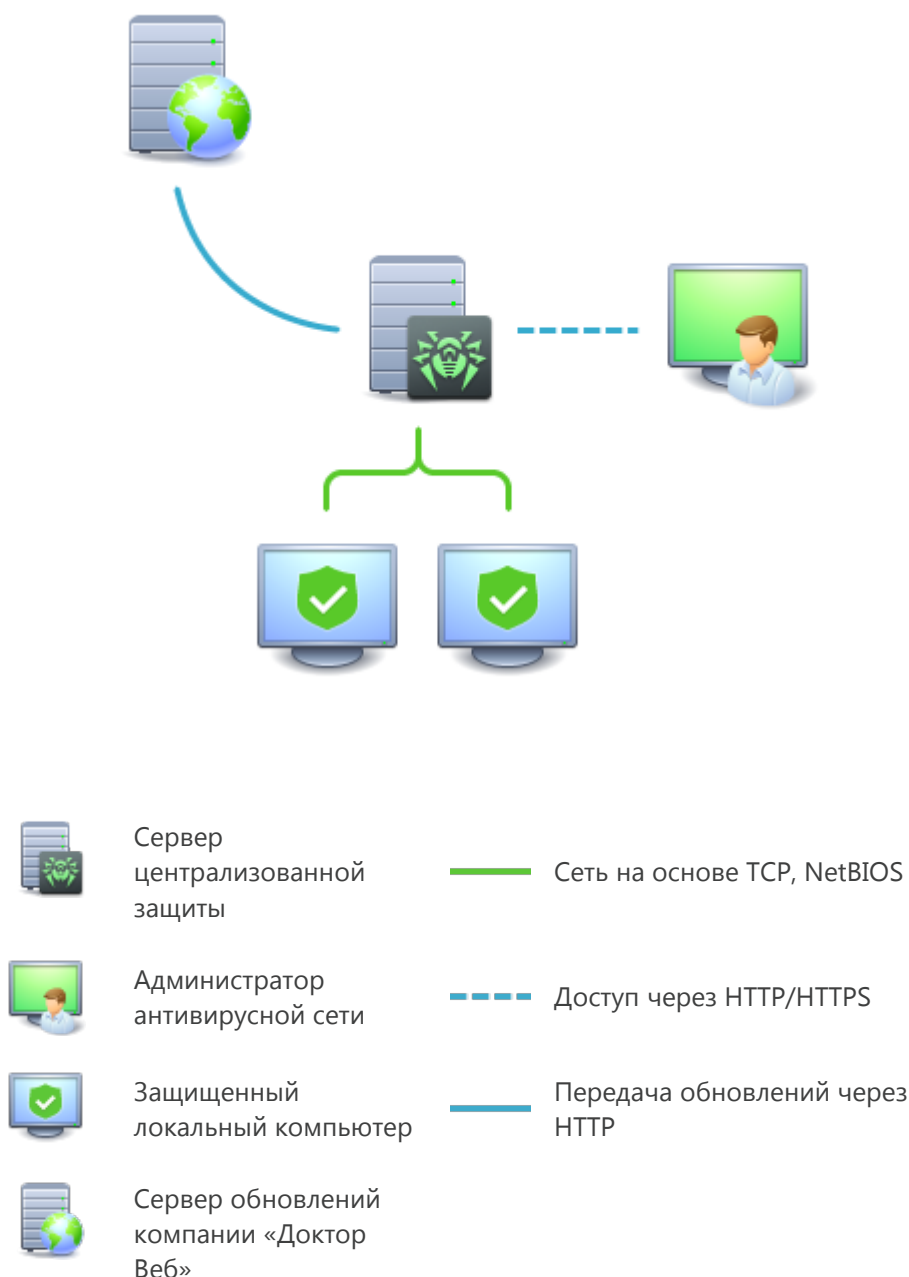
лицензионный ключевой файлы находятся на локальных дисках, а Dr.Web для Интернет-шлюзов UNIX полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании «Доктор Веб».

- В режиме централизованной защиты (*enterprise mode*) защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web для Интернет-шлюзов UNIX могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты, принятой в антивирусной сети. В этом режиме на компьютере используется особый лицензионный ключевой файл, полученный с выбранного сервера централизованной защиты, к которому подключен программный комплекс. Лицензионный или демонстрационный ключевой файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы продукта, включая статистику вирусных инцидентов. Обновление вирусных баз также выполняется с сервера централизованной защиты.
- В мобильном режиме (*mobile mode*) Dr.Web для Интернет-шлюзов UNIX 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. Возможность использования данного режима зависит от разрешений, заданных на сервере централизованной защиты.

## Принципы централизованной защиты

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

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз локальными антивирусными компонентами (в данном случае – Dr.Web для Интернет-шлюзов UNIX), 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, антивирус Dr.Web версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Обратите внимание, что в текущей версии поддержка режима централизованной защиты для Dr.Web для Интернет-шлюзов UNIX реализована *не полностью*: сервер не управляет настройками компонентов программного комплекса.

## Подключение к серверу централизованной защиты

Dr.Web для Интернет-шлюзов UNIX может быть подключен к серверу централизованной защиты антивирусной сети при помощи [команды](#) `esconnect` утилиты управления из командной строки [Dr.Web Ctl](#).



Для верификации сервера централизованной защиты используются публичные ключи шифрования, т.е. каждый сервер снабжен уникальным публичным ключом. По умолчанию агент централизованной защиты [Dr.Web ES Agent](#) не позволит произвести подключение к серверу, если вы не предоставите файл, содержащий публичный ключ, позволяющий проверить подлинность используемого сервера. Такой файл публичного ключа необходимо предварительно получить у администратора антивирусной сети, обслуживаемой сервером, к которому вы хотите подключить программный комплекс Dr.Web для Интернет-шлюзов UNIX.

Если Dr.Web для Интернет-шлюзов UNIX 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 продукта в мобильный режим работы зависит от разрешений, заданных на используемом сервере централизованной защиты



## Отключение от сервера централизованной защиты


Dr.Web для Интернет-шлюзов UNIX может быть отключен от сервера централизованной защиты антивирусной сети при помощи [команды](#) `esdisconnect` утилиты управления из командной строки [Dr.Web Ctl](#).





## Системные требования

Использование Dr.Web для Интернет-шлюзов UNIX возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
Платформа	Поддерживаются процессоры с архитектурой и системой команд <b>Intel/AMD</b> : 32-бит (IA-32, x86); 64-бит (x86_64, x64, amd64).
Место на жестком диске	Не менее 1 Гб свободного дискового пространства на томе, на котором размещаются каталоги Dr.Web для Интернет-шлюзов UNIX.
Операционная система	<p><b>GNU/Linux</b> (на основе ядра с версией не ниже 2.6.37 и использующая библиотеку <b>glibc</b> версии 2.13 и выше), <b>FreeBSD</b> или <b>Solaris</b> для платформ <b>Intel x86/amd64</b>.</p> <div><p>В случае использования 64-битной версии операционной системы, должна быть <i>обязательно</i> включена поддержка исполнения 32-битных приложений (для этого, возможно, потребуются дополнительные библиотеки, см. ниже).</p><hr/><p>Операционная система должна поддерживать механизм аутентификации <b>PAM</b>.</p><hr/><p>Для корректной работы компонента Dr.Web Firewall для Linux ядро ОС должно быть собрано со включением следующих опций:</p><ul style="list-style-type: none"><li>• <code>CONFIG_NETLINK_DIAG</code>, <code>CONFIG_INET_TCP_DIAG</code>;</li><li>• <code>CONFIG_NF_CONNTRACK_IPV4</code>, <code>CONFIG_NF_CONNTRACK_IPV6</code>, <code>CONFIG_NF_CONNTRACK_EVENTS</code>;</li><li>• <code>CONFIG_NETFILTER_NETLINK_QUEUE</code>, <code>CONFIG_NETFILTER_NETLINK_QUEUE_CT</code>, <code>CONFIG_NETFILTER_XT_MARK</code>.</li></ul><p>Конкретный набор требуемых опций из указанного перечня может зависеть от используемого дистрибутива ОС.</p></div> <p>Перечень протестированных дистрибутивов ОС перечислен ниже.</p>
Прочее	<p>Наличие сетевого подключения:</p> <ul style="list-style-type: none"><li>• Подключение к сети Интернет для обновления вирусных баз и компонентов Dr.Web для Интернет-шлюзов UNIX.</li></ul>



Компонент	Требование
	<ul style="list-style-type: none"><li>При работе в режиме <u>централизованной защиты</u> достаточно только подключения к используемому серверу в рамках локальной сети, доступ в Интернет не требуется.</li></ul>

## Перечень протестированных дистрибутивов операционных систем

Работоспособность программного продукта протестирована на следующих дистрибутивах:

- **GNU/Linux:**

Название дистрибутива Linux	Версии	Платформы
Astra Linux Special Edition (Смоленск)	1.5	x86_64
CentOS	6.9, 7.4	x86, x86_64
Debian	7.11, 8.10, 9.3	x86_64
Fedora	27	x86, x86_64
Red Hat Enterprise Linux	7.4	x86_64
SUSE Linux Enterprise Server	11 SP4, 12 SP3	x86_64
Ubuntu	14.04, 16.04	x86_64

Прочие дистрибутивы **GNU/Linux**, соответствующие описанным требованиям, не проходили тестирование на совместимость с Dr.Web для Интернет-шлюзов UNIX, но могут быть совместимы. При возникновении проблем с совместимостью с вашим дистрибутивом, обратитесь в техническую поддержку: <https://support.drweb.com/request/>

- **FreeBSD:**

Версии	Платформы
10.3, 11.1	x86, x86_64

- **Solaris:**

Версии	Платформы
10 u11	x86, x86_64



Для ОС **FreeBSD** и **Solaris** установка продукта возможна только из [универсального пакета](#).

## Дополнительные пакеты

- Для ОС **CentOS, Debian, Fedora, Red Hat Enterprise Linux, Ubuntu** на платформе **x86\_64** требуется пакет поддержки исполнения 32-битных приложений (**libc6-i386** или **glibc.i686**, в зависимости от ОС).



Для удобной работы с Dr.Web для Интернет-шлюзов UNIX 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.

## Ограничения совместимости

- Компонент SpIDer Gate *может конфликтовать* с другими брандмауэрами, установленными в вашей ОС (такими, как **Shorewall** и **SuseFirewall2** в ОС **SUSE Linux Enterprise Server** и **Firewalld** в ОС **Fedora, CentOS, RedHat Enterprise Linux**). Признаком наличия конфликта является сообщение об ошибке SpIDer Gate с кодом x109 или сообщение об ошибке Dr.Web Firewall для Linux с кодом x102. Способы устранения конфликта описаны в разделе «Описание известных ошибок», для ошибок [x109](#) и [x102](#) соответственно.
- В случае если в состав ОС включен **NetFilter** версии младше 1.4.15, в работе компонента SpIDer Gate возможно возникновение следующей проблемы, связанной с внутренней ошибкой в реализации **NetFilter**: при выключении SpIDer Gate нарушается работа сети. Рекомендуется обновить ОС до версии, включающей **NetFilter** версии 1.4.15 или новее. Руководство по устранению указанной проблемы [приведено](#) в разделе «Описание известных ошибок».

## Поддерживаемые прокси-серверы HTTP

Для [интеграции](#) с прокси-сервером HTTP требуется установленный и настроенный прокси-сервер HTTP **Squid** версии не ниже 3.0. **Squid** должен быть собран с поддержкой ICAP (скомпилирован с опцией `--enable-icap-client`).

В режиме [Интернет-барьера](#) никаких требований к веб-серверам и прокси-серверам HTTP не предъявляется.



Режимы Интернет-барьера и прозрачного прокси работают только в ОС **GNU/Linux**.

### Совместимость с подсистемами безопасности

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

В случае необходимости установки Dr.Web для Интернет-шлюзов UNIX в системы с **SELinux** (а также в системы, использующие мандатные модели доступа) необходимо выполнить дополнительные настройки подсистемы безопасности для снятия ограничений в функционировании Dr.Web для Интернет-шлюзов UNIX. Подробнее см. в разделе [Настройка подсистем безопасности](#).



## Лицензирование

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

- Перечень компонентов, которые разрешено использовать данному пользователю.
- Период, в течение которого разрешено использование продукта.
- Другие ограничения (в частности, количество компьютеров, на которых разрешено использовать приобретенную копию продукта).

Имеется также возможность активировать для приобретенной копии продукта *демонстрационный период*. В этом случае, если не нарушены условия активации демонстрационного периода, пользователь получает право на полноценное использование Dr.Web для Интернет-шлюзов UNIX в течение демонстрационного периода.

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

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода, антивирусные функции компонентов Dr.Web для Интернет-шлюзов UNIX блокируются, кроме того, недоступен сервис регулярных обновлений вирусных баз с серверов обновлений компании «Доктор Веб». Однако имеется возможность активировать продукт, подключив его к серверу централизованной защиты [антивирусной сети](#) предприятия или сети, организованной Интернет-провайдером. В этом случае управление антивирусными функциями и обновлениями копии продукта, установленной на компьютере, включенном в состав антивирусной сети, возлагается на сервер централизованной защиты.



Обратите внимание, что в текущей версии поддержка режима централизованной защиты для Dr.Web для Интернет-шлюзов UNIX реализована *не полностью*: сервер не управляет настройками компонентов программного комплекса.



## Установка и удаление продукта

В этом разделе описываются процедуры [установки](#) и [удаления](#) программного комплекса Dr.Web для Интернет-шлюзов UNIX версии 11.0, а также процедура получения [текущих обновлений](#) и процедура [перехода на новую версию](#), если на вашем компьютере уже установлен продукт Dr.Web для Интернет-шлюзов UNIX предыдущей версии.

Кроме этого, в этом разделе описана процедура [выборочной установки и удаления](#) компонентов продукта (например, для устранения ошибок, возникших в процессе эксплуатации Dr.Web для Интернет-шлюзов UNIX или для получения установки с ограниченным набором функций) и [настройка расширенных подсистем безопасности](#) (таких, как **SELinux**), что может потребоваться при установке или в процессе эксплуатации продукта.

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



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

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

Для ОС **FreeBSD** и **Solaris** установка продукта возможна только из [универсального пакета](#).



## Установка продукта

Вы можете установить Dr.Web для Интернет-шлюзов UNIX одним из двух способов:

1. Загрузив с сайта компании «Доктор Веб» установочный файл, содержащий [универсальный пакет](#) для UNIX-систем, снабженный программой установки (так как программа установки разработана для режима командной строки, для ее работы в режиме графического рабочего стола необходимо наличие эмулятора терминала).
2. Выполнив установку продукта в виде набора [нативных пакетов](#) (для этого потребуется подключиться к соответствующему репозиторию пакетов компании «Доктор Веб»).



Для ОС **FreeBSD** и **Solaris** установка продукта возможна только из [универсального пакета](#).

В процессе работы программы установки (как из универсального пакета `.run`, так и из нативных пакетов, при помощи пакетного менеджера), на локальный почтовый адрес `root@localhost` отправляются сообщения электронной почты, содержащие результаты установки продукта.

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

После установки Dr.Web для Интернет-шлюзов UNIX любым из указанных в данном руководстве способов, в начале работы, вам потребуется активировать лицензию и установить полученный ключевой файл. Кроме того, вы можете [подключить](#) программный комплекс к серверу централизованной защиты. Подробнее см. в разделе [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 установленного продукта, как это описано в разделе [Начало работы](#).



## Установка универсального пакета

Программный комплекс Dr.Web для Интернет-шлюзов UNIX распространяется в виде инсталляционного файла с именем `drweb-<версия>-av-igw-<ОС>-<платформа>.run`, где `<ОС>` – тип операционной системы семейства **UNIX**, а `<платформа>` – строка, указывающая тип платформы, для которой предназначен продукт (x86 для 32-битных платформ и amd64 для 64-битных платформ). Например:

```
drweb-11.0.7-av-igw-linux-x86.run
```

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

Чтобы установить компоненты программного комплекса Dr.Web для Интернет-шлюзов UNIX:

1. Если у вас отсутствует инсталляционный файл, содержащий универсальный пакет, загрузите его с официального сайта компании «Доктор Веб»:  
<https://download.drweb.com/>.
2. Сохраните инсталляционный файл на жесткий диск компьютера.
3. Разрешите исполнение файла, например, командой:

```
# chmod +x <имя_файла>.run
```

4. Запустите его на исполнение командой:

```
# ./<имя_файла>.run
```

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

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 **sudo**). Если попытка повышения прав окончится неудачей, установка будет завершена.



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





После этого запустится программа установки, использующая [режим командной строки](#) (для ее работы в режиме графического рабочего стола необходимо наличие эмулятора терминала).

5. Следуйте инструкциям программы установки.
6. Имеется возможность запустить программу установки в полностью автоматическом режиме, выполнив команду

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

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

Обратите внимание, что:

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



Если ваш дистрибутив **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](#) для того, чтобы в дальнейшем антивирусные компоненты работали корректно.

Об условных обозначениях путей `<opt_dir>`, `<etc_dir>` и `<var_dir>` см. [Введение](#).

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



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



## 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 «Do you want to continue?». 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 Dr.Web, который будет выведен на экран. Для перелистывания текста лицензионного соглашения пользуйтесь клавишами ENTER (перелистывание текста на одну строчку вниз) и ПРОБЕЛ (перелистывание текста вниз на экран). Обратите внимание, что перелистывание текста Лицензионного соглашения назад (вверх) не предусмотрено.
3. После прочтения Лицензионного соглашения вам будет предложено принять его условия. Введите *Yes* или *Y*, если вы принимаете условия, и *No* или *N*, если вы не согласны с условиями Лицензионного соглашения. В случае отказа от принятия условий Лицензионного соглашения работа программы установки будет завершена.
4. После принятия условий Лицензионного соглашения автоматически будет запущен процесс установки на компьютер выбранных компонентов Dr.Web. При этом на экран будет выводиться информация о ходе установки, включающая в себя перечень устанавливаемых компонентов.
5. В случае успешного окончания процесса установки, если продукт предусматривает автоматическую настройку перед запуском, будет автоматически запущен интерактивный скрипт настройки продукта. По окончании его работы на экране появится информационное сообщение, содержащее инструкции по способам управления работой продукта.

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, следует устранить проблемы, вызвавшие ошибку установки, и повторить процесс установки заново.

## Интерактивный скрипт настройки

Интерактивный скрипт настройки позволяет установить имеющийся у вас ключевой файл продукта.

1. Если вы желаете выполнить настройку интеграции, после запуска скрипта нужно ответить *y* или *yes* на вопрос «Do you want to continue?». В случае если вы ответите *n* или *no*, работа скрипта будет завершена.
2. Если в данный момент на компьютере (в стандартном для продукта каталоге) не имеется ключевого файла, скрипт предложит указать путь к нему. Если ключевой файл уже имеется, этот шаг будет автоматически пропущен.

Чтобы пропустить этот шаг, введите *0*. В этом случае вы сможете установить ключевой файл вручную позднее. Если на вашем компьютере имеется действующий ключевой



файл, укажите путь к нему и нажмите ENTER. Ключевой файл будет скопирован в стандартный для продукта каталог.

3. По окончании внесения изменений необходимо нажать клавишу ENTER для завершения работы скрипта.

## Установка из репозитория

Нативные пакеты продукта Dr.Web для Интернет-шлюзов UNIX находятся в официальном репозитории Dr.Web <https://repo.drweb.com/>. После добавления репозитория Dr.Web в список репозитория, 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 репозитория вашей операционной системы. Необходимые зависимости будут разрешаться автоматически.



Все нижеприведенные команды для подключения репозитория, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами суперпользователя. Для этого используйте команду смены пользователя **su** или команду выполнения от имени другого пользователя **sudo**.

Пожалуйста, имейте в виду, что для ОС **FreeBSD** и **Solaris** установка продукта возможно только из [универсального пакета](#).

## Debian, Mint, Ubuntu (apt)



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

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

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

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

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

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



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

3. Для установки Dr.Web для Интернет-шлюзов UNIX из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-internet-gateways
```

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

## ALT Linux, PCLinuxOS (apt-rpm)

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

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

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

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

2. Для установки Dr.Web для Интернет-шлюзов UNIX из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-internet-gateways
```

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

## Mageia, OpenMandriva Lx (urpmi)

1. Подключить репозиторий с помощью команды:

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

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

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

3. Для установки Dr.Web для Интернет-шлюзов UNIX из репозитория выполните команду:

```
# urpmi drweb-internet-gateways
```



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

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

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

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



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

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

2. Для установки Dr.Web для Интернет-шлюзов UNIX из репозитория выполните команду:

```
# yum install drweb-internet-gateways
```

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

```
# dnf install drweb-internet-gateways
```

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

## SUSE Linux (zypper)

1. Чтобы подключить репозиторий, запустите следующую команду:

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

2. Для установки Dr.Web для Интернет-шлюзов UNIX из репозитория выполните команды:

```
# zypper refresh
# zypper install drweb-internet-gateways
```

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



## Обновление продукта

Предусмотрено два режима обновления продукта Dr.Web для Интернет-шлюзов UNIX:

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

## Получение текущих обновлений

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

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

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

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

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

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

В случае выпуска новой версии продукта, пакеты, содержащие его компоненты, помещаются в раздел репозитория Dr.Web, соответствующий новой версии продукта. В этом случае для обновления необходимо переключить менеджер пакетов на новый раздел репозитория Dr.Web (см. [Переход на новую версию](#)).



## Переход на новую версию

### Предварительные замечания

Обратите внимание, что переход на новую версию Dr.Web для Интернет-шлюзов UNIX следует выполнять тем же способом, каким был установлена версия Dr.Web для Интернет-шлюзов UNIX, подлежащая обновлению:

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



Чтобы уточнить способ, которым была установлена версия продукта, подлежащая обновлению, проверьте наличие в каталоге исполняемых файлов продукта сценария программы удаления `uninst.sh`. Если этот файл присутствует, текущая версия продукта была установлена из универсального пакета, а в противном случае – из репозитория.

Пожалуйста, имейте в виду, что для ОС **FreeBSD** и **Solaris** установка продукта возможно только из [универсального пакета](#).

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

Если версия продукта, подлежащая обновлению, работает под управлением сервера [централизованной защиты](#), то перед началом обновления рекомендуется сохранить адрес сервера централизованной защиты, к которому подключен продукт. Например, для получения адреса сервера централизованной защиты, к которому подключен Dr.Web для Интернет-шлюзов UNIX с версией новее 6.0.2, вы можете воспользоваться командой:

```
$ drweb-ctl appinfo
```

из присутствующей в выводе команды строки вида

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



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

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

## Обновление установкой универсального пакета

Выполните установку Dr.Web для Интернет-шлюзов UNIX версии 11.0 из [универсального пакета](#). В случае если автоматическое обновление установленного продукта невозможно, то в процессе установки новой версии программа установки предложит вам автоматически удалить имеющиеся компоненты старой версии продукта.



Если в процессе обновления вам необходимо выполнить удаление имеющейся версии продукта и на вашем сервере *одновременно* установлено несколько серверных продуктов Dr.Web (например – для файловых серверов, для почтовых серверов и Интернет-шлюзов), то для сохранения работоспособности серверных продуктов, не подлежащих обновлению (для файловых серверов и почтовых серверов) следует отметить для удаления *только* следующие пакеты:

- `drweb-internet-gateways-doc`
- `drweb-icapd-web`
- `drweb-icapd`

## Обновление из репозитория



Обратите внимание, что вы *не сможете* обновить Dr.Web для Интернет-шлюзов UNIX версии 6.0.2 до версии 11.0 из репозитория, если на вашем сервере установлено *одновременно* несколько серверных продуктов Dr.Web версии 6.0.2 (например – для файловых серверов, для почтовых серверов и Интернет-шлюзов). В этом случае вам следует установить новую версию Dr.Web для Интернет-шлюзов UNIX на отдельную машину.

Для обновления текущей версии Dr.Web для Интернет-шлюзов UNIX, установленной из репозитория компании «Доктор Веб», в зависимости от типа используемых пакетов, вам необходимо выполнить следующие действия:

### • Пакеты RPM (`yum`, `dnf`).

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 11.0).





Имя репозитория, хранящего пакеты версии 11.0, см. в разделе [Установка из репозитория](#). Для уточнения способа смены репозитория обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

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

```
# yum update
```

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

```
# dnf update
```



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

#### • Пакеты DEB (apt-get).

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 11.0).
2. Обновите пакеты продукта, выполнив команды:

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



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

## Перенос ключевого файла

При любом способе обновления продукта уже имеющийся у вас [ключевой файл](#) будет автоматически установлен в надлежащее место для использования новой версией продукта.



В случае возникновения проблем с автоматической установкой лицензионного ключевого файла, вы можете выполнить его [установку вручную](#).



В случае утраты действующего лицензионного ключевого файла обратитесь в службу [технической поддержки](#).

## Повторное подключение к серверу централизованной защиты

Если это возможно, то после обновления (если обновляемый продукт был подключен к серверу централизованной защиты) подключение будет восстановлено автоматически. В случае если подключение не восстановилось автоматически, для подключения обновленной версии Dr.Web для Интернет-шлюзов UNIX к антивирусной сети используйте [команду](#):

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

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

## Удаление продукта

В зависимости от способа установки, вы можете удалить Dr.Web для Интернет-шлюзов UNIX одним из двух способов:

1. [Запустив программу удаления](#) универсального пакета.
2. [Удалив пакеты продукта](#), установленные из репозитория компании «Доктор Веб», используя системный менеджер пакетов.

## Удаление универсального пакета

Удаление продукта Dr.Web для Интернет-шлюзов UNIX, установленного из [универсального пакета](#), можно выполнить при помощи командной строки (в графическом режиме необходимо наличие эмулятора терминала).



Обратите внимание, что программа удаления удалит не только Dr.Web для Интернет-шлюзов UNIX, но и *все другие* продукты Dr.Web, установленные на вашем компьютере.

В случае если на вашем компьютере, кроме Dr.Web для Интернет-шлюзов UNIX, установлены и другие продукты Dr.Web, для удаления только Dr.Web для Интернет-шлюзов UNIX вместо запуска программы автоматического удаления воспользуйтесь процедурой выборочной [установки/удаления компонентов](#).



## Удаление продукта из командной строки

Для запуска программы удаления запустите файл сценария `uninst.sh`, который расположен в каталоге `<opt_dir>/bin` (в ОС **GNU/Linux** – `/opt/drweb.com/bin`). Процедура удаления Dr.Web для Интернет-шлюзов UNIX рассмотрена в разделе [Удаление в режиме командной строки](#).

Имеется возможность запустить программу удаления в полностью автоматическом режиме, запустив сценарий следующим образом:

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

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

## Удаление в 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 «Do you want to continue?». Чтобы отказаться от удаления продукта, введите *No* или *N*. В этом случае работа программы удаления будет завершена.
2. Далее будет запущена процедура автоматического удаления. При этом на экран будут выдаваться записи, фиксируемые в журнал удаления и отражающие ход процесса удаления.
3. По окончании процесса программа удаления завершит свою работу автоматически.

## Удаление продукта, установленного из репозитория



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

### Debian, Mint, Ubuntu (apt)

Для удаления корневого метапакета продукта Dr.Web для Интернет-шлюзов UNIX выполните команду:

```
# apt-get remove drweb-internet-gateways
```



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

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

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

```
# apt-get autoremove
```



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

1. Первый вариант команды удалит только пакет `drweb-internet-gateways`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы все пакеты, название которых начинается на "drweb" (стандартное наименование для пакетов программных продуктов Dr.Web). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта Dr.Web для Интернет-шлюзов UNIX.
3. Третий вариант команды удалит из системы все пакеты, которые были автоматически установлены для удовлетворения зависимостей других пакетов, но более не требуемые (например, ввиду удаления исходного пакета). Обратите внимание, что эта команда удалит из системы все более не требуемые пакеты, а не только пакеты продукта Dr.Web для Интернет-шлюзов UNIX.

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

### ALT Linux, PCLinuxOS (apt-rpm)

Удаление Dr.Web для Интернет-шлюзов UNIX в данном случае выполняется так же, как и в **Debian, Ubuntu** (см. выше).

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

### Mageia, OpenMandriva Lx (urpme)

Для удаления Dr.Web для Интернет-шлюзов UNIX выполните команду:

```
# urpme drweb-internet-gateways
```



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

```
# urpme --auto-orphans drweb-internet-gateways
```



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

1. Первый вариант команды удалит только пакет `drweb-internet-gateways`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы пакет `drweb-internet-gateways`, а также все пакеты, которые были автоматически установлены для удовлетворения зависимостей других пакетов, но более не требуемые (например, ввиду удаления исходного пакета). Обратите внимание, что эта команда удалит из системы все более не требуемые пакеты, а не только пакеты продукта Dr.Web для Интернет-шлюзов UNIX.

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

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

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

```
# yum remove drweb*
```

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

```
# dnf remove drweb*
```



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

Этот вариант команды удалит из системы все пакеты, название которых начинается на "drweb" (стандартное наименование для пакетов программных продуктов Dr.Web). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта Dr.Web для Интернет-шлюзов UNIX.

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



## SUSE Linux (zypper)

Для удаления Dr.Web для Интернет-шлюзов UNIX выполните команду:

```
# zypper remove drweb-internet-gateways
```

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

```
# zypper remove drweb*
```



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

1. Первый вариант команды удалит только пакет `drweb-internet-gateways`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы все пакеты, название которых начинается на "drweb" (стандартное наименование для пакетов программных продуктов Dr.Web). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта Dr.Web для Интернет-шлюзов UNIX.

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

## Дополнительно

### Пакеты и файлы продукта

#### Пакеты

Продукт Dr.Web для Интернет-шлюзов UNIX состоит из следующих пакетов:

Пакет	Содержимое
drweb-bases	Файлы вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine
drweb-boost	Библиотеки <b>Boost</b>
drweb-clamd	Файлы компонента Dr.Web ClamD
drweb-cloudd	Файлы компонента Dr.Web CloudD



Пакет	Содержимое
drweb-common	Основной конфигурационный файл <code>drweb.ini</code> , основные библиотеки, документация и структура каталогов продукта.  В процессе установки данного пакета также будут созданы пользователь <code>drweb</code> и группа <code>drweb</code>
drweb-configd	Файлы компонентов Dr.Web ConfigD и Dr.Web Ctl
drweb-dws	Файлы базы данных категорий веб-ресурсов
drweb-esagent	Файлы компонента Dr.Web ES Agent
drweb-filecheck	Файлы компонента Dr.Web File Checker
drweb-internet-gateways-doc	Документация PDF по продукту
drweb-internet-gateways	Корневой метапакет продукта
drweb-gated	Файлы компонента SpIDer Gate
drweb-firewall	Файлы компонента Dr.Web Firewall для Linux
drweb-httpd	Файлы компонента Dr.Web HTTPD и веб-интерфейса управления (метапакет)
drweb-httpd-bin	Файлы компонента Dr.Web HTTPD
drweb-httpd-webconsole	Файлы веб-интерфейса управления
drweb-icu	Библиотеки поддержки интернационализации и Unicode
drweb-icapd	Файлы компонента Dr.Web ICAPD
drweb-libs	Файлы основных библиотек продукта *)
drweb-lookupd	Файлы компонента Dr.Web LookupD
drweb-netcheck	Файлы компонента Dr.Web Network Checker
drweb-openssl	Библиотеки <b>OpenSSL</b>
drweb-protobuf	Библиотеки <b>Protobuf</b>
drweb-se	Файлы компонента Dr.Web Scanning Engine
drweb-snmpd	Файлы компонента Dr.Web SNMPD
drweb-update	Файлы компонента Dr.Web Updater



\*) В версии для 64-битных систем в архив включены два пакета: `drweb-libs` и `drweb-libs32`, в которых содержатся библиотеки для 64- и 32-битных компонентов соответственно.

В разделе [Выборочные установка и удаление компонентов](#) приведены типовые наборы компонентов для выборочной установки, обеспечивающие решение типовых задач продукта.

## Файлы

Файлы Dr.Web для Интернет-шлюзов UNIX размещаются в каталогах `/opt`, `/etc` и `/var` дерева файловой системы.

Структура используемых каталогов:

Каталог	Содержимое
<code>&lt;etc_dir&gt;/</code>	Общий конфигурационный файл и ключевой файл продукта.
<code>/etc/init.d/</code>	Управляющий стартовый скрипт для демона управления конфигурацией Dr.Web ConfigD.
<code>&lt;opt_dir&gt;/</code>	Основной каталог продукта.
<code>bin/</code>	Исполняемые файлы всех компонентов продукта (за исключением Dr.Web Virus-Finding Engine).
<code>include/</code>	Заголовочные файлы используемых библиотек.
<code>lib/</code> <code>lib64/</code>	Используемые библиотеки для 32- и 64-битной платформ.
<code>man/</code>	Файлы системной справки <b>man</b> .
<code>share/</code>	Вспомогательные файлы продукта.
<code>doc/</code>	Документация по продукту (файлы <code>readme</code> и текст лицензионного соглашения).
<code>drweb-bases/</code>	Файлы вирусных баз Dr.Web (исходные образы, поставляемые при установке продукта).
<code>scripts/</code>	Файлы вспомогательных сценариев.
<code>&lt;var_dir&gt;/</code>	Вспомогательные и временные файлы продукта.
<code>bases/</code>	Файлы вирусных баз Dr.Web (актуальная обновленная версия).
<code>cache/</code>	Кэш обновлений.





Каталог	Содержимое
drl/	Списки используемых серверов обновлений.
lib/	Антивирусное ядро Dr.Web Virus-Finding Engine в виде динамически загружаемой библиотеки drweb32.dll и настройки режима работы с сервером централизованной защиты.
update/	Каталог для временного хранения обновлений в процессе их получения.

Дополнительную информацию о принятой системе обозначений каталогов см. в разделе [Введение](#).

## Выборочные установка и удаление компонентов

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

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

## Типовые комплекты компонентов для выборочной установки

Если требуется установить продукт с ограниченной функциональностью, вместо установки корневого метапакета продукта 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 наборы компонентов, предназначенные для решения типовых задач продукта. В столбце **Пакет для установки** перечислены пакеты, которые необходимо установить для получения указанного набора компонентов.

Выборочный комплект компонентов	Пакет для установки	Будут установлены
Минимальный комплект для консольного сканирования	drweb-filecheck	<ul style="list-style-type: none"><li>• Dr.Web Ctl</li><li>• Dr.Web ConfigD</li><li>• Dr.Web Scanning Engine</li><li>• Dr.Web File Checker</li><li>• Dr.Web Updater</li><li>• Вирусные базы</li></ul>



Выборочный комплект компонентов	Пакет для установки	Будут установлены
Комплект для эмуляции <b>ClamAV</b> ( <b>clamd</b> )	drweb-clamd	<ul style="list-style-type: none"><li>• Dr.Web Ctl</li><li>• Dr.Web ConfigD</li><li>• Dr.Web Scanning Engine</li><li>• Dr.Web File Checker</li><li>• Dr.Web Network Checker</li><li>• Dr.Web Updater</li><li>• Dr.Web ClamD</li><li>• Вирусные базы</li></ul>
Комплект для проверки доступа к веб-сайтам через прокси-сервер по протоколу ICAP (без антивирусной проверки трафика)	drweb-icapd	<ul style="list-style-type: none"><li>• Dr.Web Ctl</li><li>• Dr.Web ConfigD</li><li>• Dr.Web ICAPD</li><li>• Dr.Web Updater</li><li>• База категорий веб-ресурсов</li></ul>
<p>Комплект для проверки доступа к веб-сайтам через прокси-сервер по протоколу ICAP (с антивирусной проверкой трафика).</p> <p><i>Примечание: Пакет drweb-se можно не устанавливать, если антивирусная проверка производится на другом сервере, передача данных для проверки на который будет организована через Dr.Web Network Checker.</i></p> <p><i>Пометкой *) отмечены компоненты, которые не будут установлены, если не устанавливать пакет drweb-se.</i></p>	drweb-icapd drweb-netcheck drweb-se *	<ul style="list-style-type: none"><li>• Dr.Web Ctl</li><li>• Dr.Web ConfigD</li><li>• Dr.Web ICAPD</li><li>• Dr.Web Network Checker</li><li>• Dr.Web Scanning Engine *)</li><li>• Dr.Web Updater</li><li>• Вирусные базы *)</li><li>• База категорий веб-ресурсов</li></ul>
<p>Комплект для локальной проверки HTTP-соединений</p> <p><i>Примечание: Если антивирусная проверка соединений не требуется, пакеты drweb-netcheck и drweb-se можно не устанавливать. Пакет drweb-se можно не устанавливать, если антивирусная проверка производится на другом сервере,</i></p>	drweb-gated drweb-firewall drweb-netcheck * drweb-se * drweb-dws **	<ul style="list-style-type: none"><li>• Dr.Web Ctl</li><li>• Dr.Web ConfigD</li><li>• SpIDer Gate</li><li>• Dr.Web Firewall для Linux</li><li>• Dr.Web Network Checker</li><li>• Dr.Web Scanning Engine *)</li><li>• Dr.Web Updater ***)</li><li>• Вирусные базы *)</li><li>• База категорий веб-ресурсов **)</li></ul>



Выборочный комплект компонентов	Пакет для установки	Будут установлены
<p>передача данных для проверки на который будет организована через Dr.Web Network Checker. Пакет drweb-dws можно не устанавливать, если не требуется проверка вхождения URL в категории нежелательных веб-ресурсов.</p> <p>Пометкой *) отмечены компоненты, которые не будут установлены, если не устанавливать пакет drweb-se.</p> <p>Пометкой **) отмечены компоненты, которые не будут установлены, если не будет установлен пакет drweb-dws.</p> <p>Компонент Dr.Web Updater (отмечен меткой ***) будет установлен только в случае если будут установлены вирусные базы или база категорий веб-ресурсов.</p>		

## 1. Установка и удаление компонентов продукта, установленного из репозитория

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

1. Чтобы удалить компонент Dr.Web ClamD (пакет drweb-clamd) из состава продукта, установленного в ОС **CentOS**, используйте команду:

```
# yum remove drweb-clamd
```

2. Чтобы добавить компонент Dr.Web ClamD (пакет drweb-clamd) в состав продукта, установленного в ОС **Ubuntu Linux**, используйте команду:

```
# apt-get install drweb-clamd
```

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



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

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

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

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

### Распаковка инсталляционного файла

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

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

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

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

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

```
$ ./<имя_файла>.run --help
```

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

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

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



## Выборочная установка компонентов

Установочный `rpm`-файл содержит пакеты всех компонентов, из которых состоит программный комплекс Dr.Web для Интернет-шлюзов UNIX (в формате RPM), а также вспомогательные файлы. Файлы пакетов каждого компонента имеют вид:

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

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

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



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

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

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

Например:

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

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

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

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

```
# ./scripts/installpkg.sh drweb-internet-gateways
```



## Выборочное удаление компонентов

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

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

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

```
# yum remove drweb-clamd
```

Если ваша ОС использует пакеты формата DEB (в т.ч., если вы используете ОС **MCBC 3.0**), либо если в составе системы не имеется менеджера пакетов (**FreeBSD, Solaris**), для выборочного удаления следует воспользоваться менеджером пакетов **zypper**, автоматически установленным в рамках установки продукта. Для этого перейдите в каталог `<opt_dir>/bin` (для **GNU/Linux** – `/opt/drweb.com/bin`), и выполните следующую команду:

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

Например:

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

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

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

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



## Настройка 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 продукта Dr.Web для Интернет-шлюзов UNIX при настройках по умолчанию. Для обеспечения корректной работы Dr.Web для Интернет-шлюзов UNIX в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web для Интернет-шлюзов UNIX.

В этом разделе рассматриваются настройки, обеспечивающие корректную работу Dr.Web для Интернет-шлюзов UNIX в следующих случаях:

- [Настройка](#) политик безопасности **SELinux**.
- [Настройка разрешений](#) для системы мандатного доступа **PARSEC** (ОС **Astra Linux**).



Настройка разрешений системы мандатного доступа **PARSEC** для Dr.Web для Интернет-шлюзов UNIX позволит обходить его компонентам ограничения установленных политик безопасности и получать доступ к файлам разных уровней привилегий.

Обратите внимание, что даже если вы не настроите разрешения системы мандатного доступа **PARSEC** для Dr.Web для Интернет-шлюзов UNIX, то вы все равно сможете запускать проверку файлов непосредственно из [командной строки](#). Для этого используйте [команду](#) **drweb-ctl** в автономном режиме работы, указав при запуске параметр `--Autonomous`. При этом будет возможна проверка файлов, для доступа к которым необходим уровень привилегий не выше уровня, с которым работает пользователь, запустивший сеанс проверки. Данный режим имеет следующие особенности:

- Для запуска автономной копии необходимо наличие действующего [ключевого файла](#), работа под управлением сервера [централизованной защиты](#) не поддерживается (имеется возможность [установить](#) ключевой файл, экспортированный с сервера централизованной защиты). При этом, даже если продукт подключен к серверу централизованной защиты, автономная копия не сообщает серверу централизованной защиты об угрозах, обнаруженных при запуске в режиме автономной копии.
- Все вспомогательные компоненты, обслуживающие работу запущенной автономной копии, будут запущены от имени текущего пользователя и будут работать со специально сформированным файлом конфигурации.
- Все временные файлы и сокеты UNIX, используемые для взаимодействия компонентов между собой, будут создаваться только в каталоге с уникальным именем, созданным запущенной автономной копии в каталоге временных файлов (указанном в системной переменной окружения `TMPDIR`).
- Пути к файлам вирусных баз, антивирусного ядра и исполняемым файлам используемых при сканировании компонентов заданы по умолчанию, либо берутся из специальных переменных окружения.



- Число одновременно работающих автономных копий не ограничено.
- При завершении работы автономно запущенной копии также завершает работу и комплект обслуживающих её работу компонентов.

## Настройка политик безопасности SELinux

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

### 1. Проблемы при установке универсального пакета

При включенном **SELinux** установка продукта в виде [универсального пакета](#) из установочного файла (`.run`) может окончиться неудачей, поскольку будет заблокирована попытка создания в системе специального пользователя *drweb*, с полномочиями которого работают компоненты Dr.Web для Интернет-шлюзов UNIX.

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

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

Если **SELinux** работает в режиме *Enforced*, следует временно (на период установки продукта) перевести ее в режим *Permissive*. Для этого выполните следующую 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 продукта из установочного файла, но до его запуска и активации верните режим *Enforced*, для чего выполните команду:

```
# setenforce 1
```

## 2. Проблемы функционирования продукта

В некоторых случаях при работающем **SELinux** отдельные компоненты Dr.Web для Интернет-шлюзов UNIX (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 в системном журнале, который ведет служба **syslog** (обычно этот журнал расположен в каталоге `/var/log/`).



Ошибки 119 и 120 также могут сигнализировать о том, что вы пытаетесь запустить Dr.Web для Интернет-шлюзов UNIX в 64-битной версии операционной системы при отсутствии библиотеки поддержки исполнения 32-битных приложений (см. раздел [Системные требования](#)).

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

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



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

### Создание политик безопасности SELinux:

1. Создайте новый файл с исходным кодом политики **SELinux** (файл с расширением `.te`). Данный файл определяет ограничения, относящиеся к описываемому модулю. Исходный файл политики может быть создан двумя способами:
  - 1) С помощью утилиты **audit2allow**. Это наиболее простой способ, поскольку данная утилита генерирует разрешающие правила на основе сообщений об отказе в доступе в файлах системных журналов. Возможно задать автоматический поиск сообщений в файлах журналов или указать путь к файлу журнала вручную.



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



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

Пример использования **audit2allow**:

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

В данном примере утилита **audit2allow** производит поиск в файле `/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`. Обратите внимание, что по умолчанию утилита **audit2allow** в качестве результата своей работы выводит на экран готовый вызов команды **semodule**. Скопировав его в командную строку и выполнив, вы выполните [пункт 4](#). Перейдите к [пункту 2](#), только если вы хотите внести изменения в политики, автоматически сформированные для компонентов Dr.Web для Интернет-шлюзов UNIX.

- 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.



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

Пример создания политик при помощи **policygentool**:

- Для 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.



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

Пример использования:

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

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

Пример:

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

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

Пример:

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

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

## Настройка разрешений PARSEC (Astra Linux)

В системах, оснащенных подсистемой безопасности **PARSEC** (система управления мандатным доступом) из-за разности уровней привилегий, необходимых для доступа к файлам, если пользователь работает на отличном от нуля уровне привилегий, утилита управления Dr.Web для Интернет-шлюзов UNIX из командной строки [Dr.Web Ctl](#) не может взаимодействовать с демоном управления конфигурацией [Dr.Web ConfigD](#), работающими на других уровнях привилегий, в том числе может отсутствовать доступ к [консолидированному карантину](#).

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



## Настройка корректного запуска Dr.Web для Интернет-шлюзов UNIX на любом уровне привилегий

Чтобы все компоненты Dr.Web для Интернет-шлюзов UNIX корректно взаимодействовали между собой при их запуске на разных уровнях привилегий, внесите изменения в сценарий запуска демона управления конфигурацией Dr.Web ConfigD (**drweb-configd**):

1. Совершите вход в систему с использованием нулевого уровня привилегий.
2. В любом текстовом редакторе откройте файл сценария `/etc/init.d/drweb-configd` (необходимы права суперпользователя).
3. Найдите в этом файле определение функции `start_daemon`, в которой замените строку

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

на строку

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

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

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

Измените данную строку следующим образом:

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

5. Сохраните файл и перезапустите систему.



## Начало работы

1. Для начала работы с установленным Dr.Web для Интернет-шлюзов UNIX выполните его [активацию](#), получив и установив [ключевой файл](#).
2. Далее рекомендуется выполнить [проверку работоспособности продукта](#).
3. Интегрируйте Dr.Web для Интернет-шлюзов UNIX с используемым вами прокси-сервером HTTP (см. [инструкцию](#) для прокси-сервера **Squid**).
4. Для защиты локального веб-сервера от угроз из внешней сети [внесите изменения](#) в настройки монитора SpIDer Gate.
5. Проверьте состав запущенных компонентов и при необходимости включите дополнительные компоненты, которые по умолчанию отключены, если они необходимы для защиты вашего сервера (например, [Dr.Web ClamD](#) или [Dr.Web SNMPD](#), в зависимости от поставки). Обратите внимание, что только включения дополнительных компонентов для их корректной работы может оказаться недостаточно. Возможно также потребуются внести изменения в их настройки, заданные по умолчанию. Для просмотра перечня установленных и запущенных компонентов, а также их настройки, вы можете воспользоваться:
  - [Утилитой управления](#) из командной строки Dr.Web Ctl (используйте команды **drweb-ctl appinfo**, **drweb-ctl cfshow** и **drweb-ctl cfset**).
  - [Веб-интерфейсом](#) управления Dr.Web для Интернет-шлюзов UNIX (по умолчанию доступ через браузер по адресу <https://127.0.0.1:4443/>).

## Регистрация и активация продукта

### Приобретение и регистрация лицензий

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

Приобрести любой антивирусный продукт Dr.Web или серийный номер для него вы можете у наших [партнеров](#) или через [интернет-магазин](#). Дополнительную информацию о сроках и типах лицензирования можно найти на официальном сайте компании «Доктор Веб» <https://www.drweb.com/>.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем продукта Dr.Web для Интернет-шлюзов UNIX и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки. Приобретенная лицензия может быть активирована непосредственно на сайте компании «Доктор Веб» по адресу <https://products.drweb.com/register/>.



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



В случае регистрации лицензии, продлевающей лицензию, срок годности которой истек, требуется указать серийный номер или лицензионный ключевой файл предыдущей лицензии, в противном случае срок действия новой лицензии будет сокращен на 150 дней.

Если имеется комплект лицензий, выданных для использования продукта на нескольких серверах, то при регистрации имеется возможность указать, что Dr.Web для Интернет-шлюзов UNIX будет использоваться только на одном сервере. В этом случае все лицензии из комплекта будут объединены в одну, и срок ее действия будет автоматически увеличен.

## Запрос демонстрационного периода

Для получения демонстрационного периода на использование продукта Dr.Web для Интернет-шлюзов UNIX следует обратиться к мастеру запроса демо на сайте компании «Доктор Веб» по адресу <https://download.drweb.com/demoreq/biz/>. После выбора продукта и заполнения анкеты вы получите по электронной почте серийный номер или ключевой файл для активации демонстрационного периода.



Демонстрационный период использования продукта может быть выдан повторно для того же компьютера только по истечении определенного периода времени.

Вы можете воспользоваться командой `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

Ключевой файл – это специальный файл, который хранится на локальном компьютере и соответствует приобретенной лицензии или активированному демонстрационному периоду для программного продукта Dr.Web для Интернет-шлюзов UNIX. В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.



При работе Dr.Web для Интернет-шлюзов UNIX ключевой файл по умолчанию должен находиться в каталоге `<etc_dir>` (для **Linux** – `/etc/opt/drweb.com`) и называться `drweb32.key`.

Компоненты программного комплекса регулярно проверяют наличие и корректность ключевого файла. Его содержимое защищено от редактирования при помощи механизма электронной цифровой подписи, поэтому редактирование делает ключевой файл недействительным. Не рекомендуется открывать ключевой файл в текстовых редакторах во избежание случайной порчи его содержимого.

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

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



По электронной почте ключевые файлы Dr.Web обычно передаются запакованными в zip-архивы. Архив, содержащий ключевой файл для активации продукта, обычно имеет имя `agent.zip` (обратите внимание, что если в письме содержится *несколько* архивов, то нужно использовать именно архив `agent.zip`). Перед установкой ключевого файла вы должны 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).

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

1. Распакуйте ключевой файл, если он был вами получен в архиве.
2. Далее выполните любое из указанных ниже действий:
  - Скопируйте его в каталог `<etc_dir>` и, при необходимости, переименуйте в `drweb32.key`.
  - В [файле конфигурации](#) Dr.Web для Интернет-шлюзов UNIX установите значение параметра **KeyPath** таким образом, чтобы он указывал на ключевой файл.
3. Перезапустите Dr.Web для Интернет-шлюзов UNIX, выполнив [команду](#):

```
# drweb-ctl reload
```

для применения внесенных изменений.



Вы можете также воспользоваться [командой](#):

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

В последнем случае перезапускать Dr.Web для Интернет-шлюзов UNIX не требуется. Ключевой файл не будет скопирован в каталог `<etc_dir>`, а останется в исходном каталоге.



Об условных обозначениях путей `<opt_dir>`, `<etc_dir>` и `<var_dir>` см. [Введение](#).

Если ключевой файл не скопирован в каталог `<etc_dir>`, 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.

## Повторная регистрация

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

Количество запросов на получение лицензионного ключевого файла ограничено – регистрация лицензии с одним и тем же серийным номером допускается *не более 25 раз*. Если это число превышено, лицензионный ключевой файл не будет выслан. В этом случае обратитесь в [службу технической поддержки](#) «Доктор Веб» (в запросе следует подробно описать ситуацию, указать персональные данные, введенные при регистрации, и серийный номер лицензии). Лицензионный ключевой файл будет выслан службой технической поддержки по электронной почте.

После получения ключевого файла по электронной почте, вам необходимо выполнить процедуру его [установки](#).

## Проверка работоспособности продукта

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





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

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

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

```
X5O!P%@AP[4\ZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

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

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

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

```
$ tail <opt_dir>/share/doc/drweb-common/readme.eicar | grep X5O > testfile &&  
drweb-ctl rawscan testfile && rm testfile
```

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



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

Об условных обозначениях путей `<opt_dir>`, `<etc_dir>` и `<var_dir>` см. [Введение](#).

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 (см. [Приложение Е. Описание 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.

## Интеграция с прокси-сервером Squid

### 1) Настройка параметров Dr.Web ICAPD

Для интеграции Dr.Web ICAPD с прокси-сервером HTTP **Squid** необходимо проверить и при необходимости изменить значения ряда параметров, находящихся в секции [настроек](#) Dr.Web ICAPD (секция [ICAPD]):

- В параметре **ListenAddress** следует указать путь к сетевому сокету (<IP-адрес>:<порт>), который Dr.Web ICAPD будет прослушивать в ожидании подключений от прокси-сервера (по умолчанию используется сокет 127.0.0.1:1344).
- В параметрах **Block\*** следует включить или отключить категории сайтов и типы угроз, которые должен блокировать и наоборот, разрешать Dr.Web ICAPD.
- При необходимости, задавая значения параметров **WhiteList** и **BlackList**, определите пути к доменам, доступ к которым не должен блокироваться, или наоборот, должен блокироваться безусловно. Обратите внимание, что параметр **BlackList** имеет приоритет над параметром **WhiteList**, т.е. если один и тот же домен включен в оба параметра, то доступ к нему будет блокироваться.
- Для более тонкой настройки доступа к сайтам (в зависимости от условий) отредактируйте [правила проверки](#).



Значения параметров **UsePreview**, **Use204** и **AllowEarlyResponse** в секции настроек Dr.Web ICAPD, заданные по умолчанию, разрешают использование компонентом соответствующих возможностей протокола ICAP (использование режима *ICAP preview*, возврат кода 204 не только в режиме *ICAP preview* и «раннее» начало отправки ответа клиенту, не дожидаясь окончания приема запроса, поступившего от прокси-сервера). Значения этих параметров рекомендуется оставить заданными по умолчанию, изменяя их только в случае возникновения проблем в обработке HTTP-запросов.

После внесения изменений в настройки следует перезапустить Dr.Web для Интернет-шлюзов UNIX (используйте [команду](#) **drweb-ctl reload**). Также вы можете выполнить перезапуск демона управления конфигурацией Dr.Web ConfigD (используйте команду **service drweb-configd restart**).



## 2) Настройка параметров Squid

Для обеспечения взаимодействия между **Squid** и Dr.Web ICAPD требуется отредактировать конфигурационный файл `squid.conf` с целью подключения возможности использования протокола ICAP (этот файл обычно находится в каталоге `/etc/squid3/`). Настройка **Squid** состоит в задании следующих параметров:

1. Включение использования **Squid** протокола ICAP.
2. Регистрация Dr.Web ICAPD в качестве службы ICAP, используемой **Squid**.
3. Включение использования режима *ICAP preview* (опционально).
4. Разрешение передачи данных клиентов (IP-адреса и аутентифицированного на прокси-сервере имени пользователя) для использования в правилах Dr.Web ICAPD (опционально).
5. Включение поддержки постоянных соединений между Dr.Web ICAPD и **Squid** (опционально; использование постоянных соединений необязательно, но повышает производительность связки **Squid** + Dr.Web ICAPD).

При настройке **Squid** следует иметь в виду следующее:

- Чтобы **Squid** проверял через ICAP HTTP-запросы (*REQMOD*) и HTTP-ответы (*RESPMOD*), требуется добавить две службы ICAP соответствующего типа.
- Чтобы **Squid** использовал Dr.Web ICAPD в качестве службы ICAP, адрес и порт, указанные в `icap_service`, должны совпадать с адресом и портом, указанными в параметре **ListenAddress** настроек Dr.Web ICAPD.
- Dr.Web ICAPD не будет работать со **Squid**, если значение `icap_preview_size` отлично от 0.
- Значения «IP-адрес клиента» и «Имя пользователя» **Squid** формирует самостоятельно и направляет их Dr.Web ICAPD в качестве заголовков ICAP-запроса. Достоверность и наличие этих данных не гарантируется. Dr.Web ICAPD предполагает, что имя пользователя и его IP-адрес передаются прокси-сервером в заголовках `X-Client-Username` и `X-Client-IP`, без использования методов кодирования значений, отличных от настроек, заданных для **Squid** по умолчанию. Поэтому не следует изменять значения параметров в настройке **Squid**, влияющих на способ передачи этих значений (таких как `icap_client_username_encode` и `icap_client_username_header`).



Используемый вами **Squid** должен быть собран с поддержкой ICAP (т.е. скомпилирован с опцией `--enable-icap-client`). В противном случае подключение **Squid** к Dr.Web ICAPD невозможно.

Перечень настраиваемых параметров настройки зависит от используемой версии сервера **Squid** (ниже приведено три варианта настройки: для **Squid** версии 3.2 (и старше), 3.1, и для версии 3.0). Если нижеприведенные строки уже есть в конфигурационном файле, то нужно исправить их значения на указанные ниже. Если указанные параметры присутствуют в файле, но закомментированы – раскомментируйте их. В случае отсутствия требуемых



параметров в файле конфигурации **Squid**, добавьте их в файл, например – в конец.



Обязательными для настройки взаимодействия между Dr.Web ICAPD и **Squid** являются только пункты #1 и #2. Если остальные настройки из приведенных ниже не требуются, просто не добавляйте их в файл конфигурации **Squid**.

### Для Squid версии 3.2 и старше

```
#1
icap_enable on

#2
icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

#3
icap_preview_enable on
icap_preview_size 0

#4 (В версии Squid 3.2 параметры icap_send_client_ip и
#icap_send_client_username были переименованы)
adaptation_send_client_ip on
adaptation_send_username on

#5
icap_persistent_connections on
```

### Для Squid версии 3.1

```
#1
icap_enable on

#2 (В версии Squid 3.1 формат определения сервиса был изменен, а параметр
#icap_access был переименован)
icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

#3
icap_preview_enable on
icap_preview_size 0

#4
icap_send_client_ip on
icap_send_client_username on

#5
icap_persistent_connections on
```



## Для Squid версии 3.0

```
#1
icap_enable on

#2
icap_service i_req reqmod_precache 0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache 0 icap://127.0.0.1:1344/respmod

icap_class icapd_class_req i_req
icap_class icapd_class_resp i_res

icap_access icapd_class_req allow all
icap_access icapd_class_resp allow all

#3
icap_preview_enable on
icap_preview_size 0

#4
icap_send_client_ip on
icap_send_client_username on

#5
icap_persistent_connections on
```

После внесения изменений в настройки **Squid** следует перезапустить его.

## Дополнительно

При необходимости вы можете ограничить размер данных, которые **Squid** будет передавать на проверку по протоколу ICAP. Для этого в файл конфигурации следует добавить условие, которому должно удовлетворять (или не удовлетворять) содержимое заголовка Content-Length, например:

```
acl <name> rep_header Content-Length ^[0-9]{7,}$
```

(условие <name> будет истинно, если заголовок Content-Length в ответе сервера содержит число, большее 999999).

Далее добавленное условие следует использовать для разрешения (allow) или запрещения (deny) проверки ответа от сервера по протоколу ICAP (следует заменить слово all в параметрах подключения **Squid** к внешнему ICAP-серверу на имя условия <name>). Так как пример, указанный выше, будет истинным при наличии в заголовке Content-Length числа, большего 999999, используем его для *запрещения* проверки ответов, для которых условие <name> будет истинно:

```
#версия Squid 3.1 и новее
adaptation_access i_res deny <name>

#версия Squid 3.0 и старше
icap_access icapd_class_resp deny <name>
```



Наличие заголовка `Content-Length` не гарантируется в ответе веб-сервера. В случае его отсутствия указанный способ ограничения размера данных, отправляемых **Squid** на проверку в ICAP-сервер, не работает.

После внесения изменений в настройки **Squid** следует перезапустить его.

За дополнительными сведениями по тонкой настройке **Squid** для ограничения проверки веб-трафика обратитесь к документации **Squid**. См. например, <http://www.squid-cache.org/Doc/> (на англ. языке).

## Защита локального веб-сервера



Данная возможность доступна только в составе дистрибутивов продукта, предназначенных для ОС семейства **GNU/Linux**.

Для защиты веб-сервера, работающего на том же узле, на который установлен Dr.Web для Интернет-шлюзов UNIX, необходимо настроить компонент [Dr.Web Firewall для Linux](#) таким образом, чтобы данные, поступающие на веб-сервер, проходили проверку в мониторе [SpIDer Gate](#).

Чтобы настроить защиту веб-сервера, измените значение параметра **InputDiver**, находящегося в [конфигурационном файле](#), в секции [настроек](#) Dr.Web Firewall для Linux (секция `[LinuxFirewall]`):

```
InputDiver = Auto(interface:<сетевой интерфейс> protected:<список портов>)
```

где:

- *<сетевой интерфейс>* – имя сетевого интерфейса (`eth0`, `wlan` и т.п.), через которые поступают входящие соединения на веб-сервер, подлежащие проверке.
- *<список портов>* – список номеров портов, которые обслуживает веб-сервер (80, 8080 и т.п.).

Для просмотра и изменения настроек Dr.Web Firewall для Linux и SpIDer Gate вы можете воспользоваться:

- [Утилитой управления](#) из командной строки Dr.Web Ctl (используйте команды **drweb-ctl cfshow** и **drweb-ctl cfset**).
- [Веб-интерфейсом](#) управления Dr.Web для Интернет-шлюзов UNIX (по умолчанию доступ через браузер по адресу `https://127.0.0.1:4443/`).

Например, команда:

```
# drweb-ctl cfset LinuxFirewall.InputDiver 'Auto(interface:eth0  
protected:80,8080) '
```



настроит Dr.Web Firewall для Linux таким образом, чтобы данные, поступающие через сетевой интерфейс `eth0`, и следующие на локальный порт 80 или 8080 (предполагается, что эти порты обслуживает веб-сервер), проходили проверку в мониторе [SpIDer Gate](#).



## Краткие инструкции

### Как подключить Dr.Web для Интернет-шлюзов UNIX к Squid

Следуйте инструкции, представленной в разделе [Интеграция с прокси-сервером Squid](#).

### Как защитить веб-сервер

Следуйте инструкции, представленной в разделе [Защита локального веб-сервера](#).

### Как перезапустить программный комплекс Dr.Web для Интернет-шлюзов UNIX

Для перезапуска уже работающего программного комплекса вы можете использовать скрипт управления демоном управления конфигурацией Dr.Web ConfigD. Запуск, останов и перезапуск этого демона приводит, соответственно, к запуску, останову и перезапуску всех компонентов программного комплекса Dr.Web для Интернет-шлюзов UNIX.

Сценарий оболочки для управления Dr.Web ConfigD стандартным образом располагается в каталоге `/etc/init.d` и называется `drweb-configd`. Он имеет следующие управляющие параметры:

Параметр	Описание
<code>start</code>	Запустить Dr.Web ConfigD, если он еще не запущен. При запуске Dr.Web ConfigD запустит все необходимые модули комплекса Dr.Web для Интернет-шлюзов UNIX.
<code>stop</code>	Завершить работу Dr.Web ConfigD, если он запущен. При завершении работы Dr.Web ConfigD завершит работу всех модулей комплекса Dr.Web для Интернет-шлюзов UNIX.
<code>restart</code>	Перезапустить (завершить и запустить) Dr.Web ConfigD. Dr.Web ConfigD, соответственно, завершит и запустит все модули комплекса Dr.Web для Интернет-шлюзов UNIX. Если Dr.Web ConfigD не был запущен, равносильно <code>start</code> .
<code>condrestart</code>	Перезапустить Dr.Web ConfigD только в том случае, если он был запущен.
<code>reload</code>	Послать Dr.Web ConfigD сигнал HUP, если он запущен. Dr.Web ConfigD перешлет этот сигнал всем модулям комплекса Dr.Web для Интернет-шлюзов UNIX. Используется для инициации процесса перечитывания конфигурации всеми компонентами комплекса.
<code>status</code>	Вывести на консоль текущее состояние Dr.Web ConfigD.





Для перезапуска (или запуска, если он не был запущен) программного комплекса Dr.Web для Интернет-шлюзов UNIX используйте команду:

```
# /etc/init.d/drweb-configd restart
```

## Как подключиться к серверу централизованной защиты

1. Получите от администратора антивирусной сети адрес сервера централизованной защиты и файл его открытого ключа, а также, возможно, дополнительные параметры, такие, как идентификатор рабочей станции и пароль, или идентификаторы основной и тарифной группы.
2. Воспользуйтесь [командой](#) `esconnect` утилиты управления продуктом Dr.Web для Интернет-шлюзов UNIX из командной строки [Dr.Web Ctl](#).

Для подключения обязательно нужно использовать опцию `--Key`, указав путь к файлу открытого ключа сервера. Дополнительно вы можете указать идентификатор узла («рабочей станции», с точки зрения сервера централизованной защиты) и пароль для аутентификации на сервере, если они вам известны, используя параметры `--Login` и `--Password`. Если эти параметры заданы, то подключение к серверу будет успешным только при указании правильной пары идентификатор/пароль. Если эти параметры не указаны, 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 использовать опцию `--Newbie` (подключиться как «новичок»). Если этот режим подключения разрешен на сервере, то, после одобрения подключения, сервер автоматически сгенерирует для хоста уникальную пару идентификатор/пароль, которая в дальнейшем будет использоваться для его подключения к этому серверу. Обратите внимание, что при подключении как «новичок», новая учетная запись для хоста будет сгенерирована сервером централизованной защиты даже в том случае, если ранее он уже имел учетную запись на этом сервере.

Типовой пример команды подключения программного комплекса Dr.Web для Интернет-шлюзов UNIX к серверу централизованной защиты:

```
# drweb-ctl esconnect <адрес сервера> --Key <путь к публичному ключу сервера>
```

После успешного подключения к серверу централизованной защиты программный комплекс будет работать в режиме централизованной защиты или в мобильном режиме, в зависимости от разрешений, установленных на сервере и значения [параметра конфигурации](#) **MobileMode** компонента Dr.Web ES Agent. Для того, чтобы потребовать безусловного использования мобильного режима, необходимо установить значение этого параметра в значение `On`. Для работы в режиме централизованной защиты параметр следует установить в значение `Off`.



Типовой пример команды перевода программного комплекса Dr.Web для Интернет-шлюзов UNIX, подключенного к серверу централизованной защиты, в мобильный режим:

```
# drweb-ctl cfset ESAgent.MobileMode On
```



Если используемый сервер централизованной защиты не поддерживает или запрещает мобильный режим работы, то изменение значения параметра конфигурации **MobileMode** не переведет программный комплекс Dr.Web для Интернет-шлюзов UNIX в мобильный режим.

## Как отключиться от сервера централизованной защиты

Для отключения продукта от сервера централизованной защиты и перевода его в одиночный (standalone) режим воспользуйтесь командой `esdisconnect` управления продуктом Dr.Web для Интернет-шлюзов UNIX из командной строки Dr.Web Ctl:

```
# drweb-ctl esdisconnect
```

Для успешной работы программного комплекса в одиночном режиме необходимо иметь действующий лицензионный ключевой файл. В противном случае антивирусные функции продукта после перехода в одиночный режим *будут заблокированы*.

## Как активировать продукт

1. Пройдите регистрацию на сайте компании «Доктор Веб» по адресу <https://products.drweb.com/register/>.
2. Получите на указанный при регистрации адрес электронной почты (или загрузите непосредственно с сайта после окончания регистрации) архив, содержащий действительный лицензионный ключевой файл.
3. Выполните процедуру установки ключевого файла.

## Как обновить версию продукта

Обновите версии компонентов или выполните переход на новую версию.

Обратите внимание, что вам может быть предложено удалить текущую версию продукта.

## Как добавить или удалить компонент продукта

Воспользуйтесь процедурой выборочной установки и удаления.

Обратите внимание, что при установке или удалении компонента для удовлетворения зависимостей могут быть дополнительно установлены или удалены другие компоненты продукта.



## Как управлять работой компонентов

Для просмотра состояния компонентов программного комплекса и управления их работой вы можете воспользоваться:

- [Утилитой управления](#) из командной строки Dr.Web Ctl (используйте команды **drweb-ctl appinfo**, **drweb-ctl cfshow** и **drweb-ctl cfset**. Для просмотра перечня доступных команд управления используйте команду **drweb-ctl --help**).
- [Веб-интерфейсом](#) управления Dr.Web для Интернет-шлюзов UNIX (по умолчанию доступ через браузер по адресу <https://127.0.0.1:4443/>).

## Как просмотреть журнал программного комплекса

При настройках по умолчанию общий журнал всех компонентов программного комплекса выводится в **syslog** (файл, в который записывает сообщения системный компонент **syslog**, зависит от системы, и располагается в каталоге `/var/log`). Общие настройки ведения журнала задаются в [конфигурационном файле](#), в [секции](#) [Root] (параметры **Log** и **DefaultLogLevel**). Для каждого из [компонентов](#), в его секции настроек, доступны параметры **Log** и **LogLevel**, задающие место хранения журнала и уровень подробности сообщений, выводимых компонентом в журнал.

Для изменения настроек ведения журнала используйте утилиту управления из командной строки Dr.Web Ctl или веб-интерфейс управления Dr.Web для Интернет-шлюзов UNIX (если он установлен).

- Для облегчения идентификации ошибок рекомендуется настроить вывод общего журнала всех компонентов в отдельный файл и разрешить вывод расширенной отладочной информации. Для этого выполните следующие команды:

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Для возврата настроек ведения общего журнала всех компонентов по умолчанию выполните следующие команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```



## Компоненты программного комплекса

В разделе перечислены компоненты, составляющие программный комплекс Dr.Web для Интернет-шлюзов UNIX. Для каждого компонента указано его назначение, принципы функционирования, а также параметры, которые он хранит в [файле конфигурации](#) программного комплекса.

### Dr.Web ConfigD

Демон управления конфигурацией Dr.Web ConfigD является центральным управляющим компонентом программного комплекса Dr.Web для Интернет-шлюзов UNIX. Он обеспечивает централизованное хранение конфигурационной информации для всех компонентов программного комплекса, управляет активностью всех компонентов и организует доверительный обмен данными между ними.

## Принципы работы

### Основные функции

1. Запускает или останавливает компоненты программного комплекса в зависимости от настроек. Производит автоматический перезапуск компонентов, прекративших свою работу в результате сбоя. Осуществляет запуск одних компонентов по запросу от других компонентов. Информировывает запущенные компоненты программного комплекса об изменении состава запущенных компонентов.
2. Обеспечивает централизованный доступ всех компонентов к настройкам конфигурации. Предоставляет интерфейс для централизованного изменения параметров конфигурации уполномоченными компонентами. Выполняет оповещение всех заинтересованных компонентов об изменении настроек.
3. Предоставляет компонентам информацию из используемого лицензионного ключевого файла. Принимает от уполномоченных компонентов новые лицензионные данные. Оповещает запущенные компоненты программного комплекса при изменении лицензионных данных и параметров конфигурации.

Демон управления конфигурацией Dr.Web ConfigD всегда запускается с правами суперпользователя *root*. Он запускает остальные компоненты программного комплекса Dr.Web для Интернет-шлюзов UNIX и связывается с ними через предварительно открытый сокет. Демон управления конфигурацией принимает подключения от прочих компонентов программного комплекса через информационный сокет (публично доступный) и управляющий сокет (доступный только компонентам, запущенным с правами суперпользователя). Выполняет загрузку параметров конфигурации и лицензионных данных из файлов или обеспечивает их получение от используемого сервера централизованной защиты через агент централизованной защиты [Dr.Web ES Agent](#), а также подстановку корректных значений по умолчанию для параметров конфигурации. Поэтому



к моменту старта любого компонента или отсылки ему сигнала `SIGHUP`, демон управления конфигурацией всегда имеет целостный и непротиворечивый набор настроек всего комплекса Dr.Web для Интернет-шлюзов UNIX.

При получении сигнала `SIGHUP` демон управления конфигурацией перечитывает параметры конфигурации и данные из лицензионного ключевого файла, рассылая компонентам, при необходимости, уведомления о необходимости перечитывании их параметров конфигурации. При получении сигнала `SIGTERM` демон управления конфигурацией сначала завершает все компоненты, а только потом завершается сам. Демон управления конфигурацией обеспечивает удаление всех временных файлов компонентов после их завершения.

### Принципы взаимодействия с другими компонентами

1. Все компоненты используют только те параметры конфигурации и лицензионную информацию, которые они получили при запуске от демона управления конфигурацией Dr.Web ConfigD.
2. Демон обеспечивает схему сбора сообщений ото всех запущенных под его управлением компонентов в единый журнал. Все сообщения, которые любой из компонентов аварийно выводит в поток ошибок `stderr`, собираются демоном управления конфигурацией и помещаются в общий журнал программного комплекса с отметкой о том, какой компонент осуществил этот вывод.
3. При завершении работы управляемые компоненты должны вернуть код завершения. Если код завершения отличен от 101, 102 и 103, то демон управления конфигурацией перезапустит компонент. Таким образом, аварийное завершение компонента вызовет его перезапуск и сообщение из `stderr` в журнале программного комплекса.
  - При завершении любого компонента с кодом возврата 101, он будет запущен вновь только при изменении параметров лицензии. Так что если компонент не может работать в условиях предоставленной лицензии, он фиксирует это в поток `stderr` и завершает работу с кодом 101.
  - При завершении работы с кодом 102, компонент будет запущен снова только при изменении параметров конфигурации. Если полученные компонентом параметры конфигурации не позволяют ему работать, то компонент выводит сообщение об этом в поток `stderr` и завершает работу с кодом 102. Новая попытка запуска компонента демоном управления конфигурацией состоится тогда, когда поменяются какие-либо параметры конфигурации.
  - Компоненты, запускаемые демоном управления конфигурацией по требованию, при отсутствии обращений к ним (т.е. при простое) могут завершаться с кодом 103. Это такие компоненты, как [Dr.Web Scanning Engine](#) и [Dr.Web File Checker](#).
  - Если новые значения параметров конфигурации, полученные компонентом от демона управления конфигурацией, не могут быть применены им «на лету», т.е. если для этого требуется перезапуск, то компонент завершает работу с кодом 0, чтобы Dr.Web ConfigD перезапустил его.



- При невозможности подключения к демону управления конфигурацией или ошибке протокола взаимодействия, компонент фиксирует сообщение об этом в *stderr* и завершает работу с кодом 1.

#### 4. Обмен сигналами:

- Демон управления конфигурацией шлет компоненту сигнал *SIGHUP* для того, чтобы он применил измененные параметры конфигурации.
- Демон управления конфигурацией шлет компоненту сигнал *SIGTERM* для завершения работы компонента. Компонент обязан завершиться в течение 30 секунд.
- Сигнал *SIGKILL* используется демоном управления конфигурацией для принудительного завершения работы компонентов, не завершивших свою работу в течение 30 секунд после получения от него сигнала *SIGTERM*.

## Аргументы командной строки

Для запуска демона управления конфигурацией Dr.Web ConfigD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-configd [<параметры>]
```

Демон управления конфигурацией Dr.Web ConfigD допускает использование следующих параметров:

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

Данная 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 программного комплекса должен быть запущен в режиме демона. В штатном режиме Dr.Web ConfigD запускается при старте операционной системы, для чего он оснащен стандартным скриптом управления, помещаемым в каталог `/etc/init.d`. Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой](#) **drweb-ctl**).



Для получения справки о компоненте из командной строки используйте команду **man 1 drweb-configd**

## Параметры конфигурации

Демон управления конфигурацией Dr.Web ConfigD использует параметры, указанные в секции [Root] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>DefaultLogLevel</b> {уровень подробности}	Определяет <a href="#">уровень подробности</a> ведения журнала для всех компонентов продукта Dr.Web для Интернет-шлюзов UNIX по умолчанию.  <i>Используется, если в конфигурации какого-либо из компонентов не указан свой уровень подробности ведения журнала.</i>  <b>Значение по умолчанию:</b> Notice
<b>LogLevel</b> {уровень подробности}	<a href="#">Уровень подробности</a> ведения журнала компонента Dr.Web ConfigD.  <b>Значение по умолчанию:</b> Notice
<b>Log</b> {тип журнала}	<a href="#">Метод ведения журнала</a> демона управления конфигурацией, а также метод ведения журнала для тех компонентов, у которых не указан свой собственный метод ведения журнала.



	<p>Обратите внимание, что при начальной загрузке, пока конфигурационный файл еще не прочитан, демон управления конфигурацией будет использовать следующие значения этого параметра:</p> <ul style="list-style-type: none"><li>• В режиме демона (если был запущен с параметром <code>-d</code>) – <code>SYSLOG:Daemon</code></li><li>• В ином случае – <code>Stderr</code></li></ul> <p>Если компонент работает в фоновом режиме (запущен с параметром командной строки <code>-d</code>), значение <code>Stderr</code> <i>не может</i> быть использовано для данного параметра.</p> <p><b>Значение по умолчанию:</b> <code>Syslog:Daemon</code></p>
<b>PublicSocketPath</b> <i>{путь к файлу}</i>	<p>Путь к сокету, используемому для взаимодействия всех компонентов Dr.Web для Интернет-шлюзов UNIX.</p> <p><b>Значение по умолчанию:</b> <code>/var/run/.com.drweb.public</code></p>
<b>AdminSocketPath</b> <i>{путь к файлу}</i>	<p>Путь к сокету, используемому для взаимодействия компонентов Dr.Web для Интернет-шлюзов UNIX, обладающих повышенными (административными) полномочиями.</p> <p><b>Значение по умолчанию:</b> <code>/var/run/.com.drweb.admin</code></p>
<b>CoreEnginePath</b> <i>{путь к файлу}</i>	<p>Путь к динамической библиотеке антивирусного ядра Dr.Web Virus-Finding Engine.</p> <p><b>Значение по умолчанию:</b> <code>&lt;var_dir&gt;/lib/drweb32.dll</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/var/opt/drweb.com/lib/drweb32.dll</code></li><li>• Для <b>FreeBSD:</b> <code>/var/drweb.com/lib/drweb32.dll</code></li></ul>
<b>VirusBaseDir</b> <i>{путь к каталогу}</i>	<p>Путь к каталогу, в котором хранятся файлы вирусных баз.</p> <p><b>Значение по умолчанию:</b> <code>&lt;var_dir&gt;/bases</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/var/opt/drweb.com/bases</code></li><li>• Для <b>FreeBSD:</b> <code>/var/drweb.com/bases</code></li></ul>
<b>KeyPath</b> <i>{путь к файлу}</i>	<p>Путь к ключевому файлу продукта (лицензионному или демонстрационному).</p> <p><b>Значение по умолчанию:</b> <code>&lt;etc_dir&gt;/drweb32.key</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/etc/opt/drweb.com/drweb32.key</code></li><li>• Для <b>FreeBSD:</b> <code>/usr/local/etc/drweb.com/drweb32.key</code></li></ul>
<b>CacheDir</b> <i>{путь к каталогу}</i>	<p>Путь к каталогу кэша (используется как для кэша обновлений, так и для кэша проверенных файлов).</p> <p><b>Значение по умолчанию:</b> <code>&lt;var_dir&gt;/cache</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/var/opt/drweb.com/cache</code></li><li>• Для <b>FreeBSD:</b> <code>/var/drweb.com/cache</code></li></ul>





<b>TempDir</b>  {путь к каталогу}	Путь к каталогу для хранения временных файлов.  <b>Значение по умолчанию:</b> <i>Путь, извлеченный из системной переменной окружения TMPDIR, TMP, TEMP или TMPDIR (переменные перебираются в указанном порядке). Если ни одна из них не обнаружена, то /tmp.</i>
<b>RunDir</b>  {путь к каталогу}	Путь к каталогу, в котором находятся PID-файлы запущенных компонентов и сокеты, используемые для взаимодействия компонентов продукта.  <b>Значение по умолчанию:</b> /var/run
<b>VarLibDir</b>  {путь к каталогу}	Путь к каталогу библиотек, используемых компонентами продукта.  <b>Значение по умолчанию:</b> <var_dir>/lib <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /var/opt/drweb.com/lib</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/lib</li></ul>
<b>VersionDir</b>  {путь к каталогу}	Путь к каталогу, в котором хранится информация о текущих версиях используемых компонентов Dr.Web для Интернет-шлюзов UNIX.  <b>Значение по умолчанию:</b> <var_dir>/version <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /var/opt/drweb.com/version</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/version</li></ul>
<b>DwsDir</b>  {путь к каталогу}	Путь к каталогу, в котором хранятся файлы автоматически обновляемой базы данных категорий веб-ресурсов .  <b>Значение по умолчанию:</b> <var_dir>/dws <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /var/opt/drweb.com/dws</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/dws</li></ul>
<b>AdminGroup</b>  {имя группы   GID}	Группа пользователей, обладающих административными правами в рамках Dr.Web для Интернет-шлюзов UNIX. Данные пользователи наряду с суперпользователем root могут повышать полномочия компонентов Dr.Web для Интернет-шлюзов UNIX до полномочий суперпользователя.  <b>Значение по умолчанию:</b> <i>Определяется автоматически в момент установки продукта.</i>
<b>TrustedGroup</b>  {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.  <i>Обратите внимание, что в этом параметре нельзя указать несуществующую группу, поскольку в этом случае SpIDer Gate не сможет запуститься.</i>



	<p>Если значение параметра отсутствует, то в настройках SplDer Gate нельзя указать значение <code>Auto</code> для параметра <code>OutputDivert</code>.</p> <p><b>Значение по умолчанию:</b> <code>drweb</code></p>
<b>DebugIpc</b> {логический}	<p>Включать или нет в журнал на отладочном уровне (при <code>LogLevel = DEBUG</code>) подробные сообщения IPC (взаимодействие демона управления конфигурацией с другими компонентами).</p> <p><b>Значение по умолчанию:</b> <code>No</code></p>
<b>UseCloud</b> {логический}	<p>Использовать обращение к сервису Dr.Web Cloud для получения сведений о вредоносности файлов и URL.</p> <p><b>Значение по умолчанию:</b> <code>No</code></p>
<b>AntispamCorePath</b> {путь к файлу}	<p>Параметр не используется.</p> <p><b>Значение по умолчанию:</b> <code>&lt;var_dir&gt;/lib/vaderetro.so</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/var/opt/drweb.com/lib/vaderetro.so</code></li><li>• Для <b>FreeBSD:</b> <code>/var/drweb.com/lib/vaderetro.so</code></li></ul>
<b>VersionNotification</b> {логический}	<p>Уведомлять пользователя о наличии обновлений для обновления текущей установленной версии продукта.</p> <p><b>Значение по умолчанию:</b> <code>Yes</code></p>



## Dr.Web Ctl

Программный комплекс Dr.Web для Интернет-шлюзов UNIX позволяет осуществлять управление своей работой из командной строки операционной системы, для чего в его состав входит специальная утилита Dr.Web Ctl (**drweb-ctl**).

Имеется возможность выполнять из командной строки следующие действия:

- Запуск проверки файлов, загрузочных записей дисков и исполняемых файлов активных процессов.
- Запуск проверки файлов на удаленных узлах сети (см. примечание [ниже](#)).
- Запуск обновления антивирусных компонентов (вирусных баз, антивирусного ядра, и прочих, в зависимости от поставки).
- Просмотр и изменение параметров конфигурации Dr.Web для Интернет-шлюзов UNIX.
- Просмотр состояния компонентов программного комплекса и статистики обнаруженных угроз.
- Просмотр карантина и управление его содержимым (через компонент [Dr.Web File Checker](#)).
- Подключение к серверу централизованной защиты и отключение от него.

Для того, 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).



Обратите внимание, что для выполнения некоторых управляющих команд требуются полномочия суперпользователя.

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

Утилита Dr.Web Ctl поддерживает стандартное автодополнение вводимых команд управления, если функция автодополнения включена в используемой вами командной оболочке. В случае если командная оболочка не поддерживает автодополнение, вы можете настроить ее при необходимости. Для этого обратитесь к справочному руководству по используемому вами дистрибутиву операционной системы.



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

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

Коды всех имеющихся ошибок приведены в разделе [Приложение Е. Описание известных ошибок](#).

## Удаленная проверка узлов

Dr.Web для Интернет-шлюзов UNIX позволяет выполнить проверку на наличие угроз файлов, находящихся на удаленных узлах сети. В качестве таких узлов могут выступать не только полноценные вычислительные машины (рабочие станции и серверы), но и роутеры, ТВ-приставки и прочие «умные» устройства, образующие так называемый «Интернет вещей». Для выполнения удаленной проверки необходимо, чтобы удаленный узел предоставлял возможность удаленного терминального доступа через SSH (Secure Shell). Кроме этого необходимо знать IP-адрес или доменное имя удаленного узла, имя и пароль пользователя, который может совершить удаленный доступ к системе через SSH. Указанный пользователь должен иметь права доступа к проверяемым файлам (как минимум – право на их чтение).

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

Удаленная проверка реализуется только через утилиту управления из командной строки Dr.Web Ctl (используется [команда](#) `remotescan`).



## Формат вызова из командной строки

### 1. Формат вызова утилиты управления из командной строки

Утилита управления работой Dr.Web для Интернет-шлюзов UNIX 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 команд. Не являются обязательными для запуска.
- *<команда>* – команда, которая должна быть выполнена Dr.Web для Интернет-шлюзов UNIX (например, запустить проверку файлов, вывести содержимое карантина и т.п.).
- *<аргумент>* – аргумент команды. Зависит от указанной команды. У некоторых команд аргументы отсутствуют.
- *<опции команды>* – опции, управляющие работой указанной команды. Зависит от команды. У некоторых команд опции отсутствуют.

### 2. Общие опции

Доступны следующие общие опции:

Опция	Описание
-h, --help	Вывести на экран краткую общую справку и завершить работу. Для вывода справки по любой команде используйте вызов: <pre>\$ drweb-ctl &lt;команда&gt; -h</pre>
-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: <pre>\$ drweb-ctl &lt;команда&gt; -d</pre>

### 3. Команды

Команды управления Dr.Web для Интернет-шлюзов UNIX разделены на следующие группы:

- Команды [антивирусной проверки](#).



- Команды [управления обновлением](#) и работой в режиме централизованной защиты.
- Команды [управления конфигурацией](#).
- Команды [управления угрозами и карантином](#).
- [Информационные команды](#).




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

### 3.1. Команды антивирусной проверки


Доступны следующие команды антивирусной проверки файловой системы:

Команда	Описание
<code>scan &lt;путь&gt;</code>	<p><b>Назначение:</b> Инициировать проверку компонентом проверки файлов <a href="#">Dr.Web File Checker</a> указанного файла или каталога.</p> <p><b>Аргументы:</b></p> <p><code>&lt;путь&gt;</code> – путь к файлу или каталогу, который нужно проверить.</p> <p><i>Этот аргумент может быть опущен в случае использования опции <code>--stdin</code> или <code>--stdin0</code>. Для проверки перечня файлов, выбираемых по некоторому условию, рекомендуется использовать утилиту <b>find</b> (см. <a href="#">Примеры использования</a>) и опцию <code>--stdin</code> или <code>--stdin0</code>.</i></p> <p><b>Опции:</b></p> <p><code>-a [--Autonomous]</code> – запустить отдельную копию <a href="#">Dr.Web Scanning Engine</a> и <a href="#">Dr.Web File Checker</a> для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой <code>threats</code> (см. <a href="#">ниже</a>), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением.</p> <p><code>--stdin</code> – получить список путей для проверки из стандартного потока ввода (<code>stdin</code>). Пути в списке должны быть разделены символом новой строки (<code>'\n'</code>).</p> <p><code>--stdin0</code> – получить список путей для проверки из стандартного потока ввода (<code>stdin</code>). Пути в списке должны быть разделены нулевым символом NUL (<code>'\0'</code>).</p>



Команда	Описание
	<div> При использовании опций <code>--stdin</code> и <code>--stdin0</code> пути в списке не должны содержать шаблонов. Предпочтительное использование опций <code>--stdin</code> и <code>--stdin0</code> – обработка в команде <code>scan</code> списка путей, сформированного внешней программой, например – <b>find</b> (см. <a href="#">Примеры использования</a>).</div> <p><code>--Report &lt;тип&gt;</code> – установить тип отчета о проверке.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• BRIEF – краткий отчет.</li><li>• DEBUG – подробный отчет.</li></ul> <p><b>Значение по умолчанию:</b> <i>BRIEF</i></p> <p><code>--ScanTimeout &lt;число&gt;</code> – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение 0 указывает, что время проверки не ограничено.</p> <p><b>Значение по умолчанию:</b> 0</p> <p><code>--PackerMaxLevel &lt;число&gt;</code> – установить максимальный уровень вложенности объектов при проверке запакованных объектов.</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p><code>--ArchiveMaxLevel &lt;число&gt;</code> – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p><code>--MailMaxLevel &lt;число&gt;</code> – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p><code>--ContainerMaxLevel &lt;число&gt;</code> – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p><code>--MaxCompressionRatio &lt;степень&gt;</code> – установить максимальную допустимую степень сжатия проверяемых объектов.</p> <p>Должна быть не менее 2.</p> <p><b>Значение по умолчанию:</b> 3000</p> <p><code>--HeuristicAnalysis &lt;On Off&gt;</code> – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию:</b> <i>On</i></p>



Команда	Описание
	<p>--OnKnownVirus &lt;действие&gt; – <u>действие</u>, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза.</p> <p><b>Возможные действия:</b> REPORT, CURE, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p> <p>--OnIncurable &lt;действие&gt; – действие, которое следует выполнить в случае если лечение (CURE) обнаруженной угрозы окончилось неудачей или оно невозможно.</p> <p><b>Возможные действия:</b> REPORT, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p> <p>--OnSuspicious &lt;действие&gt; – действие, которое следует выполнить в случае если эвристический анализ обнаружит подозрительный объект.</p> <p><b>Возможные действия:</b> REPORT, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p> <p>--OnAdware &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена рекламная программа.</p> <p><b>Возможные действия:</b> REPORT, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p> <p>--OnDialers &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа дозвона.</p> <p><b>Возможные действия:</b> REPORT, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p> <p>--OnJokes &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа-шутка.</p> <p><b>Возможные действия:</b> REPORT, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p> <p>--OnRiskware &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа.</p> <p><b>Возможные действия:</b> REPORT, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p> <p>--OnHacktools &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа взлома.</p> <p><b>Возможные действия:</b> REPORT, QUARANTINE, DELETE.</p> <p><b>Значение по умолчанию:</b> REPORT</p>
	<div> Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления (DELETE) выполняется перемещение контейнера в карантин (QUARANTINE).</div>





Команда	Описание
<code>bootscan</code> <code>&lt;устройство&gt;   ALL</code>	<p><b>Назначение:</b> Инициировать проверку компонентом проверки файлов <a href="#">Dr.Web File Checker</a> загрузочной записи на указанных дисковых устройствах. Проверяются как записи MBR, так и записи VBR.</p> <p><b>Аргументы:</b></p> <p><code>&lt;устройство&gt;</code> – 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 <code>ALL</code>, будут проверены все загрузочные записи на всех доступных дисковых устройствах.</p> <p><b>Опции:</b></p> <p><code>-a [--Autonomous]</code> – запустить отдельную копию <a href="#">Dr.Web Scanning Engine</a> и <a href="#">Dr.Web File Checker</a> для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой <code>threats</code> (см. <a href="#">ниже</a>), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением.</p> <p><code>--Report &lt;mun&gt;</code> – установить тип отчета о проверке.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• <code>BRIEF</code> – краткий отчет.</li><li>• <code>DEBUG</code> – подробный отчет.</li></ul> <p><b>Значение по умолчанию:</b> <code>BRIEF</code></p> <p><code>--ScanTimeout &lt;число&gt;</code> – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение <code>0</code> указывает, что время проверки не ограничено.</p> <p><b>Значение по умолчанию:</b> <code>0</code></p> <p><code>--HeuristicAnalysis &lt;On Off&gt;</code> – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию:</b> <code>On</code></p> <p><code>--Cure &lt;Yes No&gt;</code> – требуется ли делать попытки лечения обнаруженных угроз.</p> <p>Если указано <code>No</code>, то производится только информирование об обнаруженной угрозе.</p> <p><b>Значение по умолчанию:</b> <code>No</code></p> <p><code>--ShellTrace</code> – включить вывод дополнительной отладочной информации при проверке загрузочной записи.</p>
<code>proscan</code>	<p><b>Назначение:</b> Инициировать проверку компонентом проверки файлов <a href="#">Dr.Web File Checker</a> содержимого исполняемых файлов, содержащих код процессов, запущенных в системе. При обнаружении угрозы выполняется</p>




Команда	Описание
	<p>не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него.</p> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b></p> <p><code>--a [--Autonomous]</code> – запустить отдельную копию <a href="#">Dr.Web Scanning Engine</a> и <a href="#">Dr.Web File Checker</a> для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой <code>threats</code> (см. <a href="#">ниже</a>), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением.</p> <p><code>--Report &lt;тип&gt;</code> – установить тип отчета о проверке.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• BRIEF – краткий отчет.</li><li>• DEBUG – подробный отчет.</li></ul> <p><b>Значение по умолчанию:</b> <i>BRIEF</i></p> <p><code>--ScanTimeout &lt;число&gt;</code> – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение <i>0</i> указывает, что время проверки не ограничено.</p> <p><b>Значение по умолчанию:</b> <i>0</i></p> <p><code>--HeuristicAnalysis &lt;On Off&gt;</code> – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию:</b> <i>On</i></p> <p><code>--PackerMaxLevel &lt;число&gt;</code> – установить максимальный уровень вложенности объектов при проверке упакованных объектов.</p> <p>Значение <i>0</i> указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> <i>8</i></p> <p><code>--OnKnownVirus &lt;действие&gt;</code> – <a href="#">действие</a>, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза.</p> <p><b>Возможные действия:</b> <i>REPORT, CURE, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p><code>--OnIncurable &lt;действие&gt;</code> – действие, которое следует выполнить в случае если лечение (<i>CURE</i>) обнаруженной угрозы окончилось неудачей или оно невозможно.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p><code>--OnSuspicious &lt;действие&gt;</code> – действие, которое следует выполнить в случае если эвристический анализ обнаружит подозрительный объект.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p>



Команда	Описание
	<p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnAdware &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена рекламная программа.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnDialers &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа дозвона.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnJokes &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа-шутка.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnRiskware &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnHacktools &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа взлома.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>Обратите внимание, что при обнаружении угроз в исполняемом файле все запущенные из него процессы принудительно завершаются Dr.Web для Интернет-шлюзов UNIX.</p>
netscan <путь>	<p><b>Назначение:</b> Инициировать распределенную проверку указанного файла или каталога через агент сетевой проверки данных <a href="#">Dr.Web Network Checker</a>. 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).</p> <p><b>Аргументы:</b></p> <p>&lt;путь&gt; – путь к файлу или каталогу, который нужно проверить.</p> <p><b>Опции:</b></p> <p>--Report &lt;mun&gt; – установить тип отчета о проверке.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• BRIEF – краткий отчет.</li><li>• DEBUG – подробный отчет.</li></ul>




Команда	Описание
	<p><b>Значение по умолчанию:</b> <i>BRIEF</i></p> <p>--ScanTimeout &lt;число&gt; – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение 0 указывает, что время проверки не ограничено.</p> <p><b>Значение по умолчанию:</b> 0</p> <p>--HeuristicAnalysis &lt;On Off&gt; – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию:</b> On</p> <p>--PackerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке запакованных объектов.</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ArchiveMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--MailMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ContainerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--MaxCompressionRatio &lt;степень&gt; – установить максимальную допустимую степень сжатия проверяемых объектов.</p> <p>Должна быть не менее 2.</p> <p><b>Значение по умолчанию:</b> 3000</p> <p>--Cure &lt;Yes No&gt; – требуется ли делать попытки лечения обнаруженных угроз.</p> <p>Если указано No, то производится только информирование об обнаруженной угрозе.</p> <p><b>Значение по умолчанию:</b> No</p>
flowscan <путь>	<p><b>Назначение:</b> Инициировать проверку компонентом проверки файлов <a href="#">Dr.Web File Checker</a> указанного файла или каталога с использованием <a href="#">метода проверки</a> «flow».</p> <div> Для проверки файлов и каталогов рекомендуется использовать команду scan.</div>



Команда	Описание
	<p><b>Аргументы:</b></p> <p>&lt;путь&gt; – путь к файлу или каталогу, который нужно проверить.</p> <p><b>Опции:</b></p> <p>--ScanTimeout &lt;число&gt; – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение 0 указывает, что время проверки не ограничено.</p> <p><b>Значение по умолчанию: 0</b></p> <p>--HeuristicAnalysis &lt;On Off&gt; – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию: On</b></p> <p>--PackerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке запакованных объектов.</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию: 8</b></p> <p>--ArchiveMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию: 8</b></p> <p>--MailMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию: 8</b></p> <p>--ContainerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию: 8</b></p> <p>--MaxCompressionRatio &lt;степень&gt; – установить максимальную допустимую степень сжатия проверяемых объектов.</p> <p>Должна быть не менее 2.</p> <p><b>Значение по умолчанию: 3000</b></p> <p>--OnKnownVirus &lt;действие&gt; – <u>действие</u>, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза.</p> <p><b>Возможные действия: REPORT, CURE, QUARANTINE, DELETE.</b></p> <p><b>Значение по умолчанию: REPORT</b></p> <p>--OnIncurable &lt;действие&gt; – действие, которое следует выполнить в случае если лечение (CURE) обнаруженной угрозы окончилось неудачей или оно невозможно.</p> <p><b>Возможные действия: REPORT, QUARANTINE, DELETE.</b></p>




Команда	Описание
	<p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnSuspicious &lt;действие&gt; – действие, которое следует выполнить в случае если эвристический анализ обнаружит подозрительный объект.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnAdware &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена рекламная программа.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnDialers &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа дозвона.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnJokes &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа-шутка.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnRiskware &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <p>--OnHacktools &lt;действие&gt; – действие, которое следует выполнить в случае если обнаружена программа взлома.</p> <p><b>Возможные действия:</b> <i>REPORT, QUARANTINE, DELETE.</i></p> <p><b>Значение по умолчанию:</b> <i>REPORT</i></p> <div> Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления (<i>DELETE</i>) выполняется перемещение контейнера в карантин (<i>QUARANTINE</i>).</div>
proxyscan <путь>	<p><b>Назначение:</b> Инициировать проверку компонентом проверки файлов <a href="#">Dr.Web File Checker</a> указанного файла или каталога с использованием <a href="#">метода проверки</a> «проху» (штатно этот метод проверки используется компонентом <a href="#">Dr.Web ClamD</a>).</p>



Команда	Описание
	<div><p>Обратите внимание, что угрозы, обнаруженные этим методом проверки, не будут добавлены в общий список обнаруженных угроз, выводимый командой <code>threats</code> (см. <a href="#">ниже</a>).</p><hr/><p>Для проверки файлов и каталогов рекомендуется использовать команду <code>scan</code>.</p></div> <p><b>Аргументы:</b></p> <p>&lt;путь&gt; – путь к файлу или каталогу, который нужно проверить.</p> <p><b>Опции:</b></p> <p>--Report &lt;тип&gt; – установить тип отчета о проверке.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• BRIEF – краткий отчет.</li><li>• DEBUG – подробный отчет.</li></ul> <p><b>Значение по умолчанию:</b> BRIEF</p> <p>--ScanTimeout &lt;число&gt; – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение 0 указывает, что время проверки не ограничено.</p> <p><b>Значение по умолчанию:</b> 0</p> <p>--HeuristicAnalysis &lt;On Off&gt; – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию:</b> On</p> <p>--PackerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке упакованных объектов.</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ArchiveMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--MailMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ContainerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p>




Команда	Описание
	<p><b>Значение по умолчанию:</b> 8</p> <p>--MaxCompressionRatio &lt;степень&gt; – установить максимальную допустимую степень сжатия проверяемых объектов.</p> <p>Должна быть не менее 2.</p> <p><b>Значение по умолчанию:</b> 3000</p>
rawscan <путь>	<p><b>Назначение:</b> Инициировать «сырую» проверку указанного файла или каталога, с использованием сканирующего ядра <a href="#">Dr.Web Scanning Engine</a> напрямую, без использования компонента проверки файлов <a href="#">Dr.Web File Checker</a>.</p> <div><p>Обратите внимание, что угрозы, обнаруженные при «сыром» сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой threats (см. <a href="#">ниже</a>).</p><hr/><p>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.</p></div> <p><b>Аргументы:</b></p> <p>&lt;путь&gt; – путь к файлу или каталогу, который нужно проверить.</p> <p><b>Опции:</b></p> <p>--ScanEngine &lt;путь&gt; – путь к UNIX-сокету сканирующего ядра Dr.Web Scanning Engine. Если не указан, то для проверки будет запущена автономная копия сканирующего ядра (будет завершена после завершения проверки).</p> <p>--Report &lt;тип&gt; – установить тип отчета о проверке.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• BRIEF – краткий отчет.</li><li>• DEBUG – подробный отчет.</li></ul> <p><b>Значение по умолчанию:</b> BRIEF</p> <p>--ScanTimeout &lt;число&gt; – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение 0 указывает, что время проверки не ограничено.</p>





Команда	Описание
	<p><b>Значение по умолчанию:</b> 0</p> <p>--PackerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке запакованных объектов.</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ArchiveMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--MailMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ContainerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--MaxCompressionRatio &lt;степень&gt; – установить максимальную допустимую степень сжатия проверяемых объектов.</p> <p>Должна быть не менее 2.</p> <p><b>Значение по умолчанию:</b> 3000</p> <p>--HeuristicAnalysis &lt;On Off&gt; – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию:</b> On</p> <p>--Cure &lt;Yes No&gt; – требуется ли делать попытки лечения обнаруженных угроз.</p> <p>Если указано No, то производится только информирование об обнаруженной угрозе.</p> <p><b>Значение по умолчанию:</b> No</p> <p>--ListCleanItem – включить вывод списка чистых файлов при проверке контейнера.</p> <p>--ShellTrace – включить вывод дополнительной отладочной информации при проверке файла.</p>
remotescan <узел> <путь>	<p><b>Назначение:</b> Инициировать проверку указанного файла или каталога на указанном удаленном узле, подключившись к нему через SSH.</p>



Команда	Описание
	<div><p>Обратите внимание, что угрозы, обнаруженные при удаленном сканировании, не будут нейтрализованы, а также они не будут добавлены в общий список обнаруженных угроз, выводимый командой <code>threats</code> (см. <a href="#">ниже</a>).</p></div> <div><p>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 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.</p></div> <p><b>Аргументы:</b></p> <p>&lt;узел&gt; – IP-адрес или доменное имя узла, к которому необходимо подключиться для проверки.</p> <p>&lt;путь&gt; – путь к файлу или каталогу, который нужно проверить.</p> <p><b>Опции:</b></p> <p>-l [--Login] &lt;имя&gt; – логин (имя пользователя) для авторизации на удаленном узле через SSH.</p> <p><i>Если имя пользователя не указано, будет произведена попытка подключиться к удаленному узлу от имени пользователя, запустившего команду.</i></p> <p>-i [--Identity] &lt;путь к файлу&gt; – файл закрытого ключа для аутентификации указанного пользователя через SSH.</p> <p>-p [--Port] &lt;число&gt; – номер порта на удаленном узле для подключения через SSH.</p> <p><b>Значение по умолчанию:</b> 22</p> <p>--Password &lt;пароль&gt; – пароль для аутентификации указанного пользователя через SSH.</p> <p><i>Обратите внимание, что пароль передается в открытом виде.</i></p> <p>--Report &lt;тип&gt; – установить тип отчета о проверке.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• BRIEF – краткий отчет.</li></ul>



Команда	Описание
	<ul style="list-style-type: none"><li>• DEBUG – подробный отчет.</li></ul> <p><b>Значение по умолчанию:</b> <i>BRIEF</i></p> <p>--ScanTimeout &lt;число&gt; – установить тайм-аут на проверку одного файла в мс.</p> <p>Значение 0 указывает, что время проверки не ограничено.</p> <p><b>Значение по умолчанию:</b> 0</p> <p>--PackerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке запакованных объектов.</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ArchiveMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--MailMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--ContainerMaxLevel &lt;число&gt; – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.).</p> <p>Значение 0 указывает, что вложенные объекты будут пропущены.</p> <p><b>Значение по умолчанию:</b> 8</p> <p>--MaxCompressionRatio &lt;степень&gt; – установить максимальную допустимую степень сжатия проверяемых объектов.</p> <p>Должна быть не менее 2.</p> <p><b>Значение по умолчанию:</b> 3000</p> <p>--HeuristicAnalysis &lt;On Off&gt; – использовать ли эвристический анализ при проверке.</p> <p><b>Значение по умолчанию:</b> On</p>





### 3.2. Команды управления обновлением и работой в режиме централизованной защиты

Доступны следующие команды управления обновлением и работой в режиме централизованной защиты:

Команда	Описание
update	<b>Назначение:</b> Инициировать процесс обновления антивирусных компонентов (вирусных баз и антивирусного ядра, и прочих, в зависимости от поставки) с серверов обновлений компании «Доктор Веб»
esconnect <сервер> [ : <порт> ]	<b>Назначение:</b> Подключить Dr.Web для Интернет-шлюзов UNIX к указанному серверу централизованной защиты (например, Dr.Web Enterprise Server). О режимах работы см. в разделе <a href="#">Режимы работы</a> .  <b>Аргументы:</b> <ul style="list-style-type: none"><li>• &lt;сервер&gt; – IP-адрес или имя узла в сети, на котором располагается сервер централизованной защиты. Обязательный аргумент.</li><li>• &lt;порт&gt; – номер порта, используемого сервером централизованной защиты. Необязательный аргумент, указывается только в случае, если сервер централизованной защиты использует нестандартный порт.</li></ul> <b>Опции:</b> <ul style="list-style-type: none"><li>--Key &lt;путь&gt; – путь к файлу публичного ключа сервера централизованной защиты, к которому производится подключение.</li><li>--Login &lt;ID&gt; – логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты.</li><li>--Password &lt;пароль&gt; – пароль для подключения к серверу централизованной защиты.</li><li>--Group &lt;ID&gt; – идентификатор группы на сервере, в которую следует поместить рабочую станцию при подключении.</li><li>--Rate &lt;ID&gt; – идентификатор тарифной группы, которую следует применить к рабочей станции при ее включении в группу на сервере централизованной защиты (может быть указана только совместно с опцией --Group).</li><li>--Compress &lt;On Off&gt; – принудительно инициировать сжатие передаваемых данных (On) или запретить его (Off). Если опция не указана, использование сжатия определяется сервером.</li><li>--Encrypt &lt;On Off&gt; – принудительно инициировать шифрование передаваемых данных (On) или запретить его (Off). Если опция не указана, использование шифрования определяется сервером.</li><li>--Newbie – подключиться как «новичок» (получить новую учетную запись на сервере).</li></ul>




Команда	Описание
	 Для выполнения этой команды требуется, чтобы <b>drweb-ctl</b> была запущена от имени суперпользователя (пользователя <i>root</i> ). При необходимости используйте команды <b>su</b> или <b>sudo</b> .
esdisconnect	<p><b>Назначение:</b> Отключить Dr.Web для Интернет-шлюзов UNIX от сервера централизованной защиты и перевести его в одиночный режим работы.</p> <p><i>Команда не имеет смысла, если Dr.Web для Интернет-шлюзов UNIX уже работает в одиночном режиме (standalone mode).</i></p> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b> Нет.</p>  Для выполнения этой команды требуется, чтобы <b>drweb-ctl</b> была запущена от имени суперпользователя (пользователя <i>root</i> ). При необходимости используйте команды <b>su</b> или <b>sudo</b> .

### 3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
cfset <секция> . <параметр> <значение>	<p><b>Назначение:</b> Изменить активное значение указанного параметра текущей конфигурации.</p> <p><i>Обратите внимание, что знак равенства не используется.</i></p> <p><b>Аргументы:</b></p> <ul style="list-style-type: none"><li>• &lt;секция&gt; – имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент.</li><li>• &lt;параметр&gt; – имя изменяемого параметра. Обязательный аргумент.</li><li>• &lt;значение&gt; – значение, которое следует присвоить изменяемому параметру. Обязательный аргумент.</li></ul> <p><i>Для задания значения параметров всегда используется формат &lt;секция&gt; . &lt;параметр&gt; &lt;значение&gt;.</i></p>



Команда	Описание
	<p>Обратите внимание, что если вы хотите задать несколько значений параметра, то нужно повторить вызов команды <code>cfset</code> столько раз, сколько значений параметра вы хотите добавить. При этом для добавления нового значения в список значений параметра необходимо использовать опцию <code>-a</code> (см. ниже). Нельзя использовать вариант команды <code>&lt;параметр&gt; значение1, значение2</code>, так как строка <code>значение1, значение2</code> будет считаться единым значением параметра.</p> <p>Описание конфигурационного файла доступно в разделе <a href="#">Приложение Г. Конфигурационный файл программного комплекса</a>, а также в документации <b>man 5 drweb.ini</b>.</p> <p><b>Опции:</b></p> <p><code>-a [--Add]</code> – не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). Также эту опцию следует использовать для добавления новых групп параметров с тегом.</p> <p><code>-e [--Erase]</code> – не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). Также эту опцию можно использовать для удаления группы параметров с тегом целиком.</p> <p><code>-r [--Reset]</code> – сбросить параметр в значение по умолчанию. <code>&lt;значение&gt;</code> в этом случае в команде не указывается, а если указано – игнорируется.</p> <p>Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе – список значений) заменяется на указанное значение.</p> <p>Для секций, описывающих индивидуальные параметры точек подключения компонента <a href="#">Dr.Web ClamD</a>, применение опции <code>-r</code> приводит к замене значения параметра в индивидуальной секции на значение, указанное у соответствующего «родительского» параметра в секции настроек компонента.</p> <p>Если требуется добавить новую <a href="#">точку подключения</a> <code>&lt;point&gt;</code> для Dr.Web ClamD, используйте команду:</p> <pre>cfset ClamD.Endpoint.&lt;point&gt; -a, например: cfset ClamD.Endpoint.point1 -a</pre> <div> Для выполнения этой команды требуется, чтобы <b>drweb-ctl</b> была запущена от имени суперпользователя (пользователя <i>root</i>). При необходимости используйте команды <b>su</b> или <b>sudo</b>.</div>



Команда	Описание
<code>cfshow</code> [ <секция> ] [ . <параметр> ]	<p><b>Назначение:</b> Вывести на экран параметры текущей конфигурации программного комплекса. Для вывода параметров по умолчанию используется формат &lt;секция&gt;.&lt;параметр&gt; = &lt;значение&gt;. Секции и параметры не установленных компонентов по умолчанию не выводятся.</p> <p><b>Аргументы:</b></p> <ul style="list-style-type: none"><li>• &lt;секция&gt; – имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла.</li><li>• &lt;параметр&gt; – 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.</li></ul> <p><b>Опции:</b></p> <p>--Uncut – вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. В противном случае выводятся только те параметры, которые используются имеющимися компонентами.</p> <p>--Changed – вывести только те параметры, для которых заданы значения, отличающиеся от значений по умолчанию.</p> <p>--Ini – вывести значения параметров в формате INI-файла: сначала в отдельной строке выводится имя секции, заключенное в квадратные скобки, после чего параметры, принадлежащие секции, перечисляются в виде пар &lt;параметр&gt; = &lt;значение&gt; (по одному в строке).</p> <p>--Value – вывести только значение указанного параметра. В этом случае аргумент &lt;параметр&gt; обязателен.</p>
<code>reload</code>	<p><b>Назначение:</b> Послать сигнал <code>SIGHUP</code> демону управления конфигурацией <a href="#">Dr.Web ConfigD</a>.</p> <p>Получив этот сигнал, Dr.Web ConfigD перечитывает <a href="#">конфигурацию</a> и рассылает ее изменения всем компонентам Dr.Web для Интернет-шлюзов UNIX; переоткрывает журнал программного комплекса; перезагружает компоненты, использующие вирусные базы (включая антивирусное ядро), а также пытается перезапустить компоненты, работа которых была нештатно завершена.</p> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b> Нет.</p>



### 3.4. Команды управления угрозами и карантином

Доступны следующие команды управления угрозами и карантином:

Команда	Описание
threats [ <действие> <объект> > ]	<p><b>Назначение:</b> Выполнить указанное действие с обнаруженными ранее угрозами по их идентификаторам. Тип действия определяется указанной опцией команды.</p> <p>Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. Для каждой угрозы выводится следующая информация:</p> <ul style="list-style-type: none"><li>• Идентификатор, присвоенный угрозе (порядковый номер)</li><li>• Полный путь к инфицированному файлу</li><li>• Информация об угрозе (имя, тип по классификации компании «Доктор Веб»)</li><li>• Информация о файле: размер, пользователь-владелец, дата последнего изменения</li><li>• История действий с инфицированным файлом: обнаружение, применявшиеся действия и т.п.</li></ul> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b></p> <p><code>-f [--Follow]</code> – выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (CTRL+C прерывает ожидание).</p> <p><i>Если эта опция указана совместно с любой из опций-действий, она игнорируется.</i></p> <p><code>--Cure &lt;список угроз&gt;</code> – выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую).</p> <p><code>--Quarantine &lt;список угроз&gt;</code> – выполнить перемещение в <a href="#">карантин</a> перечисленных угроз (идентификаторы угроз перечисляются через запятую).</p> <p><code>--Delete &lt;список угроз&gt;</code> – выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую).</p> <p><code>--Ignore &lt;список угроз&gt;</code> – игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую).</p> <p>Если требуется применить данную команду ко всем обнаруженным угрозам, вместо &lt;список угроз&gt; следует указать All. Например, команда:</p> <pre>\$ drweb-ctl threats --Quarantine All</pre> <p>перемещает в карантин все обнаруженные объекты с угрозами.</p>





Команда	Описание
<code>quarantine</code> [<действие> <объект>] >]	<p><b>Назначение:</b> Применить действие к указанному объекту, находящемуся в <a href="#">карантине</a>.</p> <p>Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине, с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в карантин. Для каждого изолированного объекта выводится следующая информация:</p> <ul style="list-style-type: none"><li>• Идентификатор, присвоенный изолированному объекту в карантине</li><li>• Исходный путь к файлу, перемещенному в карантин</li><li>• Дата перемещения файла в карантин</li><li>• Информация о файле: размер, пользователь-владелец, дата последнего изменения</li><li>• Информация об угрозе (имя, тип по классификации компании «Доктор Веб»)</li></ul> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b></p> <p><code>-a [--Autonomous]</code> – запустить отдельную копию компонента проверки файлов <a href="#">Dr.Web File Checker</a> для выполнения заданного действия с карантином, завершив его работу после окончания действия.</p> <p><i>Эта опция может быть применена совместно с любой из опций, указанных ниже.</i></p> <p><code>--Delete &lt;объект&gt;</code> – удалить указанный объект из карантина.</p> <p><i>Обратите внимание, что удаление из карантина – необратимая операция.</i></p> <p><code>--Cure &lt;объект&gt;</code> – попытаться вылечить указанный объект в карантине.</p> <p><i>Обратите внимание, что, даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина следует воспользоваться командой восстановления <code>--Restore</code>.</i></p> <p><code>--Restore &lt;объект&gt;</code> – восстановить указанный объект из карантина в исходное место.</p> <p><i>Обратите внимание, что для выполнения этой команды может потребоваться, чтобы <b>drweb-ctl</b> была запущена от имени суперпользователя. Восстановить файл из карантина можно, даже если он инфицирован.</i></p> <p><code>--TargetPath &lt;путь&gt;</code> – восстановить объект из карантина в указанное место: как файл с указанным именем, если <code>&lt;путь&gt;</code> – это путь к файлу, или в указанный каталог (если <code>&lt;путь&gt;</code> – это путь к каталогу). Применяется только совместно с командой восстановления <code>--Restore</code>.</p>



Команда	Описание
	<p>В качестве &lt;объект&gt; используется идентификатор объекта в карантине. Если требуется применить данную команду ко всем объектам, находящимся в карантине, вместо &lt;объект&gt; следует указать All. Например, команда:</p> <pre>\$ drweb-ctl quarantine --Restore All</pre> <p>восстанавливает из карантина все имеющиеся в нем объекты.</p> <p><i>Обратите внимание, что для варианта --Restore All дополнительная опция --TargetPath, если указана, должна задавать путь к каталогу, а не к файлу.</i></p>

### 3.5. Информационные команды


Доступны следующие информационные команды:

Команда	Описание
appinfo	<p><b>Назначение:</b> Вывести на экран информацию о работающих компонентах Dr.Web для Интернет-шлюзов UNIX.</p> <p>Для каждого запущенного компонента выводится следующая информация:</p> <ul style="list-style-type: none"><li>• Внутреннее имя</li><li>• Идентификатор процесса <b>GNU/Linux</b> (PID)</li><li>• Состояние (запущен, остановлен и т.п.)</li><li>• Код ошибки, если работа компонента завершена вследствие ошибки</li><li>• Дополнительная информация (опционально).</li></ul> <p>Для демона управления конфигурацией Dr.Web ConfigD в качестве дополнительной информации выводятся:</p> <ul style="list-style-type: none"><li>• Перечень установленных компонентов – <i>Installed</i></li><li>• Перечень компонентов, запуск которых должен быть обеспечен демоном – <i>Should run</i>.</li></ul> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b></p> <p><code>-f [--Follow]</code> – выполнять ожидание поступления новых сообщений об изменении состояния компонентов и выводить их на экран сразу, как только они будут поступать (нажатие CTRL+C прерывает ожидание).</p>
baseinfo	<p><b>Назначение:</b> Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз.</p> <p>Выводится следующая информация:</p>



Команда	Описание
	<ul style="list-style-type: none"><li>• Версия антивирусного ядра</li><li>• Дата и время выпуска используемых вирусных баз</li><li>• Число доступных вирусных записей</li><li>• Момент последнего успешного обновления вирусных баз и антивирусного ядра</li><li>• Момент следующего запланированного автоматического обновления</li></ul> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b> Нет.</p>
certificate	<p><b>Назначение:</b> Вывести на экран содержимое доверенного сертификата Dr.Web, который используется Dr.Web для Интернет-шлюзов UNIX. Для сохранения сертификата в файл <code>&lt;cert_name&gt;.pem</code> вы можете использовать команду:</p> <pre>\$ drweb-ctl certificate &gt; &lt;cert_name&gt;.pem</pre> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b> Нет.</p>
idpass <идентификатор>	<p><b>Назначение:</b> 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 <b>RepackPassword</b> был установлен в значение <b>НМАС (&lt;secret&gt;)</b>).</p> <p><b>Аргументы:</b></p> <ul style="list-style-type: none"><li>• <code>&lt;идентификатор&gt;</code> – идентификатор сообщения электронной почты.</li></ul> <p><b>Опции:</b></p> <p><code>-s [--Secret] &lt;secret&gt;</code> – Секретное слово, использованное для генерации пароля архива.</p> <p><i>Если секретное слово не указано при вызове команды, будет использовано текущее секретное слово &lt;secret&gt;, указанное в настройках Dr.Web MailD. Если при этом параметр RepackPassword отсутствует или установлен в значение, отличное от НМАС (&lt;secret&gt;), команда вернет ошибку.</i></p>
license	<p><b>Назначение:</b> Вывести на экран информацию об активной лицензии, получить демонстрационную лицензию или получить ключевой файл для уже зарегистрированной лицензии (например – на сайте компании).</p> <p>Если не указана ни одна опция, то выводится следующая информация (если используется лицензия для одиночного режима работы):</p>



Команда	Описание
	<ul style="list-style-type: none"><li>• Номер лицензии</li><li>• Дата и время окончания действия лицензии</li></ul> <p>Если используется лицензия, выданная сервером централизованной защиты (для работы в режиме централизованной защиты или в мобильном режиме), выводится соответствующая информация.</p> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b></p> <p>--GetRegistered &lt;серийный номер&gt; – 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).</p> <p><i>Если серийный номер не является серийным номером демонстрационного периода, то он должен быть предварительно зарегистрирован на сайте компании.</i></p> <p>Подробнее о лицензировании продуктов Dr.Web см. раздел <a href="#">Лицензирование</a>.</p> <div> Для регистрации серийного номера требуется наличие подключения к сети Интернет.</div>
stat	<p><b>Назначение:</b> Вывести на экран статистику работы компонентов, обрабатывающих файлы (нажатие CTRL+C или Q прерывает отображение статистики) или агента сетевой проверки данных <a href="#">Dr.Web Network Checker</a>.</p> <p>В статистике отображается:</p> <ul style="list-style-type: none"><li>• имя компонента, инициировавшего проверку файлов.</li><li>• PID компонента.</li><li>• усреднённое количество файлов, обрабатываемых в секунду за последнюю минуту, 5 минут, 15 минут.</li><li>• процент использования кэша проверенных файлов.</li><li>• среднее количество ошибок проверки в секунду.</li></ul> <p>Для агента распределенной проверки на экран выводится:</p> <ul style="list-style-type: none"><li>• перечень локальных клиентов, инициировавших сканирование.</li><li>• перечень удаленных узлов, которым переданы файлы на сканирование.</li><li>• перечень удаленных узлов, от которых получены файлы на сканирование.</li></ul> <p>Для локальных клиентов агента распределенной проверки указывается имя и PID, а для удаленных – адрес и порт узла.</p> <p>Для каждого клиента, как локального, так и удаленного выводится:</p> <ul style="list-style-type: none"><li>• среднее за секунду количество проверенных файлов.</li></ul>



Команда	Описание
	<ul style="list-style-type: none"><li>• среднее за секунду количество переданных и полученных байт.</li><li>• среднее за секунду количество ошибок.</li></ul> <p><b>Аргументы:</b> Нет.</p> <p><b>Опции:</b></p> <p><code>-n [--netcheck]</code> – Вывести на экран статистику работы агента сетевой проверки данных.</p>

## Примеры использования

Примеры использования утилиты Dr.Web Ctl (**drweb-ctl**):

### 1. Проверка объектов

#### 1.1. Простые команды проверки

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

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

2. Выполнить проверку списка путей, перечисленных в файле `daily_scan` (по одному пути в строке файла):

```
$ drweb-ctl scan --stdin < daily_scan
```

3. Выполнить проверку загрузочной записи на диске **sda**:

```
$ drweb-ctl bootscan /dev/sda
```

4. Выполнить проверку запущенных процессов:

```
$ drweb-ctl procscan
```

#### 1.2. Проверка файлов, отобранных по критериям

В нижеприведенных примерах для формирования выборки файлов, подлежащих проверке, используется результат работы утилиты **find**. Полученный перечень файлов передается команде **drweb-ctl scan** с параметром `--stdin` или `--stdin0`.

1. Выполнить проверку списка файлов, возвращенных утилитой **find**, и разделенных символом NUL (`'\0'`):

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Проверить все файлы всех каталогов, начиная с корневого, находящихся на одном разделе файловой системы:



```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Проверить все файлы всех каталогов, начиная с корневого, кроме файлов `/var/log/messages` и `/var/log/syslog`:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog | drweb-ctl scan --stdin
```

4. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователю `root`:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям `root` и `admin`:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям с UID из диапазона 1000 – 1005:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Проверить файлы во всех каталогах, начиная с корневого, но находящихся не более чем на пятом уровне вложенности относительно корневого каталога:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Проверить файлы в корневом каталоге, не заходя во вложенные каталоги:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Проверить файлы во всех каталогах, начиная с корневого, при этом следовать по встречающимся символическим ссылкам:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Проверить файлы во всех каталогах, начиная с корневого, при этом не следовать по встречающимся символическим ссылкам:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Проверить во всех каталогах, начиная с корневого, файлы, созданные не позже, чем 01 мая 2017 года:

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

### 1.3. Проверка дополнительных объектов

1. Проверка объектов, расположенном в каталоге `/tmp` на удаленном узле `192.168.0.1`, подключившись к нему через SSH как пользователь `user` с паролем `passw`:



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

## 2. Управление конфигурацией

1. Вывести на экран информацию о текущем составе программного комплекса, включая информацию о запущенных компонентах:

```
$ drweb-ctl appinfo
```

2. Вывести на экран все параметры из [секции](#) [Root] активной конфигурации:

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

3. Задать значение 'No' для параметра **Start** в секции [ClamD] активной конфигурации (это приведет к остановке работы компонента [Dr.Web ClamD](#)):

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

Обратите внимание на то, что в данном случае требуются полномочия суперпользователя. Пример вызова этой же команды с использованием **sudo** для временного повышения полномочий:

```
$ sudo drweb-ctl cfset ClamD.Start No
```

4. Запретить компоненту обновления выполнять получение обновлений файлов 123.vdb и 567.dws:

```
# drweb-ctl cfset Update.ExcludedFiles -a 123.vdb  
# drweb-ctl cfset Update.ExcludedFiles -a 567.dws
```

Обратите внимание на то, что в данном случае используется опция **-a** для добавления нового значения к уже имеющемуся списку значений параметра **Update.ExcludedFiles**.

5. Удалить файл 123.vdb из списка файлов, обновление которых запрещено для компонента обновления:

```
# drweb-ctl cfset Update.ExcludedFiles -r 123.vdb
```

6. Сбросить список файлов, обновление которых запрещено для компонента обновления, в значение по умолчанию:

```
# drweb-ctl cfset Update.ExcludedFiles -e
```

7. Выполнить принудительное обновление антивирусных компонентов продукта:

```
$ drweb-ctl update
```

8. Выполнить перезагрузку конфигурации для компонентов установленного программного комплекса Dr.Web:



```
# drweb-ctl reload
```

Обратите внимание на то, что в данном случае требуются полномочия суперпользователя. Пример вызова этой же команды с использованием **sudo** для временного повышения полномочий:

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

9. Подключить продукт к серверу [централизованной защиты](#), работающему на узле `192.168.0.1`, при условии, что открытый ключ сервера располагается в файле `/home/user/cskey.pub`:

```
$ drweb-ctl esconnect 192.168.0.1 --Key /home/user/cskey.pub
```

10. Отключить продукт от сервера централизованной защиты:

```
# drweb-ctl esdisconnect
```

Обратите внимание на то, что в данном случае требуются полномочия суперпользователя. Пример вызова этой же команды с использованием **sudo** для временного повышения полномочий:

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

### 3. Управление угрозами

1. Вывести на экран информацию об обнаруженных угрозах:

```
$ drweb-ctl threats
```

2. Переместить все файлы, содержащие необезвреженные угрозы, в карантин:

```
$ drweb-ctl threats --Quarantine All
```

3. Вывести на экран список файлов, перемещенных в карантин:

```
$ drweb-ctl quarantine
```

4. Восстановить все файлы из карантина:

```
$ drweb-ctl quarantine --Restore All
```

### 4. Пример работы в режиме автономной копии

1. Проверить файлы и обработать карантин в режиме автономной копии:

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

Первая команда проверит файлы в каталоге `/home/user` в режиме автономной копии, и файлы, содержащие известные вирусы, будут помещены в карантин. Вторая команда





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

## Параметры конфигурации

Утилита управления из командной строки Dr.Web Ctl не имеет собственной секции параметров в объединенном [конфигурационном файле](#) продукта Dr.Web для Интернет-шлюзов UNIX. Она использует параметры, указанные в [секции](#) [Root].



## Веб-интерфейс управления Dr.Web

Веб-интерфейс управления Dr.Web для Интернет-шлюзов UNIX позволяет выполнять следующие действия:

1. Просматривать состояние компонентов программного комплекса, запускать и останавливать работу некоторых из них.
2. Просматривать состояние обновлений и запускать обновление вручную при необходимости.
3. Просматривать состояние лицензии и загружать лицензионный ключ при необходимости.
4. Просматривать перечень обнаруженных угроз и управлять содержимым карантина (отображаются только угрозы, обнаруженные в файлах локальной файловой системы при помощи компонента [Dr.Web File Checker](#)).
5. Выполнять редактирование настроек компонентов Dr.Web для Интернет-шлюзов UNIX.
6. Подключать программный комплекс к серверу централизованной защиты или переводить его в автономный режим работы.
7. Запускать проверку локальных файлов по требованию (в том числе – перетаскиванием их на страницу, открытую в браузере).

## Системные требования веб-интерфейса

Корректная работа веб-интерфейса управления гарантируется в следующих браузерах:

- **Internet Explorer** – версия 11 и новее.
- **Mozilla Firefox** – версия 25 и новее.
- **Google Chrome** – версия 30 и новее.

## Доступ к управлению через веб-интерфейс

Для доступа к веб-интерфейсу необходимо в адресной строке браузера ввести адрес вида:

```
https://<host_with_drweb>:<port>/
```

где *<host\_with\_drweb>* – IP-адрес или имя узла, на котором работает продукт, в составе которого функционирует сервер веб-интерфейса Dr.Web HTTPD, а *<port>* – порт на этом узле, прослушиваемый Dr.Web HTTPD. Для доступа к компонентам продукта, работающего на локальном узле, достаточно использовать IP-адрес 127.0.0.1 или имя localhost. При [настройках](#) по умолчанию *<port>* равен 4443.

Таким образом, для доступа к веб-интерфейсу на локальном компьютере при настройках по умолчанию необходимо ввести адрес:

```
https://127.0.0.1:4443/
```



В случае успешного подключения к серверу управления, на экране появится стартовая страница, содержащая форму аутентификации. Для доступа к управлению необходимо пройти аутентификацию, введя в соответствующие поля формы логин и пароль пользователя, обладающего административными полномочиями на узле, на котором функционирует программный комплекс.

## Главное меню

В левой части страниц веб-интерфейса управления, открывающихся после успешного прохождения аутентификации, расположено главное меню, пункты которого позволяют выполнить следующее:

- **Главная** – открывает [главную страницу](#), на которой отображается перечень установленных компонентов Dr.Web для Интернет-шлюзов UNIX и их состояние.
- **Угрозы** – открывает страницу, [отображающую все угрозы](#), обнаруженные на сервере. В этом разделе вы можете осуществлять управление обнаруженными угрозами, в том числе – перемещать инфицированные объекты в карантин, осуществлять повторную проверку, лечение и удаление вредоносных объектов.
- **Настройки** – открывает страницу управления [настройками компонентов](#) Dr.Web для Интернет-шлюзов UNIX, установленных на сервере.
- **Информация** – открывает страницу просмотра краткой информации о версии веб-интерфейса и состоянии вирусных баз.
- **Справка** – открывает (в новой вкладке браузера) справку по установленным компонентам продукта.
- **Проверить файл** – показывает панель оперативной [проверки файлов](#), которая будет доступна поверх любой страницы веб-интерфейса до момента ее закрытия.
- **Выйти** – завершает сеанс работы текущего пользователя с веб-интерфейсом управления.

## Управление компонентами

Просмотр перечня компонентов, включенных в состав Dr.Web для Интернет-шлюзов UNIX, и управление их работой осуществляются на странице **Главная**.

Отображаемые компоненты продукта разделены на две части: основные, выполняющие обнаружение угроз, и сервисные, обеспечивающие корректную работу продукта в целом. Перечень основных компонентов отображается в виде таблицы, расположенной в верхней части страницы (перечень компонентов в таблице зависит от поставки продукта). Для каждого компонента указывается:

1. **Название.** Щелчок мышью по названию позволяет перейти к [странице настроек](#) этого компонента;
2. **Состояние.** Состояние, в котором находится компонент, иллюстрируется переключателем и текстовой подписью, отображающей текущее состояние, в котором он находится. Чтобы запустить компонент или приостановить его работу, достаточно щелкнуть мышью по переключателю. Возможные состояния переключателя:



	– Компонент отключен и не используется;
	– Компонент включен и корректно функционирует;
	– Компонент включен, но не функционирует вследствие произошедшей ошибки.

Если в работе компонента произошла ошибка, вместо состояния выводится сообщение об ошибке. Щелчок мышью по значку выводит на экран всплывающее окно с подробной информацией о произошедшей ошибке и рекомендациями по ее устранению.

3. **Средняя нагрузка.** Среднее число файлов, обработанных компонентом за секунду в течение последней минуты, 5 минут, 15 минут (три числа, разделенных косой чертой).
4. **Ошибки.** Среднее число ошибок за секунду, произошедших с компонентом в течение последней минуты, 5 минут, 15 минут (три числа, разделенных косой чертой).

При наведении курсора мыши на значок можно получить всплывающую подсказку.

Под таблицей основных компонентов в виде набора плиток перечисляются вспомогательные компоненты продукта (такие, как [сканирующее ядро](#), [компонент проверки файлов](#) и т.д.). Для них также указываются состояние и статистика их работы. Щелчок мышью по названию компонента открывает страницу его настроек. Как правило, эти компоненты запускаются и завершаются автоматически, по мере необходимости. Если какой-либо из них может быть запущен или остановлен пользователем вручную, то кроме названия и статистики работы, в плитке вспомогательного компонента доступен выключатель для управления его запуском.

В нижней части страницы указывается информация о состоянии обновлений вирусных баз и о состоянии [лицензии](#). Нажатие кнопки **Обновить** позволяет выполнить принудительное обновление вирусных баз, а нажатие кнопки **Продлить** (или **Активировать**, в зависимости от текущего состояния лицензии) – продлить или активировать лицензию путем загрузки на сервер действующего ключевого файла, подходящего для продукта.

## Управление угрозами

Обзор перечня обнаруженных угроз и управление ими осуществляются на странице **Угрозы**.

На этой странице показывается полный перечень угроз, обнаруженных в процессе работы компонентами Dr.Web для Интернет-шлюзов UNIX, выполняющими мониторинг и проверку файловой системы. В верхней части страницы располагается меню, позволяющее отфильтровать угрозы по категориям:

- **Все** – Отобразить в списке все обнаруженные угрозы (в том числе – активные и те, которые были помещены в карантин).
- **Активные** – Отобразить в списке только активные угрозы, т.е. такие, которые были обнаружены, но все еще не нейтрализованы.



- **Заблокированные** – Отобразить в списке угрозы, которые не нейтрализованы, но файлы, содержащие их, были заблокированы для доступа пользователей.
- **В карантине** – Отобразить в списке угрозы, перемещенные в карантин.
- **Ошибки** – Отобразить в списке угрозы, при попытке обработки которых произошла ошибка.

Справа от названия каждой категории в меню отображается число, показывающее количество обнаруженных угроз, соответствующих данной категории. Активная категория, угрозы из которой в данный момент отображаются в списке, отмечается в меню жирным шрифтом. Для отображения в списке угроз требуемой категории угроз достаточно щелкнуть мышью по названию требуемой категории в меню.



На странице **Угрозы** не отображаются угрозы, обнаруженные компонентами, проверяющими сетевой трафик ([SpIDer Gate](#), [Dr.Web ICAPD](#)), а также компонентом [Dr.Web ClamD](#). Для отслеживания угроз, обнаруженных этими компонентами, вы можете контролировать состояние счетчиков угроз и отслеживать уведомления, доступные по протоколу SNMP (доступ к счетчикам угроз и уведомлениям об инцидентах обеспечивает компонент [Dr.Web SNMPD](#) согласно [структуре MIB Dr.Web](#)).

В списке угроз для каждой угрозы выводится следующая информация:

- **Файл** – Имя файла, содержащего вредоносный объект (путь к файлу не указывается).
- **Владелец** – Имя пользователя, являющегося владельцем файла, содержащего угрозу.
- **Компонент** – Имя компонента Dr.Web для Интернет-шлюзов UNIX, обнаружившего угрозу в данном файле.
- **Угроза** – Имя вредоносного объекта, обнаруженного в файле, по классификации компании «Доктор Веб».




Для объекта, выделенного в списке, справа от списка выводится подробная информация, включающая в себя:



- Имя угрозы (выводится в виде ссылки, при щелчке по которой в новой вкладке браузера открывается страница Вирусной библиотеки Dr.Web с описанием угрозы).
- Размер файла в байтах.
- Имя компонента, обнаружившего угрозу.
- Дата и время обнаружения угрозы.
- Дата и время последнего изменения файла.
- Имя пользователя-владельца файла с угрозой.
- Имя группы, которой принадлежит пользователь-владелец.
- Идентификатор файла с угрозой в карантине, если файл уже был изолирован в карантин.
- Полный путь к файлу в исходном месте (там, где в нем была обнаружена угроза).



Чтобы выделить объект в списке, достаточно щелкнуть левой кнопкой мыши в строке списка. Чтобы выделить в списке более одного объекта, необходимо отметить флажки в строках выделяемых объектов. Чтобы за один раз выделить все объекты, или снять выделение со всех объектов в списке, необходимо отметить или снять отметку у флажка, расположенного в поле **Файл** в заголовке списка угроз.

Для применения действий к объектам, выделенным в списке угроз, необходимо нажать соответствующую кнопку на панели инструментов, расположенной непосредственно над списком угроз. В панели инструментов доступны следующие кнопки (обратите внимание, что некоторые из них могут быть недоступны в зависимости от типа выделенных угроз):

	– Удалить отмеченные файлы.
	– Восстановить отмеченные файлы из карантина в исходное место.
	<p>– Применить некоторое дополнительное действие к отмеченным файлам (выбирается из выпадающего списка). Доступны следующие дополнительные действия:</p> <ul style="list-style-type: none"><li>• <b>В карантин</b> – Переместить файлы с угрозами в карантин</li><li>• <b>Вылечить</b> – Попытаться вылечить угрозы</li><li>• <b>Игнорировать</b> – Игнорировать угрозы, обнаруженные в отмеченных файлах, и удалить их из списка обнаруженных угроз</li></ul>

На странице списка угроз доступна также панель фильтрации списка угроз на основании поискового запроса. Чтобы отфильтровать список угроз, оставив в нем только те объекты, в описании которых присутствует заданная строка, необходимо воспользоваться строкой поиска. Она расположена в правой части панели инструментов и отмечена значком . Для фильтрации списка следует ввести произвольное слово в строку поиска, при этом из списка угроз будут скрыты все объекты, не содержащие в своем названии или описании указанного слова (регистр букв не имеет значения для поиска). Для очистки результатов поиска и возвращения к исходному списку, необходимо щелкнуть левой кнопкой мыши по значку  в строке поиска или очистить поисковое слово.

## Управление настройками

Просмотр и изменение текущих [параметров конфигурации](#) компонентов, входящих в состав продукта Dr.Web для Интернет-шлюзов UNIX и перечисленных на [главной странице](#), производятся на странице **Настройки**. Кроме того, на этой странице вы можете переключить программный комплекс в режим *централизованной защиты* или в *одиночный режим работы* (подробнее о режимах работы см. в разделе [Режимы работы](#)).

В левой части страницы располагается меню, в котором перечисляются все компоненты программного комплекса, настройки которых доступны для просмотра и редактирования. Для просмотра и возможного изменения настроек компонента необходимо выбрать его в меню, для чего необходимо щелкнуть по его имени. Имя компонента, настройки которого в данный момент просматриваются в редакторе, выделяется в меню слева.



- Пункт меню **Централизованная защита** позволяет перейти на [страницу управления](#) работой в режиме централизованной защиты.
- Пункт меню **Общие настройки** соответствует [настройкам](#) Dr.Web ConfigD, обеспечивающего общую работу программного комплекса.

Если компонент имеет кроме основной секции настроек также и дополнительные, специфичные секции настроек (например, такие секции имеются у компонента эмуляции интерфейса **ClamAV®** Dr.Web ClamD – в каждой из них задаются индивидуальные параметры проверки для клиентов, использующих определенный адрес подключения), то слева от имени компонента в меню выводится значок сворачивания/разворачивания дополнительных (подчиненных) секций настроек этого компонента. Если значок сворачивания имеет вид ▸, то дополнительные секции скрыты и не видны. Если значок сворачивания имеет вид ▾, то дополнительные секции также отображаются в меню, по одной строке на дополнительную секцию. Чтобы развернуть или свернуть список подчиненных секций компонента, необходимо щелкнуть по значку сворачивания/разворачивания сбоку от имени интересующего компонента в меню.



- Дополнительные секции настроек компонента отображаются с отступом вправо. Чтобы просмотреть или отредактировать параметры дополнительной секции, достаточно щелкнуть по ее названию в меню левой кнопкой мыши.
- Чтобы добавить для компонента новую подчиненную секцию параметров, если он допускает такую возможность, необходимо щелкнуть левой кнопкой мыши по значку **+**, располагающемуся в меню справа от имени компонента (значок отображается в меню при наведении курсора мыши на имя компонента). Далее в появившемся окне следует указать уникальное имя (тег) дополнительной секции параметров и нажать кнопку **ОК**. Чтобы отказаться от добавления новой секции, следует нажать кнопку **Отмена**.
- Чтобы удалить подчиненную секцию параметров, необходимо щелкнуть левой кнопкой мыши по значку **×**, располагающемуся в меню справа от имени (тега) секции (значок отображается в меню при наведении курсора мыши на имя компонента). Далее в появившемся окне следует подтвердить удаление выбранной секции, нажав кнопку **Да**, или отказаться от него, нажав кнопку **Нет**.

В верхней части страницы просмотра настроек располагается меню, управляющее режимом просмотра настроек. Доступны следующие режимы:

- **Все** – Отобразить в редакторе (в табличной форме) все параметры конфигурации компонента, доступные для просмотра и изменения.
- **Измененные** – Отобразить в редакторе (в табличной форме) для просмотра и изменения только те параметры конфигурации компонента, которые имеют значения, отличные от значений по умолчанию.
- **Редактор ini** – Отобразить параметры конфигурации компонента, которые имеют значения, отличные от значений по умолчанию, в текстовом редакторе в формате [файла конфигурации](#) (в виде пар параметр = значение).

На странице управления настройками доступна также панель фильтрации списка отображаемых параметров на основании поискового запроса. Чтобы отфильтровать список параметров, оставив в нем только те параметры, в описании которых присутствует



заданная строка, необходимо воспользоваться строкой поиска. Она расположена в правой части меню, управляющего режимом просмотра, и отмечена значком . Для фильтрации списка параметров следует ввести произвольное слово в строку поиска, при этом из списка параметров будут скрыты все параметры, не содержащие в своем описании указанного слова (регистр букв не имеет значения для поиска). Для очистки результатов поиска и возвращения к исходному списку параметров, необходимо щелкнуть левой кнопкой мыши по значку  в строке поиска или очистить поисковое слово.



Фильтрация списка параметров работает только при просмотре списка параметров в табличной форме (режим **Все** или **Измененные**).

## Просмотр и изменение настроек компонента в табличной форме

При просмотре списка параметров в табличной форме (режим **Все** или **Измененные**), они отображаются в виде таблицы, каждая строка которой содержит описание параметра (слева) и его текущее значение (справа). Для параметров логического типа (имеющих только два допустимых значения – «Да» и «Нет»), вместо значения параметра отображается флажок (включенное состояние соответствует заданному значению «Да», а выключенное – значению «Нет»).



В режиме просмотра всех параметров, а не только измененных, значения, отличные от значений, определенных для этих параметров по умолчанию, выводятся в списке жирным шрифтом.

Общий список параметров разбит на разделы (такие как **Основные**, **Дополнительные** и т.д.). Для сворачивания и разворачивания раздела таблицы достаточно щелкнуть левой кнопкой мыши по заголовку раздела. Если раздел свернут, и параметры, входящие в него, не отображаются в таблице, то слева от имени раздела отображается значок . Если раздел развернут и входящие в него параметры отображаются в таблице, слева от имени раздела отображается значок .

Для изменения параметра необходимо щелкнуть левой кнопкой мыши по текущему значению параметра в таблице (для параметра логического типа – включить или выключить флажок). Если параметр имеет строго ограниченный набор значений, то при щелчке по значению откроется выпадающее меню, в котором необходимо выбрать требуемое значение. Если значение параметра – число, то при щелчке оно будет доступно в поле редактирования прямо в таблице. В этом случае следует указать новое требуемое значение и нажать клавишу ENTER. Во всех этих случаях измененное значение параметра сразу же фиксируется в конфигурации компонента.





Параметр	Значение
MaxForks	4
LogLevel	Информационный
Log	Auto
FixedSocketPath	Не задано
MaxForksPerFile	2

**Рисунок 2. Представление настроек компонента в табличной форме**

Если параметр имеет строковое значение или список произвольных значений, то при щелчке по текущему значению параметра на экране появляется всплывающее окно, в котором выводится текущее значение параметра. В случае если параметр имеет список значений, то элементы списка выводятся в многострочном поле редактирования, по одному в строке, как показано на рисунке ниже. Для редактирования элементов списка необходимо изменить, удалить или добавить требуемые строки в поле редактирования.

**Рисунок 3. Редактирование списка значений**



После редактирования значения параметра, для сохранения внесенных изменений и закрытия окна, следует нажать кнопку **Сохранить**. Для закрытия окна без сохранения внесенных изменений следует нажать кнопку **Отмена** или нажать значок **X** в верхнем правом углу всплывающего окна.

## Просмотр и изменение настроек компонента в текстовом редакторе

При просмотре параметров в режиме **Редактор ini**, они отображаются в простом текстовом редакторе в формате файла конфигурации (в виде пар параметр = значение), где параметр – имя параметра, задаваемое непосредственно в секции настроек компонента в конфигурационном файле. В этом режиме отображаются только те параметры конфигурации, значения которых отличаются от значений, определенных по умолчанию (т.е. те параметры, значения которых в таблице **Все** выводятся жирным шрифтом). Пример отображения параметров в редакторе простого вида показан на рисунке ниже.

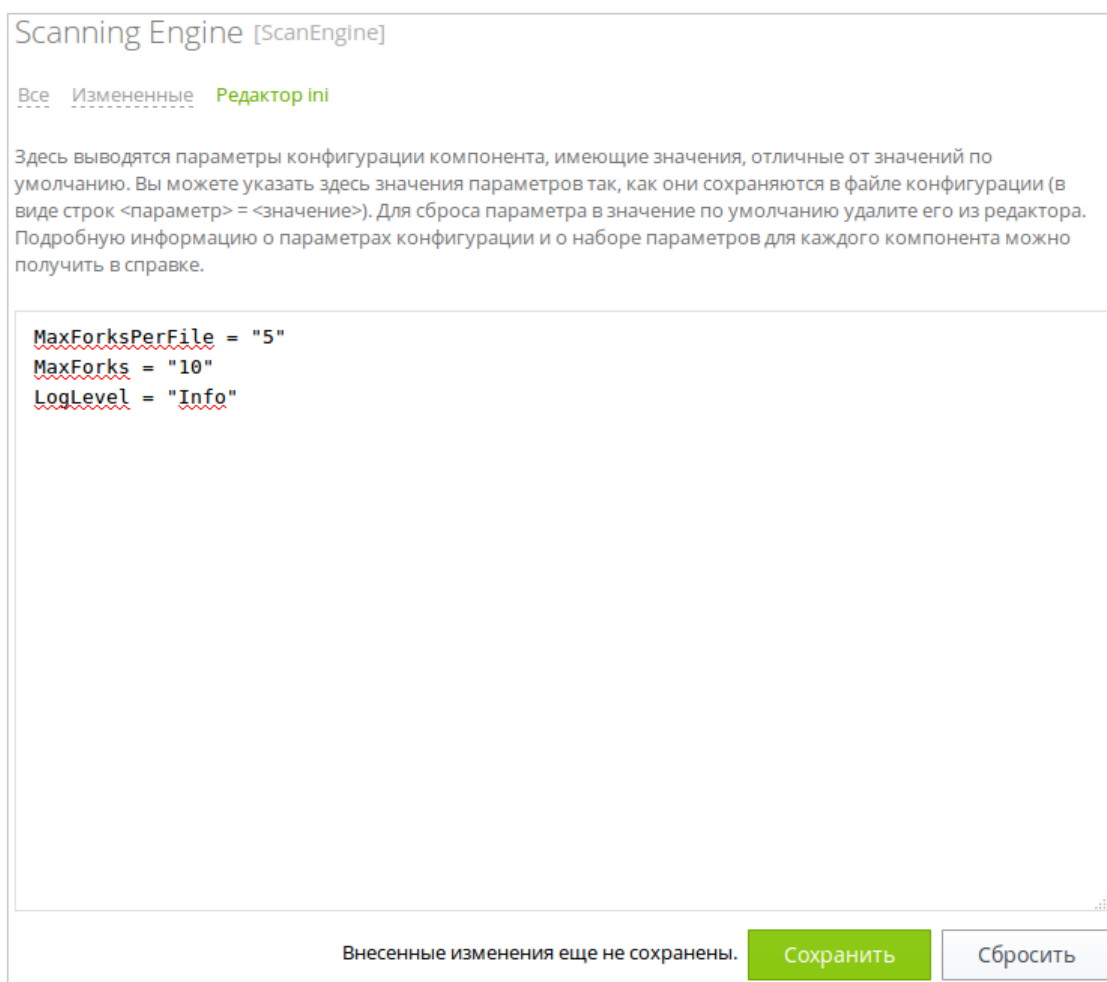


Рисунок 4. Редактор настроек для простого вида

Для внесения изменений необходимо отредактировать текст в текстовом редакторе, учитывая правила формирования файла конфигурации (всегда редактируется только секция файла конфигурации, относящаяся к компоненту, выделенному в меню слева). При



необходимости вы можете указать в редакторе любой из параметров, доступных для компонента. В этом случае его значение, установленное по умолчанию, будет заменено на значение, указанное вами в редакторе. Если требуется сбросить параметр в значение по умолчанию, достаточно удалить его строчку из редактора. В этом случае после сохранения изменений параметру будет присвоено значение по умолчанию.

После редактирования, для сохранения внесенных изменений, следует нажать кнопку **Сохранить**. Для отмены внесенных изменений следует нажать кнопку **Отмена**.



При нажатии кнопки **Сохранить** выполняется проверка корректности текста, введенного в редактор: проверяется, что не указаны несуществующие параметры, а также, что все указанные значения параметров допустимы. В случае обнаружения ошибок на экран выдается соответствующее сообщение.

Подробно ознакомиться с общим описанием файла конфигурации, его структурой и особенностями задания значений параметров можно в разделе [Приложение Г. Конфигурационный файл программного комплекса](#).

## Дополнительно

- [Параметры конфигурации](#) компонента Dr.Web ConfigD (общие настройки).
- [Параметры конфигурации](#) компонента Dr.Web ICAPD.
- [Параметры конфигурации](#) компонента SpIDer Gate.
- [Параметры конфигурации](#) компонента Dr.Web Firewall для Linux.
- [Параметры конфигурации](#) компонента Dr.Web ES Agent.
- [Параметры конфигурации](#) компонента Dr.Web Updater.
- [Параметры конфигурации](#) компонента Dr.Web ClamD.
- [Параметры конфигурации](#) компонента Dr.Web File Checker.
- [Параметры конфигурации](#) компонента Dr.Web Scanning Engine.
- [Параметры конфигурации](#) компонента Dr.Web Network Checker.
- [Параметры конфигурации](#) компонента Dr.Web SNMPD.
- [Параметры конфигурации](#) компонента Dr.Web CloudD.
- [Параметры конфигурации](#) компонента Dr.Web LookupD.
- [Управление централизованной защитой](#).

## Управление централизованной защитой

Вы можете подключить Dr.Web для Интернет-шлюзов UNIX к серверу централизованной защиты или отключить его от сервера централизованной защиты, переведя его в автономный режим работы. Для перехода на страницу управления централизованной



защитой выберите пункт **Централизованная защита** в меню настроек на странице **Настройки**.

Чтобы подключить Dr.Web для Интернет-шлюзов UNIX к серверу централизованной защиты или отключиться от него, используйте соответствующий флажок на этой странице.

## Подключение к серверу централизованной защиты

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

The dialog box is titled 'Задать вручную' (Manual configuration) and contains the following fields and controls:

- A dropdown menu at the top left for selecting the connection method.
- A text input field labeled 'Адрес и порт сервера:' (Server address and port).
- A text input field labeled 'Файл публичного ключа сервера:' (Server public key file) with an 'Обзор...' (Browse...) button next to it.
- An expanded section 'Аутентификация (дополнительно)' (Authentication (optional)) containing:
  - A text input field labeled 'Идентификатор станции:' (Station identifier).
  - A text input field labeled 'Пароль:' (Password).
  - A checkbox labeled 'Подключиться как «новичок»' (Connect as «newbie»).
- Two buttons at the bottom: 'Подключить' (Connect) and 'Cancel'.

Рисунок 5. Окно подключения к серверу централизованной защиты

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

- *Загрузить из файла*
- *Задать вручную*
- *Определить автоматически*

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



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

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



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

Для подключения к серверу, после указания всех параметров, следует нажать кнопку **Подключить** и дождаться окончания процесса подключения. Чтобы закрыть окно без подключения к серверу, нажмите кнопку **Отмена**.



После того, как вы подключили Dr.Web для Интернет-шлюзов UNIX 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 программного комплекса.

## Проверка локальных файлов

Веб-интерфейс предоставляет возможность оперативной проверки на наличие угроз файлов, находящихся на локальном компьютере, с которого осуществляется доступ к веб-интерфейсу управления, используя сканирующее ядро, входящее в состав Dr.Web для Интернет-шлюзов UNIX. Проверяемые файлы будут загружены на сервер по протоколу HTTP, но после проверки, даже в случае обнаружения угроз, они не будут сохранены на сервере, в том числе – не будут добавлены в карантин. Пользователь, отправивший файлы на проверку, будет только проинформирован о ее результате.

## Открытие панели проверки локальных файлов и настройка параметров проверки

Выбор и загрузка файлов для проверки осуществляются на панели проверки локальных файлов, которая отображается при выборе пункта **Проверить файл** в главном меню веб-интерфейса. Активированная панель отображается в нижнем правом углу страницы веб-интерфейса. Внешний вид панели проверки локальных файлов показан на рисунке ниже.

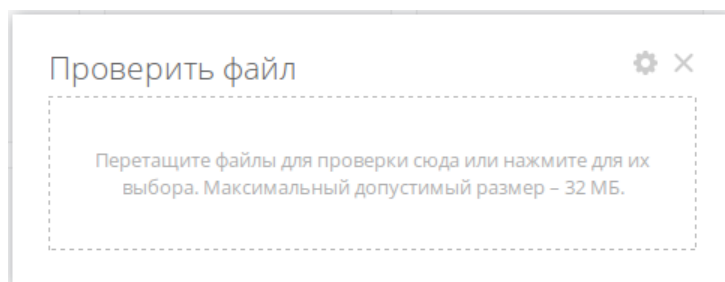


Рисунок 6. Панель проверки локальных файлов

Для закрытия панели следует нажать значок **X** в верхнем правом углу панели. Нажатие значка **⚙** позволяет перейти к настройкам проверки локальных файлов. В режиме настройки имеется возможность указать следующие параметры проверки локальных файлов: максимальное время отведенное на проверку файла (не считая времени его загрузки на сервер с локального компьютера), использование эвристического анализа при проверке, а также максимальную степень сжатия для сжатых объектов и глубину вложенности для объектов, упакованных в контейнеры (такие, как архивы).

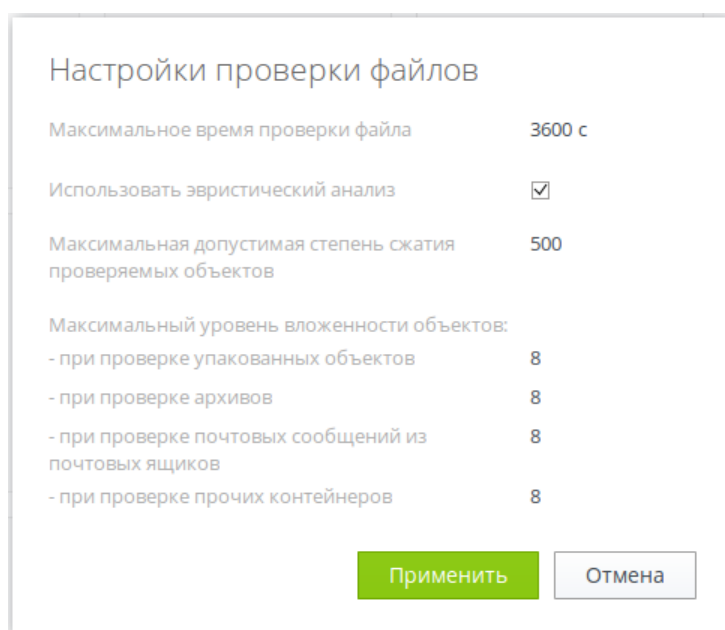


Рисунок 7. Настройка параметров проверки локальных файлов

Для применения измененных настроек и возврата к режиму выбора файлов для проверки нажмите **Применить**. Для возврата к выбору файлов без изменения настроек нажмите **Отмена**.

## Запуск проверки локальных файлов

Для начала проверки файлов щелкните левой клавишей мыши по надписи-мишени **Перетащите файлы для проверки сюда или нажмите для их выбора**. При щелчке по надписи откроется стандартное окно выбора файлов файлового менеджера операционной системы. Вы можете выбрать одновременно несколько файлов для проверки. Обратите внимание, что выбор каталогов для проверки не допускается. Также вы можете перетащить



выбранные для проверки файлы мышью непосредственно на мишень из окна файлового менеджера. После указания проверяемых файлов начнется их загрузка на сервер с Dr.Web для Интернет-шлюзов UNIX и проверка по мере загрузки. В процессе загрузки и проверки файлов панель проверки отображает общий прогресс процесса проверки.

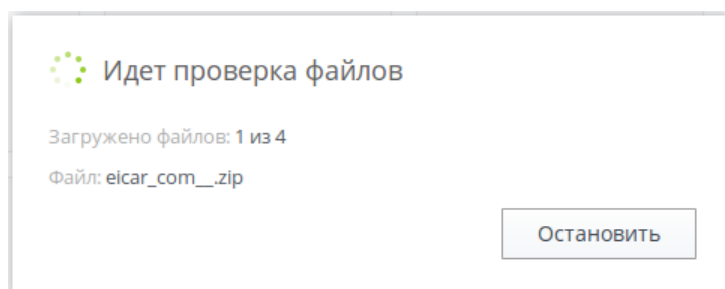


Рисунок 8. Прогресс проверки локальных файлов

В случае необходимости вы можете прервать процесс загрузки и проверки файлов. Для этого нажмите **Остановить**. По окончании проверки на панели отображается отчет о проверке загруженных файлов.

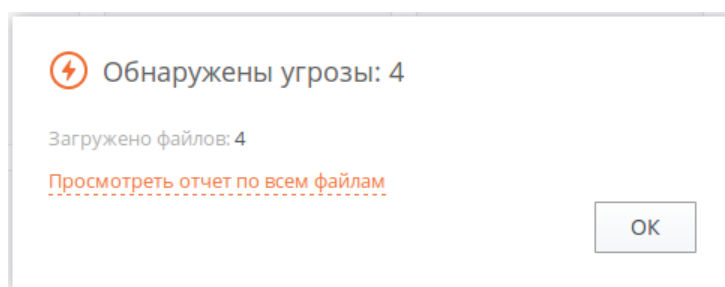
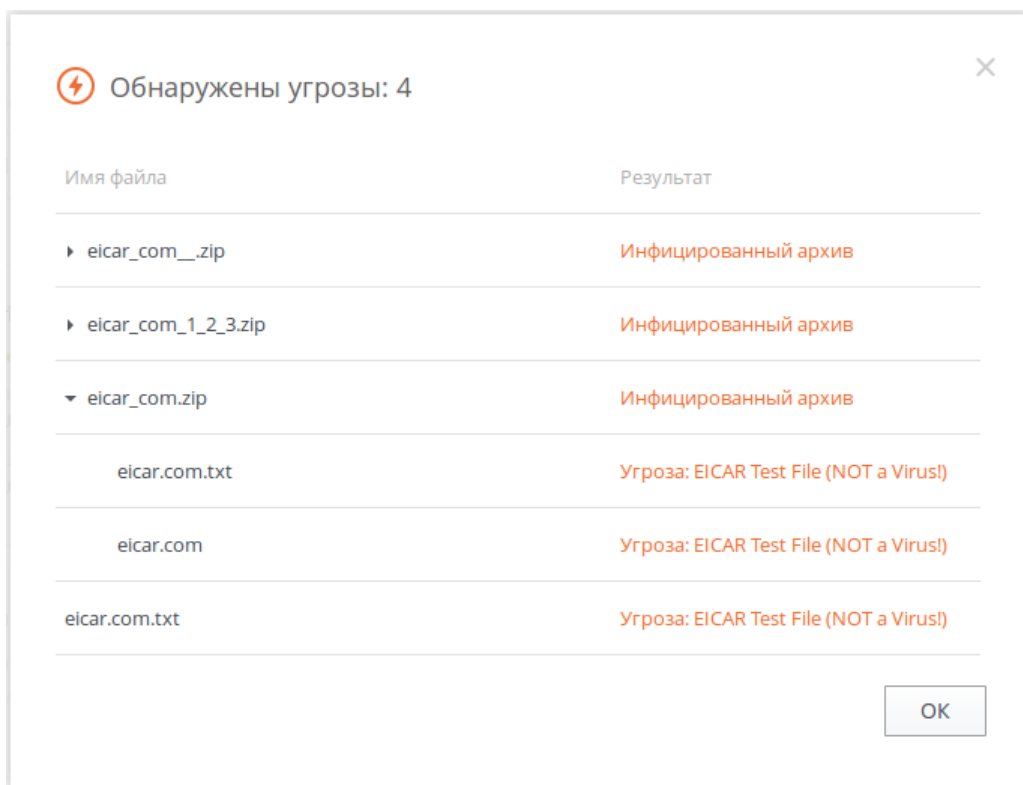


Рисунок 9. Результат проверки локальных файлов

Если вами было загружено более одного файла, доступен расширенный отчет о проверке файлов. Чтобы просмотреть расширенный отчет, нажмите **Просмотреть отчет по всем файлам**.



**Рисунок 10. Расширенный отчет о проверке локальных файлов**

Чтобы закрыть отчет и перевести панель в состояние готовности к выбору новых файлов для проверки, нажмите **ОК**.



Запуск проверки локальных файлов (с текущими настройками проверки) возможен даже тогда, когда панель проверки локальных файлов закрыта. Для начала загрузки и проверки локальных файлов просто перетащите их мышью из окна файлового менеджера на открытую в браузере страницу веб-интерфейса управления.





## Dr.Web ICAPD

Компонент Dr.Web ICAPD предназначен для подключения по протоколу ICAP к прокси-серверу HTTP, установленному на шлюзе, через который пользователи, находящиеся в локальной сети, осуществляют доступ в сеть Интернет (такому, как **Squid**). Прокси-сервер использует Dr.Web ICAPD в качестве внешнего фильтра, которому на анализ передаются как запросы, совершаемые пользователями, так и ответы, поступающие от внешних веб-серверов в ответ на запросы пользователей. Если доступ пользователя к некоторому ресурсу, расположенному во внешней сети, должен быть запрещен, или передаваемые данные (запрос пользователя или ответ, который вернул сервер) содержат угрозу, или не могут быть проверены из-за ошибки, Dr.Web ICAPD заставляет прокси-сервер вернуть пользователю HTML-страницу ответа, сформированную Dr.Web ICAPD на основании шаблона.



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 величину лимита на число файловых дескрипторов, доступных Dr.Web для Интернет-шлюзов UNIX.

## Принципы работы

Компонент Dr.Web ICAPD использует протокол ICAP (*Internet Content Adaptation Protocol*, [RFC 3507](#)) для взаимодействия с внешним по отношению к программному комплексу Dr.Web для Интернет-шлюзов UNIX прокси-сервером, обслуживающим соединения узлов локальной сети с веб-серверами по протоколу HTTP/HTTPS.

Компонент получает от прокси-сервера запросы на проверку («адаптацию» в терминах протокола ICAP) как запросов, исходящих от локальных узлов к серверам, так и ответов, поступающих от серверов. Если URL, содержащийся в запросе клиента, находится в черном списке или принадлежит одной из категорий веб-ресурсов, отмеченной в качестве нежелательной для посещения, Dr.Web ICAPD, предписывает прокси-серверу вместо соединения с веб-сервером вернуть клиенту HTML-страницу, сформированную Dr.Web ICAPD 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 прокси-сервером клиенту в случае если в содержимом запроса пользователя или ответа, поступившего от веб-сервера, Dr.Web ICAPD обнаружит угрозу, подлежащую блокировке, или если передаваемые данные не могут быть проверены из-за ошибки. Схема работы компонента показана на рисунке ниже.

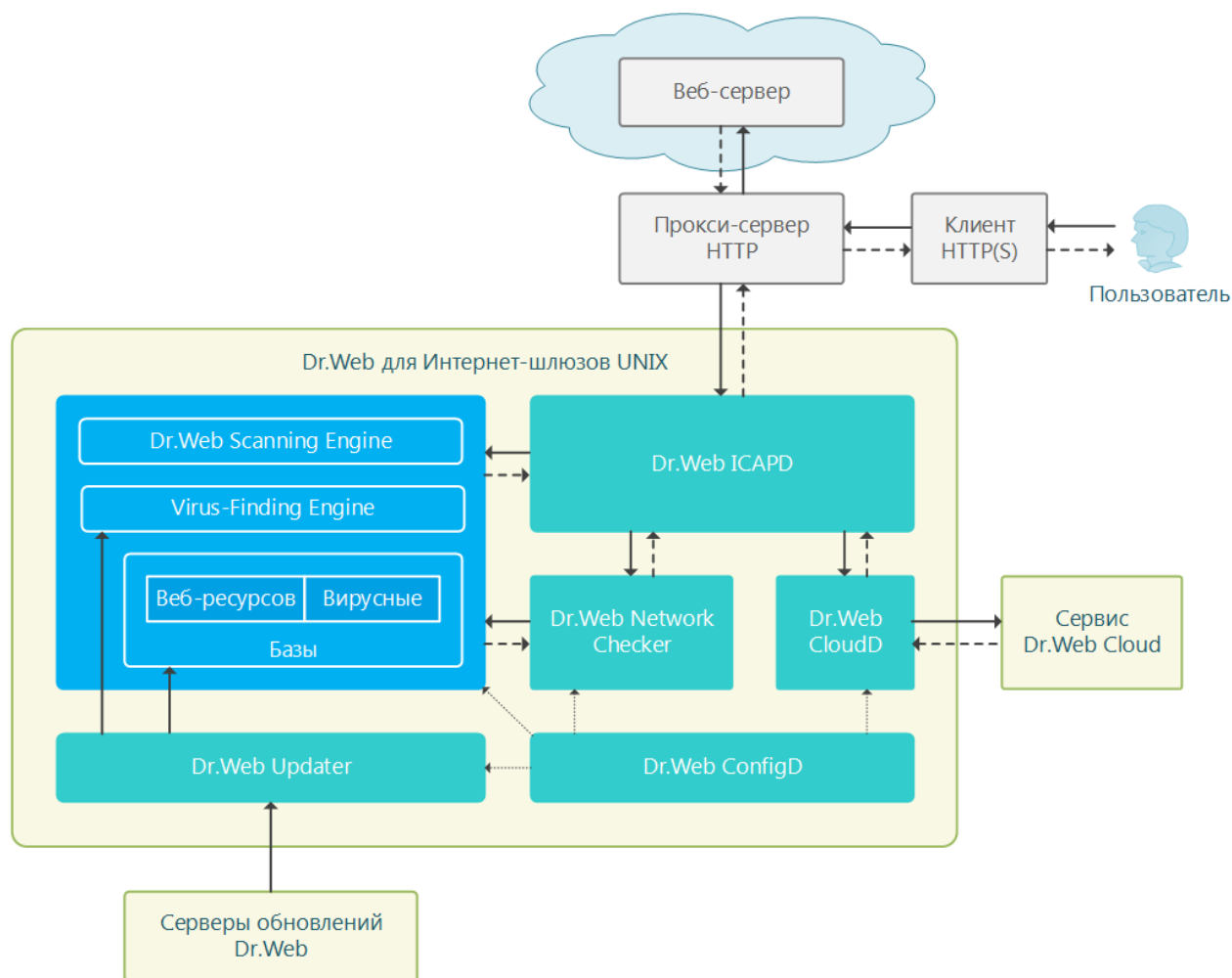


Рисунок 11. Схема работы компонента

Для проверки принадлежности URL той или иной категории 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 вирусов»).
- *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.).

В настройках компонента системный администратор может определять, какие категории веб-ресурсов являются нежелательными для посещения пользователями. Дополнительно администратор может формировать собственные черные списки веб-ресурсов, доступ пользователей к которым будет блокироваться, а также белые списки веб-сайтов, доступ пользователей к которым будет разрешаться, даже если они входят в нежелательные категории. Запросы к облачному сервису Dr.Web Cloud производятся для URL, информация о которых отсутствует в локальных черных списках и базе категорий веб-ресурсов. Такие запросы выполняются с целью проверки, не имеется ли информации о вредоносности этих URL, полученной от других продуктов Dr.Web в режиме реального времени.



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

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

В силу особенностей протокола ICAP, проверка данных большого объема (образы .iso, большие архивы, файлы видео и т.п.) может занимать продолжительное время. Рекомендуется [настроить ограничения](#) по MIME-типу данных, подлежащих проверке, а также ограничить в настройках прокси-сервера HTTP максимальный размер данных, которые разрешено отправлять на проверку по протоколу ICAP (см. [пример](#) для прокси-сервера **Squid**).

Для регулярного автоматического обновления базы категорий веб-ресурсов с серверов обновлений компании «Доктор Веб» используется тот же компонент обновления [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 для



Интернет-шлюзов UNIX, и при необходимости может быть отключено). Для проверки передаваемых данных Dr.Web ICAPD использует агента сетевой проверки данных [Dr.Web Network Checker](#), который, в свою очередь, инициирует их проверку сканирующим ядром [Dr.Web Scanning Engine](#).

## Аргументы командной строки

Для запуска компонента Dr.Web ICAPD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-icapd [<параметры>]
```

Dr.Web ICAPD допускает использование следующих параметров:

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

**Пример:**

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

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

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости. Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду  
**man 1 drweb-icapd**



## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [ICAPD] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>LogLevel</b>  {уровень подробности}	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> [Root].  <b>Значение по умолчанию:</b> Notice
<b>Log</b>  {тип журнала}	<a href="#">Метод ведения журнала</a>
<b>ExePath</b>  {путь к файлу}	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <opt_dir>/bin/drweb-icapd <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /opt/drweb.com/bin/drweb-icapd</li><li>• Для <b>FreeBSD</b> : /usr/local/libexec/drweb.com/bin/drweb-icapd</li></ul>
<b>RunAsUser</b>  {UID   имя пользователя}	Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр (т.е. похоже на числовой UID), то оно указывается с префиксом «name:», например: <b>RunAsUser</b> = name:123456.  <i>Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.</i>  <b>Значение по умолчанию:</b> drweb
<b>Start</b>  {логический}	Компонент должен быть запущен демоном управления конфигурацией <a href="#">Dr.Web ConfigD</a> .  Установка данного параметра в Yes предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение No – немедленно завершить работу компонента.  <b>Значение по умолчанию:</b> No



<b>DebugDumpIcap</b> {логический}	Сохранять в журнал содержимое сообщений, передаваемых по протоколу ICAP, если уровень подробности ведения журнала – отладочный (при <b>LogLevel</b> = <b>DEBUG</b> ).  <b>Значение по умолчанию:</b> No
<b>ListenAddress</b> {сетевой сокет}	Определяет сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web ICAPD в ожидании подключений от прокси-серверов HTTP.  <b>Значение по умолчанию:</b> 127.0.0.1:1344
<b>UsePreview</b> {логический}	Определяет использование Dr.Web ICAPD режима <i>ICAP preview</i> .  <i>Не рекомендуется изменять значение данного параметра без необходимости.</i>  <b>Значение по умолчанию:</b> Yes
<b>Use204</b> {логический}	Определяет, может ли Dr.Web ICAPD возвращать код ответа 204 не только в режиме <i>ICAP preview</i> .  <i>Не рекомендуется изменять значение данного параметра без необходимости.</i>  <b>Значение по умолчанию:</b> Yes
<b>AllowEarlyResponse</b> {логический}	Определяет, может ли Dr.Web ICAPD использовать режим «раннего» ответа ICAP, т.е. начинать отправлять ответ клиенту, не прочитав до конца запрос от прокси-сервера HTTP.  <i>Не рекомендуется изменять значение данного параметра без необходимости.</i>  <b>Значение по умолчанию:</b> Yes
<b>TemplatesDir</b> {путь к каталогу}	Путь к каталогу, в котором хранятся файлы шаблонов HTML-страниц уведомлений о блокировке веб-ресурсов.  <b>Значение по умолчанию:</b> <var_dir>/templates/icapd <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/templates/icapd</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/templates/icapd</li></ul>
<b>Whitelist</b> {список доменов}	Список доменов, который может быть использован в качестве белого списка (т.е. списка доменов, подключение к которым должно быть разрешено пользователям, даже если эти домены относятся к блокируемым категориям веб-ресурсов. При этом



доступ пользователей будет разрешаться 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 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

```
[ICAPD]
Whitelist = "example.com",
"example.net"
```

- Две строки (по одному значению в строке)

```
[ICAPD]
Whitelist = example.com
Whitelist = example.net
```

2. Добавление значений через **команду** `drwebctl cfset`.

```
# drwebctl cfset ICAPD.Whitelist -a
example.com
# drwebctl cfset ICAPD.Whitelist -a
example.net
```



Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.

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. Кроме этого набор правил по умолчанию гарантирует, что данные, загружаемые с доменов из белого списка, *будут проверяться на наличие угроз*.

**Значение по умолчанию:** *(не задано)*

**Blacklist***{список доменов}*

Список доменов, который *может быть использован в качестве черного списка* (т.е списка доменов, подключение к которым должно быть запрещено пользователям, даже если эти домены не относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет запрещаться 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 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

```
[ICAPD]
Blacklist = "example.com",
"example.net"
```

- Две строки (по одному значению в строке)


```
[ICAPD]
Blacklist = example.com
Blacklist = example.net
```

2. Добавление значений через [команду drweb-ctl](#) `cfset`.


```
# drweb-ctl cfset ICAPD.Blacklist -a
example.com
# drweb-ctl cfset ICAPD.Blacklist -a
example.net
```





	<div><p>Реальное использование списка доменов, указанного в данном параметре, зависит от того, как он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.</p><p>В перечне правил, заданных по умолчанию (см. <a href="#">ниже</a>), гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет запрещен всегда. Если домен добавлен одновременно в список Whitelist и список Blacklist, то правила, заданные по умолчанию, гарантируют, что доступ пользователей к нему будет заблокирован.</p></div> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>Adlist</b> <i>{список строк}</i>	<p>Список регулярных выражений, которые описывают рекламные сайты: URL, соответствующий любому из указанных здесь регулярных выражений, считается рекламным.</p> <p><i>Значения в списке указываются через запятую (каждое значение – в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).</i></p> <p><b>Пример:</b> Добавить в список выражения <code>'.*ads.+'</code> и <code>'.*ad/.*\.gif\$'</code>.</p> <ol style="list-style-type: none"><li>Добавление значений в файл конфигурации.<ul style="list-style-type: none"><li>Два значения в одной строке<div><pre>[ICAPD] Adlist = ".*ads.+", ".*ad/.*\.gif\$"</pre></div></li><li>Две строки (по одному значению в строке)<div><pre>[ICAPD] Adlist = .*ads.+ Adlist = .*ad/.*\.gif\$</pre></div></li></ul></li><li>Добавление значений через <a href="#">команду drwebctl cfset</a>.</li></ol>



	<pre># drweb-ctl cfset ICAPD.Adlist -a '.*ads.+' # drweb-ctl cfset ICAPD.Adlist -a '.*/ad/*\.gif\$'</pre> <p>Регулярные выражения записываются с использованием синтаксиса POSIX (BRE, ERE) или Perl (PCRE, PCRE2).</p> <div><p>Реальное использование списка выражений, указанного в данном параметре, зависит от того, как он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.</p><p>В перечне правил, заданных по умолчанию (см. <a href="#">ниже</a>), гарантируется, что доступ к URL из данного списка будет запрещен только в том случае, если домены, на которые ведут эти URL, не находятся в списке Whitelist.</p></div> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>BlockInfectionSource</b> {логический}	<p>Блокировать попытки подключения к сайтам, содержащим вредоносное ПО (входящим в категорию <i>InfectionSource</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockNotRecommended</b> {логический}	<p>Блокировать попытки подключения к не рекомендуемым сайтам (входящим в категорию <i>NotRecommended</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>



<b>BlockAdultContent</b> <i>{логический}</i>	<p>Блокировать попытки подключения к сайтам, содержащим материалы для взрослых (входящим в категорию <i>AdultContent</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockViolence</b> <i>{логический}</i>	<p>Блокировать попытки подключения к сайтам, содержащим сцены насилия (входящим в категорию <i>Violence</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockWeapons</b> <i>{логический}</i>	<p>Блокировать попытки подключения к сайтам, посвященным оружию (входящим в категорию <i>Weapons</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockGambling</b> <i>{логический}</i>	<p>Блокировать попытки подключения к сайтам, посвященным азартным играм и играм на деньги (входящим в категорию <i>Gambling</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockDrugs</b>	<p>Блокировать попытки подключения к сайтам, посвященным наркотикам (входящим в категорию</p>



<b>{логический}</b>	<p><i>Drugs).</i></p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockObsceneLanguage</b> <b>{логический}</b>	<p>Блокировать попытки подключения к сайтам, содержащим нецензурную лексику (входящим в категорию <i>ObsceneLanguage</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockChats</b> <b>{логический}</b>	<p>Блокировать попытки подключения к сайтам чатов (входящим в категорию <i>Chats</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockTerrorism</b> <b>{логический}</b>	<p>Блокировать попытки подключения к сайтам, посвященным терроризму (входящим в категорию <i>Terrorism</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockFreeEmail</b> <b>{логический}</b>	<p>Блокировать попытки подключения к сайтам бесплатных почтовых служб (входящим в категорию <i>FreeEmail</i>).</p>



	<p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockSocialNetworks</b> {логический}	<p>Блокировать попытки подключения к сайтам социальных сетей (входящим в категорию <i>SocialNetworks</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockDueToCopyrightNotice</b> {логический}	<p>Блокировать попытки подключения к сайтам, ссылки на которые были добавлены по обращению правообладателей (входящим в категорию <i>DueToCopyrightNotice</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>ScanTimeout</b> {интервал времени}	<p>Устанавливает тайм-аут на проверку одного файла по запросу Dr.Web ICAPD.</p> <p>Может быть указано значение в диапазоне от 1s до 1h.</p> <p><b>Значение по умолчанию:</b> 30s</p>
<b>HeuristicAnalysis</b> {On   Off}	<p>Определяет, использовать ли эвристический анализ для поиска возможных неизвестных угроз при проверке данных, инициированной по запросу Dr.Web ICAPD. Использование эвристического анализа повышает надежность проверки, но увеличивает её длительность.</p> <p>Реакция на срабатывание эвристического анализа задается в параметре <b>BlockSuspicious</b>.</p>



	<p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• On – Использовать эвристический анализ при проверке.</li><li>• Off – Не использовать эвристический анализ.</li></ul> <p><b>Значение по умолчанию:</b> On</p>
<p><b>PackerMaxLevel</b></p> <p>{целое число}</p>	<p>Устанавливает максимальный уровень вложенности объектов при проверке запакованных объектов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке данных, инициированной по запросу Dr.Web ICAPD.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p> <p><b>Значение по умолчанию:</b> 8</p>
<p><b>ArchiveMaxLevel</b></p> <p>{целое число}</p>	<p>Устанавливает максимальный уровень вложенности объектов при проверке архивов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке данных, инициированной по запросу Dr.Web ICAPD.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p> <p><b>Значение по умолчанию:</b> 0</p>
<p><b>MailMaxLevel</b></p> <p>{целое число}</p>	<p>Устанавливает максимальный уровень вложенности объектов при проверке почтовых сообщений и почтовых ящиков (mailboxes). Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке данных, инициированной по запросу Dr.Web ICAPD.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p> <p><b>Значение по умолчанию:</b> 0</p>
<p><b>ContainerMaxLevel</b></p> <p>{целое число}</p>	<p>Устанавливает максимальный уровень вложенности объектов при проверке прочих контейнеров (таких, как HTML-страницы). Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке данных, инициированной по запросу Dr.Web ICAPD.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p>



	<b>Значение по умолчанию:</b> 8
<b>MaxCompressionRatio</b> <i>{целое число}</i>	<p>Устанавливает максимальную допустимую степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке данных, инициированной по запросу Dr.Web ICAPD.</p> <p><i>Величина степени сжатия должна быть не менее 2.</i></p> <p><b>Значение по умолчанию:</b> 500</p>
<b>BlockKnownVirus</b> <i>{логический}</i>	<p>Блокировать получение или передачу данных, если они содержат известную угрозу.</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockSuspicious</b> <i>{логический}</i>	<p>Блокировать получение или передачу данных, если они содержат неизвестную угрозу (обнаруженную эвристическим анализатором).</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockAdware</b> <i>{логический}</i>	<p>Блокировать получение или передачу данных, если они содержат рекламную программу.</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockDialers</b> <i>{логический}</i>	<p>Блокировать получение или передачу данных, если они содержат программу дозвона.</p>



	<p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockJokes</b> {логический}	<p>Блокировать получение или передачу данных, если они содержат программу-шутку.</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockRiskware</b> {логический}	<p>Блокировать получение или передачу данных, если они содержат потенциально опасную программу.</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockHacktools</b> {логический}	<p>Блокировать получение или передачу данных, если они содержат программу взлома.</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockUnchecked</b> {логический}	<p>Блокировать получение или передачу данных, если они не могут быть проверены.</p> <p><b>Значение по умолчанию:</b> No</p>





## Правила проверки трафика и блокировки доступа

В дополнение к параметрам, перечисленным выше, в секции присутствует семь *наборов правил* **RuleSet\*** (**RuleSet0**, ..., **RuleSet6**), непосредственно управляющих проверкой трафика и блокировкой доступа пользователей к веб-ресурсам, а также загрузкой контента из Интернет. Для некоторых значений в условиях (например – диапазоны IP-адресов, перечни категорий сайтов, черные и белые списки веб-ресурсов и т.п.) предусмотрена подстановка значений, загружаемых из текстовых файлов, а также извлеченных из внешних источников данных через LDAP (используется компонент [Dr.Web LookupD](#)). 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.

Подробно правила рассмотрены в разделе [Правила проверки трафика](#) Приложения Г.

### Просмотр и редактирование правил

Для удобства редактирования списка правил, по умолчанию в списке оставлены «пустоты», т.е. наборы **RuleSet<i>**, не содержащие правил. и удаления их оттуда (где *<i>* – номер набора **RuleSet**). Обратите внимание, что вы *не можете* добавлять элементы списка, отличные от уже имеющихся **RuleSet<i>**, но имеете возможность добавить и удалить любое правило в любом элементе **RuleSet<i>**. Просмотр и редактирование правил могут осуществляться любым из нижеуказанных способов:

- путем просмотра и изменения (в любом текстовом редакторе) [файла конфигурации](#) (помните, что в этом файле сохраняются только те параметры, значение которых отличается от значений по умолчанию);
- через [веб-интерфейс](#) управления продуктом (если установлен);
- 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 необходимо перезапустить программный комплекс. Для этого воспользуйтесь командой **drweb-ctl** `reload`.

Использование команды **drweb-ctl** `cfshow` для просмотра правил.

Для просмотра содержимого набора правил **ICAPD.RuleSet1** используйте команду.

```
# drweb-ctl cfshow ICAPD.RuleSet1
```

Использование команды **drweb-ctl** `cfset` для редактирования правил (здесь и далее *<правило>* – текст правила).

- Замена всех правил в наборе правил **ICAPD.RuleSet1** на новое правило:



```
# drweb-ctl cfset ICAPD.RuleSet1 '<правило>'
```

- Добавление еще одного правила в набор правил **ICAPD.RuleSet1**:

```
# drweb-ctl cfset -a ICAPD.RuleSet1 '<правило>'
```

- Удаление конкретного правила из набора правил **ICAPD.RuleSet1**:

```
# drweb-ctl cfset -e ICAPD.RuleSet1 '<правило>'
```

- Возврат набора правил **ICAPD.RuleSet1** к состоянию по умолчанию:

```
# drweb-ctl cfset -r ICAPD.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» следует записать цепочку правил, в условии каждого из которых будет указано условие-дизъюнкт.

Чтобы добавить в набор правил **ICAPD.RuleSet1** правило безусловного пропуска (действие *PASS*), достаточно выполнить команду:

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'PASS'
```

Однако, чтобы удалить это правило из указанного набора правил, необходимо выполнить команду:

```
# drweb-ctl cfset -e ICAPD.RuleSet1 ' : PASS'
```



Чтобы добавить в набор правил **ICAPD.RuleSet1** правило, изменяющее для соединений, следующих с неразрешенных адресов, путь к стандартным шаблонам и выполняющее блокировку, достаточно выполнить команду:

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :  
set http_template_dir = "mytemplates", BLOCK'
```

Однако, эта команда добавит *два правила* в указанный набор правил, поэтому, чтобы удалить их, необходимо выполнить две команды:

```
# drweb-ctl cfset -e ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :  
set http_template_dir = "mytemplates"  
# drweb-ctl cfset -e ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :  
BLOCK'
```

Чтобы добавить в набор правил **ICAPD.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 ICAPD.RuleSet1 'threat_category in (KnownVirus) : BLOCK  
as _match'  
# drweb-ctl cfset -a ICAPD.RuleSet1 'url_category in (Terrorism) : BLOCK as  
_match'
```

Для их удаления их также потребуется две команды, как в примере выше.

### Набор правил по умолчанию

По умолчанию задан следующий набор правил, управляющих блокировкой:

```
RuleSet0 =  
RuleSet1 = direction request, url_host in "ICAPD.Blacklist" : BLOCK as  
BlackList  
RuleSet1 = direction request, url_host not in "ICAPD.Whitelist", url match  
"ICAPD.Adlist" : BLOCK as BlackList  
RuleSet2 =  
RuleSet3 = direction request, url_host not in "ICAPD.Whitelist",  
url_category in "ICAPD.BlockCategory" : BLOCK as _match  
RuleSet4 =  
RuleSet5 = threat_category in "ICAPD.BlockThreat" : BLOCK as _match  
RuleSet6 =
```

Первые два правила посвящены обработке исходящих HTTP-соединений: если узел (или URL), с которым производится попытка установить соединение, включен в черный список, соединение блокируется по причине попадания в черный список, дальнейшие проверки не производятся. Если же узел (URL) не находится в белом списке и относится к любой из категорий сайтов, отмеченной как нежелательные для посещения, или соответствует списку регулярных выражений, описывающих рекламные сайты, то соединение блокируется по причине попадания URL в запрещенную к посещению категорию.



Правило, указанное в **RuleSet5**, проверяет, не содержатся ли в теле проверяемого HTTP-запроса или HTTP-ответа угрозы, относящиеся к категориям, которые следует блокировать, и если да, то соединение блокируется по причине обнаружения угрозы. Обратите внимание, что из-за отсутствия условия *direction* по умолчанию проверяются как запросы клиентов (*request*), так и ответы серверов (*response*).

### Примеры правил проверки трафика и блокировки доступа

1. Разрешить для пользователей с диапазона IP-адресов *10.10.0.0 – 10.10.0.254* доступ к сайтам любых категорий, кроме категории *Chats*:

```
src_ip in (10.10.0.0/24), url_category not in (Chats) : PASS
```

Обратите внимание, что если правило

```
url_host in "ICAPD.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 *ICAPD.Blacklist*, будет блокироваться и для пользователей с диапазона IP-адресов *10.10.0.0 – 10.10.0.254*. А если это правило разместить ниже (т.е. позже), то пользователям с диапазона 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 вирусы производиться также не будет. Чтобы разрешить пользователям с диапазона 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:

```
url_category not in (Chats), url_host not in "ICAPD.Blacklist",  
threat_category not in "ICAPD.BlockCategory" : PASS
```

2. Не выполнять проверку содержимого видео-файлов (т.е. данных с типом MIME *'video/\*'*, где *\** соответствует любому типу MIME-класса *video*):

```
content_type in ("video/*") : PASS
```

## Интеграция с прокси-сервером HTTP Squid

Интеграция Dr.Web ICAPD с прокси-сервером HTTP **Squid** описана в разделе [Интеграция с прокси-сервером Squid](#).



## SpIDer Gate



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

Компонент проверки сетевого трафика и URL SpIDer Gate предназначен для проверки данных (загружаемых на локальный узел из сети, а также 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.

В настройках компонента имеется возможность указать, протоколы каких типов следует подвергать проверке.

Для проверки принадлежности URL той или иной категории (используется 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 вирусов»).
- *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.).

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 входят в нежелательные категории. 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 веб-сайт может принадлежать одновременно нескольким категориям. Доступ к такому веб-сайту будет заблокирован, если он принадлежит хотя бы одной из категорий, доступ к которой нежелателен.

Даже если веб-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 величину лимита](#) на число файловых дескрипторов, доступных Dr.Web для Интернет-шлюзов UNIX.

В рамках серверных продуктов Dr.Web для Интернет-шлюзов UNIX в первую очередь может быть использован для организации «барьера» между сервером компании, например – веб-сервером с публичным доступом, и внешней сетью Интернет, поскольку функции управления доступом пользователей локальной сети к сети Интернет по умолчанию делегированы компоненту [Dr.Web ICAPD](#), работающему в связке с прокси-сервером, обеспечивающим доступ к Интернет из локальной сети.

## 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 нежелательной для посещения. Кроме этого компонент может отправлять запросы на проверку URL в облачный сервис Dr.Web Cloud. Если URL обнаружен в любой из нежелательных категорий (в том числе – возвращенной по запросу 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 на разрешенность установления соединения с данным узлом.

Перенаправление соединений, устанавливаемых клиентскими приложениями с удаленными серверами, осуществляется прозрачно для клиентских приложений – вспомогательным компонентом [Dr.Web Firewall для Linux](#), выполняющим динамическое управление правилами **NetFilter** – системного компонента **GNU/Linux**. Схема работы компонента проверки сетевого трафика и URL показана на рисунке ниже.

В рамках серверных продуктов Dr.Web для Интернет-шлюзов UNIX под клиентскими приложениями в первую очередь понимается некоторый защищаемый серверный ресурс компании, например – веб-сервер с публичным доступом, поскольку функции управления доступом пользователей локальной сети к сети Интернет по умолчанию делегированы компоненту [Dr.Web ICAPD](#), работающему в связке с прокси-сервером, обеспечивающим доступ к сети Интернет из локальной сети.

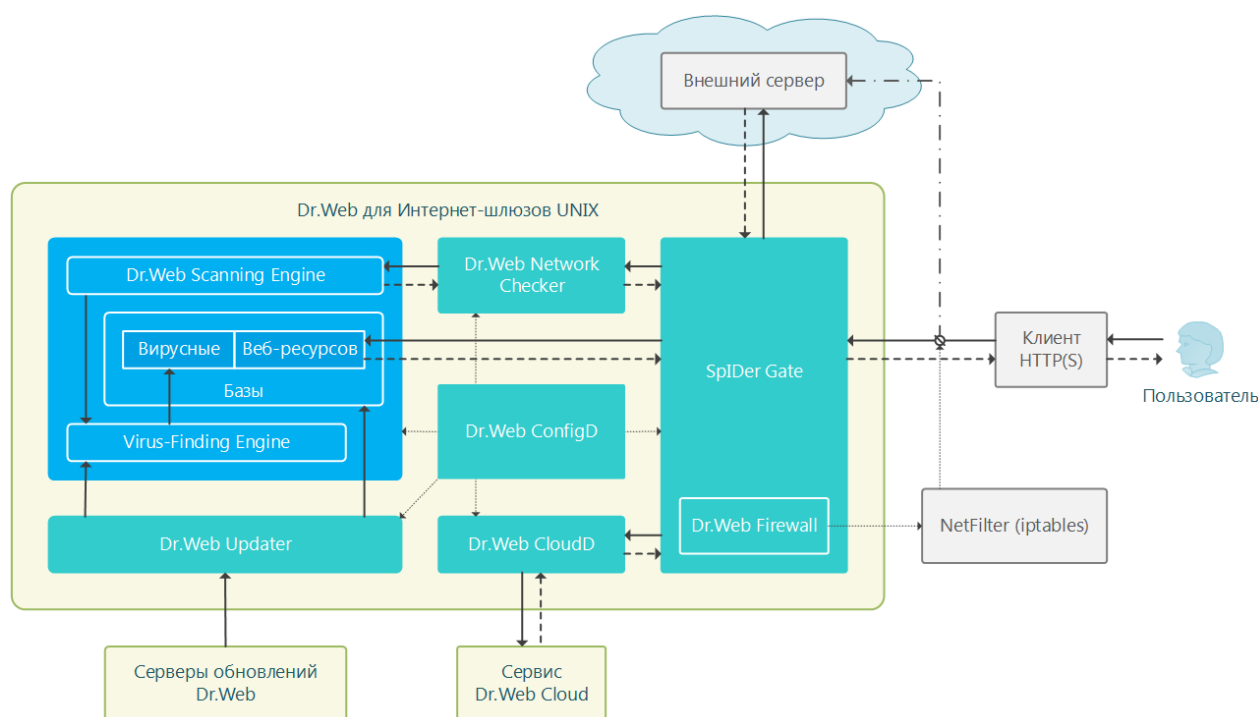


Рисунок 12. Схема работы компонента

Для регулярного автоматического обновления базы категорий веб-ресурсов с серверов обновлений компании «Доктор Веб» используется тот же компонент обновления [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 для Интернет-шлюзов UNIX, 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](#).

## Аргументы командной строки

Для запуска компонента SpIDer Gate из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-gated [<параметры>]
```

SpIDer Gate допускает использование следующих параметров:

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

**Пример:**

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

Данная команда выведет на экран краткую справку компонента SpIDer Gate.

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости. Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду  
**man 1 drweb-gated**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [GateD] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.





В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<p><u>Уровень подробности</u> ведения журнала компонента.</p> <p>Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <u>секции</u> [Root].</p> <p><b>Значение по умолчанию:</b> Notice</p>
<b>Log</b> <i>{тип журнала}</i>	<p><u>Метод ведения журнала</u></p>
<b>ExePath</b> <i>{путь к файлу}</i>	<p>Путь к исполняемому файлу компонента.</p> <p><b>Значение по умолчанию:</b> &lt;opt_dir&gt;/bin/drweb-gated</p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /opt/drweb.com/bin/drweb-gated</li><li>• Для <b>FreeBSD:</b> /usr/local/libexec/drweb.com/bin/drweb-gated</li></ul>
<b>RunAsUser</b> <i>{UID   имя пользователя}</i>	<p>Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр (т.е. похоже на числовой UID), то оно указывается с префиксом «name:», например: <b>RunAsUser</b> = name:123456.</p> <p><i>Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.</i></p> <p><b>Значение по умолчанию:</b> drweb</p>
<b>IdleTimeLimit</b> <i>{интервал времени}</i>	<p>Максимальное время простоя компонента, по превышению которого он завершает свою работу.</p> <p>Минимальное значение – 10s.</p> <p><b>Значение по умолчанию:</b> 30s</p>
<b>TemplatesDir</b> <i>{путь к каталогу}</i>	<p>Путь к каталогу, в котором хранятся файлы шаблонов HTML-страниц уведомлений о блокировке веб-ресурсов.</p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/templates/gated</p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /var/opt/drweb.com/templates/gated</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/templates/gated</li></ul>
<b>CaPath</b> <i>{путь}</i>	<p>Путь к каталогу или файлу, в котором располагается перечень корневых сертификатов, являющихся доверенными.</p> <p><b>Значение по умолчанию:</b> Путь к системному перечню доверенных сертификатов. Зависит от дистрибутива <b>GNU/Linux</b>:</p> <ul style="list-style-type: none"><li>• Для <b>Astra Linux, Debian, Linux Mint, SUSE Linux и Ubuntu</b> это обычно путь /etc/ssl/certs/;</li><li>• Для <b>CentOS и Fedora</b> – путь /etc/pki/tls/certs/ca-bundle.crt.</li></ul>



- Для других дистрибутивов путь может быть определен через результат вызова 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.

Более тонкие параметры настройки проверки трафика, включая правила проверки, задаются в [настройках](#) вспомогательного компонента Dr.Web Firewall для Linux.



## 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. Он играет роль менеджера соединений для SpIDer Gate. Dr.Web Firewall для Linux обеспечивает прохождение соединений, устанавливаемых на компьютере, через SpIDer Gate для проверки передаваемого через них трафика.

## Принципы работы

Компонент Dr.Web Firewall для Linux обеспечивает корректную работу компонента SpIDer Gate, анализируя правила маршрутизации, заданные для **NetFilter** (системного компонента **GNU/Linux**), и модифицируя их таким образом, чтобы устанавливаемые соединения перенаправлялись на SpIDer 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 соединений.

## Аргументы командной строки

Для запуска компонента Dr.Web Firewall для Linux из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-firewall [<параметры>]
```

Dr.Web Firewall для Linux допускает использование следующих параметров:

Параметр	Описание
----------	----------



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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости. Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой](#) `drweb-ctl`).



Для получения справки о компоненте из командной строки используйте команду  
**man 1 drweb-firewall**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[LinuxFirewall]` объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> <code>[Root]</code> .  <b>Значение по умолчанию:</b> Notice
<b>Log</b> <i>{тип журнала}</i>	<a href="#">Метод ведения журнала</a>




<b>ExePath</b>  {путь к файлу}	<p>Путь к исполняемому файлу компонента.</p> <p><b>Значение по умолчанию:</b> &lt;opt_dir&gt;/bin/drweb-firewall</p> <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /opt/drweb.com/bin/drweb-firewall</li><li>• Для <b>FreeBSD</b> : /usr/local/libexec/drweb.com/bin/drweb-firewall</li></ul>
<b>XtablesLockPath</b>  {путь к файлу}	<p>Путь к файлу блокировки таблиц <b>iptables (NetFilter)</b>. 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, при запуске компонента происходит ошибка.</p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>InspectHttp</b>  {On   Off}	<p>Проверять данные, передаваемые по протоколу HTTP.</p> <p><i>Реальная проверка данных будет осуществляться в соответствии с заданными правилами проверки (см. <a href="#">ниже</a>).</i></p> <p><b>Значение по умолчанию:</b> On</p>
<b>InspectSmtп</b>  {On   Off}	<p>Проверять данные, передаваемые по протоколу SMTP (использует компонент Dr.Web MailD, если установлен).</p> <p><i>Реальная проверка данных будет осуществляться в соответствии с заданными правилами проверки (см. <a href="#">ниже</a>).</i></p> <p><b>Значение по умолчанию:</b> Off</p>
<b>InspectPop3</b>  {On   Off}	<p>Проверять данные, передаваемые по протоколу POP3 (использует компонент Dr.Web MailD, если установлен).</p> <p><i>Реальная проверка данных будет осуществляться в соответствии с заданными правилами проверки (см. <a href="#">ниже</a>).</i></p> <p><b>Значение по умолчанию:</b> Off</p>
<b>InspectImap</b>  {On   Off}	<p>Проверять данные, передаваемые по протоколу IMAP (использует компонент Dr.Web MailD, если установлен).</p>





	<p>Реальная проверка данных будет осуществляться в соответствии с заданными правилами проверки (см. <a href="#">ниже</a>).</p> <p><b>Значение по умолчанию:</b> <code>off</code></p>
<p><b>InputDivert</b></p> <p><code>{Off   Auto(interface:&lt;i_name&gt; protected:&lt;p_list&gt;)}</code></p>	<p>Настройки перенаправления входящих соединений в SpIDer Gate для проверки.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• <code>off</code> – перенаправление входящих соединений отключено.</li><li>• <code>Auto(interface:&lt;i_name&gt; protected:&lt;p_list&gt;)</code> – перенаправление входящих соединений в автоматическом режиме. Правилами управляет Dr.Web Firewall для Linux. Контролируются соединения, входящие через указанный сетевой интерфейс <code>&lt;i_name&gt;</code> на указанный список портов <code>&lt;p_list&gt;</code>. Номера портов в списке <code>&lt;p_list&gt;</code> указываются через запятую. Пример: <code>Auto(interface:eth0 protected:80,8080).</code></li></ul> <p><b>Значение по умолчанию:</b> <code>off</code></p>
<p><b>OutputDivert</b></p> <p><code>{Off   Auto}</code></p>	<p>Настройки перенаправления исходящих соединений в SpIDer Gate для проверки.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• <code>off</code> – перенаправление исходящих соединений отключено.</li><li>• <code>Auto</code> – перенаправление исходящих соединений в автоматическом режиме, правилами управляет Dr.Web Firewall для Linux.</li></ul> <p><b>Значение по умолчанию:</b> <code>Auto</code></p>
<p><b>ExcludedProc</b></p> <p><code>{путь к файлу}</code></p>	<p>Список процессов, который <i>может быть использован в качестве белого списка процессов</i>, т.е. списка процессов, сетевая активность которых не должна контролироваться.</p> <p><i>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).</i></p> <p><b>Пример:</b> Добавить в список процессы <b>wget</b> и <b>curl</b>.</p>



	<p>1. Добавление значений в файл конфигурации.</p> <ul style="list-style-type: none"><li>• Два значения в одной строке</li></ul> <pre>[LinuxFirewall] ExcludedProc = "/usr/bin/wget", "/usr/bin/curl"</pre> <ul style="list-style-type: none"><li>• Две строки (по одному значению в строке)</li></ul> <pre>[LinuxFirewall] ExcludedProc = /usr/bin/wget ExcludedProc = /usr/bin/curl</pre> <p>2. Добавление значений через <b>команду drweb-ctl cfset</b>.</p> <pre># drweb-ctl cfset LinuxFirewall.ExcludedProc - a /usr/bin/wget # drweb-ctl cfset LinuxFirewall.ExcludedProc - a /usr/bin/curl</pre> <div><p>Реальное использование списка процессов, указанного в данном параметре, зависит от того, как он используется в правилах проверки, заданных для Dr.Web Firewall для Linux.</p><p>В перечне правил, заданных по умолчанию (см. <a href="#">ниже</a>), гарантируется, что трафик всех процессов, указанных в этом списке пропускается <i>без какой-либо проверки</i>.</p></div> <p><b>Значение по умолчанию:</b> <i>(не задано)</i></p>
<b>SniCheckAddress</b>  {логический}	<p>Выполнять проверку SNI узла, с которым выполняется соединение, на этапе «SSL handshake» с целью проверить, находится он в черном списке или в блокируемых категориях, без вскрытия SSL.</p>



	<div><p>В текущей реализации значение данной переменной не оказывает никакого влияния на проверку защищенного трафика. Для реального управления проверкой нужно создать правила, в которых содержатся условия <code>sni_host in</code> и <code>sni_category in</code> (см. <a href="#">ниже</a>).</p><p>Если значение параметра изменять через <a href="#">команду</a> <code>cfset</code> утилиты <b>drweb-ctl</b> или через <a href="#">веб-интерфейс управления</a>, то зависимые правила будут перестраиваться автоматически.</p></div> <p><b>Значение по умолчанию:</b> No</p>
<b>UnwrapSsl</b> <i>{логический}</i>	<p>Выполнять проверку зашифрованного трафика, передаваемого через SSL.</p> <div><p>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 <code>SET Unwrap_SSL = true/false</code> (см. <a href="#">ниже</a>).</p><p>Если значение параметра изменять через <a href="#">команду</a> <code>cfset</code> утилиты <b>drweb-ctl</b> или через <a href="#">веб-интерфейс управления</a>, то зависимые правила будут перестраиваться автоматически.</p></div> <p><b>Значение по умолчанию:</b> No</p>
<b>HttpSafeSearch</b> <i>{логический}</i>	<p>Использовать опцию «Безопасный поиск» поисковых машин, которые поддерживают данный режим.</p> <p><b>Значение по умолчанию:</b> No</p>





<b>BlockInfectionSource</b>  {логический}	<p>Блокировать попытки подключения к сайтам, содержащим вредоносное ПО (входящим в категорию <i>InfectionSource</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockNotRecommended</b>  {логический}	<p>Блокировать попытки подключения к не рекомендуемым сайтам (входящим в категорию <i>NotRecommended</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockAdultContent</b>  {логический}	<p>Блокировать попытки подключения к сайтам, содержащим материалы для взрослых (входящим в категорию <i>AdultContent</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockViolence</b>  {логический}	<p>Блокировать попытки подключения к сайтам, содержащим сцены насилия (входящим в категорию <i>Violence</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre>



	<b>Значение по умолчанию:</b> No
<b>BlockWeapons</b> {логический}	<p>Блокировать попытки подключения к сайтам, посвященным оружию (входящим в категорию <i>Weapons</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <b>Значение по умолчанию:</b> No
<b>BlockGambling</b> {логический}	<p>Блокировать попытки подключения к сайтам, посвященным азартным играм и играм на деньги (входящим в категорию <i>Gambling</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <b>Значение по умолчанию:</b> No
<b>BlockDrugs</b> {логический}	<p>Блокировать попытки подключения к сайтам, посвященным наркотикам (входящим в категорию <i>Drugs</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <b>Значение по умолчанию:</b> No
<b>BlockObsceneLanguage</b> {логический}	<p>Блокировать попытки подключения к сайтам, содержащим нецензурную лексику (входящим в категорию <i>ObsceneLanguage</i>).</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p>



	<pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockChats</b> {логический}	<p>Блокировать попытки подключения к сайтам чатов (входящим в категорию <i>Chats</i>).</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockTerrorism</b> {логический}	<p>Блокировать попытки подключения к сайтам, посвященным терроризму (входящим в категорию <i>Terrorism</i>).</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockFreeEmail</b> {логический}	<p>Блокировать попытки подключения к сайтам бесплатных почтовых служб (входящим в категорию <i>FreeEmail</i>).</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockSocialNetworks</b> {логический}	<p>Блокировать попытки подключения к сайтам социальных сетей (входящим в категорию <i>SocialNetworks</i>).</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p>



	<pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockDueToCopyrightNotice</b> {логический}	<p>Блокировать попытки подключения к сайтам, ссылки на которые были добавлены по обращению правообладателей (входящим в категорию <i>DueToCopyrightNotice</i>).</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>Whitelist</b> {список доменов}	<p>Список доменов, который <i>может быть использован в качестве белого списка</i> (т.е. списка доменов, подключение к которым должно быть разрешено пользователям, даже если эти домены относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет разрешаться и ко всем поддоменам доменов, указанных в этом списке).</p> <p><i>Значения в списке указываются через запятую (каждое значение – в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).</i></p> <p><b>Пример:</b> Добавить в список домены example.com и example.net.</p> <ol style="list-style-type: none"><li>Добавление значений в файл конфигурации.<ul style="list-style-type: none"><li>Два значения в одной строке<pre>[LinuxFirewall] Whitelist = "example.com", "example.net"</pre></li><li>Две строки (по одному значению в строке)<pre>[LinuxFirewall] Whitelist = example.com Whitelist = example.net</pre></li></ul></li><li>Добавление значений через <a href="#">команду</a> <b>drwebctl cfset</b>.</li></ol>



```
# 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 набор правил по умолчанию гарантирует, 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}*

Список доменов, который *может быть использован в качестве черного списка* (т.е. списка доменов, подключение к которым должно быть запрещено пользователям, даже если эти домены не относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет запрещаться 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 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]
Blacklist = "example.com",
"example.net"
```

- Две строки (по одному значению в строке)

```
[LinuxFirewall]
Blacklist = example.com
Blacklist = example.net
```

2. Добавление значений через [команду drwebctl](#) cfset.

```
# drwebctl cfset
LinuxFirewall.Blacklist -a
example.com
# drwebctl 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.

В перечне правил, заданных по умолчанию (см. [ниже](#)), гарантируется, 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 нему по протоколу HTTP будет заблокирован.

**Значение по умолчанию:** (не задано)



<b>ScanTimeout</b> <i>{интервал времени}</i>	<p>Устанавливает тайм-аут на проверку одного файла по запросу SpIDer Gate.</p> <p><i>Может быть указано значение в диапазоне от 1s до 1h.</i></p> <p><b>Значение по умолчанию:</b> 30s</p>
<b>HeuristicAnalysis</b> <i>{On   Off}</i>	<p>Определяет, использовать ли эвристический анализ для поиска возможных неизвестных угроз при проверке файла, инициированной по запросу SpIDer Gate. Использование эвристического анализа повышает надежность проверки, но увеличивает её длительность.</p> <p><i>Реакция на срабатывание эвристического анализа задается в параметре <b>BlockSuspicious</b>.</i></p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• On – Использовать эвристический анализ при проверке.</li><li>• Off – Не использовать эвристический анализ.</li></ul> <p><b>Значение по умолчанию:</b> On</p>
<b>PackerMaxLevel</b> <i>{целое число}</i>	<p>Устанавливает максимальный уровень вложенности объектов при проверке запакованных объектов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке файла, инициированной по запросу SpIDer Gate.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p> <p><b>Значение по умолчанию:</b> 8</p>
<b>ArchiveMaxLevel</b> <i>{целое число}</i>	<p>Устанавливает максимальный уровень вложенности объектов при проверке архивов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке файла, инициированной по запросу SpIDer Gate.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p> <p><b>Значение по умолчанию:</b> 8</p>




<b>MailMaxLevel</b> <i>{целое число}</i>	<p>Устанавливает максимальный уровень вложенности объектов при проверке почтовых сообщений и почтовых ящиков (mailboxes). Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке файла, инициированной по запросу SpIDer Gate.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p> <p><b>Значение по умолчанию:</b> 8</p>
<b>ContainerMaxLevel</b> <i>{целое число}</i>	<p>Устанавливает максимальный уровень вложенности объектов при проверке прочих контейнеров (таких, как HTML-страницы). Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке файла, инициированной по запросу SpIDer Gate.</p> <p><i>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</i></p> <p><b>Значение по умолчанию:</b> 8</p>
<b>MaxCompressionRatio</b> <i>{целое число}</i>	<p>Устанавливает максимальную допустимую степень сжатия упакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке файла, инициированной по запросу SpIDer Gate.</p> <p><i>Величина степени сжатия должна быть не менее 2.</i></p> <p><b>Значение по умолчанию:</b> 500</p>
<b>BlockKnownVirus</b> <i>{логический}</i>	<p>Блокировать получение или передачу данных, если они содержат известную угрозу.</p> <p><i>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</i></p> <div><pre>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</pre></div> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockSuspicious</b> <i>{логический}</i>	<p>Блокировать получение или передачу данных, если они содержат неизвестную угрозу, обнаруженную эвристическим анализатором.</p>





	<p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockAdware</b> {логический}	<p>Блокировать получение или передачу данных, если они содержат рекламную программу.</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockDialers</b> {логический}	<p>Блокировать получение или передачу данных, если они содержат программу дозвона.</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> Yes</p>
<b>BlockJokes</b> {логический}	<p>Блокировать получение или передачу данных, если они содержат программу-шутку.</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockRiskware</b> {логический}	<p>Блокировать получение или передачу данных, если они содержат потенциально опасную программу.</p>



	<p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockHacktools</b>  {логический}	<p>Блокировать получение или передачу данных, если они содержат программу взлома.</p> <p>Для реальной блокировки следует убедиться, что в настройках также присутствует правило вида (см. <a href="#">ниже</a>):</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</pre> <p><b>Значение по умолчанию:</b> No</p>
<b>BlockUnchecked</b>  {логический}	<p>Блокировать получение или передачу данных, если они не могут быть проверены.</p> <div><p>Значение этого параметра влияет на обработку <a href="#">правил</a>, 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.</p></div> <p><b>Значение по умолчанию:</b> No</p>



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 Интернет. Для некоторых значений в условиях (например – диапазоны IP-адресов, перечни категорий сайтов, черные и белые списки веб-ресурсов и т.п.) предусмотрена подстановка значений, загружаемых из текстовых файлов, а также извлеченных из внешних источников данных через LDAP (используется компонент [Dr.Web LookupD](#)). 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.

Подробно правила рассмотрены в разделе [Правила проверки трафика](#) Приложения Г.

## Просмотр и редактирование правил

Для удобства редактирования списка правил, по умолчанию в списке оставлены «пустоты», т.е. наборы **RuleSet**<*i*>, не содержащие правил. и удаления их оттуда (где <*i*> – номер набора **RuleSet**). Обратите внимание, что вы *не можете* добавлять элементы списка, отличные от уже имеющихся **RuleSet**<*i*>, но имеете возможность добавить и удалить любое правило в любом элементе **RuleSet**<*i*>. Просмотр и редактирование правил могут осуществляться любым из нижеуказанных способов:

- путем просмотра и изменения (в любом текстовом редакторе) [файла конфигурации](#) (помните, что в этом файле сохраняются только те параметры, значение которых отличается от значений по умолчанию);
- через [веб-интерфейс](#) управления продуктом (если установлен);
- 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 необходимо перезапустить программный комплекс. Для этого воспользуйтесь командой **drweb-ctl** `reload`.

Использование команды **drweb-ctl** `cfshow` для просмотра правил.

Для просмотра содержимого набора правил **LinuxFirewall.RuleSet1** используйте команду.

```
# drweb-ctl cfshow LinuxFirewall.RuleSet1
```

Использование команды **drweb-ctl** `cfset` для редактирования правил (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» следует записать цепочку правил, в условии каждого из которых будет указано условие-дизъюнкт.

Чтобы добавить в набор правил **LinuxFirewall.RuleSet1** правило безусловного пропуска (действие *PASS*), достаточно выполнить команду:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'PASS'
```

Однако, чтобы удалить это правило из указанного набора правил, необходимо выполнить 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, достаточно выполнить команду:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'src_ip not in  
file("/etc/trusted_ip") : set http_template_dir = "mytemplates", BLOCK'
```



Однако, эта команда добавит *два правила* в указанный набор правил, поэтому, чтобы удалить их, необходимо выполнить 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 их 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 (Smtп), threat_category in  
"LinuxFirewall.BlockThreat" : REJECT  
RuleSet9 = protocol in (Smtп), url_category in "LinuxFirewall.BlockCategory"  
: REJECT  
RuleSet9 = protocol in (Smtп), 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 вскрытие содержимого защищенных соединений. Это правило, как и все нижележащие, будет анализироваться только если соединение не связано с исключаемым процессом. Кроме того, поскольку все последующие правила зависят от определения типа протокола, то, если вскрытие содержимого защищенных соединений запрещено, а соединение защищенное, в этом случае все они не сработают из-за невозможности определить истинность условий.

Последующие пять нижележащих правил посвящены обработке исходящих HTTP-соединений:

1. Если узел, с которым производится попытка установить соединение, включен в черный список, соединение блокируется по причине попадания в черный список, дальнейшие проверки не производятся.
2. Если узел находится в белом списке, соединение пропускается, дальнейшие проверки не производятся.
3. Если URL, к которому обращается клиент, находится в категориях веб-ресурсов, отмеченных как нежелательные для посещения, то соединение блокируется по причине попадания URL в запрещенную к посещению категорию, дальнейшие проверки не производятся.
4. Если ответ, поступивший от удаленного узла по HTTP, содержит угрозу, относящуюся к категориям, которые следует блокировать, то соединение блокируется по причине обнаружения угрозы, 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 по причине обнаружения угрозы, 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**, предназначены для проверки данных, передаваемых по протоколам электронной почты, и срабатывают, если будет обнаружено, что передается сообщение электронной почты (по протоколу SMTP, POP3 или IMAP), содержащее вложения, или URL, относящиеся к категориям, которые следует блокировать, либо оцененные как спам (с оценкой достоверности 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 («перепакровка»).



Если компонент проверки сообщений электронной почты на наличие признаков спама Dr.Web ASE отсутствует в составе продукта, то проверка писем на наличие признаков спама не производится. В этом случае правила, содержащие проверку порога спама (переменную `total_spam_score`) отсутствуют.

Обратите внимание, что правила проверки электронной почты будут работать только в том случае, если соответствующие разрешающие параметры **Inspect**<*EmailProtocol*> имеют значение **On**. В противном случае ни одно из них не сработает. Кроме того, для физического исследования передаваемого письма на предмет обнаружения в нем вредоносных вложений 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 **InspectSmtп**, **InspectPop3** и **InspectImap**.



Обратите внимание, что набор правил по умолчанию может автоматически изменяться при изменении значений параметров **SniCheckAddress** и **UnwrapSsl**.

## Примеры правил проверки трафика и блокировки доступа

1. Разрешить для пользователей с диапазона 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
```

Обратите внимание, что 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 диапазона IP-адресов *10.10.0.0 – 10.10.0.254*. А если это правило разместить ниже (т.е. позже), то пользователям с диапазона 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 вирусы производиться также не будет. Чтобы разрешить пользователям с диапазона 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 Интернет* видео-файлов (т.е. данных с типом MIME 'video/\*', где \* соответствует любому типу MIME-класса video):

```
direction response, content_type in ("video/*") : PASS
```

Обратите внимание, что 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`.





## Dr.Web ClamD

Компонент Dr.Web ClamD выполняет эмуляцию продуктом Dr.Web для Интернет-шлюзов UNIX интерфейса антивирусного демона **clamd**, являющегося центральным компонентом антивирусного продукта **Clam AntiVirus (ClamAV®)** от Sourcefire, Inc. Этот интерфейс позволяет внешним приложениям, которые могут использовать антивирусный продукт **ClamAV®**, использовать для антивирусной проверки файлов продукт Dr.Web для Интернет-шлюзов UNIX.

## Принципы работы

Компонент позволяет выполнять по запросу от внешних приложений проверку на наличие угроз как содержимого файлов, расположенных в локальной файловой системе, так и непосредственно потоки данных, передаваемые внешним приложением через сокет. Кроме того, компонент может проверять содержимое файлов, для которых внешнее приложение передало через сокет открытый дескриптор.



Проверка файла по переданному дескриптору осуществляется только через локальный UNIX-сокет.

В случае если внешнее приложение предоставило путь к файлу в локальной файловой системе, компонент передает задание на проверку этого файла компоненту проверки файлов [Dr.Web File Checker](#), иначе он передает данные, полученные от приложения через сокет, агенту распределенной проверки [Dr.Web Network Checker](#), как показано на рисунке ниже.

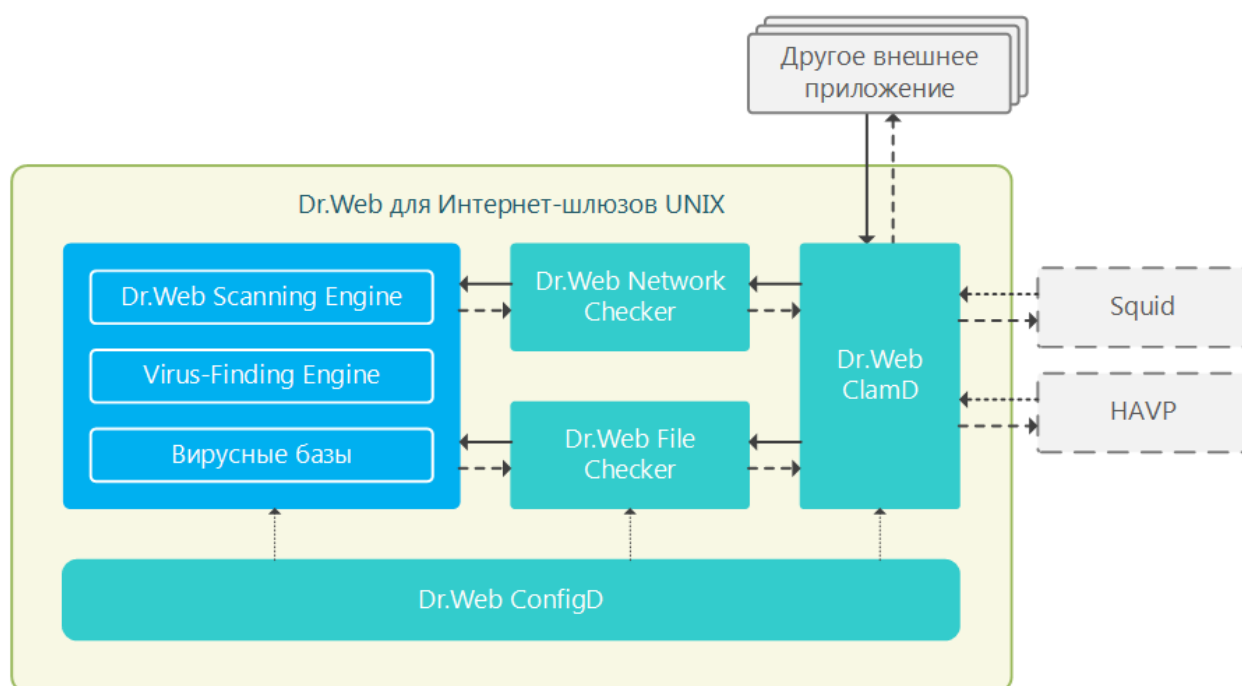


Рисунок 13. Схема работы компонента



По умолчанию компонент не запускается автоматически при старте программного комплекса Dr.Web для Интернет-шлюзов UNIX, чтобы обеспечить его запуск, необходимо выполнить не только его включение [настройкой](#) Start, но и определить не менее одной точки подключения. После запуска компонент ожидает поступления запросов от внешних приложений на проверку указанных файлов или потоков передаваемых данных. В настройках можно определить набор различных точек подключения внешних приложений, указав для каждой свои собственные настройки проверки.

Как указано на рисунке выше, в качестве внешних приложений могут выступать и непосредственно прокси-серверы HTTP (такие, как **Squid** и **HAVP**), если они оснащены модулем интеграции с **clamd**. Подробнее см. в разделе [Интеграция с внешними приложениями](#).



Обнаруженные угрозы *не нейтрализуются* средствами Dr.Web для Интернет-шлюзов UNIX, внешнему приложению только возвращается результат проверки. Таким образом, внешнее приложение само несет ответственность за нейтрализацию обнаруженной угрозы.

## Аргументы командной строки

Для запуска компонента Dr.Web ClamD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-clamd [<параметры>]
```

Dr.Web ClamD допускает использование следующих параметров:

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

### Пример:

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

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



## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости (обычно при старте операционной системы). Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается командой **drweb-ctl**).



Для получения справки о компоненте из командной строки используйте команду  
**man 1 drweb-clamd**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [ClamD] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> [Root].  <b>Значение по умолчанию:</b> Notice
<b>Log</b> <i>{тип журнала}</i>	<a href="#">Метод ведения журнала</a>
<b>ExePath</b> <i>{путь к файлу}</i>	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <opt_dir>/bin/drweb-clamd <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /opt/drweb.com/bin/drweb-clamd</li><li>• Для <b>FreeBSD</b> : /usr/local/libexec/drweb.com/bin/drweb-clamd</li></ul>
<b>Start</b> <i>{логический}</i>	Компонент должен быть запущен демоном управления конфигурацией <a href="#">Dr.Web ConfigD</a> .  Установка данного параметра в Yes предписывает демону управления



	<p>конфигурацией немедленно попытаться запустить компонент, а установка его в значение No – немедленно завершить работу компонента.</p> <p><b>Значение по умолчанию:</b> No</p>
<p><code>Endpoint.&lt;тег&gt;.ClamdSocket</code></p> <p><i>{IP-адрес   UNIX-сокеты}</i></p>	<p>Определяет точку подключения с именем &lt;тег&gt; и сокет (адрес IPv4 или адрес сокета UNIX) для клиентов, желающих проверять файлы на наличие угроз.</p> <p><i>Для одной точки &lt;тег&gt; может быть задан только один сокет.</i></p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<p><code>[Endpoint.&lt;тег&gt;.]DetectSuspicious</code></p> <p><i>{логический}</i></p>	<p>Сообщать о подозрительных файлах, обнаруженных эвристическим анализатором.</p> <p><i>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</i></p> <p><b>Значение по умолчанию:</b> Yes</p>
<p><code>[Endpoint.&lt;тег&gt;.]DetectAdware</code></p> <p><i>{логический}</i></p>	<p>Сообщать о файлах, содержащих рекламные программы.</p> <p><i>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</i></p> <p><b>Значение по умолчанию:</b> Yes</p>
<p><code>[Endpoint.&lt;тег&gt;.]DetectDialers</code></p> <p><i>{логический}</i></p>	<p>Сообщать о файлах, содержащих программы дозвона.</p> <p><i>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</i></p> <p><b>Значение по умолчанию:</b> Yes</p>
<p><code>[Endpoint.&lt;тег&gt;.]DetectJokes</code></p> <p><i>{логический}</i></p>	<p>Сообщать о файлах, содержащих программы-шутки.</p> <p><i>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех</i></p>



	<p>точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> No</p>
<p>[Endpoint.&lt;тег&gt;.] <b>DetectRiskware</b></p> <p>{логический}</p>	<p>Сообщать о файлах, содержащих потенциально опасные программы.</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> No</p>
<p>[Endpoint.&lt;тег&gt;.] <b>DetectHacktools</b></p> <p>{логический}</p>	<p>Сообщать о файлах, содержащих программы взлома.</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> No</p>
<p>[Endpoint.&lt;тег&gt;.] <b>ReadTimeout</b></p> <p>{интервал времени}</p>	<p>Определяет тайм-аут на ожидание данных от клиента.</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> 5s</p>
<p>[Endpoint.&lt;тег&gt;.] <b>StreamMaxLength</b></p> <p>{размер}</p>	<p>Определяет максимальный размер данных, которые могут быть получены от клиента (при передаче данных для проверки в виде потока байтов).</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> 25mb</p>
<p>[Endpoint.&lt;тег&gt;.] <b>ScanTimeout</b></p> <p>{интервал времени}</p>	<p>Определяет таймаут на проверку одного файла (или одной порции данных), поступившего от клиента.</p>



	<p>Может быть указано значение в диапазоне от 1s до 1h.</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> 3m</p>
<p>[Endpoint.&lt;тег&gt;.] <b>HeuristicAnalysis</b></p> <p>{On   Off}</p>	<p>Определяет, следует ли использовать эвристический анализ при проверке.</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> On</p>
<p>[Endpoint.&lt;тег&gt;.] <b>PackerMaxLevel</b></p> <p>{целое число}</p>	<p>Определяет максимальный уровень вложенности для проверки запакованных объектов.</p> <p>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> 8</p>
<p>[Endpoint.&lt;тег&gt;.] <b>ArchiveMaxLevel</b></p> <p>{целое число}</p>	<p>Определяет максимальный уровень вложенности для проверки архивов.</p> <p>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</p> <p>Если указан префикс Endpoint.&lt;тег&gt;, то значение параметра определено только для точки &lt;тег&gt;, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> 8</p>
<p>[Endpoint.&lt;тег&gt;.] <b>MailMaxLevel</b></p>	<p>Определяет максимальный уровень вложенности для проверки почтовых файлов.</p>



<code>{целое число}</code>	<p>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</p> <p>Если указан префикс <code>Endpoint.&lt;тег&gt;</code>, то значение параметра определено только для точки <code>&lt;тег&gt;</code>, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> 8</p>
<code>[Endpoint.&lt;тег&gt;.]ContainerMaxLevel</code> <code>{целое число}</code>	<p>Определяет максимальный уровень вложенности для проверки объектов, находящихся в контейнерах.</p> <p>Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.</p> <p>Если указан префикс <code>Endpoint.&lt;тег&gt;</code>, то значение параметра определено только для точки <code>&lt;тег&gt;</code>, иначе оно определено для всех точек, у которых значение этого параметра не задано.</p> <p><b>Значение по умолчанию:</b> 8</p>
<code>[Endpoint.&lt;тег&gt;.]MaxCompressionRatio</code> <code>{целое число}</code>	<p>Устанавливает максимальную допустимую степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке.</p> <p>Величина степени сжатия должна быть не менее 2.</p> <p><b>Значение по умолчанию:</b> 500</p>

## Особенность настроек компонента

Параметры, отмеченные необязательным префиксом `Endpoint.<тег>`, могут быть сгруппированы. Каждая такая группа определяет *точку подключения (endpoint)* с задаваемым уникальным идентификатором `<тег>`, используемую клиентами для подключения к компоненту. Все параметры проверки, включенные в одну группу, определяют параметры, которые будут применяться при проверке данных от клиентов, подключившихся к этой точке. Если параметр указан без префикса `Endpoint.<тег>`, то он определяет значение, применяемое для всех точек подключения. Если из точки подключения удалить параметр, то для точки подключения будет применяться не значение параметра по умолчанию, а значение, указанное в соответствующем одноименном «родительском» параметре (без префикса `Endpoint.<тег>`).



Параметр **ClamSocket** должен обязательно задаваться с префиксом `Endpoint.<me2>`, поскольку он не только определяет прослушиваемый сокет, но и определяет группу (точку подключения), к которой этот сокет привязывается.

### Пример:

Пусть требуется организовать две точки подключения для двух групп внешних приложений (серверов) *servers1* и *servers2*. При этом серверы из группы *servers1* могут подключаться через UNIX-сокет, а серверы из группы *servers2* – через сетевое соединение. Кроме того, по умолчанию эвристический анализ должен быть выключен, но для серверов из группы *servers2* его нужно использовать. Пример соответствующих настроек:

- 1) Для задания в [файле конфигурации](#):

```
[ClamD]
HeuristicAnalysis = Off

[ClamD.Endpoint.servers1]
ClamSocket = /tmp/srv1.socket

[ClamD.Endpoint.servers2]
ClamSocket = 127.0.0.1:1234
HeuristicAnalysis = On
```

- 2) Для задания через утилиту командной строки [Dr.Web Ctl](#):

```
# drweb-ctl cfset ClamD.HeuristicAnalysis Off
# drweb-ctl cfset ClamD.Endpoint -a servers1
# drweb-ctl cfset ClamD.Endpoint -a servers2
# drweb-ctl cfset ClamD.Endpoint.servers1.ClamSocket /tmp/srv1.socket
# drweb-ctl cfset ClamD.Endpoint.servers2.ClamSocket 127.0.0.1:1234
# drweb-ctl cfset ClamD.Endpoint.servers2.HeuristicAnalysis On
```



Оба способа задания настроек приведут к одинаковому результату, но в случае непосредственной правки файла конфигурации необходимо применить измененные настройки, отправив сигнал `SIGHUP` модулю **drweb-configd** (для этого вы можете выполнить [команду](#) **drweb-ctl reload**).

## Интеграция с внешними приложениями

За счет использования интерфейса, эмулирующего интерфейс антивирусного демона **clamd**, входящего в состав антивирусного решения **ClamAV**, Dr.Web ClamD может быть сопряжен с любыми внешними приложениями, способными подключаться к антивирусному демону **clamd**.





В таблице ниже перечислены примеры приложений, которые могут использовать **clamd** для антивирусной проверки:

Продукт	Интеграция
<b>Службы HTTP</b>	
Прокси-сервер HTTP <b>Squid</b>	<p><b>Использование clamd:</b></p> <p>Проверка файлов, получаемых через Интернет.</p> <p><b>Требование для интеграции:</b></p> <p>Использование промежуточного компонента <b>squidclamav</b> или <b>HAVP</b>.</p> <p><b>Ссылки на документацию:</b></p> <p>Документация по продукту <b>Squid</b>: <a href="http://www.squid-cache.org/Doc/">http://www.squid-cache.org/Doc/</a></p> <p>Описание и исходные коды <b>squidclamav</b>: <a href="http://squidclamav.darold.net/">http://squidclamav.darold.net/</a></p>
Прокси-сервер HTTP с функциями антивирусной проверки <b>HAVP</b>	<p><b>Использование clamd:</b></p> <p>Проверка файлов, получаемых через Интернет.</p> <p><b>Требование для интеграции:</b></p> <p>Настройка в файле конфигурации <b>HAVP</b> использования <b>clamd</b> для антивирусной проверки:</p> <pre>ENABLECLAMD true CLAMDSOCKET &lt;path_to_clamd_UNIX_socket&gt;</pre> <p>или (если вместо UNIX-сокета используется TCP-соединение):</p> <pre>ENABLECLAMD true CLAMDSERVER &lt;IP&gt; CLAMDPORTR &lt;port&gt;</pre> <p>где &lt;path_to_clamd_UNIX_socket&gt; или пара &lt;IP&gt;:&lt;port&gt; соответствуют сокету точки подключения (<i>endpoint</i>), настроенной в конфигурации Dr.Web ClamD.</p> <p><b>Ссылки на документацию:</b></p> <p>Документация по продукту <b>HAVP</b>: <a href="http://www.server-side.de/documentation.htm">http://www.server-side.de/documentation.htm</a></p>

В настройке компонента, обращающегося непосредственно к Dr.Web ClamD как к антивирусному демону **clamd**, следует указать в качестве адреса подключения к антивирусному демону **clamd** путь к UNIX-сокету или TCP-сокету, прослушиваемому Dr.Web ClamD на одной из созданных в его настройках точек подключения (*endpoint*).

Пример подключения **HAVP** к Dr.Web ClamD:

1. Настройка Dr.Web ClamD:



```
[ClamD]
Start = yes

[ClamD.Endpoint.proxy]
ClamSocket = /var/run/drweb.clamd
```

## 2. Настройка **HAVP**:

```
ENABLECLAMD true
CLAMDSOCKET /var/run/drweb.clamd
```

Настройки подключения к прочим антивирусным продуктам (параметры вида ENABLE\*) должны быть установлены в значение false.



## Dr.Web File Checker

Компонент проверки файлов Dr.Web File Checker предназначен для проверки файлов и каталогов файловой системы. Он используется другими компонентами программного комплекса Dr.Web для Интернет-шлюзов UNIX 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.

## Принципы работы

Компонент используется для доступа к любым объектам файловой системы (файлы, каталоги, загрузочные записи). Запускается с правами суперпользователя *root*.

Индексирует все проверенные файлы и каталоги и сохраняет данные о проверенных объектах в специальном кэше, 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 кэша). Схема работы компонента показана на рисунке ниже.

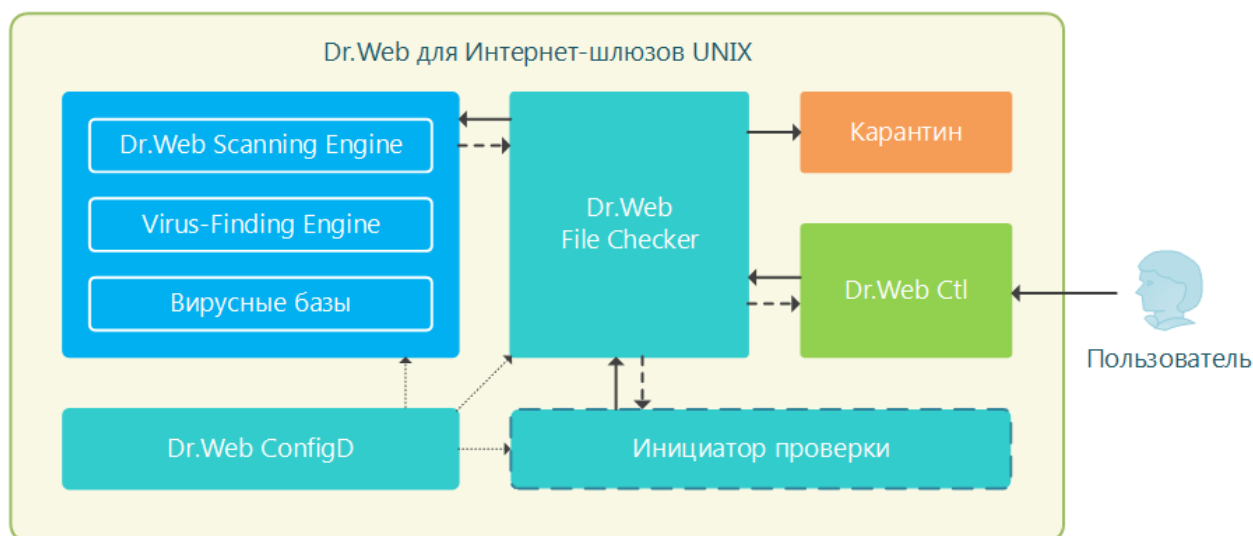


Рисунок 14. Схема работы компонента

При поступлении запросов на проверку объектов файловой системы от компонентов программного комплекса Dr.Web для Интернет-шлюзов UNIX проверяет, требуется ли проверка запрошенного объекта, и если да, то формирует задание на проверку его содержимого для сканирующего ядра [Dr.Web Scanning Engine](#). В случае если проверенный объект содержал угрозу, то Dr.Web File Checker заносит его в реестр обнаруженных угроз, применяет к нему нейтрализующее действие (лечение, удаление или перемещение в карантин), в случае если это действие задано клиентским компонентом, инициировавшим проверку, в качестве реакции на угрозу. В качестве инициаторов проверки могут выступать различные компоненты продукта.



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 данный метод, один раз инициализирует параметры проверки и обезвреживания угроз, и далее эти параметры будут применяться ко всему потоку заявок на проверку файлов, поступающих от компонента.
- *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 компонентом [Dr.Web ClamD](#).

Имеется возможность проверить файлы с использованием методов «flow» и «proxy», используя [команды](#) `flowscan` и `proxyscan` утилиты [Dr.Web Ctl](#) (запускается командой **drweb-ctl**), однако для обычной проверки файлов по требованию рекомендуется использовать только команду `scan`.

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.

## Аргументы командной строки

Для запуска компонента Dr.Web File Checker из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-filecheck [<параметры>]
```

Dr.Web File Checker допускает использование следующих параметров:

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



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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) при поступлении от других компонентов программного комплекса Dr.Web для Интернет-шлюзов UNIX заявок на проверку объектов файловой системы. Для управления параметрами работы компонента, а также для проверки файлов по требованию пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).

Для проверки сканирования произвольного файла или каталога компонентом Dr.Web File Checker вы можете воспользоваться командой `scan` утилиты Dr.Web Ctl:

```
$ drweb-ctl scan <путь к каталогу или файлу>
```



Для получения справки о компоненте из командной строки используйте команду **man 1 drweb-filecheck**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[FileCheck]` объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

Эта секция хранит следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> <code>[Root]</code> .  <b>Значение по умолчанию:</b> Notice
<b>Log</b> <i>{тип журнала}</i>	<a href="#">Метод ведения журнала</a>
<b>ExePath</b> <i>{путь к файлу}</i>	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <code>&lt;opt_dir&gt;/bin/drweb-filecheck</code>



	<ul style="list-style-type: none"><li>• Для <b>Linux, Solaris</b>: /opt/drweb.com/bin/drweb-filecheck</li><li>• Для <b>FreeBSD</b>: /usr/local/libexec/drweb.com/bin/drweb-filecheck</li></ul>
<b>DebugClientIpc</b> {логический}	Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) подробные сообщения IPC. <b>Значение по умолчанию:</b> No
<b>DebugScan</b> {логический}	Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) подробные сообщения, поступающие в процессе проверки файлов. <b>Значение по умолчанию:</b> No
<b>DebugFlowScan</b> {логический}	Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) подробные сообщения о проверке файлов методом «flow». <b>Значение по умолчанию:</b> No
<b>DebugProxyScan</b> {логический}	Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) подробные сообщения о проверке файлов методом «proxy». (Обычно метод «proxy» используется компонентом <a href="#">Dr.Web ClamD</a> ). <b>Значение по умолчанию:</b> No
<b>DebugCache</b> {логический}	Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) подробные сообщения о состоянии кэша проверенных файлов. <b>Значение по умолчанию:</b> No
<b>MaxCacheSize</b> {размер}	Максимальный разрешенный размер кэша для хранения информации о проверенных файлах. <i>Если указано 0 – кэширование отключено.</i> <b>Значение по умолчанию:</b> 50mb
<b>RescanInterval</b> {интервал времени}	Длительность интервала, в течение которого не производится повторная проверка содержимого файлов, информация о предыдущей проверке которых имеется в кэше (период актуальности кэшированной информации). <i>Допустимо значение от 0s до 1m (включительно). Если указан интервал менее 1s – задержка отсутствует, файл будет проверяться при любом запросе.</i> <b>Значение по умолчанию:</b> 1s
<b>IdleTimeLimit</b> {интервал времени}	Максимальное время простоя компонента, по превышению которого он завершает свою работу. <i>Допустимо значение от 10s до 30d (включительно).</i>



Значение по умолчанию: 30s



## Dr.Web Network Checker

Агент 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 продуктом Dr.Web для Интернет-шлюзов UNIX с целью приема и передачи данных (например – содержимого файлов) между узлами сети для их проверки. 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.

Обратите внимание, что этот компонент всегда используется для проверки данных, полученных через сетевые соединения. Поэтому, если данный компонент отсутствует или недоступен, будет нарушена работоспособность компонентов, отправляющих данные на проверку через сетевое соединение (Dr.Web ICAPD, Dr.Web ClamD).



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 величину лимита](#) на число файловых дескрипторов, доступных Dr.Web для Интернет-шлюзов UNIX.

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, при необходимости, можно воспользоваться утилитой **openssl**. Пример использования утилиты **openssl** для генерации сертификатов и закрытых ключей приведен в разделе [Приложение Д. Генерация сертификатов SSL](#).

## Принципы работы

Компонент Dr.Web Network Checker позволяет организовать соединение Dr.Web для Интернет-шлюзов UNIX с заданным набором узлов в сети с установленным на них продуктом Dr.Web для Интернет-шлюзов UNIX (или любым другим решением Dr.Web для UNIX версии не ниже 10.1) для организации распределенной проверки данных (например – содержимого файлов) на наличие в них угроз. Компонент позволяет создать и настроить *сканирующий кластер*, организовав набор подключений между узлами сети (на каждом узле должен быть запущен свой экземпляр агента распределенной проверки Dr.Web Network Checker).

На каждом узле сети, включенном в сканирующий кластер, агент Dr.Web Network Checker организует автоматическое распределение задач на проверку данных, передавая их по сети





на все доступные узлы, с которыми настроено соединение. При этом агент обеспечивает балансировку 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 этом узле). Также оцениваются длины очередей файлов, ожидающих проверки на каждом используемом узле. Данные, принятые по сети для проверки, передаются сканирующему ядру [Dr.Web Scanning Engine](#), как показано на рисунке ниже.

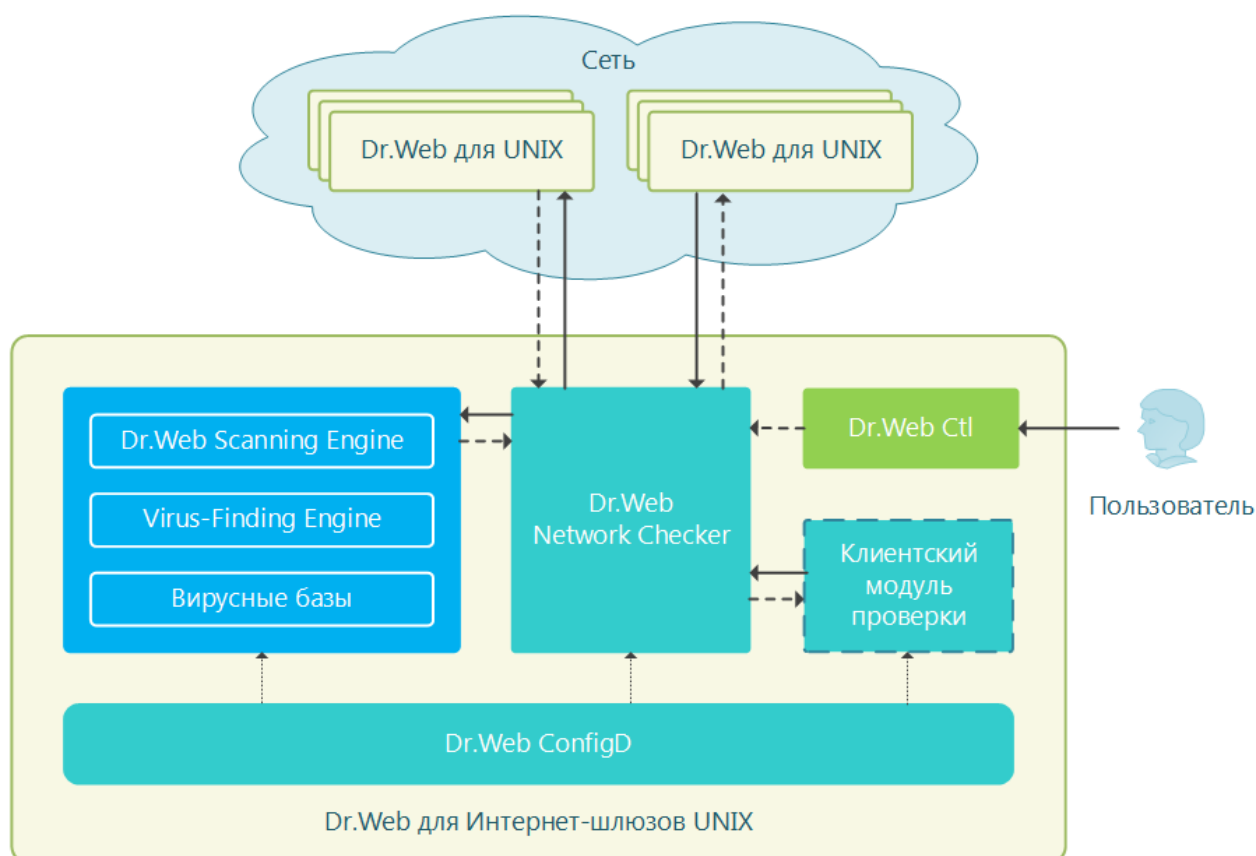


Рисунок 15. Схема работы компонента

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.

На локальном узле отправка данных на проверку через Dr.Web Network Checker может быть инициировано как непосредственно по команде пользователя, заданной через утилиту управления из командной строки [Dr.Web Ctl](#), так и по запросам от некоторых компонентов продукта, например – компонента [Dr.Web ClamD](#), предоставляющего интерфейс демона **clamd**, входящего в состав антивирусного решения **ClamAV®**. Поэтому на схеме указан абстрактный «Клиентский модуль проверки».



Следует иметь в виду, что компоненты, обозначенные на схеме как «Клиентский модуль проверки», всегда используют Dr.Web Network Checker для передачи файлов на проверку сканирующему ядру Dr.Web Scanning Engine, даже если он расположен на локальном узле. Поэтому, если Dr.Web Network Checker недоступен, эти компоненты не смогут корректно функционировать.



Имеется возможность создать свой собственный компонент (внешнее приложение), использующий Dr.Web Network Checker для проверки файлов (в том числе - путем распределения проверки по узлам сканирующего кластера). 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`.

## Аргументы командной строки

Для запуска компонента Dr.Web Network Checker из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-netcheck [<параметры>]
```

Dr.Web Network Checker допускает использование следующих параметров:

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

### Пример:

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

Данная команда выведет на экран краткую справку компонента Dr.Web Network Checker.

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости (обычно при старте операционной



системы). При этом, если в [конфигурации](#) компонента задано значение параметра **FixedSocketPath**, то агент всегда будет запущен демоном управления конфигурацией и доступен клиентам через этот UNIX-сокет. Для управления параметрами работы компонента, а также для запуска сетевого сканирования (при наличии настроенного соединения с другими узлами сети) пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)). Если соединение с другими узлами сети не настроено, вместо сетевого сканирования будет запущено обычное сканирование силами локального сканирующего ядра.

Для проверки обработки произвольного файла или каталога компонентом Dr.Web Network Checker вы можете воспользоваться командой `netscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```



Для получения справки о компоненте из командной строки используйте команду **man 1 drweb-netcheck**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [NetCheck] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> [Root].  <b>Значение по умолчанию:</b> Notice
<b>Log</b> <i>{тип журнала}</i>	<a href="#">Метод ведения журнала</a>
<b>ExePath</b> <i>{путь к файлу}</i>	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <code>&lt;opt_dir&gt;/bin/drweb-netcheck</code> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris</b>: <code>/opt/drweb.com/bin/drweb-netcheck</code></li><li>• Для <b>FreeBSD</b>: <code>/usr/local/libexec/drweb.com/bin/drweb-netcheck</code></li></ul>
<b>FixedSocketPath</b> <i>{путь к файлу}</i>	Путь к файлу UNIX-сокета фиксированной копии агента Dr.Web Network Checker.



	<p>При задании этого параметра демон управления конфигурацией <a href="#">Dr.Web ConfigD</a> следит за тем, чтобы всегда имелась запущенная копия агента распределенной проверки файлов, доступная клиентам через этот сокет.</p> <p><b>Значение по умолчанию:</b> <i>(не задано)</i></p>
<b>RunAsUser</b>  {UID   имя пользователя}	<p>Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр (т.е. похоже на числовой UID), то оно указывается с префиксом «name:», например: <b>RunAsUser</b> = name:123456.</p> <p><i>Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.</i></p> <p><b>Значение по умолчанию:</b> drweb</p>
<b>IdleTimeLimit</b>  {интервал времени}	<p>Максимальное время простоя компонента, по превышению которого он завершает свою работу.</p> <p>Минимальное значение – 10s.</p> <p><i>Если задано значение параметра <b>LoadBalanceAllowFrom</b> или <b>FixedSocketPath</b>, то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя).</i></p> <p><b>Значение по умолчанию:</b> 30s</p>
<b>LoadBalanceUseSsl</b>  {логический}	<p>Флаг, определяющий использование для соединения с другими узлами безопасного соединения SSL/TLS.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• Yes – Использовать SSL/TLS.</li><li>• No – Не использовать SSL/TLS.</li></ul> <p><i>В случае если этот параметр установлен в Yes, для данного узла и для всех узлов, с которыми он взаимодействует, должны быть обязательно заданы соответствующие друг другу сертификат и закрытый ключ (параметры <b>LoadBalanceSslCertificate</b> и <b>LoadBalanceSslKey</b>).</i></p> <p><b>Значение по умолчанию:</b> No</p>
<b>LoadBalanceSslCertificate</b>  {путь к файлу}	<p>Путь к файлу сертификата SSL, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS.</p> <p><i>Обратите внимание, что файл сертификата и файл закрытого ключа (определяется следующим параметром) должны соответствовать друг другу.</i></p>



	Значение по умолчанию: (не задано)
<b>LoadBalanceSslKey</b> <i>{путь к файлу}</i>	<p>Путь к файлу закрытого ключа, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS.</p> <p><i>Обратите внимание, что файл сертификата и файл закрытого ключа (определяется предыдущим параметром) должны соответствовать друг другу.</i></p> <p><b>Значение по умолчанию: (не задано)</b></p>
<b>LoadBalanceSslCa</b> <i>{путь}</i>	<p>Путь к каталогу или файлу, в котором располагается перечень корневых сертификатов, являющихся доверенными. Среди данных сертификатов должен находиться сертификат, удостоверяющий подлинность сертификатов, используемых агентами внутри сканирующего кластера при обмене данными через SSL/TLS.</p> <p><i>Если значение параметра не задано, то Dr.Web Network Checker, работающий на данном узле, не проверяет подлинность сертификатов взаимодействующих агентов, однако они, в свою очередь, могут, в зависимости от заданных для них настроек, проверять подлинность сертификата, используемого агентом, работающим на данном узле.</i></p> <p><b>Значение по умолчанию: (не задано)</b></p>
<b>LoadBalanceServerSocket</b> <i>{адрес}</i>	<p>Сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web Network Checker на данном узле для получения файлов на проверку от удаленных узлов (если она может работать как сервер сетевого сканирования).</p> <p><b>Значение по умолчанию: (не задано)</b></p>
<b>LoadBalanceAllowFrom</b> <i>{IP-адрес}</i>	<p>IP-адрес удаленного узла сети, от которого Dr.Web Network Checker на данном узле может принимать файлы на проверку (как сервер сетевого сканирования).</p> <p><i>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).</i></p> <p><b>Пример:</b> Добавить в список адреса узлов 192.168.0.1 и 10.20.30.45.</p> <p>1. Добавление значений в файл конфигурации.</p> <ul style="list-style-type: none"><li>• Два значения в одной строке</li></ul> <div><pre>[NetCheck] LoadBalanceAllowFrom = "192.168.0.1", "10.20.30.45"</pre></div>



	<ul style="list-style-type: none"><li>• Две строки (по одному значению в строке)</li></ul> <pre>[NetCheck] LoadBalanceAllowFrom = 192.168.0.1 LoadBalanceAllowFrom = 10.20.30.45</pre> <p>2. Добавление значений через <u>команды drweb-ctl</u> cfset.</p> <pre># drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 192.168.0.1 # drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 10.20.30.45</pre> <p><i>Если параметр пуст, удаленные файлы на проверку не принимаются (узел не работает в режиме сервера).</i></p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>LoadBalanceSourceAddress</b> <i>{IP-адрес}</i>	<p>IP-адрес сетевого интерфейса, используемого Dr.Web Network Checker на данном узле для передачи файлов на удаленную проверку, если узел работает как клиент сетевого сканирования и если на узле доступно несколько сетевых интерфейсов.</p> <p><i>Если указать пустое значение, то используемый сетевой интерфейс будет автоматически выбран ядром ОС.</i></p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>LoadBalanceTo</b> <i>{адрес}</i>	<p>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).</p> <p><i>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).</i></p> <p><b>Пример:</b> Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.</p> <p>1. Добавление значений в файл конфигурации.</p> <ul style="list-style-type: none"><li>• Два значения в одной строке</li></ul> <pre>[NetCheck] LoadBalanceTo = "192.168.0.1:1234", "10.20.30.45:5678"</pre> <ul style="list-style-type: none"><li>• Две строки (по одному значению в строке)</li></ul> <pre>[NetCheck] LoadBalanceTo = 192.168.0.1:1234 LoadBalanceTo = 10.20.30.45:5678</pre>



	<p>2. Добавление значений через <a href="#">команды drweb-ctl</a> cfset.</p> <pre># drweb-ctl cfset NetCheck.LoadBalanceTo -a 192.168.0.1:1234 # drweb-ctl cfset NetCheck.LoadBalanceTo -a 10.20.30.45:5678</pre> <p>Если параметр пуст, локальные файлы не передаются на удаленную проверку (узел не работает в режиме клиента сетевого сканирования).</p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>LoadBalanceStatusInterval</b> {интервал времени}	<p>Интервал времени между рассылками данным узлом информации о своей загрузке для всех агентов распределенной проверки, перечисленных в параметре <b>LoadBalanceAllowFrom</b>.</p> <p><b>Значение по умолчанию:</b> 1s</p>
<b>SpoolDir</b> {путь к каталогу}	<p>Каталог в локальной файловой системе, используемый для хранения файлов, принятых Dr.Web Network Checker по сети от клиентов сканирования для проверки.</p> <p><b>Значение по умолчанию:</b> /tmp/netcheck</p>
<b>LocalScanPreference</b> {дробное число}	<p>Относительный вес (предпочтительность) данного узла при выборе места для проверки файла (локального или принятого по сети). Если в некоторый момент времени вес локального узла больше весов всех доступных узлов-серверов сканирования, файл будет оставлен агентом для локальной проверки.</p> <p>Минимальное значение – 1.</p> <p><b>Значение по умолчанию:</b> 1</p>



## 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 комплекса Dr.Web для Интернет-шлюзов UNIX запросы на проверку объектов файловой системы на наличие угроз. *При отсутствии или недоступности компонентов Dr.Web Scanning Engine и Dr.Web Virus-Finding Engine никакая антивирусная проверка не производится.*

## Принципы работы

Компонент работает в качестве сервиса, принимающего от других компонентов программного комплекса Dr.Web для Интернет-шлюзов UNIX запросы на проверку объектов файловой системы (файлов, загрузочных записей на дисках) на наличие внедренных угроз. Формирует очереди задач на проверку объектов, 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. Схема функционирования сканирующего ядра Dr.Web Scanning Engine показана на рисунке ниже.

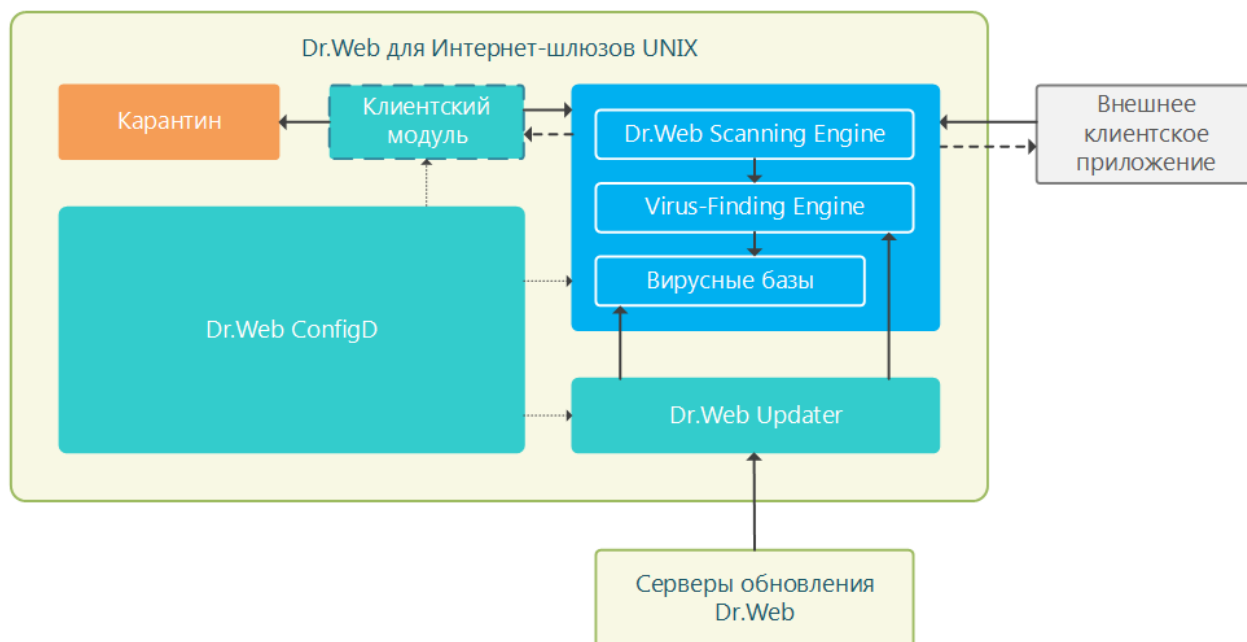


Рисунок 16. Схема работы компонента





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 продукта, 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 программный комплекс Dr.Web для Интернет-шлюзов UNIX функционирует в режиме централизованной защиты, то функции обновления вирусных баз и антивирусного ядра берет на себя агент централизованной защиты [Dr.Web ES Agent](#) (не показан на приведенной схеме). Этот компонент взаимодействует с сервером централизованной защиты и получает обновления от него.

Сканирующее ядро 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 антивирусных баз возлагаются на использующее его внешнее приложение. Компоненты программного комплекса Dr.Web для Интернет-шлюзов UNIX, выполняющие запросы к сканирующему ядру на предмет проверки файлов (обозначены на схеме как «Клиентский модуль»), используют тот же программный интерфейс, что и внешние приложения.



Имеется возможность 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» (<https://partners.drweb.com/>).

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 сканирующим ядром 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.



Следует помнить, что эвристический анализ не гарантирует достоверного распознавания угроз и может допускать ошибки первого и второго рода.

- *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 анализом, 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 и лечение как простых файлов, так и запакованных объектов и объектов, содержащихся в различных контейнерах (таких, как архивы, письма электронной почты и т.п.).

## Аргументы командной строки

Для запуска сканирующего ядра Dr.Web Scanning Engine из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-se <socket> [<параметры>]
```

где обязательный аргумент *<socket>* указывает адрес сокета, используемого Dr.Web Scanning Engine для обслуживания запросов клиентских компонентов. Может задаваться только в виде пути к файлу (сокеты UNIX).

Dr.Web Scanning Engine допускает использование следующих параметров:

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

*Дополнительные параметры запуска (совпадают с параметрами из конфигурационного файла и замещают их при необходимости):*



--EnginePath	<p><b>Назначение:</b> Указать путь к файлу библиотеки антивирусного ядра Dr.Web Virus-Finding Engine.</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;путь к файлу&gt; – полный путь к файлу используемой библиотеки.</p>
--VirusBaseDir	<p><b>Назначение:</b> Указать путь к каталогу, содержащему файлы вирусных баз.</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;путь к каталогу&gt; – полный путь к каталогу вирусных баз.</p>
--TempDir	<p><b>Назначение:</b> Указать путь к каталогу временных файлов.</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;путь к каталогу&gt; – полный путь к каталогу временных файлов.</p>
--Key	<p><b>Назначение:</b> Указать путь к используемому ключевому файлу.</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;путь к файлу&gt; – полный путь к ключевому файлу.</p>
--MaxForks	<p><b>Назначение:</b> Определить максимальное разрешенное число дочерних процессов, которые Dr.Web Scanning Engine может породить в процессе проверки.</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;число&gt; – максимальное разрешенное число дочерних процессов.</p>
--MaxForksPerFile	<p><b>Назначение:</b> Определить максимальное разрешенное число дочерних процессов, которые Dr.Web Scanning Engine может использовать при проверке одного составного файла (архива, контейнера и т.п.).</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;число&gt; – максимальное разрешенное число дочерних процессов. Не может быть меньше 1 и не может быть больше значения параметра --MaxForks.</p>
--WatchdogInterval	<p><b>Назначение:</b> Установить периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность дочерних процессов, занимающихся проверкой содержимого файлов, для остановки зависших при проверке.</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;интервал времени&gt; – периодичность проверки дочерних процессов.</p>
--Shelltrace	<p><b>Назначение:</b> Включить отслеживание оболочки (вывод в журнал расширенной информации о проверке файлов ядром Dr.Web Virus-Finding Engine).</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> Нет.</p>
--LogLevel	<p><b>Назначение:</b> Задать уровень подробности ведения журнала ядром Dr.Web Scanning Engine в процессе работы.</p> <p><b>Краткий вариант:</b> Нет.</p>



	<p><b>Аргументы:</b> &lt;уровень подробности&gt;. Возможные значения:</p> <ul style="list-style-type: none"><li>• <b>DEBUG</b> – Самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация.</li><li>• <b>INFO</b> – Выводятся все сообщения.</li><li>• <b>NOTICE</b> – Выводятся сообщения об ошибках, предупреждения, уведомления.</li><li>• <b>WARNING</b> – Выводятся сообщения об ошибках и предупреждения.</li><li>• <b>ERROR</b> – Выводятся только сообщения об ошибках.</li></ul>
--Log	<p><b>Назначение:</b> Задать способ ведения журнала сообщений компонента.</p> <p><b>Краткий вариант:</b> Нет.</p> <p><b>Аргументы:</b> &lt;тип журнала&gt;. Возможные значения:</p> <ul style="list-style-type: none"><li>• <b>Stderr[:ShowTimestamp]</b> – Сообщения будут выводиться в стандартный поток ошибок <b>stderr</b>. Дополнительная опция <b>ShowTimestamp</b> предписывает добавлять к каждому сообщению метку времени.</li><li>• <b>Syslog[:&lt;facility&gt;]</b> – Сообщения будут передаваться системной службе журналирования <b>syslog</b>. Дополнительная метка &lt;facility&gt; используется для указания типа журнала, в котором <b>syslog</b> будет сохранять сообщения. Возможные значения:<ul style="list-style-type: none"><li>○ <b>DAEMON</b> – сообщения демонов;</li><li>○ <b>USER</b> – сообщения пользовательских процессов;</li><li>○ <b>MAIL</b> – сообщения почтовых программ;</li><li>○ <b>LOCAL0</b> – сообщения локальных процессов 0;</li><li>...</li><li>○ <b>LOCAL7</b> – сообщения локальных процессов 7.</li></ul></li><li>• <b>&lt;path&gt;</b> – Путь к файлу, в который будут сохраняться сообщения журнала.</li></ul> <p><b>Примеры:</b></p> <pre>--Log /var/opt/drweb.com/log/se.log --Log Stderr:ShowTimestamp --Log Syslog:DAEMON</pre>

**Пример:**

```
$ /opt/drweb.com/bin/drweb-se /tmp/drweb.ipc/.se --MaxForks=5
```

Данная команда запустит копию сканирующего ядра Dr.Web Scanning Engine, заставив его создать для взаимодействия с клиентскими компонентами UNIX-сокеты /tmp/drweb.ipc/.se и породить не более 5 сканирующих дочерних процессов при проверке файлов.



## Замечания о запуске

При необходимости может быть запущено произвольное количество копий сканирующего ядра Dr.Web Scanning Engine, предоставляющих клиентским приложениям (не обязательно только компонентами комплекса Dr.Web для Интернет-шлюзов UNIX) сервис по проверке файлов на наличие угроз. При этом, если в [конфигурации](#) компонента задано значение параметра **FixedSocketPath**, то одна копия сканирующего ядра всегда будет автоматически запущена демоном управления конфигурацией [Dr.Web ConfigD](#) и доступна клиентам через этот 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 пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).

Для проверки сканирования произвольного файла или каталога компонентом Dr.Web Scanning Engine вы можете воспользоваться командой `rawscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl rawscan <путь к каталогу или файлу>
```



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

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ScanEngine]` объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

Эта секция хранит следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> <code>[Root]</code> .  <b>Значение по умолчанию:</b> <code>Notice</code>
<b>Log</b> <i>{тип журнала}</i>	<a href="#">Метод ведения журнала</a>
<b>ExePath</b> <i>{путь к файлу}</i>	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <code>&lt;opt_dir&gt;/bin/drweb-se</code> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/opt/drweb.com/bin/drweb-se</code></li><li>• Для <b>FreeBSD:</b> <code>/usr/local/libexec/drweb.com/bin/drweb-se</code></li></ul>



<b>FixedSocketPath</b> <i>{путь к файлу}</i>	<p>Путь к файлу UNIX-сокета фиксированной копии сканирующего ядра Dr.Web Scanning Engine.</p> <p>При задании этого параметра демон управления конфигурацией <a href="#">Dr.Web ConfigD</a> следит за тем, чтобы всегда имела запуская копия сканирующего ядра, доступная клиентам через этот сокет.</p> <p><b>Значение по умолчанию:</b> <i>(не задано)</i></p>
<b>IdleTimeLimit</b> <i>{интервал времени}</i>	<p>Максимальное время простоя компонента, по превышению которого он завершает свою работу.</p> <p>Минимальное значение – 10с.</p> <p><i>Если задано значение параметра <b>FixedSocketPath</b>, то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя).</i></p> <p><b>Значение по умолчанию:</b> 30с</p>
<b>MaxForks</b> <i>{целое число}</i>	<p>Определяет максимальное разрешенное количество копий дочерних сканирующих процессов, порождаемых сканирующим ядром Dr.Web Scanning Engine, которые одновременно могут быть запущены.</p> <p><b>Значение по умолчанию:</b> Автоматически определяется при старте, как удвоенное число доступных процессорных ядер, или 4, если полученное число меньше 4.</p>
<b>MaxForksPerFile</b> <i>{целое число}</i>	<p>Определяет максимальное разрешенное количество копий дочерних сканирующих процессов, которые одновременно могут быть запущены Dr.Web Scanning Engine при проверке файлов-контейнеров (таких как архивы).</p> <p>Не может быть меньше 1 и не может быть больше значения, указанного в параметре <b>MaxForks</b>.</p> <p><b>Значение по умолчанию:</b> Автоматически определяется при старте, как величина <math>\text{MaxForks} / 2</math>.</p>
<b>BufferedIo</b> <i>{On   Off}</i>	<p>Использовать буферизованный ввод-вывод при проверке файлов.</p> <p><i>Использование буферизованного ввода-вывода в ОС <b>FreeBSD</b> и <b>Linux</b> может увеличить скорость проверки файлов, расположенных на медленных дисковых устройствах.</i></p> <p><b>Значение по умолчанию:</b> Off</p>
<b>WatchdogInterval</b> <i>{интервал времени}</i>	<p>Определяет периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность порожденных им дочерних сканирующих процессов для обнаружения зависаний при проверке («сторожевой таймер»).</p> <p><b>Значение по умолчанию:</b> 1.5с</p>



## Dr.Web Updater

Компонент обновлений Dr.Web Updater предназначен для получения всех имеющихся обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine с серверов обновлений компании «Доктор Веб».

Если Dr.Web для Интернет-шлюзов UNIX работает в режиме централизованной защиты, то в качестве источника обновлений используется сервер централизованной защиты (например, Dr.Web Enterprise Server), причем все обновления получают с сервера через Dr.Web ES Agent, а Dr.Web Updater для загрузки обновлений не используется.

## 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. Списки серверов, образующих доступную зону обновлений, хранятся в специальном файле (этот файл подписан с целью невозможности его модификации).

Если программный комплекс 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. Запуск производится с периодичностью, указанной в настройках. Также компонент может быть запущен демоном управления конфигурацией в ответ на поступившую команду пользователя (внеочередное обновление). Схема работы компонента показана на рисунке ниже.

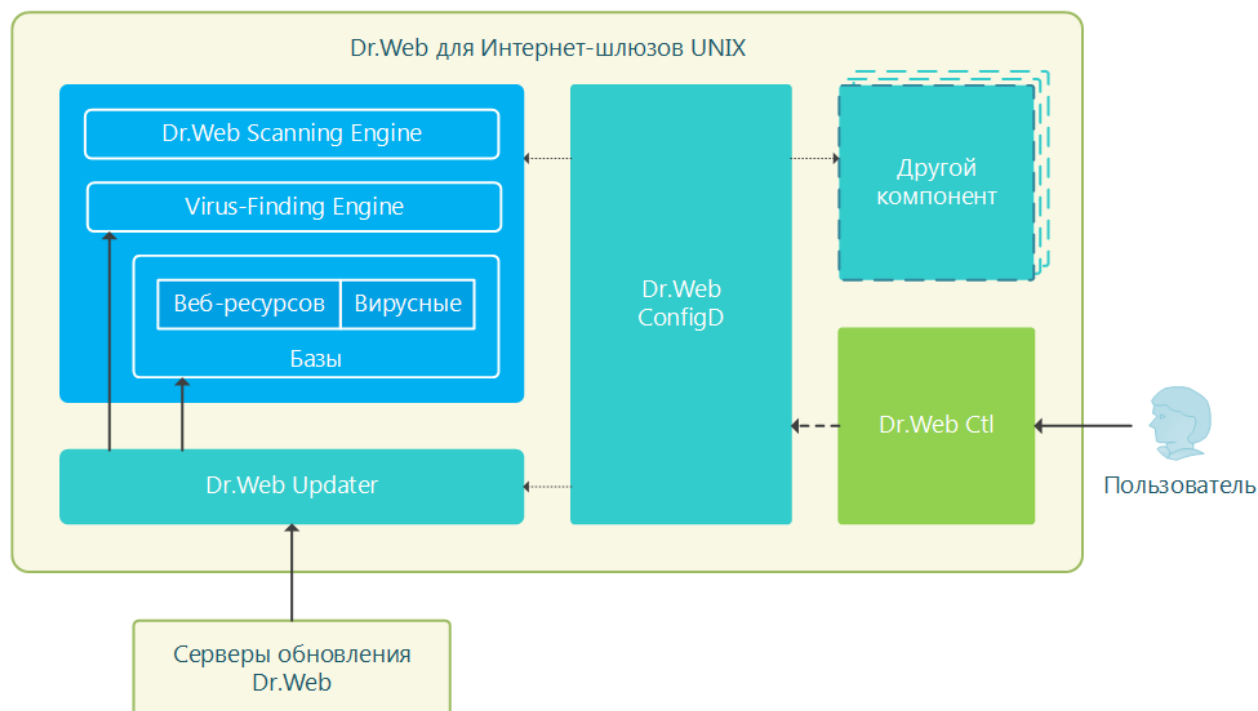


Рисунок 17. Схема работы компонента



При наличии на серверах обновлений доступных обновлений, они загружаются в каталог `<var_dir>/cache` (для **Linux** – `/var/opt/drweb.com/cache/`), после чего размещаются в рабочих каталогах программного продукта Dr.Web для Интернет-шлюзов UNIX.

По умолчанию все обновления производятся 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 **\*Dr1Dir**, сгруппированных по типу выполняемого обновления: для вирусных баз и антивирусного ядра, для базы категорий веб-ресурсов). При необходимости по запросу клиента может быть создана особая зона обновления (для каждого вида обновления), список серверов который указывается в отдельном файле (по умолчанию – с именем `custom.drl`), располагающемся в каталоге, указанном в соответствующем параметре **\*CustomDr1Dir**. В этом случае компонент обновлений будет получать только с этих серверов, не используя серверы из зоны по умолчанию.

Для отказа от использования особой зоны обновления достаточно очистить значение соответствующего параметра **\*CustomDr1Dir** 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 продуктом Dr.Web для Интернет-шлюзов UNIX из командной строки [Dr.Web Ctl](#) (запускается командой **drweb-ctl**).

## Аргументы командной строки

Для запуска компонента Dr.Web Updater из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-update [<параметры>]
```

Dr.Web Updater допускает использование следующих параметров:

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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. 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 для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду **man 1 drweb-update**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [Update] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> [Root].  <b>Значение по умолчанию:</b> Notice
<b>Log</b> <i>{тип журнала}</i>	<a href="#">Метод ведения журнала</a>
<b>ExePath</b> <i>{путь к файлу}</i>	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <opt_dir>/bin/drweb-update <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /opt/drweb.com/bin/drweb-update</li><li>• Для <b>FreeBSD:</b> /usr/local/libexec/drweb.com/bin/drweb-update</li></ul>
<b>RunAsUser</b>	Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой



<b>{UID   имя пользователя}</b>	<p>UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр (т.е. похоже на числовой UID), то оно указывается с префиксом «name:», например: <b>RunAsUser</b> = name:123456.</p> <p><i>Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.</i></p> <p><b>Значение по умолчанию:</b> drweb</p>
<b>UpdateInterval</b> <b>{интервал времени}</b>	<p>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.</p> <p><b>Значение по умолчанию:</b> 30m</p>
<b>RetryInterval</b> <b>{интервал времени}</b>	<p>Частота повторных попыток выполнить обновление с серверов обновления в случае если очередная попытка выполнить обновление завершилась неудачей.</p> <p>Параметр может принимать значение от 1m до 30m включительно.</p> <p><b>Значение по умолчанию:</b> 3m</p>
<b>MaxRetries</b> <b>{целое число}</b>	<p>Количество повторных попыток выполнить обновление с серверов обновления Dr.Web (предпринимаемых через промежутки времени, указанные в параметре <b>RetryInterval</b>), если предыдущая попытка выполнить обновление с серверов обновления окончилась неудачей.</p> <p><i>Если значение параметра – 0, повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени, указанный в параметре <b>UpdateInterval</b>).</i></p> <p><b>Значение по умолчанию:</b> 3</p>
<b>Прoxy</b> <b>{строка подключения}</b>	<p>Хранит 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).</p> <p>Если значение параметра не задано, прокси-сервер не используется.</p> <p><b>Возможные значения:</b></p> <p>&lt;строка подключения&gt; – Строка подключения к прокси-серверу. Имеет следующий формат (URL):</p> <p>[ &lt;protocol&gt; : // ] [ &lt;user&gt; : &lt;password&gt; @ ] &lt;proxyhost&gt; : &lt;port&gt;</p> <p>где:</p>



- `<protocol>` – Типа используемого протокола (в текущей версии доступен только `http`).
- `<user>` – Имя пользователя для подключения к прокси.
- `<password>` – Пароль для подключения к прокси.
- `<proxyhost>` – Адрес узла, на котором работает прокси (IP-адрес или имя домена, т.е. FQDN).
- `<port>` – Используемый порт.

Параметры `<protocol>` и `<user>:<password>` могут отсутствовать. Адрес прокси `<proxyhost>:<port>` является обязательным.

Если имя пользователя (`<user>`) или пароль (`<password>`) содержат символы '@', '%' или ':', то они должны быть заменены на коды "%40", "%25" и "%3A" соответственно.

#### Примеры:

##### 1. В файле конфигурации:

- Подключение к прокси на узле `proxyhost.company.org` на порт `123`:

**Proxy** = `proxyhost.company.org:123`

- Подключение к прокси 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 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 использованием [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}

Определяет 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`.



	<p>1. Добавление значений в файл конфигурации.</p> <ul style="list-style-type: none"><li>• Два значения в одной строке</li></ul> <pre>[Update] ExcludedFiles = "123.vdb", "456.dws"</pre> <ul style="list-style-type: none"><li>• Две строки (по одному значению в строке)</li></ul> <pre>[Update] ExcludedFiles = 123.vdb ExcludedFiles = 456.dws</pre> <p>2. Добавление значений через <b>команду drweb-ctl</b> cfset.</p> <pre># drweb-ctl cfset Update.ExcludedFiles -a 123.vdb # drweb-ctl cfset Update.ExcludedFiles -a 456.dws</pre> <p><b>Значение по умолчанию:</b> drweb32.lst</p>
<b>NetworkTimeout</b> {интервал времени}	<p>Тайм-аут на сетевые операции компонента обновления при выполнении обновлений с серверов обновления Dr.Web.</p> <p>Используется для ожидания продолжения обновления в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то обновление будет продолжено.</p> <p><i>Не имеет смысла указывать величину тайм-аута более 75s, т.к. за это время соединение закроется по тайм-ауту TCP.</i></p> <p><i>Минимально допустимое значение – 5s.</i></p> <p><b>Значение по умолчанию:</b> 60s</p>
<b>BaseDrlPath</b> {путь к файлу}	<p>Определяет путь к подписанному файлу списка серверов стандартной зоны обновления, используемых компонентом обновлений для обновления вирусных баз и антивирусного ядра.</p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/drl/bases/update.drl</p> <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/drl/bases/update.drl</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/drl/bases/update.drl</li></ul>
<b>BaseCustomDrlPath</b> {путь к файлу}	<p>Определяет путь к подписанному файлу списка серверов особой зоны обновления, используемых компонентом обновлений для обновления вирусных баз и антивирусного ядра.</p> <p><i>Если этот параметр не пуст, и указанный файл существует, для обновления используются только эти серверы. Основной файл списка (см. выше) игнорируется. Если файл, на который указывает параметр, пуст, попытка обновления завершится ошибкой.</i></p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/drl/bases/custom.drl</p>



	<ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/drl/bases/custom.drl</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/drl/bases/custom.drl</li></ul>
<b>BaseUpdateEnabled</b> {логический}	<p>Флаг, указывающий, разрешено или запрещено обновление вирусных баз и антивирусного ядра.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• Yes – Обновление разрешено и будет производиться.</li><li>• No – Обновление не разрешено и не будет производиться.</li></ul> <p><b>Значение по умолчанию:</b> Yes</p>
<b>VersionDrlPath</b> {путь к файлу}	<p>Определяет путь к подписанному файлу списка серверов зоны обновления, используемых компонентом обновлений для обновления версий компонентов Dr.Web для Интернет-шлюзов UNIX.</p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/drl/version/update.drl</p> <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/drl/version/update.drl</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/drl/version/update.drl</li></ul>
<b>VersionUpdateEnabled</b> {логический}	<p>Флаг, указывающий, разрешено или запрещено обновление версий компонентов Dr.Web для Интернет-шлюзов UNIX.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• Yes – Обновление разрешено и будет производиться.</li><li>• No – Обновление не разрешено и не будет производиться.</li></ul> <p><b>Значение по умолчанию:</b> Yes</p>
<b>DwsDrlPath</b> {путь к файлу}	<p>Определяет путь к подписанному файлу списка серверов стандартной зоны обновления, используемых компонентом обновлений для обновления базы категорий веб-ресурсов.</p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/drl/dws/update.drl</p> <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/drl/dws/update.drl</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/drl/dws/update.drl</li></ul>
<b>DwsCustomDrlPath</b> {путь к файлу}	<p>Определяет путь к подписанному файлу списка серверов особой зоны обновления, используемых компонентом обновлений для обновления базы категорий веб-ресурсов.</p> <p><i>Если этот параметр не пуст, и указанный файл существует, для обновления используются только эти серверы. Основной файл списка (см. выше) игнорируется. Если файл, на который указывает параметр, пуст, попытка обновления завершится ошибкой.</i></p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/drl/dws/custom.drl</p>



	<ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/drl/dws/custom.drl</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/drl/dws/custom.drl</li></ul>
<b>DwsUpdateEnabled</b> <i>{логический}</i>	<p>Флаг, указывающий, разрешено или запрещено обновление базы категорий веб-ресурсов.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• Yes – Обновление разрешено и будет производиться.</li><li>• No – Обновление не разрешено и не будет производиться.</li></ul> <p><b>Значение по умолчанию:</b> Yes</p>
<b>AntispamDrlPath</b> <i>{путь к файлу}</i>	<p>Параметр не используется.</p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/drl/antispam/update.drl</p> <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/drl/antispam/update.drl</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/drl/antispam/update.drl</li></ul>
<b>AntispamCustomDrlPath</b> <i>{путь к файлу}</i>	<p>Параметр не используется.</p> <p><b>Значение по умолчанию:</b> &lt;var_dir&gt;/drl/antispam/custom.drl</p> <ul style="list-style-type: none"><li>• Для <b>Linux</b>, <b>Solaris:</b> /var/opt/drweb.com/drl/antispam/custom.drl</li><li>• Для <b>FreeBSD:</b> /var/drweb.com/drl/antispam/custom.drl</li></ul>
<b>AntispamUpdateEnabled</b> <i>{логический}</i>	<p>Параметр не используется.</p> <p><b>Значение по умолчанию:</b> No</p>
<b>BackupDir</b> <i>{путь к каталогу}</i>	<p>Определяет путь к каталогу, в который сохраняются старые версии обновляемых файлов для возможности отката обновлений. При каждом обновлении сохраняются резервные копии только обновленных файлов.</p> <p><b>Значение по умолчанию:</b> /tmp/update-backup</p>
<b>MaxBackups</b> <i>{целое число}</i>	<p>Максимальное количество сохраняемых предыдущих версий обновляемых файлов. При превышении этой величины самая старая копия удаляется при очередном обновлении.</p> <p><i>Если значение параметра – 0, то предыдущие версии файлов для восстановления не сохраняются.</i></p> <p><b>Значение по умолчанию:</b> 0</p>



## Dr.Web ES Agent

Агент централизованной защиты Dr.Web ES Agent предназначен для подключения программного комплекса Dr.Web для Интернет-шлюзов UNIX к серверу [централизованной защиты](#) (например, к Dr.Web Enterprise Server).

Когда Dr.Web для Интернет-шлюзов UNIX подключен к серверу централизованной защиты, Dr.Web ES Agent синхронизирует лицензионный [ключевой файл](#) в соответствии с ключами, хранящимися на сервере централизованной защиты. Кроме того, Dr.Web ES Agent передает на сервер централизованной защиты, к которому он подключен, статистику вирусных инцидентов, перечень запущенных компонентов и их состояние.

Также Dr.Web ES Agent выполняет обновление вирусных баз Dr.Web для Интернет-шлюзов UNIX непосредственно с подключенного сервера централизованной защиты, минуя компонент обновления [Dr.Web Updater](#).

## Принципы работы

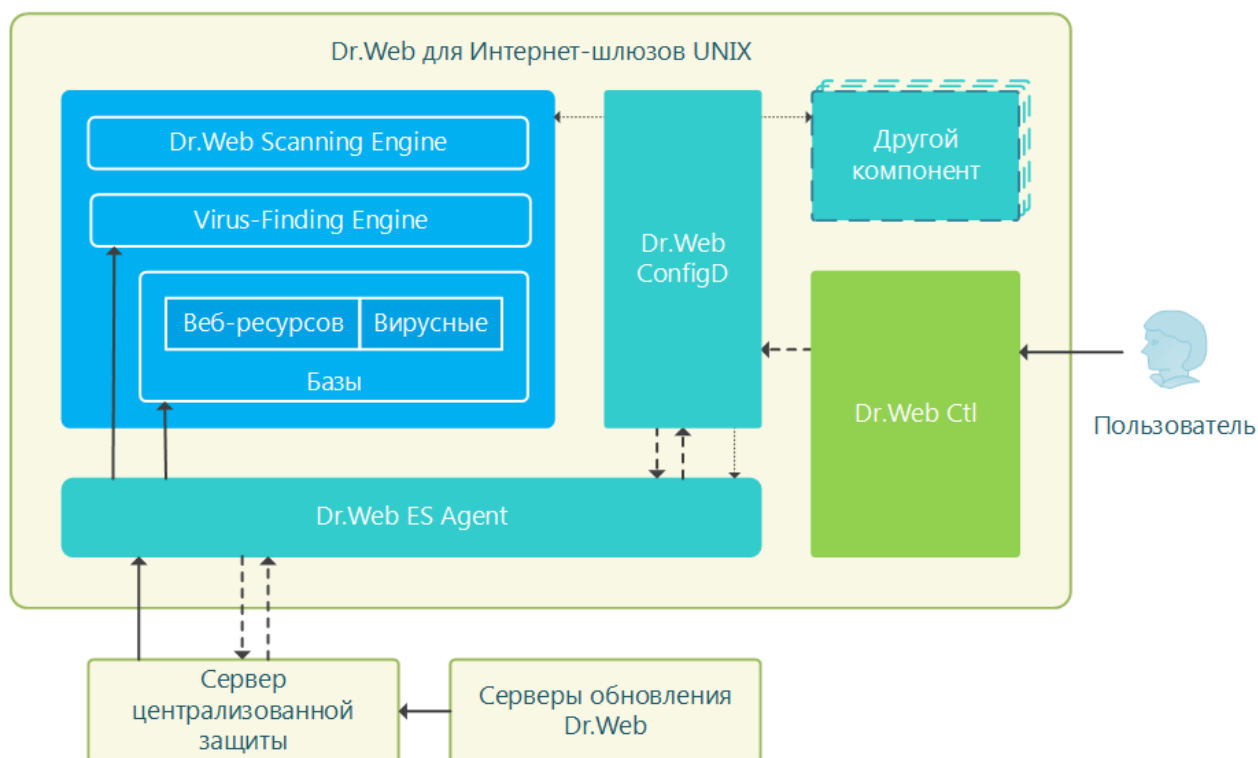
Компонент Dr.Web ES Agent осуществляет подключение к серверу централизованной защиты (например, к Dr.Web Enterprise Server), который позволяет администратору сети реализовать на всем пространстве сети единую политику безопасности, в частности – настроить на всех рабочих станциях и серверах сети одинаковые 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).



Обратите внимание, что в текущей версии поддержка режима централизованной защиты для Dr.Web для Интернет-шлюзов UNIX реализована *не полностью*: сервер не управляет настройками компонентов программного комплекса.

Dr.Web ES Agent собирает и отправляет на сервер, к которому он подключен, статистику обнаружения различных угроз и примененных действий. Схема работы компонента показана на рисунке ниже.



**Рисунок 18. Схема работы компонента**

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, обеспечивающего управление антивирусной защитой сети через сервер централизованной защиты.

Кроме того, если данная возможность разрешена на сервере централизованной защиты, имеется возможность подключить к нему узел с защищаемым сервером («рабочую станцию») в режиме «новичок». В этом случае, после подтверждения заявки на подключение станции администратором, сервер централизованной защиты автоматически сгенерирует для узла новые идентификатор и пароль, которые отправит агенту для использования при последующих подключениях.





## Аргументы командной строки

Для запуска компонента Dr.Web ES Agent из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-esagent [<параметры>]
```

Dr.Web ES Agent допускает использование следующих параметров:

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

**Пример:**

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

Данная команда выведет на экран краткую справку компонента Dr.Web ES Agent.

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически, при старте операционной системы, демоном управления конфигурацией [Dr.Web ConfigD](#). Для управления параметрами работы компонента, а также для подключения Dr.Web для Интернет-шлюзов UNIX к серверу централизованной защиты пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду **man 1 drweb-esagent**

## Параметры конфигурации


Компонент использует параметры конфигурации, заданные в секции [ESAgent] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.



В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<p><u>Уровень подробности</u> ведения журнала компонента.</p> <p>Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <u>секции</u> [Root].</p> <p><b>Значение по умолчанию:</b> Notice</p>
<b>Log</b> <i>{тип журнала}</i>	<p><u>Метод ведения журнала</u></p>
<b>ExePath</b> <i>{путь к файлу}</i>	<p>Путь к исполняемому файлу компонента.</p> <p><b>Значение по умолчанию:</b> &lt;opt_dir&gt;/bin/drweb-esagent</p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /opt/drweb.com/bin/drweb-esagent</li><li>• Для <b>FreeBSD:</b> /usr/local/libexec/drweb.com/bin/drweb-esagent</li></ul>
<b>DebugIpc</b> <i>{логический}</i>	<p>Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) подробные сообщения IPC (взаимодействие Dr.Web ES Agent и демона управления конфигурацией <u>Dr.Web ConfigD</u>).</p> <p><b>Значение по умолчанию:</b> No</p>
<b>MobileMode</b> <i>{On   Off   Auto}</i>	<p>Определяет возможность программного комплекса, при подключении к серверу централизованной защиты, работать в мобильном режиме.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• On – Использовать мобильный режим, если он разрешен сервером централизованной защиты (выполнять обновления с серверов обновлений компании «Доктор Веб» через <u>Dr.Web Updater</u>).</li><li>• Off – Не использовать мобильный режим, оставаться в режиме централизованной защиты (обновления всегда получаются только с сервера централизованной защиты).</li><li>• Auto – Использовать мобильный режим, если он разрешен сервером централизованной защиты, а обновления выполнять как с серверов обновлений компании «Доктор Веб» через Dr.Web Updater, так и с сервера централизованной защиты, в зависимости от того, какое соединение доступно и качество какого соединения лучше.</li></ul> <p><i>Обратите внимание, что поведение данного параметра зависит от разрешений на сервере: если мобильный режим на используемом сервере не разрешен, то этот параметр не имеет никакого эффекта.</i></p> <p><b>Значение по умолчанию:</b> Auto</p>
<b>Discovery</b> <i>{On   Off}</i>	<p>Разрешает или запрещает агенту принимать <i>discovery</i>-запросы от инспектора сети, встроенного в сервер централизованной защиты (<i>discovery</i>-запросы используются инспектором для проверки структуры и состояния антивирусной сети).</p>



	<p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• On – Разрешать агенту принимать и обрабатывать <i>discovery</i>-запросы.</li><li>• Off – Не разрешать агенту принимать и обрабатывать <i>discovery</i>-запросы.</li></ul> <p>Обратите внимание, что параметр имеет приоритет выше, чем настройки сервера централизованной защиты: если указано значение Off, агент не будет принимать <i>discovery</i>-запросы, даже если эта функция включена на сервере.</p> <p><b>Значение по умолчанию:</b> On</p>
<p><b>UpdatePlatform</b> <i>{название платформы}</i></p>	<p>Указывает агенту получать с сервера централизованной защиты обновления для антивирусного ядра, разработанного для указанной платформы, где <i>название платформы</i> – строка, содержащая название платформы.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• <b>GNU/Linux:</b> unix-linux-32, unix-linux-64, unix-linux-mips</li><li>• <b>FreeBSD:</b> unix-freebsd-32, unix-freebsd-64</li><li>• <b>Solaris:</b> unix-solaris-32, unix-solaris-64</li><li>• <b>Darwin:</b> unix-darwin-32, unix-darwin-64</li></ul> <div><p>Настоятельно не рекомендуется изменять значение параметра, если вы не уверены, что это действительно необходимо.</p></div> <p><b>Значение по умолчанию:</b> Зависит от текущей используемой платформы</p>



## Dr.Web HTTPD

Компонент Dr.Web HTTPD обеспечивает инфраструктуру для локального или удаленного взаимодействия с Dr.Web для Интернет-шлюзов UNIX посредством протокола HTTP (например – через веб-браузер). Компонент предоставляет два интерфейса: интерфейс для управления продуктом (соответствующий пакет с файлами веб-интерфейса управления, предназначенного для доступа через браузер, должен быть установлен отдельно, в дополнение к Dr.Web HTTPD), а также служебный интерфейс, используемый компонентом Dr.Web Link Checker – расширением для браузеров **Mozilla Firefox** и **Google Chrome** (также устанавливается отдельно).

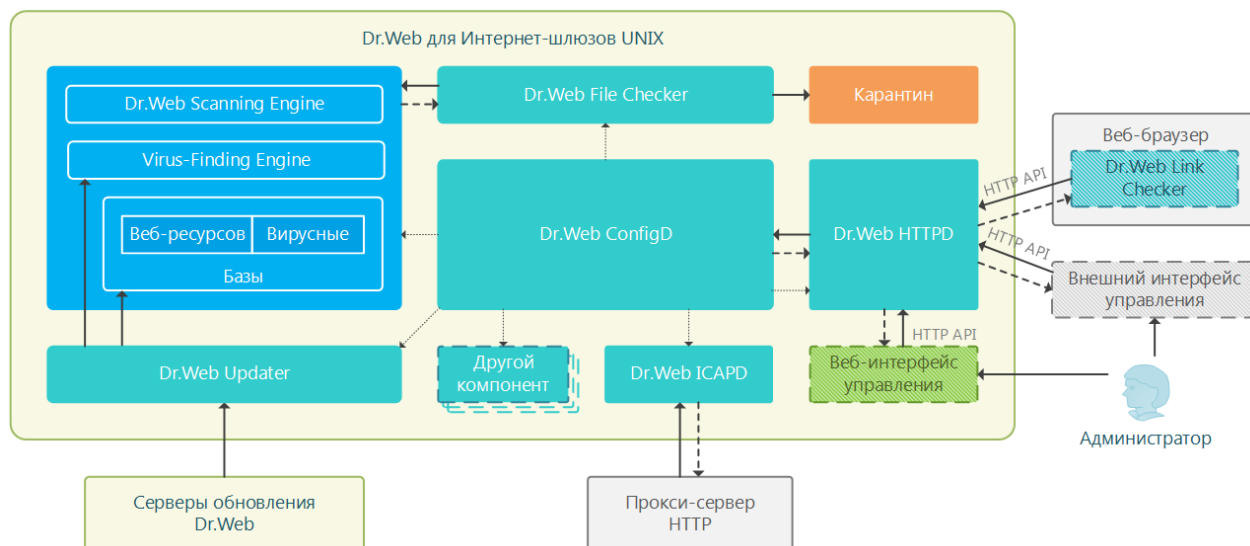
Помимо управления Dr.Web для Интернет-шлюзов UNIX через веб-интерфейс от Dr.Web, имеется возможность использовать непосредственно командный интерфейс (HTTP API) Dr.Web HTTPD для взаимодействия с компонентами Dr.Web для Интернет-шлюзов UNIX по протоколу HTTPS. Данная возможность позволяет разработать для Dr.Web для Интернет-шлюзов UNIX собственный управляющий интерфейс.

При использовании защищенного соединения HTTPS необходимо обеспечить сервер Dr.Web HTTPD корректным сертификатом и закрытым ключом SSL. По умолчанию для Dr.Web HTTPD серверный сертификат и закрытый ключ SSL генерируются автоматически, в процессе установки, но при необходимости вы можете сгенерировать для сервера собственную пару сертификат/ключ. При необходимости генерации ключей и сертификатов SSL вы можете воспользоваться утилитой **openssl**. Пример использования утилиты **openssl** для генерации сертификатов и закрытых ключей приведен в разделе [Приложение Д. Генерация сертификатов SSL](#).

## Принципы работы

Dr.Web HTTPD представляет собой веб-сервер, специально разработанный для управления работой Dr.Web для Интернет-шлюзов UNIX, позволяя тем самым не использовать для этих целей как сторонние веб-серверы (такие как **Apache HTTP Server** или **Nginx**), так и управляющие сервисы наподобие **Webmin**. Более того, он может работать с ними на одном узле, не препятствуя их функционированию.

Сервер Dr.Web HTTPD обслуживает запросы, поступающие по протоколам HTTP и HTTPS на сокеты, заданные в его настройках, что позволяет ему не конфликтовать с другими веб-серверами, если они также используются на этом узле. Схема работы компонента показана на рисунке ниже.

**Рисунок 19. Схема работы компонента**

Безопасный протокол HTTPS используется для управления продуктом, а протокол HTTP – для обслуживания запросов расширения веб-браузеров Dr.Web Link Checker (устанавливается в браузер отдельно).



Веб-интерфейс управления Dr.Web и расширение Dr.Web Link Checker не являются обязательными для функционирования продукта, и могут отсутствовать, поэтому соответствующие блоки на схеме обведены пунктирной границей.

Компонент Dr.Web HTTPD формирует управляющие команды к демону управления конфигурацией [Dr.Web ConfigD](#) Dr.Web для Интернет-шлюзов UNIX, компоненту проверки файлов [Dr.Web File Checker](#), на основании команд, полученных через HTTP API, (в том числе – через веб-интерфейс управления или от запросов расширения Dr.Web Link Checker).

Если веб-интерфейс управления Dr.Web для Интернет-шлюзов UNIX, использующий Dr.Web HTTPD, входит в состав продукта, то его описание приведено в соответствующем [разделе](#).

Если в состав продукта не включен веб-интерфейс управления Dr.Web, имеется возможность подключить к продукту любой внешний интерфейс управления, использующий для взаимодействия с компонентами продукта HTTP API Dr.Web HTTPD (не описывается в данном руководстве).



Для получения описания HTTP API Dr.Web HTTPD обратитесь в отдел по работе с партнерами компании «Доктор Веб» (<https://partners.drweb.com/>).



## Аргументы командной строки

Для запуска компонента Dr.Web HTTPD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-httpd [<параметры>]
```

Dr.Web HTTPD допускает использование следующих параметров:

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

**Пример:**

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

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

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости (обычно при старте операционной системы). Если компонент запущен, а также если установлен веб-интерфейс управления, то для управления работой компонентов Dr.Web для Интернет-шлюзов UNIX достаточно выполнить HTTPS-подключение к одному из адресов, обслуживающих функционирование веб-интерфейса, при помощи любого стандартного браузера. Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду **man 1 drweb-httpd**



## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [HTTPD] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>LogLevel</b>  {уровень подробности}	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> [Root].  <b>Значение по умолчанию:</b> Notice
<b>Log</b>  {тип журнала}	<a href="#">Метод ведения журнала</a>
<b>ExecPath</b>  {путь к файлу}	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <opt_dir>/bin/drweb-httpd <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /opt/drweb.com/bin/drweb-httpd</li><li>• Для <b>FreeBSD:</b> /usr/local/libexec/drweb.com/bin/drweb-httpd</li></ul>
<b>Start</b>  {логический}	Компонент должен быть запущен демоном управления конфигурацией <a href="#">Dr.Web ConfigD</a> .  Установка данного параметра в Yes предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение No – немедленно завершить работу компонента.  <b>Значение по умолчанию:</b> Зависит от того, установлен ли веб-интерфейс управления продуктом.
<b>WebConsoleAddress</b>  {адрес, ...}	Определяет список сетевых сокетов (каждый сетевой сокет определяется парой <IP-адрес>:<порт>), прослушиваемых Dr.Web HTTPD в ожидании подключений к <a href="#">веб-интерфейсу</a> управления продуктом, если он установлен. Доступ к веб-интерфейсу на данные адреса производится через HTTPS.  Если не указано ни одного значения, то использование веб-интерфейса управления невозможно.  <b>Значение по умолчанию:</b> 127.0.0.1:4443
<b>LinkCheckerAddress</b>  {адрес, ...}	Определяет список сетевых сокетов (каждый сетевой сокет определяется парой <IP-адрес>:<порт>), прослушиваемых Dr.Web HTTPD в ожидании подключений по HTTP от расширения Dr.Web Link Checker, проверяющего веб-страницы, загружаемые в браузер, на наличие вредоносных объектов.



	<p>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).</p> <p><b>Пример:</b> Добавить в список сокет 192.168.0.1:1234 и 10.20.30.45:5678.</p> <p>1. Добавление значений в файл конфигурации.</p> <ul style="list-style-type: none"><li>• Два значения в одной строке</li></ul> <pre>[&lt;%HTTPD_SECTION%&gt;] LinkCheckerAddress = "192.168.0.1:1234", "10.20.30.45:5678"</pre> <ul style="list-style-type: none"><li>• Две строки (по одному значению в строке)</li></ul> <pre>[&lt;%HTTPD_SECTION%&gt;] LinkCheckerAddress = 192.168.0.1:1234 LinkCheckerAddress = 10.20.30.45:5678</pre> <p>2. Добавление значений через <b>команду drweb-ctl cfset</b>.</p> <pre># drweb-ctl cfset &lt;%HTTPD_SECTION%&gt; &gt;.LinkCheckerAddress -a 192.168.0.1:1234 # drweb-ctl cfset &lt;%HTTPD_SECTION%&gt; &gt;.LinkCheckerAddress -a 10.20.30.45:5678</pre> <p>Если не указано ни одного значения, то использование расширения Dr.Web Link Checker невозможно. Подключиться к веб-интерфейсу управления продуктом, используя данные адреса, невозможно.</p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>ServerSslCertificate</b> <i>{путь к файлу}</i>	<p>Определяет путь к файлу серверного сертификата, используемого сервером веб-интерфейса управления для взаимодействия с клиентами по протоколу HTTPS.</p> <p>Данный файл генерируется автоматически при установке компонента.</p> <p>Обратите внимание, что файл сертификата и файл закрытого ключа (определяется следующим параметром) должны соответствовать друг другу.</p> <p><b>Значение по умолчанию:</b> &lt;etc_dir&gt;/certs/serv.crt</p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /etc/opt/drweb.com/certs/serv.crt</li><li>• Для <b>FreeBSD:</b> /usr/local/etc/drweb.com/certs/serv.crt</li></ul>
<b>ServerSslKey</b> <i>{путь к файлу}</i>	<p>Определяет путь к файлу закрытого ключа, используемого сервером веб-интерфейса управления для взаимодействия с клиентами по протоколу HTTPS.</p>





	<p>Данный файл генерируется автоматически при установке компонента.</p> <p>Обратите внимание, что файл сертификата (определяется предыдущим параметром) и файл закрытого ключа должны соответствовать друг другу.</p> <p><b>Значение по умолчанию:</b> <code>&lt;etc_dir&gt;/certs/serv.key</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/etc/opt/drweb.com/certs/serv.key</code></li><li>• Для <b>FreeBSD:</b> <code>/usr/local/etc/drweb.com/certs/serv.key</code></li></ul>
<b>WebconsoleRoot</b> <i>{путь к каталогу}</i>	<p>Определяет путь к каталогу, в котором хранятся файлы, используемые веб-интерфейсом управления, если он установлен (аналог каталога <code>htdocs</code> для <b>Apache HTTP Server</b>).</p> <p><b>Значение по умолчанию:</b> <code>&lt;opt_dir&gt;/share/drweb-httpd/webconsole</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/opt/drweb.com/share/drweb-httpd/webconsole</code></li><li>• Для <b>FreeBSD:</b> <code>/usr/local/libexec/drweb.com/share/drweb-httpd/webconsole</code></li></ul>
<b>LinkcheckerRoot</b> <i>{путь к каталогу}</i>	<p>Определяет путь к каталогу, в котором хранятся файлы, используемые расширением для веб-браузеров Dr.Web Link Checker.</p> <p><b>Значение по умолчанию:</b> <code>&lt;opt_dir&gt;/share/drweb-httpd/linkchecker</code></p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> <code>/opt/drweb.com/share/drweb-httpd/linkchecker</code></li><li>• Для <b>FreeBSD:</b> <code>/usr/local/libexec/drweb.com/share/drweb-httpd/linkchecker</code></li></ul>
<b>AccessLogPath</b> <i>{путь к файлу}</i>	<p>Определяет путь к файлу, хранящему журнал всех запросов HTTP/HTTPS, поступающих от клиентов к серверу веб-интерфейса управления.</p> <p>Если параметр не задан, журнал HTTP/HTTPS-запросов сервером не ведется.</p> <p><b>Значение по умолчанию:</b> (не задано)</p>



## Dr.Web SNMPD

SNMP-агент Dr.Web Dr.Web SNMPD предназначен для интеграции программного комплекса Dr.Web для Интернет-шлюзов UNIX с системами мониторинга посредством протокола SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов Dr.Web для Интернет-шлюзов UNIX, а также собирать статистику обнаружения и нейтрализации угроз. Агент поддерживает предоставление системам мониторинга или любым SNMP-менеджерам следующей информации:

- Состояние любого компонента программного комплекса.
- Счетчики количества обнаруженных угроз различных типов (в соответствии с классификацией Dr.Web).

Кроме того, агент может рассылать уведомления SNMP trap по факту обнаружения угроз и по факту ошибок при попытках нейтрализации обнаруженных угроз. Агент поддерживает протокол SNMP версий 2с и 3.

Описание информации, которая может быть предоставлена агентом, содержится в специально сформированном компанией «Доктор Веб» разделе MIB (*Management Information Base*). В разделе MIB, определенном для продуктов Dr.Web для UNIX-подобных ОС, описывается следующая информация:

1. Форматы оповещений SNMP trap об обнаружении и нейтрализации угроз, а также об ошибках компонентов программного комплекса.
2. Статистика работы программного комплекса.
3. Состояние компонентов программного комплекса.

Подробнее о данных, которые можно получить, используя протокол SNMP, см. в соответствующем [разделе](#).

## Принципы работы

По умолчанию компонент запускается автоматически при старте программного комплекса Dr.Web для Интернет-шлюзов UNIX. После запуска компонент формирует структуры данных в соответствии со структурой, описанной в MIB Dr.Web, и начинает ожидать поступление запросов на получение информации от внешних менеджеров SNMP. Компонент получает информацию о статусе компонентов программного комплекса, а также уведомления об обнаружении угроз непосредственно от демона управления конфигурацией [Dr.Web ConfigD](#), как показано на рисунке ниже.

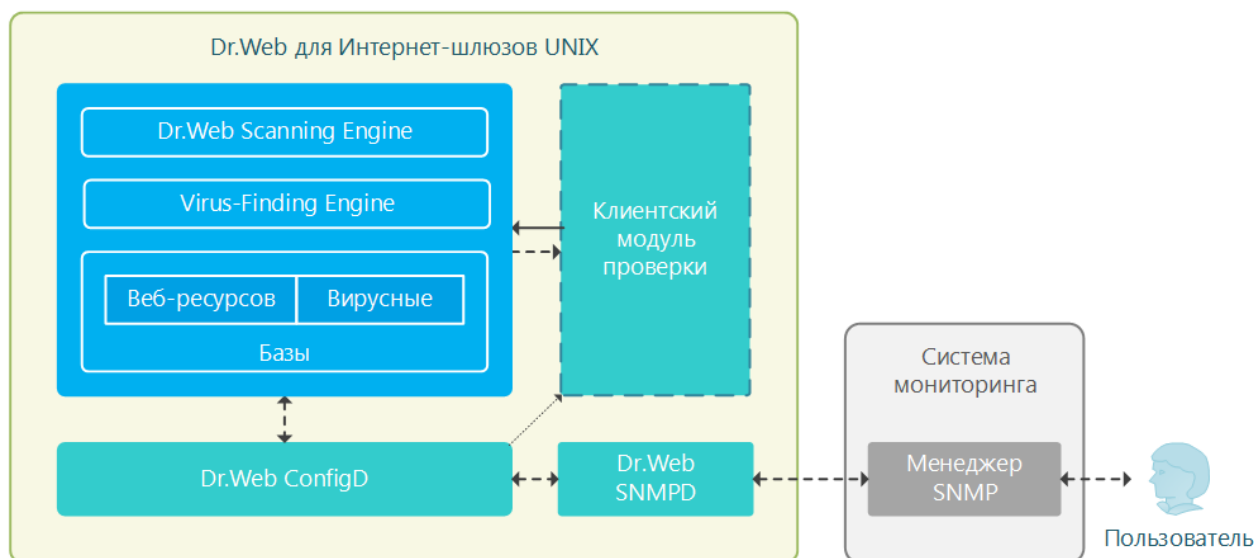


Рисунок 20. Схема работы компонента

Обнаружение угроз сканирующим ядром может происходить при проверках файлов, производящихся по запросам от различных компонентов Dr.Web для Интернет-шлюзов UNIX, поэтому на схеме указан абстрактный «Клиентский модуль проверки». При обнаружении любой угрозы происходит увеличение счетчика количества обнаруженных угроз, соответствующего типу угрозы, а всем менеджерам SNMP, получающим оповещения, рассылается SNMP trap с информацией об обнаруженной угрозе.



Накопленные значения счетчиков (например, счетчиков обнаруженных угроз) не сохраняются между запусками Dr.Web SNMPD. Таким образом, при перезапуске Dr.Web SNMPD по любой причине (в том числе – при общем перезапуске Dr.Web для Интернет-шлюзов UNIX) накопленные значения счетчиков сбрасываются в 0.

## Интеграция с системным SNMP-агентом

Для корректной работы SNMP-агента Dr.Web в случае, если на сервере уже работает основной системный SNMP-агент **snmpd (net-snmp)**, необходимо настроить передачу SNMP-запросов по ветке MIB Dr.Web от **snmpd** к Dr.Web SNMPD. Для этого необходимо отредактировать конфигурационный файл **snmpd** (обычно для **Linux** – `/etc/snmp/snmpd.conf`), добавив в него строку следующего вида:

```
proxy -v <версия> -c <community> <адрес>:<порт> <ветвь MIB>
```

Где:

- **<версия>** – используемая версия SNMP (2с, 3).
- **<community>** – «community string», используемая Dr.Web SNMPD.
- **<адрес>:<порт>** – сетевой сокет, прослушиваемый Dr.Web SNMPD.
- **<ветвь MIB>** – OID ветви дерева MIB, содержащей [описания](#) переменных и уведомлений SNMP (*trap*), используемых Dr.Web (этот OID равен .1.3.6.1.4.1.29690).



При использовании настроек SNMP-агента Dr.Web по умолчанию добавляемая строка имеет следующий вид:

```
proxy -v 2c -c public localhost:50000 .1.3.6.1.4.1.29690
```

Обратите внимание, что, поскольку в этом случае порт 161 будет использоваться стандартным системным **snmpd**, то для Dr.Web SNMPD в [параметре ListenAddress](#) следует указать другой порт (50000 в данном примере).

## Аргументы командной строки

Для запуска компонента Dr.Web SNMPD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-snmpd [<параметры>]
```

Dr.Web SNMPD допускает использование следующих параметров:

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

### Пример:

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

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

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости (обычно при старте операционной системы). Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду  
**man 1 drweb-snmpd**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [SNMPD] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.

В секции представлены следующие параметры:

<b>LogLevel</b>  {уровень подробности}	<a href="#">Уровень подробности</a> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <a href="#">секции</a> [Root].  <b>Значение по умолчанию:</b> Notice
<b>Log</b>  {тип журнала}	<a href="#">Метод ведения журнала</a>
<b>ExePath</b>  {путь к файлу}	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <opt_dir>/bin/drweb-snmpd <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /opt/drweb.com/bin/drweb-snmpd</li><li>• Для <b>FreeBSD</b> : /usr/local/libexec/drweb.com/bin/drweb-snmpd</li></ul>
<b>Start</b>  {логический}	Компонент должен быть запущен демоном управления конфигурацией <a href="#">Dr.Web ConfigD</a> .  Установка данного параметра в Yes предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение No – немедленно завершить работу компонента.  <b>Значение по умолчанию:</b> No
<b>RunAsUser</b>  {UID   имя пользователя}	Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр (т.е. похоже на числовой UID), то оно указывается с префиксом «name:», например: <b>RunAsUser</b> = name:123456.



	<p>Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.</p> <p><b>Значение по умолчанию:</b> drweb</p>
<b>ListenAddress</b> <i>{адрес}</i>	<p>Адрес (IP-адрес и порт), прослушиваемый агентом Dr.Web SNMPD в ожидании подключений от клиентов (менеджеров SNMP).</p> <p>Обратите внимание, что для совместной работы с <b>snmpd</b> необходимо указать порт, отличный от стандартного (161), а кроме того, у <b>snmpd</b> необходимо <a href="#">настроить</a> проксирование.</p> <p><b>Значение по умолчанию:</b> 127.0.0.1:161</p>
<b>SnmpVersion</b> <i>{V2c   V3}</i>	<p>Используемая версия протокола SNMP (SNMPv2c или SNMPv3).</p> <p><b>Значение по умолчанию:</b> V2c</p>
<b>V3EngineId</b> <i>{строка}</i>	<p>Строка-идентификатор <i>Engine ID</i> для SNMPv3 (согласно <a href="#">RFC 3411</a>).</p> <p><b>Значение по умолчанию:</b> 800073FA044452574542</p>
<b>TrapReceiver</b> <i>{список адресов}</i>	<p>Список адресов (IP-адрес и порт), на которые Dr.Web SNMPD будет отправлять уведомления <i>SNMP trap</i> при обнаружении угроз компонентами Dr.Web для Интернет-шлюзов UNIX.</p> <p>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).</p> <p><b>Пример:</b> Добавить в список сокет 192.168.0.1:1234 и 10.20.30.45:5678.</p> <p>1. Добавление значений в файл конфигурации.</p> <ul style="list-style-type: none"><li>• Два значения в одной строке</li></ul> <div><pre>[SNMPD] TrapReceiver = "192.168.0.1:1234", "10.20.30.45:5678"</pre></div> <ul style="list-style-type: none"><li>• Две строки (по одному значению в строке)</li></ul> <div><pre>[SNMPD] TrapReceiver = 192.168.0.1:1234 TrapReceiver = 10.20.30.45:5678</pre></div>



	<p>2. Добавление значений через <a href="#">команды drweb-ctl</a> cfset.</p> <div><pre># drweb-ctl cfset SNMPD.TrapReceiver - a 192.168.0.1:1234 # drweb-ctl cfset SNMPD.TrapReceiver - a 10.20.30.45:5678</pre></div> <p><b>Значение по умолчанию:</b> (не задан)</p>
<b>V2cCommunity</b>  {строка}	<p>Строка «SNMP read community» для аутентификации менеджеров SNMP (протокол <i>SNMPv2c</i>) при доступе к <a href="#">переменным MIB</a> Dr.Web для чтения.</p> <p>Параметр используется в случае если задано <b>SnmpVersion</b> = V2c.</p> <p><b>Значение по умолчанию:</b> public</p>
<b>V3UserName</b>  {строка}	<p>Имя пользователя для аутентификации менеджеров SNMP (протокол <i>SNMPv3</i>) для доступа к <a href="#">переменным MIB</a> Dr.Web.</p> <p>Параметр используется в случае если задано <b>SnmpVersion</b> = V3.</p> <p><b>Значение по умолчанию:</b> noAuthUser</p>
<b>V3Auth</b>  {SHA(<pwd>)   MD5(<pwd>)   None}	<p>Метод аутентификации менеджеров SNMP (протокол <i>SNMPv3</i>) для доступа к <a href="#">переменным MIB</a> Dr.Web.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• SHA (&lt;PWD&gt;) – используется SHA-хэш пароля (строки &lt;PWD&gt;).</li><li>• MD5 (&lt;PWD&gt;) – используется MD5-хэш пароля (строки &lt;PWD&gt;).</li><li>• None – аутентификация не производится.</li></ul> <p>где &lt;PWD&gt; – пароль в открытом виде (<i>plain text</i>).</p> <p>При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа \.</p> <p><b>Примеры:</b></p> <ol style="list-style-type: none"><li>1. Значение параметра в файле конфигурации: <b>V3Auth</b> = MD5(123456)</li><li>2. Задание этого же значения из командной строки с использованием <a href="#">команды drweb-ctl</a> cfset: <b>drweb-ctl</b> cfset SNMPD.V3Auth MD5\ (123456\)</li></ol>



	<p>Параметр используется в случае если задано <b>SnmpVersion</b> = V3.</p> <p><b>Значение по умолчанию:</b> None</p>
<b>V3Privacy</b>  {DES(<secret>)   AES128(<secret>)   None}	<p>Метод шифрования содержимого SNMP-сообщений (протокол <i>SNMPv3</i>).</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• DES (&lt;secret&gt;) – используется алгоритм шифрования DES.</li><li>• AES128 (&lt;secret&gt;) – используется алгоритм шифрования AES128.</li><li>• None – шифрование содержимого SNMP-сообщений не производится.</li></ul> <p>где &lt;secret&gt; – секрет, разделяемый менеджером и агентом (<i>plain text</i>).</p> <p>При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа \.</p> <p><b>Примеры:</b></p> <ol style="list-style-type: none"><li>1. Значение параметра в файле конфигурации: <b>V3Privacy</b> = AES128(supersecret)</li><li>2. Задание этого же значения из командной строки с использованием <b>команды drweb-ctl</b> cfset: <b>drweb-ctl</b> cfset SNMPD.V3Privacy AES128\ (supersecret\)</li></ol> <p>Параметр используется в случае если задано <b>SnmpVersion</b> = V3.</p> <p><b>Значение по умолчанию:</b> None</p>

## Интеграция с системами мониторинга

SNMP-агент Dr.Web может выступать поставщиком данных для любой системы мониторинга, использующей протокол SNMP версии 2с или 3. Перечень данных, доступных для контроля и их структура [описаны](#) в файле описания MIB Dr.Web `DrWeb-Snmpd.mib`, поставляемом совместно с продуктом. Этот файл находится в каталоге `<opt_dir>/share/drweb-snmpd/mibs`.

Для удобства настройки, совместно с компонентом поставляются необходимые шаблоны настроек для популярных систем мониторинга:

- [Munin](#)
- [Nagios](#)





- [Zabbix](#)

Шаблоны настроек для систем мониторинга находятся в каталоге `<opt_dir>/share/drweb-snmpd/connectors`.

## Интеграция с системой мониторинга Munin

Система мониторинга **Munin** состоит из централизованного сервера (мастера) **munin**, собирающего статистику от клиентов **munin-node**, располагающихся локально на узлах, подлежащих наблюдению. Каждый клиент мониторинга по запросу от сервера собирает данные о работе наблюдаемого узла, запуская *подключаемые модули (plug-ins)*, предоставляющие данные для передачи на сервер.

Для подключения Dr.Web SNMPD к системе мониторинга **Munin** в каталоге `<opt_dir>/share/drweb-snmpd/connectors/munin/plugins` поставляются готовые подключаемые модули сбора данных Dr.Web, используемые **munin-node**. Эти модули собирают данные для построения следующих графиков:

- Количество обнаруженных угроз.
- Статистика проверки файлов.
- Статистика проверки почтовых сообщений.

Указанные модули поддерживают использование протокола SNMP версий 1, 2с и 3. На основе этих шаблонных модулей можно создать любые подключаемые модули, опрашивающие состояние программного комплекса Dr.Web для Интернет-шлюзов UNIX через Dr.Web SNMPD.

В каталоге `<opt_dir>/share/drweb-snmpd/connectors/munin` поставляются следующие файлы.

Файл	Описание
<code>plugins/snmp__drweb_malware</code>	Подключаемый модуль <b>munin-node</b> для опроса Dr.Web SNMPD через SNMP с целью получения количества угроз, обнаруженных продуктом Dr.Web на узле.
<code>plugins/snmp__drweb_filecheck</code>	Подключаемый модуль <b>munin-node</b> для опроса Dr.Web SNMPD через SNMP с целью получения статистики проверки файлов продуктом Dr.Web на узле.
<code>plugins/snmp__drweb_maild_multi</code>	Подключаемый модуль <b>munin-node</b> для опроса Dr.Web SNMPD через SNMP с целью получения статистики проверки сообщений электронной почты продуктом Dr.Web на узле.



Файл	Описание
	Обратите внимание, что данный модуль использует <i>multigraph</i> – особенность, реализованная в <b>Munin</b> версий старше 1.4.
plugin-conf.d/drweb.cfg	Пример конфигурации в <b>munin-node</b> значений переменных среды исполнения подключаемых модулей Dr.Web.

## Подключение узла к Munin

В данной инструкции предполагается, что система мониторинга **Munin** уже корректно развернута на сервере мониторинга, а на наблюдаемом узле установлены и корректно функционируют Dr.Web SNMPD (возможно, в режиме [прокси](#) совместно с **snmpd**) и **munin-node**.

### 1. Настройка на наблюдаемом узле

- Скопируйте файлы `snmp__drweb_*` в каталог библиотек подключаемых модулей **munin-node** (этот путь зависит от используемой ОС. Например, в **Debian/Ubuntu** это путь `/usr/share/munin/plugins`).
- Сконфигурируйте **munin-node**, подключив к нему поставляемые подключаемые модули Dr.Web. Для этого используйте утилиту **munin-node-configure**, которая поставляется совместно с **munin-node**.

Например, команда

```
$ munin-node-configure --shell --snmp localhost
```

выведет на экран терминала список команд для создания необходимых символических ссылок на подключаемые модули. Скопируйте и выполните их в командной строке. Обратите внимание, что указанная команда предполагает, что:

- 1) **munin-node** установлена на том же узле в сети, что и Dr.Web SNMPD. Если это не так, то следует указать вместо `localhost` правильный FQDN или IP-адрес наблюдаемого узла;
  - 2) Dr.Web SNMPD использует протокол SNMP версии 2с. Если это не так, то следует указать правильную версию протокола SNMP в вызове команды **munin-node-configure**. Эта команда имеет набор ключей, которые позволяют гибко настроить подключаемые модули, в том числе – указать используемую версию протокола SNMP, порт, используемый SNMP-агентом на наблюдаемом узле, строку *community string* и т.п. При необходимости воспользуйтесь справкой по команде **munin-node-configure**.
- При необходимости определите (или переопределите) значения параметров среды, в которой должны исполняться установленные подключаемые модули Dr.Web для **munin-node**. В качестве параметров среды используется значение *community string*, используемый SNMP-агентом порт и так далее. Эти параметры необходимо



определить в файле `/etc/munin/plugin-conf.d/drweb` (создайте его при необходимости). В качестве примера данного файла используйте поставляемый файл `drweb.cfg`.

- В файле конфигурации **munin-node** (`munin-node.conf`) укажите регулярное выражение, которому должны соответствовать IP-адреса узлов сети, с которых серверам (мастерам) **munin** разрешено подключаться к **munin-node** на данном узле для получения значений контролируемых параметров, например:

```
allow ^10\.20\.30\.40$
```

В данном случае регулярное выражение разрешает получение параметров этого узла только узлу с IP-адресом `10.20.30.40`.

- Перезапустите **munin-node**, например, командой:

```
# service munin-node restart
```

## 2. Настройка на сервере (мастере) Munin

В конфигурационный файл мастера **Munin** `munin.conf`, который по умолчанию хранится в каталоге `/etc` (в системах **Debian/Ubuntu** – `/etc/munin/munin.conf`), добавьте запись с адресом и идентификатором наблюдаемого узла:

```
[ <ID>; <hostname> . <domain> ]
address <host IP address>
use_node_name yes
```

где `<ID>` – отображаемый идентификатор узла; `<hostname>` – имя узла; `<domain>` – имя домена; `<host IP address>` – IP-адрес узла.

С официальной документацией по настройке системы мониторинга **Munin** вы можете ознакомиться по ссылке <http://munin.readthedocs.io>.

## Интеграция с системой мониторинга Zabbix

Для подключения Dr.Web SNMPD к системе мониторинга **Zabbix** в каталоге `<opt_dir>/share/drweb-snmpd/connectors/zabbix` поставляются следующие файлы шаблонов.

Файл	Описание
<code>zbx_drweb.xml</code>	Шаблон описания наблюдаемого узла с установленным антивирусным продуктом Dr.Web
<code>snmptt.drweb.zabbix.conf</code>	Настройки утилиты <b>snmptt</b> – приемника уведомлений <i>SNMP trap</i>



Шаблон описания наблюдаемого узла содержит:

- Набор описаний счетчиков («*items*», в терминологии **Zabbix**). По умолчанию шаблон настроен на использование протокола SNMP v2.
- Набор настроенных графиков: количество проверенных файлов и распределение обнаруженных угроз по типам.

### Подключение узла к Zabbix

В данной инструкции предполагается, что система мониторинга **Zabbix** уже корректно развернута на сервере мониторинга, а на наблюдаемом установлен и корректно функционирует Dr.Web SNMPD (возможно, в режиме [прокси](#) совместно с **snmpd**). Кроме того, если планируется получать с наблюдаемого узла оповещения *SNMP trap* (в частности – об обнаружении Dr.Web для Интернет-шлюзов UNIX угроз на защищаемом сервере), на сервере мониторинга также должен быть установлен пакет **net-snmp** (используются стандартные утилиты **snmptt** и **snmptrapd**).

1. В веб-интерфейсе **Zabbix**, на вкладке **Configuration** → **Templates**, импортируйте шаблон наблюдаемого узла из файла `<opt_dir>/share/drweb-snmppd/connectors/zabbix/zbx_drweb.xml`.
2. Добавьте наблюдаемый узел в список узлов (используйте ссылку **Hosts** → **Create host**). Укажите параметры узла и корректные настройки SNMP-интерфейса (должны соответствовать настройкам **drweb-snmppd** и **snmpd** на узле):

- Вкладка **Host**:

**Host name:** *drweb-host*

**Visible name:** *DRWEB\_HOST*

**Groups:** выбрать *Linux servers*

**Snmp interfaces:** Нажмите **add** и укажите IP-адрес и порт, используемый Dr.Web SNMPD (по умолчанию предполагается, что Dr.Web SNMPD работает на локальном узле, поэтому здесь указан адрес *127.0.0.1*, а в качестве порта указан стандартный порт *161*).

- Вкладка **Templates**:

Нажмите **Add**, отметьте *DRWEB*, нажмите **select**.

- Вкладка **Macros**:

**Macro:** `{ $SNMP_COMMUNITY }`

**Value:** укажите «read community» для SNMP V2c (по умолчанию – *public*).

Нажмите **Save**.

Примечание: Макрос `{ $SNMP_COMMUNITY }` можно указать непосредственно в шаблоне узла.



По умолчанию импортированный шаблон *DRWEB* настроен на использование версии SNMP v2. Если требуется использовать другую версию SNMP, его необходимо отредактировать на соответствующей странице редактирования шаблона.

3. После привязки шаблона к наблюдаемому узлу, если настройки SNMP корректны, система мониторинга **Zabbix** начнет сбор данных для счетчиков (*items*), содержащихся в шаблоне, на вкладках веб-интерфейса **Monitoring** → **Latest Data** и **Monitoring** → **Graphs** будут отображаться собранные данные счетчиков.
4. Специальный элемент (*item*) *drweb-traps* служит для сбора уведомлений *SNMP trap* от Dr.Web SNMPD. Журнал полученных оповещений *SNMP trap* доступен на странице **Monitoring** → **Latest Data** → **drweb-traps** → **history**. Для сбора оповещений **Zabbix** использует стандартные утилиты **snmptt** и **snmptrapd** из пакета *net-snmp*. О их настройке для получения уведомлений *SNMP trap* от Dr.Web SNMPD см. ниже.
5. В случае необходимости, вы можете настроить для добавленного наблюдаемого узла триггер, изменяющий свое состояние при получении уведомлений *SNMP trap* от Dr.Web SNMPD. Изменение состояния этого триггера можно использовать как источник событий для формирования соответствующих нотификаций. Триггер для наблюдаемого узла добавляется стандартным способом, ниже показан пример выражения, указываемого в поле **trigger expression** для описанного триггера:

- Для **Zabbix** версии 2.x:

```
{ {TRIGGER.VALUE}=0 &
{DRWEB:snmptrap[.*\1\3\6\1\4\1\29690\..*].nodata(60)}=1 } |
{ {TRIGGER.VALUE}=1 &
{DRWEB:snmptrap[.*\1\3\6\1\4\1\29690\..*].nodata(60)}=0 }
```

- Для **Zabbix** версии 3.x:

```
{ {TRIGGER.VALUE}=0 and {drweb-host:snmptrap["29690"].nodata(60)}=1 } or
{ {TRIGGER.VALUE}=1 and {drweb-host:snmptrap["29690"].nodata(60)}=0 }
```

Данный триггер срабатывает (устанавливается в значение 1), если журнал уведомлений *SNMP trap*, поступающих от Dr.Web SNMPD был обновлен в течение минуты. Если же журнал в течение минуты не обновлялся, то триггер выключается (меняет состояние на 0).

В поле **Severity (Важность)** для этого триггера рекомендуется устанавливать вид уведомления, отличный от *Not classified (Не классифицировано)*, например – *Warning (Предупреждение)*.

## Настройка приема уведомлений *SNMP trap* для **Zabbix**

1. На наблюдаемом узле в настройках Dr.Web SNMPD (параметр **TrapReceiver**) указывается адрес, который прослушивается **snmptrapd** на узле с **Zabbix**, например:

```
SNMPD.TrapReceiver = 10.20.30.40:162
```



2. В конфигурационном файле **snmptrapd** (`snmptrapd.conf`) указывается тот же адрес, а также приложение, которое будет обрабатывать полученные уведомления *SNMP trap* (в данном случае – **snmptthandler**, компонент **snmptt**):

```
snmpTrapdAddr 10.20.30.40:162
traphandle default /usr/sbin/snmptthandler
```

Чтобы **snmptt** не отклонял, как неизвестные, уведомления *SNMP trap*, отправленные Dr.Web SNMPD, добавьте в этот файл также строку:

```
outputOption n
```

3. Компонент **snmptthandler** сохраняет принимаемые уведомления *SNMP trap* в файл на диске в соответствии с указанным форматом, который должен соответствовать регулярному выражению, заданному в шаблоне узла для **Zabbix** (элемент (*item*) *drweb-traps*). Формат сохраняемого сообщения о поступлении уведомления *SNMP trap* поставляется в файле `<opt_dir>/share/drweb-snmppd/connectors/zabbix/snmptt.drweb.zabbix.conf`, который необходимо скопировать в каталог `/etc/snmp`.
4. Кроме этого, путь к файлам формата необходимо указать в конфигурационном файле `snmptt.ini`:

```
[TrapFiles]
# A list of snmptt.conf files (this is NOT the snmptrapd.conf file).
# The COMPLETE path and filename. Ex: '/etc/snmp/snmptt.conf'
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
/etc/snmp/snmptt.drweb.zabbix.conf
END
```

После этого, если **snmptt** запущен в режиме демона, то его надо перезапустить.

5. В конфигурационном файле сервера **Zabbix** (`zabbix-server.conf`) необходимо задать (или проверить наличие) следующих настроек:

```
SNMPTrapperFile=/var/log/snmptt/snmptt.log
StartSNMPTrapper=1
```

где `/var/log/snmptt/snmptt.log` – это файл журнала, в который **snmptt** записывает информацию о поступивших уведомлениях *SNMP trap*.

Подробнее с официальной документацией по **Zabbix** вы можете ознакомиться по ссылке <https://www.zabbix.com/documentation/>.



## Интеграция с системой мониторинга Nagios

Для подключения Dr.Web SNMPD к системе мониторинга **Nagios** в каталоге `<opt_dir>/share/drweb-snmpd/connectors/nagios` поставляются следующие файлы примеров конфигурации **Nagios**.

Файл	Описание
<code>nagiosgraph/rrdopts.conf-sample</code>	Пример конфигурационного файла RRD
<code>objects/drweb.cfg</code>	Конфигурационный файл, описывающий объекты <i>drweb</i>
<code>objects/nagiosgraph.cfg</code>	Конфигурационный файл компонента построения графиков <b>Nagiosgraph</b> , используемого <b>Nagios</b>
<code>plugins/check_drweb</code>	Сценарий сбора данных от узла с продуктом Dr.Web
<code>plugins/eventhandlers/submit_check_result</code>	Сценарий обработки уведомлений <i>SNMP trap</i>
<code>snmp/snmpptt.drweb.nagios.conf</code>	Настройки утилиты <b>snmpptt</b> – приемника уведомлений <i>SNMP trap</i>

### Подключение узла к Nagios

В данной инструкции предполагается, что система мониторинга **Nagios** уже корректно развернута на сервере мониторинга, включая настройку веб-сервера и графического средства **Nagiosgraph**, а на наблюдаемом установлен и корректно функционирует Dr.Web SNMPD (возможно, в режиме [прокси](#) совместно с **snmpd**). Кроме того, если планируется получать с наблюдаемого узла уведомления *SNMP trap* (в частности – об обнаружении Dr.Web для Интернет-шлюзов UNIX угроз на защищаемом сервере), на сервере мониторинга также должен быть установлен пакет `net-snmp` (используются стандартные утилиты **snmpptt** и **snmptrapd**).

В данном руководстве по подключению используются следующие соглашения о путях (реальные пути зависят от ОС и установки **Nagios**):

- `<NAGIOS_PLUGINS_DIR>` – каталог плагинов **Nagios**, например: `/usr/lib64/nagios/plugins`.
- `<NAGIOS_ETC_DIR>` – каталог настроек **Nagios**, например: `/etc/nagios`.
- `<NAGIOS_OBJECTS_DIR>` – каталог объектов **Nagios**, например: `/etc/nagios/objects`.
- `<NAGIOSGRAPH_DIR>` – каталог **Nagiosgraph**, например: `/usr/local/nagiosgraph`.
- `<NAGIOS_PERFDATA_LOG>` – файл, в который **Nagios** записывает результаты выполнения команд проверки сервисов (должен совпадать с файлом `perflog` из `<NAGIOSGRAPH_DIR>/etc/nagiosgraph.conf`). Записи из этого файла считываются



сценарием `<NAGIOSGRAPH_DIR>/bin/insert.pl` и записываются в соответствующие RRA-архивы **RRD Tool**.

### Настройка **Nagios**:

1. Скопируйте файл `check_drweb` в каталог `<NAGIOS_PLUGINS_DIR>`, а файл `drweb.cfg` – в каталог `<NAGIOS_OBJECTS_DIR>`.
2. Добавьте в группу `drweb` узлы с установленным продуктом Dr.Web, подлежащие наблюдению (на них должен быть запущен Dr.Web SNMPD), по умолчанию в данную группу включен только локальный узел `localhost`.
3. Отредактируйте (при необходимости) команду `check_drweb`, в которой указывается обращение к Dr.Web SNMPD на узлах `drweb` через утилиту **snmpwalk**:

```
snmpwalk -c public -v 2c $HOSTADDRESS$:161
```

укажите правильную версию протокола SNMP и параметры (такие, как "*community string*" или параметры аутентификации), а также порт. Переменную `$HOSTADDRESS$` необходимо оставить в команде (она автоматически заменяется **Nagios** на правильный адрес узла при вызове команды). OID в команде указывать не требуется. Рекомендуется также указать команду вместе с полным путем к исполняемому файлу (обычно – `/usr/local/bin/snmpwalk`).

4. Подключите объекты *DrWeb* в конфигурационном файле `<NAGIOS_ETC_DIR>/nagios.cfg`, добавив в него строку:

```
cfg_file= <NAGIOS_OBJECTS_DIR>/drweb.cfg
```

5. Добавьте настройки **RRD Tool** для графиков *DrWeb* из файла `rrdopts.conf-sample` в файл `<NAGIOSGRAPH_DIR>/etc/rrdopts.conf`.
6. Если компонент **Nagiosgraph** еще не настроен, то выполните его настройку:
  - Скопируйте файл `nagiosgraph.cfg` в каталог `<NAGIOS_OBJECTS_DIR>` и исправьте путь к файлу сценария `insert.pl` в команде **process-service-perfdata-for-nagiosgraph**, например, так:

```
$ awk '$1 == "command_line" { $2 = "<NAGIOSGRAPH_DIR>/bin/insert.pl" } { print }' ./objects/nagiosgraph.cfg > <NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
```

- Подключите этот файл в конфигурационном файле `<NAGIOS_ETC_DIR>/nagios.cfg`, добавив в него строку:

```
cfg_file=<NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
```

7. Проверьте значения переменных конфигурации **Nagios** в конфигурационном файле `<NAGIOS_ETC_DIR>/nagios.cfg`:





```
check_external_commands=1
execute_host_checks=1
accept_passive_host_checks=1
enable_notifications=1
enable_event_handlers=1

process_performance_data=1
service_perfddata_file=/usr/nagiosgraph/var/rrd/perfddata.log
service_perfddata_file_template=$LASTSERVICECHECK$|$HOSTNAME$|$SERVICEDE
SC$|$SERVICEOUTPUT$|$SERVICEPERFDATA$
service_perfddata_file_mode=a
service_perfddata_file_processing_interval=30
service_perfddata_file_processing_command=process-service-perfddata-for-
nagiosgraph

check_service_freshness=1
enable_flap_detection=1
enable_embedded_perl=1
enable_environment_macros=1
```

### Настройка приема уведомлений SNMP trap для Nagios

1. На наблюдаемом узле в настройках Dr.Web SNMPD (параметр **TrapReceiver**) укажите адрес, который прослушивается **snmptrapd** на узле с **Nagios**, например:

```
SNMPD.TrapReceiver = 10.20.30.40:162
```

2. Проверьте наличие файла сценария `<NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result`, который будет вызываться при получении уведомлений *SNMP trap*. Если этого файла нет, то следует скопировать в это место файл `submit_check_result` из каталога `<opt_dir>/share/drweb-snmppd/connectors/nagios/plugins/eventhandlers/`. Необходимо в этом файле исправить путь, указанный в параметре `CommandFile`. Он должен иметь такое же значение, что и параметр `command_file` в файле `<NAGIOS_ETC_DIR>/nagios.cfg`.
3. Скопируйте файл `snmptt.drweb.nagios.conf` в каталог `/etc/snmp/snmp/`. В этом файле измените путь к файлу сценария `submit_check_result`, например, используя следующую команду:

```
$ awk '$1 == "EXEC" { $2 =
<NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result }{ print}'
./snmp/snmptt.drweb.nagios.conf > /etc/snmp/snmp/snmptt.drweb.nagios.conf
```

4. Добавьте в файл `/etc/snmp/snmptt.ini` строку `«/etc/snmp/snmptt.drweb.nagios.conf»`. После этого, если **snmptt** запущен в режиме демона, то его надо перезапустить.

После того как все требуемые файлы конфигурации **Nagios** были добавлены и отредактированы, необходимо запустить **Nagios** в режиме отладки командой

```
# nagios -v <NAGIOS_ETC_DIR>/nagios.cfg
```



В этом случае **Nagios** проверит наличие ошибок конфигурации. Если при проверке ошибки не найдены, перезапустите **Nagios** стандартным способом (например, командой ОС `service nagios restart`).

Подробнее с официальной документацией по **Nagios** вы можете ознакомиться по ссылке <http://www.nagios.org/documentation/>.

## Dr.Web SNMP MIB

Перечень параметров работы программного комплекса Dr.Web для Интернет-шлюзов UNIX, которые могут быть получены внешними системами мониторинга по протоколу SNMP, представлен в таблице ниже.

Имя параметра	OID параметра	Тип и описание параметра
Общий префикс имен: .iso.org.dod.internet.private.enterprises.drweb.drwebSnmpd Общий префикс OID: .1.3.6.1.4.1.29690.2		
<b>alert</b>	<b>Асинхронные уведомления о событиях (SNMP trap)</b>	
threatAlert	.1.1	Уведомление об обнаруженной угрозе
threatAlertFile	.1.1.1	Имя инфицированного файла (строка)
threatAlertType	.1.1.2	Тип угрозы (целое число *)
threatAlertName	.1.1.3	Название угрозы (строка)
threatAlertOrigin	.1.1.4	Идентификатор компонента, обнаружившего угрозу (целое число***)
threatActionErrorAlert	.1.2	Уведомление об ошибке при попытке нейтрализации угрозы
threatActionErrorAlertFile	.1.2.1	Имя инфицированного файла (строка)
threatActionErrorAlertType	.1.2.2	Тип угрозы (целое число *)
threatActionErrorAlertName	.1.2.3	Название угрозы (строка)
threatActionErrorAlertOrigin	.1.2.4	Идентификатор компонента, обнаружившего угрозу (целое число***)
threatActionErrorAlertError	.1.2.5	Описание ошибки (строка)



Имя параметра	OID параметра	Тип и описание параметра
<i>threatActionErrorAlertErrorCode</i>	.1.2.6	Код ошибки (целое число, соответствует кодам из таблицы каталога ошибок)
<i>threatActionErrorAlertAction</i>	.1.2.7	Действие, попытка совершить которое привела к ошибке (целое число: 1 – лечить; 2 – переместить в карантин; 3 – удалить; 4 – информировать; 5 – игнорировать)
<i>componentFailureAlert</i>	.1.3	Уведомление о сбое в работе компонента
<i>componentFailureAlertName</i>	.1.3.1	Идентификатор компонента (целое число***)
<i>componentFailureAlertExitCodeDescription</i>	.1.3.2	Описание кода завершения компонента (строка)
<i>componentFailureAlertExitCode</i>	.1.3.3	Код завершения компонента (целое число, соответствует кодам из таблицы каталога ошибок)
<i>infectedUrlAlert</i>	.1.4	Уведомление о блокировании доступа к веб-ресурсу, содержащему угрозу (для соединений HTTP/HTTPS)
<i>infectedUrlAlertUrl</i>	.1.4.1	Заблокированный URL (строка)
<i>infectedUrlAlertDirection</i>	.1.4.2	Направление HTTP-сообщения (целое число: 1 – запрос, 2 – ответ)
<i>infectedUrlAlertType</i>	.1.4.3	Тип угрозы (целое число *)
<i>infectedUrlAlertName</i>	.1.4.4	Название угрозы (строка)
<i>infectedUrlAlertOrigin</i>	.1.4.5	Идентификатор компонента, обнаружившего угрозу (целое число***)
<i>infectedUrlAlertSrcIp</i>	.1.4.6	IP-адрес источника соединения (строка)
<i>infectedUrlAlertSrcPort</i>	.1.4.7	Порт источника соединения (целое число)



Имя параметра	OID параметра	Тип и описание параметра
<i>infectedUrlAlertDstIp</i>	.1.4.8	IP-адрес точки назначения соединения (строка)
<i>infectedUrlAlertDstPort</i>	.1.4.9	Порт точки назначения соединения (целое число)
<i>infectedUrlAlertSniHost</i>	.1.4.10	SNI точки назначения соединения (для SSL-соединений) (строка)
<i>infectedUrlAlertExePath</i>	.1.4.11	Исполняемый путь программы-инициатора соединения (строка)
<i>infectedUrlAlertUserName</i>	.1.4.12	Имя пользователя, с правами которого выполняется программа-инициатор соединения (строка)
<i>infectedAttachmentAlert</i>	.1.5	Уведомление об обнаружении вредоносного вложения в сообщении электронной почты
<i>infectedAttachmentAlertType</i>	.1.5.1	Тип угрозы (целое число *)
<i>infectedAttachmentAlertName</i>	.1.5.2	Название угрозы (строка)
<i>infectedAttachmentAlertOrigin</i>	.1.5.3	Идентификатор компонента, обнаружившего угрозу (целое число***)
<i>infectedEmailAttachmentAlertSocket</i>	.1.5.4	IP-адрес, с которого было получено сообщение электронной почты (строка)
<i>infectedEmailAttachmentAlertMailFrom</i>	.1.5.5	Отправитель сообщения электронной почты (строка)
<i>infectedEmailAttachmentAlertRcptTo</i>	.1.5.6	Список получателей сообщения электронной почты (строка)
<i>infectedEmailAttachmentAlertMessageId</i>	.1.5.7	Значение заголовка Message-ID сообщения электронной почты (строка)
<i>infectedEmailAttachmentAlertAction</i>	.1.5.8	Действие, примененное к сообщению электронной почты в целом или инфицированному вложению (целое число: 1 –



Имя параметра	OID параметра	Тип и описание параметра
		перепакковано; 2 – отклонено; 3 – отброшено; 4 – вылечено; 5 – перемещено в карантин, 6 – удалено)
<i>infectedEmailAttachmentAlertDivert</i>	.1.5.9	Направление движения сообщения электронной почты (целое число: 1 – входящее; 2 – исходящее)
<i>infectedEmailAttachmentAlertSrcIp</i>	.1.5.10	IP-адрес источника соединения (строка)
<i>infectedEmailAttachmentAlertSrcPort</i>	.1.5.11	Порт источника соединения (целое число)
<i>infectedEmailAttachmentAlertDstIp</i>	.1.5.12	IP-адрес точки назначения соединения (строка)
<i>infectedEmailAttachmentAlertDstPort</i>	.1.5.13	Порт точки назначения соединения (целое число)
<i>infectedEmailAttachmentAlertSniHost</i>	.1.5.14	SNi точки назначения соединения (для SSL-соединений) (строка)
<i>infectedEmailAttachmentAlertProtocol</i>	.1.5.15	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
<i>infectedEmailAttachmentAlertExePath</i>	.1.5.16	Исполняемый путь программы-инициатора соединения (строка)
<i>infectedEmailAttachmentAlertUserName</i>	.1.5.17	Имя пользователя, с правами которого выполняется программа-инициатор соединения (строка)
<i>categoryUrlAlert</i>	.1.6	Уведомление о блокировании доступа к веб-ресурсу, входящему в нежелательную категорию
<i>categoryUrlAlertUrl</i>	.1.6.1	Заблокированный URL (строка)
<i>categoryUrlAlertCategory</i>	.1.6.2	Категория веб-ресурсов, к которой относится URL (целое число**)



Имя параметра	OID параметра	Тип и описание параметра
<i>categoryUrlAlertOrigin</i>	.1.6.3	Идентификатор компонента, обнаружившего угрозу (целое число***)
<i>categoryUrlAlertSrcIp</i>	.1.6.4	IP-адрес источника соединения (строка)
<i>categoryUrlAlertSrcPort</i>	.1.6.5	Порт источника соединения (целое число)
<i>categoryUrlAlertDstIp</i>	.1.6.6	IP-адрес точки назначения соединения (строка)
<i>categoryUrlAlertDstPort</i>	.1.6.7	Порт точки назначения соединения (целое число)
<i>categoryUrlAlertSniHost</i>	.1.6.8	SNI точки назначения соединения (для SSL-соединений) (строка)
<i>categoryUrlAlertExePath</i>	.1.6.9	Исполняемый путь программы-инициатора соединения (строка)
<i>categoryUrlAlertUserName</i>	.1.6.10	Имя пользователя, с правами которого выполняется программа-инициатор соединения (строка)
<i>categoryUrlEmailAttachmentAlert</i>	.1.7	Уведомление об обнаружении нежелательного URL в сообщении электронной почты
<i>categoryUrlEmailAttachmentAlertType</i>	.1.7.1	Категория веб-ресурсов, к которой относится URL (целое число**)
<i>categoryUrlEmailAttachmentAlertOrigin</i>	.1.7.2	Идентификатор компонента, обнаружившего угрозу (целое число***)
<i>categoryUrlEmailAttachmentAlertSocket</i>	.1.7.3	IP-адрес, с которого было получено сообщение электронной почты (строка)
<i>categoryUrlEmailAttachmentAlertMailFrom</i>	.1.7.4	Отправитель сообщения электронной почты (строка)



Имя параметра	OID параметра	Тип и описание параметра
<i>categoryUrlEmailAttachmentAlertRcptTo</i>	.1.7.5	Список получателей сообщения электронной почты (строка)
<i>categoryUrlEmailAttachmentAlertMessageId</i>	.1.7.6	Значение заголовка Message-ID сообщения электронной почты (строка)
<i>categoryUrlEmailAttachmentAlertAction</i>	.1.7.7	Действие, примененное к сообщению электронной почты в целом или к вложению (целое число: 1 – перепакковано; 2 – отклонено; 3 – отброшено; 4 – вылечено; 5 – перемещено в карантин, 6 – удалено)
<i>categoryUrlEmailAttachmentAlertDivert</i>	.1.7.8	Направление движения сообщения электронной почты (целое число: 1 – входящее; 2 – исходящее)
<i>categoryUrlEmailAttachmentAlertSrcIp</i>	.1.7.9	IP-адрес источника соединения (строка)
<i>categoryUrlEmailAttachmentAlertSrcPort</i>	.1.7.10	Порт источника соединения (целое число)
<i>categoryUrlEmailAttachmentAlertDstIp</i>	.1.7.11	IP-адрес точки назначения соединения (строка)
<i>categoryUrlEmailAttachmentAlertDstPort</i>	.1.7.12	Порт точки назначения соединения (целое число)
<i>categoryUrlEmailAttachmentAlertSniHost</i>	.1.7.13	SNИ точки назначения соединения (для SSL-соединений) (строка)
<i>categoryUrlEmailAttachmentAlertProtocol</i>	.1.7.14	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
<i>categoryUrlEmailAttachmentAlertExePath</i>	.1.7.15	Исполняемый путь программы-инициатора соединения (строка)
<i>categoryUrlEmailAttachmentAlertUserName</i>	.1.7.16	Имя пользователя, с правами которого выполняется программа-инициатор соединения (строка)



Имя параметра	OID параметра	Тип и описание параметра
spamEmailAlert	.1.8	Уведомление о признании сообщения электронной почты спамом
spamEmailAlertOrigin	.1.8.1	Идентификатор компонента, обнаружившего угрозу (целое число***)
spamEmailAlertSocket	.1.8.2	IP-адрес, с которого было получено сообщение электронной почты (строка)
spamEmailAlertMailFrom	.1.8.3	Отправитель сообщения электронной почты (строка)
spamEmailAlertRcptTo	.1.8.4	Список получателей сообщения электронной почты (строка)
spamEmailAlertMessageId	.1.8.5	Значение заголовка Message-ID сообщения электронной почты (строка)
spamEmailAlertAction	.1.8.6	Действие, примененное к сообщению электронной почты в целом или к вложению (целое число: 1 – перепаковано; 2 – отклонено; 3 – отброшено; 4 – вылечено; 5 – перемещено в карантин, 6 – удалено)
spamEmailAlertDivert	.1.8.7	Направление движения сообщения электронной почты (целое число: 1 – входящее; 2 – исходящее)
spamEmailAlertSrcIp	.1.8.8	IP-адрес источника соединения (строка)
spamEmailAlertSrcPort	.1.8.9	Порт источника соединения (целое число)
spamEmailAlertDstIp	.1.8.10	IP-адрес точки назначения соединения (строка)
spamEmailAlertDstPort	.1.8.11	Порт точки назначения соединения (целое число)
spamEmailAlertSniHost	.1.8.12	SNI точки назначения соединения (для SSL-





Имя параметра	OID параметра	Тип и описание параметра
		соединений) (строка)
<i>spamEmailAlertProtocol</i>	.1.8.13	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
<i>spamEmailAlertExePath</i>	.1.8.14	Исполняемый путь программы-инициатора соединения (строка)
<i>spamEmailAlertUserName</i>	.1.8.15	Имя пользователя, с правами которого выполняется программа-инициатор соединения (строка)
<i>blockedConnectionAlert</i>	.1.9	Уведомление о блокировке сетевого соединения
<i>blockedConnectionAlertOrigin</i>	.1.9.1	Идентификатор компонента, обнаружившего угрозу (целое число***)
<i>blockedConnectionAlertDivert</i>	.1.9.2	Направление соединения (целое число: 1 – входящее; 2 – исходящее)
<i>blockedConnectionAlertSrcIp</i>	.1.9.3	IP-адрес источника соединения (строка)
<i>blockedConnectionAlertSrcPort</i>	.1.9.4	Порт источника соединения (целое число)
<i>blockedConnectionAlertDstIp</i>	.1.9.5	IP-адрес точки назначения соединения (строка)
<i>blockedConnectionAlertDstPort</i>	.1.9.6	Порт точки назначения соединения (целое число)
<i>blockedConnectionAlertSniHost</i>	.1.9.7	SNИ точки назначения соединения (для SSL-соединений) (строка)
<i>blockedConnectionAlertProtocol</i>	.1.9.8	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
<i>blockedConnectionAlertExePath</i>	.1.9.9	Исполняемый путь программы-инициатора соединения (строка)



Имя параметра	OID параметра	Тип и описание параметра
<i>blockedConnectionAlertUserName</i>	.1.9.10	Имя пользователя, с правами которого выполняется программа-инициатор соединения (строка)
<b>stat</b>	<b>Статистические показатели работы программного комплекса</b>	
<i>threatCounters</i>	.2.1	Счетчики обнаруженных угроз
<i>knownVirus</i>	.2.1.1	Число обнаруженных известных вирусов (счетчик; целое число)
<i>suspicious</i>	.2.1.2	Число обнаруженных подозрительных объектов (счетчик; целое число)
<i>adware</i>	.2.1.3	Число обнаруженных рекламных программ (счетчик; целое число)
<i>dialers</i>	.2.1.4	Число обнаруженных программ дозвона (счетчик; целое число)
<i>joke</i>	.2.1.5	Число обнаруженных шуточных программ (счетчик; целое число)
<i>riskware</i>	.2.1.6	Число обнаруженных потенциально опасных программ (счетчик; целое число)
<i>hacktool</i>	.2.1.7	Число обнаруженных программ взлома (счетчик; целое число)
<i>scanErrors</i>	.2.2	Счетчики произошедших ошибок проверки файлов
<i>sePathNotAbsolute</i>	.2.2.1	Количество возникновений ошибки «Не абсолютный путь» (счетчик; целое число)
<i>seFileNotFound</i>	.2.2.2	Количество возникновений ошибки «Файл не найден» (счетчик; целое число)
<i>seFileNotRegular</i>	.2.2.3	Количество возникновений ошибки «Специальный (не



Имя параметра	OID параметра	Тип и описание параметра
		регулярный) файл» (счетчик; целое число)
<i>seFileNotBlockDevice</i>	.2.2.4	Количество возникновений ошибки «Файл – не блочное устройство» (счетчик; целое число)
<i>seNameTooLong</i>	.2.2.5	Количество возникновений ошибки «Слишком длинный путь или имя файла» (счетчик; целое число)
<i>seNoAccess</i>	.2.2.6	Количество возникновений ошибки «Доступ запрещен» (счетчик; целое число)
<i>seReadError</i>	.2.2.7	Количество возникновений ошибки «Ошибка чтения» (счетчик; целое число)
<i>seWriteError</i>	.2.2.8	Количество возникновений ошибки «Ошибка записи» (счетчик; целое число)
<i>seFileTooLarge</i>	.2.2.9	Количество возникновений ошибки «Файл слишком большой» (счетчик; целое число)
<i>seFileBusy</i>	.2.2.10	Количество возникновений ошибки «Файл занят» (счетчик; целое число)
<i>seUnpackingError</i>	.2.2.20	Количество возникновений ошибки «Ошибка распаковки» (счетчик; целое число)
<i>sePasswordProtectd</i>	.2.2.21	Количество возникновений ошибки «Защищено паролем» (счетчик; целое число)
<i>seArchCrcError</i>	.2.2.22	Количество возникновений ошибки «Ошибка контрольной суммы архива» (счетчик; целое число)



Имя параметра	OID параметра	Тип и описание параметра
<i>seArchInvalidHeader</i>	.2.2.23	Количество возникновений ошибки «Недопустимый заголовок архива» (счетчик; целое число)
<i>seArchNoMemory</i>	.2.2.24	Количество возникновений ошибки «Недостаточно памяти для обработки архива» (счетчик; целое число)
<i>seArchIncomplete</i>	.2.2.25	Количество возникновений ошибки «Неожиданный конец архива» (счетчик; целое число)
<i>seCanNotBeCured</i>	.2.2.26	Количество возникновений ошибки «Объект не может быть вылечен» (счетчик; целое число)
<i>sePackerLevelLimit</i>	.2.2.30	Количество возникновений ошибки «Превышение допустимого уровня вложенности для запакованных объектов» (счетчик; целое число)
<i>seArchiveLevelLimit</i>	.2.2.31	Количество возникновений ошибки «Превышение допустимого уровня вложенности для архивов» (счетчик; целое число)
<i>seMailLevelLimit</i>	.2.2.32	Количество возникновений ошибки «Превышение допустимого уровня вложенности для почтовых файлов» (счетчик; целое число)
<i>seContainerLevelLimit</i>	.2.2.33	Количество возникновений ошибки «Превышение допустимого уровня вложенности для контейнеров» (счетчик; целое число)
<i>seCompressionLimit</i>	.2.2.34	Количество возникновений ошибки «Превышение допустимой величины



Имя параметра	OID параметра	Тип и описание параметра
		коэффициента сжатия» (счетчик; целое число)
<i>seReportSizeLimit</i>	.2.2.35	Количество возникновений ошибки «Превышение допустимого размера отчета о проверке» (счетчик; целое число)
<i>seScanTimeout</i>	.2.2.40	Количество возникновений ошибки «Истекло время на проверку файла» (счетчик; целое число)
<i>seEngineCrash</i>	.2.2.41	Количество возникновений ошибки «Обнаружен сбой сканирующего ядра» (счетчик; целое число)
<i>seEngineHangup</i>	.2.2.42	Количество возникновений ошибки «Перестало отвечать сканирующее ядро» (счетчик; целое число)
<i>seEngineError</i>	.2.2.44	Количество возникновений ошибки «Внутренняя ошибка сканирующего ядра» (счетчик; целое число)
<i>seNoLicense</i>	.2.2.45	Количество возникновений ошибки «Не найдена действующая лицензия» (счетчик; целое число)
<i>seNonSupportedDisk</i>	.2.2.50	Количество возникновений ошибки «Не поддерживаемый диск» (счетчик; целое число)
<i>seUnexpectedError</i>	.2.2.100	Количество возникновений ошибки «Неожиданная ошибка» (счетчик; целое число)
<i>scanLoadAverage</i>	.2.3	Показатели нагрузки проверки файлов
<i>filesScannedTable</i>	.2.3.1	Скорость проверки файлов по запросам от компонентов



Имя параметра	OID параметра	Тип и описание параметра
filesScannedEntry	.2.3.1.1	Компонент (строка таблицы; запись)
filesScannedIndex	.2.3.1.1.1	Индекс компонента (идентификатор, целое число***)
filesScannedOrigin	.2.3.1.1.2	Имя компонента
filesScanned1min	.2.3.1.1.3	Среднее (за минуту) количество файлов, проверенных в секунду (строка)
filesScanned5min	.2.3.1.1.4	Среднее (за 5 минут) количество файлов, проверенных в секунду (строка)
filesScanned15min	.2.3.1.1.5	Среднее (за 15 минут) количество файлов, проверенных в секунду (строка)
bytesScannedTable	.2.3.2	Скорость проверки (в байтах) по запросам от компонентов
bytesScannedEntry	.2.3.2.1	Компонент (строка таблицы; запись)
bytesScannedIndex	.2.3.2.1.1	Индекс компонента (идентификатор, целое число***)
bytesScannedOrigin	.2.3.2.1.2	Имя компонента
bytesScanned1min	.2.3.2.1.3	Среднее (за минуту) количество байт, проверенных в секунду (строка)
bytesScanned5min	.2.3.2.1.4	Среднее (за 5 минут) количество байт, проверенных в секунду (строка)
bytesScanned15min	.2.3.2.1.5	Среднее (за 15 минут) количество байт, проверенных в секунду (строка)
cacheHitFilesTable	.2.3.3	Использование кэша проверенных файлов по запросам от компонентов



Имя параметра	OID параметра	Тип и описание параметра
cacheHitFilesEntry	.2.3.3.1	Компонент (строка таблицы; запись)
cacheHitFilesIndex	.2.3.3.1.1	Индекс компонента (идентификатор, целое число***)
cacheHitFilesOrigin	.2.3.3.1.2	Имя компонента
cacheHitFiles1min	.2.3.3.1.3	Среднее (за минуту) количество отчетов о проверке, извлеченных из кэша в секунду (строка)
cacheHitFiles5min	.2.3.3.1.4	Среднее (за 5 минут) количество отчетов о проверке, извлеченных из кэша в секунду (строка)
cacheHitFiles15min	.2.3.3.1.5	Среднее (за 15 минут) количество отчетов о проверке, извлеченных из кэша в секунду (строка)
errorsTable	.2.3.4	Число ошибок проверки по запросам от компонентов
errorsEntry	.2.3.4.1	Компонент (строка таблицы; запись)
errorsIndex	.2.3.4.1.1	Индекс компонента (идентификатор, целое число***)
errorsOrigin	.2.3.4.1.2	Имя компонента
errors1min	.2.3.4.1.3	Среднее (за минуту) количество ошибок в секунду (строка)
errors5min	.2.3.4.1.4	Среднее (за 5 минут) количество ошибок в секунду (строка)
errors15min	.2.3.4.1.5	Среднее (за 15 минут) количество ошибок в секунду (строка)
net	.2.4	Показатели сетевой активности



Имя параметра	OID параметра	Тип и описание параметра
<i>markedAsSpam</i>	.2.4.1	Число сообщений электронной почты, отмеченных, как спам (счетчик; целое число)
<i>blockedInfectionSource</i>	.2.4.101	Число заблокированных URL из категории «Источники распространения вирусов» (счетчик; целое число)
<i>blockedNotRecommended</i>	.2.4.102	Число заблокированных URL из категории «Нерекомендуемые» (счетчик; целое число)
<i>blockedAdultContent</i>	.2.4.103	Число заблокированных URL из категории «Сайты для взрослых» (счетчик; целое число)
<i>blockedViolence</i>	.2.4.104	Число заблокированных URL из категории «Насилие» (счетчик; целое число)
<i>blockedWeapons</i>	.2.4.105	Число заблокированных URL из категории «Оружие» (счетчик; целое число)
<i>blockedGambling</i>	.2.4.106	Число заблокированных URL из категории «Азартные игры» (счетчик; целое число)
<i>blockedDrugs</i>	.2.4.107	Число заблокированных URL из категории «Наркотики» (счетчик; целое число)
<i>blockedObsceneLanguage</i>	.2.4.108	Число заблокированных URL из категории «Нецензурная лексика» (счетчик; целое число)
<i>blockedChats</i>	.2.4.109	Число заблокированных URL из категории «Чаты» (счетчик; целое число)
<i>blockedTerrorism</i>	.2.4.110	Число заблокированных URL из категории «Терроризм» (счетчик; целое число)





Имя параметра	OID параметра	Тип и описание параметра
<i>blockedFreeEmail</i>	.2.4.111	Число заблокированных URL из категории «Бесплатная электронная почта» (счетчик; целое число)
<i>blockedSocialNetworks</i>	.2.4.112	Число заблокированных URL из категории «Социальные сети» (счетчик; целое число)
<i>blockedOwnersNotice</i>	.2.4.113	Число заблокированных URL из категории «По обращению правообладателя» (счетчик; целое число)
<i>blockedBlackList</i>	.2.4.120	Число заблокированных URL из пользовательского черного списка (счетчик; целое число)
<b>info</b>	<b>Информация о состоянии программного комплекса</b>	
components	.3.1	Состояние компонентов программного комплекса
configd	.3.1.1	Данные о компоненте <b>drweb-configd</b>
configdState	.3.1.1.1	Состояние компонента (целое число****)
configdExitCode	.3.1.1.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
configdExitTime	.3.1.1.3	Время завершения работы ( <i>UNIX time</i> )
configdInstalledApps	.3.1.1.101	Перечень установленных компонентов
configdAppEntry	.3.1.1.101.1	Информация об установленном компоненте (строка таблицы; запись)
configdAppIndex	.3.1.1.101.1.1	Индекс (номер) установленного компонента (целое число)
configdAppName	.3.1.1.101.1.2	Имя установленного компонента (строка)



Имя параметра	OID параметра	Тип и описание параметра
configdAppExePath	.3.1.1.101.1.3	Путь к исполняемому файлу компонента (строка)
configdAppInstallTime	.3.1.1.101.1.4	Время установки компонента ( <i>UNIX time</i> )
configdAppIniSection	.3.1.1.101.1.5	Имя секции с параметрами компонента в конфигурационном файле (строка)
scanEngine	.3.1.2	Данные о компоненте <b>drweb-se</b>
scanEngineState	.3.1.2.1	Состояние компонента (целое число****)
scanEngineExitCode	.3.1.2.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
scanEngineExitTime	.3.1.2.3	Время завершения работы ( <i>UNIX time</i> )
scanEngineStatus	.3.1.2.101	Состояние Dr.Web Virus-Finding Engine (целое число)
scanEngineVersion	.3.1.2.102	Версия Dr.Web Virus-Finding Engine (строка)
scanEngineVirusRecords	.3.1.2.103	Число вирусных записей (целое число)
scanEngineMaxForks	.3.1.2.104	Максимальное число дочерних сканирующих процессов (целое число)
scanEngineQueues	.3.1.2.105	Очереди задач на проверку
scanEngineQueuesLow	.3.1.2.105.1	Очередь низкоприоритетных задач
scanEngineQueueLowOut	.3.1.2.105.1.1	Число низкоприоритетных задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueLowSize	.3.1.2.105.1.2	Число низкоприоритетных задач, ожидающих обработки в



Имя параметра	OID параметра	Тип и описание параметра
		очереди (счетчик; целое число)
scanEngineQueuesMedium	.3.1.2.105.2	Очередь задач обычного приоритета
scanEngineQueueMediumOut	.3.1.2.105.2.1	Число задач обычного приоритета, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueMediumSize	.3.1.2.105.2.2	Число задач обычного приоритета, ожидающих обработки в очереди (счетчик; целое число)
scanEngineQueuesHigh	.3.1.2.105.3	Очередь высокоприоритетных задач
scanEngineQueueHighOut	.3.1.2.105.3.1	Число высокоприоритетных задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueHighSize	.3.1.2.105.3.2	Число высокоприоритетных задач, ожидающих обработки в очереди (счетчик; целое число)
scanEngineVirusBasesTable	.3.1.2.106	Перечень вирусных баз
scanEngineVirusBasesEntry	.3.1.2.106.1	Информация о вирусной базе (строка таблицы; запись)
scanEngineVirusBaseIndex	.3.1.2.106.1.1	Индекс вирусной базы (целое число)
scanEngineVirusBasePath	.3.1.2.106.1.2	Путь к файлу вирусной базы (строка)
scanEngineVirusBaseRecords	.3.1.2.106.1.3	Число записей в вирусной базе (целое число)
scanEngineVirusBaseVersion	.3.1.2.106.1.4	Версия вирусной базы (целое число)
scanEngineVirusBaseTimestamp	.3.1.2.106.1.5	Метка времени для вирусной базы ( <i>UNIX time</i> )



Имя параметра	OID параметра	Тип и описание параметра
scanEngineVirusBaseMD5	.3.1.2.106.1.6	Контрольная сумма MD5 (строка)
scanEngineVirusBaseLoadResult	.3.1.2.106.1.7	Результат загрузки вирусной базы (строка)
scanEngineQueuesTab	.3.1.2.107	Перечень очередей задач на проверку
scanEngineQueueEntry	.3.1.2.107.1	Информация об очереди (строка таблицы; запись)
scanEngineQueueIndex	.3.1.2.107.1.1	Индекс (номер) очереди (целое число)
scanEngineQueueName	.3.1.2.107.1.2	Имя очереди (строка)
scanEngineQueueOut	.3.1.2.107.1.3	Число задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueSize	.3.1.2.107.1.4	Число задач, ожидающих обработки в очереди (счетчик; целое число)
<i>fileCheck</i>	.3.1.3	Данные о компоненте <b>drweb-filecheck</b>
fileCheckState	.3.1.3.1	Состояние компонента (целое число****)
fileCheckExitCode	.3.1.3.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
fileCheckExitTime	.3.1.3.3	Время завершения работы (UNIX time)
fileCheckScannedFiles	.3.1.3.101	Число проверенных файлов (счетчик; целое число)
fileCheckScannedBytes	.3.1.3.102	Число проверенных байт (счетчик; целое число)
fileCheckCacheHitFiles	.3.1.3.103	Число отчетов о проверке, извлеченных из кэша



Имя параметра	OID параметра	Тип и описание параметра
		проверенных файлов (счетчик; целое число)
fileCheckScanErrors	.3.1.3.104	Число ошибок сканирующего ядра (счетчик; целое число)
fileCheckScanStat	.3.1.3.105	Перечень клиентов
fileCheckClientEntry	.3.1.3.105.1	Информация о клиенте (строка таблицы; запись)
fileCheckClientIndex	.3.1.3.105.1.1	Индекс (номер) клиента (целое число)
fileCheckClientName	.3.1.3.105.1.2	Имя компонента-клиента (строка)
fileCheckClientScannedFiles	.3.1.3.105.1.3	Число файлов, проверенных для данного клиента (счетчик; целое число)
fileCheckClientScannedBytes	.3.1.3.105.1.4	Число байт, проверенных для данного клиента (счетчик; целое число)
fileCheckClientCacheHitFiles	.3.1.3.105.1.5	Число отчетов о проверке для данного клиента, извлеченных из кэша проверенных файлов (счетчик; целое число)
fileCheckClientScanErrors	.3.1.3.105.1.6	Число ошибок сканирующего ядра для данного клиента (счетчик; целое число)
update	.3.1.4	Данные о компоненте <b>drweb-update</b>
updateState	.3.1.4.1	Состояние компонента (целое число****)
updateExitCode	.3.1.4.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
updateExitTime	.3.1.4.3	Время завершения работы (UNIX time)



Имя параметра	OID параметра	Тип и описание параметра
updateBytesSent	.3.1.4.101	Число отправленных байт (счетчик; целое число)
updateBytesReceived	.3.1.4.102	Число принятых байт (счетчик; целое число)
<i>esagent</i>	.3.1.5	Данные о компоненте <b>drweb-esagent</b>
esagentState	.3.1.5.1	Состояние компонента (целое число****)
esagentExitCode	.3.1.5.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
esagentExitTime	.3.1.5.3	Время завершения работы ( <i>UNIX time</i> )
esagentWorkStatus	.3.1.5.101	Режим работы компонента (целое число: 1 – одиночный, 2 – подключается, 3 – ожидает подключения, 4 – подключение одобрено)
esagentIsConnected	.3.1.5.102	Подключен ли к серверу (целое число: 0 – нет, 1 – да)
esagentServer	.3.1.5.103	Адрес используемого сервера централизованной защиты (строка)
<i>netcheck</i>	.3.1.6	Данные о компоненте <b>drweb-netcheck</b>
netcheckState	.3.1.6.1	Состояние компонента (целое число****)
netcheckExitCode	.3.1.6.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
netcheckExitTime	.3.1.6.3	Время завершения работы ( <i>UNIX time</i> )
netcheckLocalSeForks	.3.1.6.101	Число ядер сканирования, доступных локально (целое



Имя параметра	OID параметра	Тип и описание параметра
		число)
netcheckRemoteSeForks	.3.1.6.102	Число доступных удаленных ядер сканирования (целое число)
netcheckLocalFilesScanned	.3.1.6.103	Число файлов, проверенных локально (счетчик; целое число)
netcheckNetworkFilesScanned	.3.1.6.104	Число файлов, проверенных удаленно (счетчик; целое число)
netcheckLocalBytesScanned	.3.1.6.105	Число байт, проверенных локально (счетчик; целое число)
netcheckNetworkBytesScanned	.3.1.6.106	Число байт, проверенных удаленно (счетчик; целое число)
netcheckLocalBytesIn	.3.1.6.107	Число байт, полученных от локальных клиентов (счетчик; целое число)
netcheckLocalBytesOut	.3.1.6.108	Число байт, отправленных локальным клиентам (счетчик; целое число)
netcheckNetworkBytesIn	.3.1.6.109	Число байт, полученных от удаленных узлов (счетчик; целое число)
netcheckNetworkBytesOut	.3.1.6.110	Число байт, отправленных на удаленные узлы (счетчик; целое число)
netcheckLocalScanErrors	.3.1.6.111	Число ошибок локальных ядер сканирования (счетчик; целое число)
netcheckNetworkScanErrors	.3.1.6.112	Число ошибок удаленных ядер сканирования (счетчик; целое число)
httpd	.3.1.7	Данные о компоненте <b>drweb-httpd</b>



Имя параметра	OID параметра	Тип и описание параметра
httpdState	.3.1.7.1	Состояние компонента (целое число****)
httpdExitCode	.3.1.7.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
httpdExitTime	.3.1.7.3	Время завершения работы (UNIX time)
<i>snmpd</i>	.3.1.8	Данные о компоненте <b>drweb-snmpd</b>
snmpdState	.3.1.8.1	Состояние компонента (целое число****)
snmpdExitCode	.3.1.8.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
snmpdExitTime	.3.1.8.3	Время завершения работы (UNIX time)
<i>clamd</i>	.3.1.20	Данные о компоненте <b>drweb-clamd</b>
clamdState	.3.1.20.1	Состояние компонента (целое число****)
clamdExitCode	.3.1.20.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
clamdExitTime	.3.1.20.3	Время завершения работы (UNIX time)
<i>icapd</i>	.3.1.21	Данные о компоненте <b>drweb-icapd</b>
icapdState	.3.1.21.1	Состояние компонента (целое число****)
icapdExitCode	.3.1.21.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)





Имя параметра	OID параметра	Тип и описание параметра
icapdExitTime	.3.1.21.3	Время завершения работы ( <i>UNIX time</i> )
icapdConnectionsIn	.3.1.21.101	Число принятых соединений (счетчик; целое число)
icapdConnectionsCount	.3.1.21.102	Текущее число открытых соединений (счетчик; целое число)
icapdOptions	.3.1.21.103	Число запросов <i>OPTIONS</i> (счетчик; целое число)
icapdReqmod	.3.1.21.104	Число запросов <i>REQMOD</i> (счетчик; целое число)
icapdRespmod	.3.1.21.105	Число запросов <i>RESPMOD</i> (счетчик; целое число)
icapdBad	.3.1.21.106	Число некорректных запросов (счетчик; целое число)
<i>smbspider</i>	.3.1.40	Данные о компоненте <b>drweb-smbspider-daemon</b>
smbspiderState	.3.1.40.1	Состояние компонента (целое число****)
smbspiderExitCode	.3.1.40.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
smbspiderExitTime	.3.1.40.3	Время завершения работы ( <i>UNIX time</i> )
smbspiderConnectionsIn	.3.1.40.101	Общее число открытых соединений (счетчик; целое число)
smbspiderConnectionsCount	.3.1.40.102	Текущее число открытых соединений (счетчик; целое число)
smbspiderShareTable	.3.1.40.103	Статистика по защищаемым ресурсам <b>Samba</b>
smbspiderShareEntry	.3.1.40.103.1	Информация о защищаемом ресурсе <b>Samba</b> (строка)



Имя параметра	OID параметра	Тип и описание параметра
		таблицы; запись)
smbspiderShareIndex	.3.1.40.103.1.1	Индекс (номер) защищаемого ресурса <b>Samba</b> (целое число)
smbspiderSharePath	.3.1.40.103.1.2	Путь к защищаемому ресурсу <b>Samba</b> (строка)
smbspiderShareConnectionsIn	.3.1.40.103.1.3	Общее число открытых соединений (счетчик; целое число)
smbspiderShareConnectionsCount	.3.1.40.103.1.4	Число соединений, открытых в данный момент (счетчик; целое число)
<i>gated</i>	.3.1.41	Данные о компоненте <b>drweb-gated</b>
gatedState	.3.1.41.1	Состояние компонента (целое число****)
gatedExitCode	.3.1.41.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
gatedExitTime	.3.1.41.3	Время завершения работы ( <i>UNIX time</i> )
gatedInterceptedIn	.3.1.41.101	Число перехваченных соединений (счетчик; целое число)
gatedInterceptedCount	.3.1.41.102	Число соединений, которые находятся под наблюдением в данный момент (счетчик; целое число)
<i>maild</i>	.3.1.42	Данные о компоненте <b>drweb-maild</b>
maildState	.3.1.42.1	Состояние компонента (целое число****)
maildExitCode	.3.1.42.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)



Имя параметра	OID параметра	Тип и описание параметра
maildExitTime	.3.1.42.3	Время завершения работы (UNIX time)
maildStat	.3.1.42.4	Статистика работы компонента <b>drweb-maild</b>
maildStatNative	.3.1.42.4.1	Статистика проверки сообщений электронной почты через внутренний интерфейс компонента <b>drweb-maild</b> (сообщения, полученные от SpIDer Gate в рамках проверки перехваченных соединений SMTP, POP3, IMAP)
maildStatNativePassed	.3.1.42.4.1.1	Число пропущенных сообщений (счетчик; целое число)
maildStatNativeRepacked	.3.1.42.4.1.2	Число перепакованных сообщений (счетчик; целое число)
maildStatNativeRejected	.3.1.42.4.1.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatNativeFailed	.3.1.42.4.1.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatNativeQueueSize	.3.1.42.4.1.5	Длина очереди, т.е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
maildStatMilter	.3.1.42.4.2	Статистика проверки сообщений электронной почты через интерфейс <i>Milter</i> компонента <b>drweb-maild</b>
maildStatMilterPassed	.3.1.42.4.2.1	Число пропущенных сообщений (счетчик; целое число)
maildStatMilterRepacked	.3.1.42.4.2.2	Число перепакованных сообщений (счетчик; целое число)



Имя параметра	OID параметра	Тип и описание параметра
maildStatMilterRejected	.3.1.42.4.2.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatMilterFailed	.3.1.42.4.2.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatMilterQueueSize	.3.1.42.4.2.5	Длина очереди, т.е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
maildStatSpamc	.3.1.42.4.3	Статистика проверки сообщений электронной почты через интерфейс <i>Spamc</i> компонента <b>drweb-maild</b>
maildStatSpamcPassed	.3.1.42.4.3.1	Число пропущенных сообщений (счетчик; целое число)
maildStatSpamcRepacked	.3.1.42.4.3.2	Число перепакованных сообщений (счетчик; целое число)
maildStatSpamcRejected	.3.1.42.4.3.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatSpamcFailed	.3.1.42.4.3.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatSpamcQueueSize	.3.1.42.4.3.5	Длина очереди, т.е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
maildStatRspamc	.3.1.42.4.4	Статистика проверки сообщений электронной почты через интерфейс <i>Rspamc</i> компонента <b>drweb-maild</b>
maildStatRspamcPassed	.3.1.42.4.4.1	Число пропущенных сообщений (счетчик; целое число)
maildStatRspamcRepacked	.3.1.42.4.4.2	Число перепакованных сообщений (счетчик; целое число)



Имя параметра	OID параметра	Тип и описание параметра
maildStatRspamcRejected	.3.1.42.4.4.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatRspamcFailed	.3.1.42.4.4.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatRspamcQueueSize	.3.1.42.4.4.5	Длина очереди, т.е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
<i>lookupd</i>	.3.1.43	Данные о компоненте <b>drweb-lookupd</b>
lookupdState	.3.1.43.1	Состояние компонента (целое число****)
lookupdExitCode	.3.1.43.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
lookupdExitTime	.3.1.43.3	Время завершения работы (UNIX time)
<i>cloudd</i>	.3.1.50	Данные о компоненте <b>drweb-cloudd</b>
clouddState	.3.1.50.1	Состояние компонента (целое число****)
clouddExitCode	.3.1.50.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
clouddExitTime	.3.1.50.3	Время завершения работы (UNIX time)
<i>vpnd</i>	.3.1.51	Данные о компоненте <b>drweb-vpnd</b>
vpndState	.3.1.51.1	Состояние компонента (целое число****)
vpndExitCode	.3.1.51.2	Последний код завершения (целое число, соответствует



Имя параметра	OID параметра	Тип и описание параметра
		кодам из таблицы каталога ошибок)
vpndExitTime	.3.1.51.3	Время завершения работы ( <i>UNIX time</i> )
vpndWorkStatus	.3.1.51.101	Режим работы компонента (целое число: 0 – выключен, 1 – сервер, 2 – клиент)
vpndConnectionState	.3.1.51.102	Состояние созданного соединения (целое число: 0 – не задано, 1 – подключение, 2 – подключено, 3 – ошибка, 4 – организация NAT, 5 – создание защищенного туннеля)
vpndNetworkName	.3.1.51.103	Имя созданной персональной сети (строка)
<i>meshd</i>	.3.1.52	Данные о компоненте <b>drweb-meshd</b>
meshdState	.3.1.52.1	Состояние компонента (целое число****)
meshdExitCode	.3.1.52.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
meshdExitTime	.3.1.52.3	Время завершения работы ( <i>UNIX time</i> )
<i>lotus</i>	.3.1.60	Данные о компоненте <b>drweb-lotus</b>
lotusState	.3.1.60.1	Состояние компонента (целое число****)
lotusExitCode	.3.1.60.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
lotusExitTime	.3.1.60.3	Время завершения работы ( <i>UNIX time</i> )



Имя параметра	OID параметра	Тип и описание параметра
<i>macgui</i>	.3.1.100	Данные о компоненте <b>drweb-gui</b> (для <b>OS X</b> )
macguiState	.3.1.100.1	Состояние компонента (целое число****)
macguiExitCode	.3.1.100.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
macguiExitTime	.3.1.100.3	Время завершения работы ( <i>UNIX time</i> )
<i>macspider</i>	.3.1.102	Данные о компоненте <b>drweb-spider</b> (для <b>OS X</b> )
macspiderState	.3.1.102.1	Состояние компонента (целое число****)
macspiderExitCode	.3.1.102.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
macspiderExitTime	.3.1.102.3	Время завершения работы ( <i>UNIX time</i> )
macspiderWorkStatus	.3.1.102.101	Режим работы компонента (целое число: 0 – не задан, 1 – загружается, 2 – запущен)
<i>macfirewall</i>	.3.1.103	Данные о компоненте <b>drweb-firewall</b> (для <b>OS X</b> )
macfirewallState	.3.1.103.1	Состояние компонента (целое число****)
macfirewallExitCode	.3.1.103.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
macfirewallExitTime	.3.1.103.3	Время завершения работы ( <i>UNIX time</i> )
<i>linuxgui</i>	.3.1.200	Данные о компоненте <b>drweb-gui</b> (для <b>Linux</b> )



Имя параметра	OID параметра	Тип и описание параметра
linuxguiState	.3.1.200.1	Состояние компонента (целое число****)
linuxguiExitCode	.3.1.200.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxguiExitTime	.3.1.200.3	Время завершения работы (UNIX time)
<i>linuxspider</i>	.3.1.201	Данные о компоненте <b>drweb-spider</b> (для <b>Linux</b> )
linuxspiderState	.3.1.201.1	Состояние компонента (целое число****)
linuxspiderExitCode	.3.1.201.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxspiderExitTime	.3.1.201.3	Время завершения работы (UNIX time)
linuxspiderWorkStatus	.3.1.201.101	Режим работы компонента (целое число: 0 – не задан, 1 – загружается, 2 – через <b>fanotify</b> , 3 – LKM)
<i>linuxnss</i>	.3.1.202	Данные о компоненте <b>drweb-nss</b> (для <b>Linux</b> )
linuxnssState	.3.1.202.1	Состояние компонента (целое число****)
linuxnssExitCode	.3.1.202.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxnssExitTime	.3.1.202.3	Время завершения работы (UNIX time)
linuxnssScannedFiles	.3.1.202.101	Число проверенных файлов (счетчик; целое число)
linuxnssScannedBytes	.3.1.202.102	Число проверенных байт (счетчик; целое число)





Имя параметра	OID параметра	Тип и описание параметра
linuxnssScanErrors	.3.1.202.103	Число ошибок сканирования (счетчик; целое число)
linuxfirewall	.3.1.203	Данные о компоненте <b>drweb-firewall</b> (для <b>Linux</b> )
linuxfirewallState	.3.1.203.1	Состояние компонента (целое число****)
linuxfirewallExitCode	.3.1.203.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxfirewallExitTime	.3.1.203.3	Время завершения работы ( <i>UNIX time</i> )
ctl	.3.1.300	Данные о компоненте <b>drweb-ctl</b>
ctlState	.3.1.300.1	Состояние компонента (целое число****)
ctlExitCode	.3.1.300.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
ctlExitTime	.3.1.300.3	Время завершения работы ( <i>UNIX time</i> )
license	.3.2	Состояние лицензии
licenseEsMode	.3.2.1	Лицензия выдана сервером централизованной защиты (целое число: 0 – нет, 1 – да)
licenseNumber	.3.2.2	Номер лицензии (целое число)
licenseOwner	.3.2.3	Владелец лицензии (строка)
licenseActivated	.3.2.4	Дата активации лицензии ( <i>UNIX time</i> )
licenseExpires	.3.2.5	Дата прекращения действия лицензии ( <i>UNIX time</i> )

\*) Типы угроз:



Код	Тип угрозы
1	Известный вирус ( <i>known virus</i> )
2	Подозрительный объект ( <i>suspicious</i> )
3	Рекламная программа ( <i>adware</i> )
4	Программа дозвона ( <i>dialer</i> )
5	Программа-шутка ( <i>joke program</i> )
6	Потенциально опасная программа ( <i>riskware</i> )
7	Программа взлома ( <i>hacktool</i> )

\*\*) Категории URL:

Код	Тип угрозы
1	Источник распространения вирусов ( <i>infectionSource</i> )
2	Не рекомендуемый ( <i>notRecommended</i> )
3	Сайты для взрослых ( <i>adultContent</i> )
4	Насилие ( <i>violence</i> )
5	Оружие ( <i>weapons</i> )
6	Азартные игры ( <i>gambling</i> )
7	Наркотики ( <i>drugs</i> )
8	Нецензурная лексика ( <i>obsceneLanguage</i> )
9	Чаты ( <i>chats</i> )
10	Терроризм ( <i>terrorism</i> )
11	Бесплатная электронная почта ( <i>freeEmail</i> )
12	Социальные сети ( <i>socialNetworks</i> )
13	Добавленные по обращению правообладателя ( <i>ownerNotice</i> )
14	Черный список ( <i>blackList</i> )

\*\*\*) Коды компонентов Dr.Web:



Код	Компонент
1	Dr.Web ConfigD ( <b>drweb-configd</b> )
2	Dr.Web Scanning Engine ( <b>drweb-se</b> )
3	Dr.Web File Checker ( <b>drweb-filecheck</b> )
4	Dr.Web Updater ( <b>drweb-update</b> )
5	Dr.Web ES Agent ( <b>drweb-esagent</b> )
6	Dr.Web Network Checker ( <b>drweb-netcheck</b> )
7	Dr.Web HTTPD ( <b>drweb-httpd</b> )
8	Dr.Web SNMPD ( <b>drweb-snmpd</b> )
20	Dr.Web ClamD ( <b>drweb-clamd</b> )
21	Dr.Web ICAPD ( <b>drweb-icapd</b> )
40	SpIDer Guard для SMB ( <b>drweb-smbspider-daemon</b> )
41	SpIDer Gate ( <b>drweb-gated</b> )
42	Dr.Web MailD ( <b>drweb-maild</b> )
43	Dr.Web LookupD ( <b>drweb-lookupd</b> )
50	Dr.Web CloudD ( <b>drweb-cloudd</b> )
51	Dr.Web VPND ( <b>drweb-vpnd</b> )
52	Dr.Web MeshD ( <b>drweb-meshd</b> )
60	Dr.Web для Lotus
100	<b>drweb-gui</b> для macOS
102	SpIDer Guard для macOS
103	Dr.Web Firewall для Linux для macOS
200	<b>drweb-gui</b> для Linux
201	SpIDer Guard ( <b>drweb-spider</b> )
202	SpIDer Guard для NSS ( <b>drweb-nss</b> )
203	Dr.Web Firewall для Linux ( <b>drweb-firewall</b> ) для Linux



Код	Компонент
300	Dr.Web Ctl ( <b>drweb-ctl</b> )
400	Сканирование по заданию сервера централизованной защиты (не является компонентом продукта)

\*\*\*\*) Состояния компонентов:

Код	Состояние
0	Не установлен
1	Установлен, но не запущен
2	Запускается
3	Работает
4	Завершает работу

Для непосредственного получения значений переменных вы можете воспользоваться утилитой **snmpwalk**:

```
$ snmpwalk -Os -c <community> -v <версия SNMP> <адрес узла> <OID>
```

Например, для получения статистики по обнаруженным угрозам на локальном узле (при настройках Dr.Web SNMPD по умолчанию) используйте следующую команду:

```
$ snmpwalk -Os -c public -v 2c 127.0.0.1 .1.3.6.1.4.1.29690.2.2.1
```



## Dr.Web CloudD

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 с целью ограждения пользователей от посещения нежелательных веб-сайтов и защиты операционных систем серверов и рабочих станций от инфицированных файлов, содержащих новейшие угрозы, описание которых еще не внесено в вирусные базы Dr.Web. Кроме этого, использование облачного сервиса Dr.Web Cloud снижает вероятность ложных срабатываний сканирующего ядра [Dr.Web Scanning Engine](#) и компонентов проверки доступа к Интернет.

## Принципы работы

Компонент предназначен для обращения к облачному сервису Dr.Web Cloud компании «Доктор Веб» с целью проверки содержимого указанного файла на наличие угроз, неизвестных локальному сканирующему ядру [Dr.Web Scanning Engine](#), а также с целью проверки, к каким из predeterminedенных компанией «Доктор Веб» категорий Интернет-ресурсов относится указанный URL.

Dr.Web CloudD автоматически запускается демоном управления конфигурацией. Запуск производится в ответ на поступившую команду от пользователя или некоторого компонента программного комплекса Dr.Web для Интернет-шлюзов UNIX. Схема работы компонента показана на рисунке ниже.

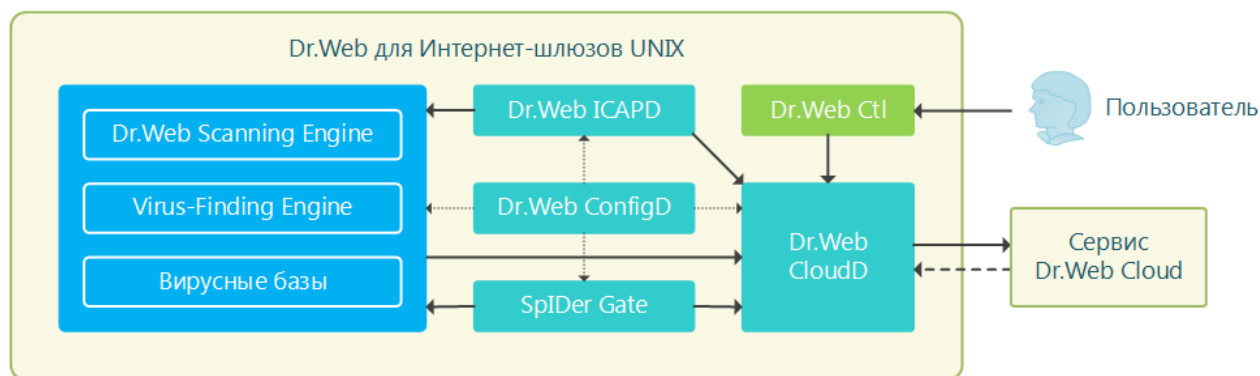


Рисунок 21. Схема работы компонента

Через данный компонент запросы к облачному сервису Dr.Web на проверку URL, по которым обращается пользователь, производит компонент проверки сетевого трафика и URL [SpIDer Gate](#) и компонент [Dr.Web ICAPD](#).

Кроме того, компонент используется при проверке файлов по команде от утилиты управления продуктом Dr.Web для Интернет-шлюзов UNIX из командной строки [Dr.Web Ctl](#) (запускается командой **drweb-ctl**): при обнаружении угроз сканирующее ядро [Dr.Web Scanning Engine](#) отправляет отчет о файле в облачный сервис Dr.Web Cloud.



## Аргументы командной строки

Для запуска компонента Dr.Web CloudD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-cloudd [<параметры>]
```

Dr.Web CloudD допускает использование следующих параметров:

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

**Пример:**

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

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

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости. Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду  
**man 1 drweb-cloudd**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [CloudD] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.



В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<u>Уровень подробности</u> ведения журнала компонента.  Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <u>секции</u> [Root].  <b>Значение по умолчанию:</b> Notice
<b>Log</b> <i>{тип журнала}</i>	<u>Метод ведения журнала</u>
<b>ExePath</b> <i>{путь к файлу}</i>	Путь к исполняемому файлу компонента.  <b>Значение по умолчанию:</b> <opt_dir>/bin/drweb-cloudd <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris:</b> /opt/drweb.com/bin/drweb-cloudd</li><li>• Для <b>FreeBSD:</b> /usr/local/libexec/drweb.com/bin/drweb-cloudd</li></ul>
<b>RunAsUser</b> <i>{UID   имя пользователя}</i>	Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр (т.е. похоже на числовой UID), то оно указывается с префиксом «name:», например: <b>RunAsUser</b> = name:123456.  <i>Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.</i>  <b>Значение по умолчанию:</b> drweb
<b>IdleTimeLimit</b> <i>{интервал времени}</i>	Максимальное время простоя компонента, по превышению которого он завершает свою работу.  Минимальное значение – 10s.  <b>Значение по умолчанию:</b> 30s
<b>PersistentCache</b> <i>{On   Off}</i>	Включать или нет сохранение на диск кэша ответов, получаемых от Dr.Web Cloud.  <b>Значение по умолчанию:</b> Off
<b>DebugSdk</b> <i>{логический}</i>	Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) подробные сообщения от Dr.Web Cloud.  <b>Значение по умолчанию:</b> No



## Dr.Web LookupD

Компонент Dr.Web LookupD предназначен для запроса данных из внешних хранилищ данных (служб каталогов), таких как **Active Directory**, используя протокол LDAP ([RFC 4511](#)). Данные, получаемые компонентом в ответ на запрос из хранилищ данных, используются в правилах проверки сетевых соединений (например, для проверки полномочий пользователей и их авторизации) и для блокировки доступа к URL в зависимости от выполнения условия.

В настройках компонента можно указать параметры подключения к нескольким источникам данных. Подключение компонента Dr.Web LookupD к требуемому источнику данных производится только в момент поступления запроса данных от некоторого компонента программного комплекса Dr.Web для Интернет-шлюзов UNIX.

Обмен данными по протоколу LDAP может производиться как по открытому каналу, так и по защищенному, с использованием SSL/TLS. При использовании защищенного соединения необходимо обеспечить Dr.Web LookupD корректным сертификатом и ключом SSL. Для генерации ключей и сертификатов, при необходимости, можно воспользоваться утилитой **openssl**. Пример использования утилиты **openssl** для генерации сертификатов и закрытых ключей приведен в разделе [Приложение Д. Генерация сертификатов SSL](#).

## Принципы работы

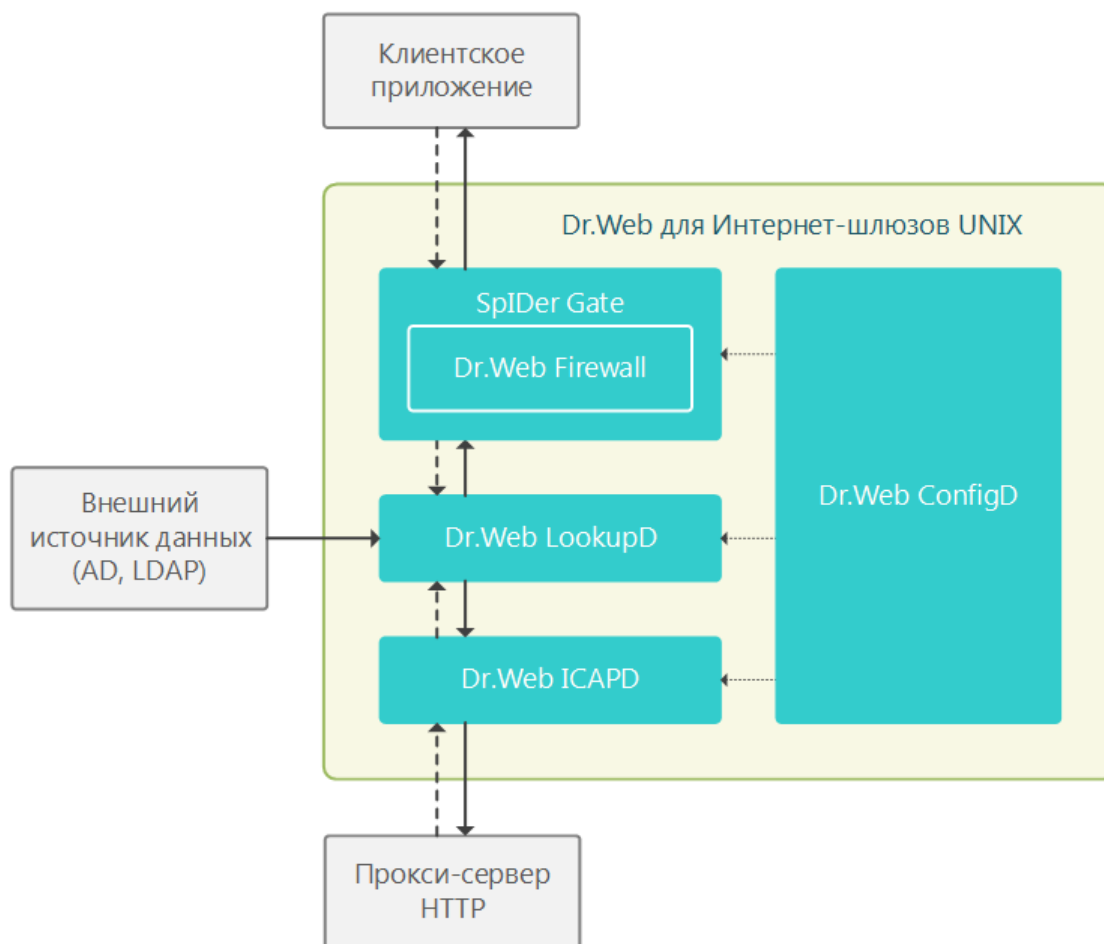
Компонент предназначен для выполнения запросов данных из служб каталогов (таких, как **Active Directory**) и прочих хранилищ данных, поддерживающих протокол LDAP. Получаемые данные (такие, как идентификаторы пользователей и их полномочия) передаются затребовавшим их компонентам программного комплекса Dr.Web для Интернет-шлюзов UNIX для использования в различных правилах проверки (например, для разрешения доступа пользователя к запрошенному URL и т.п.).



Данное руководство не описывает механизмы работы **LDAP** и **Active Directory**. При необходимости обратитесь к соответствующим справочным материалам, например, [RFC 4511](#).

Компонент Dr.Web LookupD автоматически запускается демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости (при возникновении запросов на получение данных из хранилищ). Схема работы компонента показана на рисунке ниже.





**Рисунок 22. Схема работы компонента**

При поступлении от некоторого компонента программного комплекса запроса на получение данных (например, [Dr.Web Firewall для Linux](#) или [Dr.Web ICAPD](#)), демон управления конфигурацией [Dr.Web ConfigD](#) запускает Dr.Web LookupD (если он еще не запущен), после чего компонент выполняет запрос из требуемого источника данных, возвращая ответ (как правило – это список строк, удовлетворяющих некоторому условию поиска). В настройках Dr.Web LookupD может быть задано неограниченное число источников данных, при этом, формируя запрос на выборку данных, клиентский компонент программного комплекса должен указать, из какого источника должны быть выбраны данные. После старта и выполнения поступившего запроса, Dr.Web LookupD продолжает работу некоторое время, ожидая поступления новых запросов. В случае их отсутствия, по окончании периода ожидания, Dr.Web LookupD автоматически завершает свою работу.

Базовый способ использования компонента Dr.Web LookupD другими компонентами программного комплекса – это выборка данных для проверки истинности условий специального вида, указанных в правилах работы компонентов. При проверке правил и определении истинности такого условия запрос данных у Dr.Web LookupD производится автоматически.



## Аргументы командной строки

Для запуска компонента Dr.Web LookupD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-lookupd [<параметры>]
```

Dr.Web LookupD допускает использование следующих параметров:

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

**Пример:**

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

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

## Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией [Dr.Web ConfigD](#) по мере необходимости. Для управления параметрами работы компонента пользуйтесь утилитой [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)).



Для получения справки о компоненте из командной строки используйте команду  
**man 1 drweb-lookupd**

## Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции [LookupD] объединенного [конфигурационного файла](#) продукта Dr.Web для Интернет-шлюзов UNIX.



В секции представлены следующие параметры:

<b>LogLevel</b> <i>{уровень подробности}</i>	<p><u>Уровень подробности</u> ведения журнала компонента.</p> <p>Если значение параметра не указано, используется значение параметра <b>DefaultLogLevel</b> из <u>секции</u> [Root].</p> <p><b>Значение по умолчанию:</b> Notice</p>
<b>Log</b> <i>{тип журнала}</i>	<p><u>Метод ведения журнала</u></p>
<b>ExePath</b> <i>{путь к файлу}</i>	<p>Путь к исполняемому файлу компонента.</p> <p><b>Значение по умолчанию:</b> &lt;opt_dir&gt;/bin/drweb-lookupd</p> <ul style="list-style-type: none"><li>• Для <b>Linux, Solaris</b>: /opt/drweb.com/bin/drweb-lookupd</li><li>• Для <b>FreeBSD</b>: /usr/local/libexec/drweb.com/bin/drweb-lookupd</li></ul>
<b>RunAsUser</b> <i>{UID   имя пользователя}</i>	<p>Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр (т.е. похоже на числовой UID), то оно указывается с префиксом «name:», например: <b>RunAsUser</b> = name:123456.</p> <p><i>Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.</i></p> <p><b>Значение по умолчанию:</b> drweb</p>
<b>IdleTimeLimit</b> <i>{интервал времени}</i>	<p>Максимальное время простоя компонента, по превышению которого он завершает свою работу.</p> <p>Минимальное значение – 10s.</p> <p><b>Значение по умолчанию:</b> 30s</p>
<b>DebugLibldap</b> <i>{логический}</i>	<p>Включать или нет в журнал на отладочном уровне (при <b>LogLevel</b> = DEBUG) также и отладочные сообщения библиотеки <b>libldap</b>.</p> <p><b>Значение по умолчанию:</b> No</p>
<b>LdapCheckCertificate</b> <i>{No   Allow   Try   Yes}</i>	<p>Режим проверки сертификатов при подключении к LDAP через SSL/TLS.</p> <p><b>Возможные значения:</b></p> <ul style="list-style-type: none"><li>• No – Никогда не запрашивать сертификат сервера.</li><li>• Allow – Запрашивать сертификат сервера, и если он не будет предоставлен, сессия будет продолжена нормальным образом; если же серверный сертификат предоставлен, но не может быть проверен (не удалось найти соответствующий корневой</li></ul>



	<p>сертификат), то сертификат сервера будет проигнорирован и сессия будет продолжена нормальным образом.</p> <ul style="list-style-type: none"><li>• <b>Try</b> – Запрашивать сертификат сервера, и если он не будет предоставлен, сессия будет продолжена нормальным образом; если же серверный сертификат предоставлен, но не может быть проверен (не удалось найти соответствующий корневой сертификат), то сессия будет прервана.</li><li>• <b>Yes</b> – Запрашивать сертификат сервера, и если он не будет предоставлен, сессия будет прервана; если серверный сертификат не может быть проверен (не удалось найти соответствующий корневой сертификат), то сессия также будет прервана.</li></ul> <p><i>Для источников данных типа LDAP влияет на обработку URL по схеме ldaps:// или с использованием расширения StartTLS; для источников данных типа AD влияет на соединение с сервером, если в соответствующей секции установлено UseSSL=Yes (см. ниже).</i></p> <p><b>Значение по умолчанию:</b> Yes</p>
<b>LdapCertificatePath</b> <i>{путь к файлу}</i>	<p>Путь к файлу сертификата SSL, используемого для подключения к серверам LDAP (<b>Active Directory</b>) через безопасное соединение SSL/TLS.</p> <p><i>Обратите внимание, что файл сертификата и файл закрытого ключа (определяется следующим параметром) должны соответствовать друг другу.</i></p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>LdapKeyPath</b> <i>{путь к файлу}</i>	<p>Путь к файлу закрытого ключа, используемого для подключения к серверам LDAP (<b>Active Directory</b>) через безопасное соединение SSL/TLS.</p> <p><i>Обратите внимание, что файл сертификата и файл закрытого ключа (определяется предыдущим параметром) должны соответствовать друг другу.</i></p> <p><b>Значение по умолчанию:</b> (не задано)</p>
<b>LdapCaPath</b> <i>{путь}</i>	<p>Путь к каталогу или файлу, в котором располагается перечень корневых сертификатов, являющихся доверенными при обмене данными по протоколу LDAP через SSL/TLS.</p> <p><b>Значение по умолчанию:</b> Путь к системному перечню доверенных сертификатов. Зависит от дистрибутива GNU/Linux:</p> <ul style="list-style-type: none"><li>• Для <b>Astra Linux, Debian, Linux Mint, SUSE Linux и Ubuntu</b> это обычно путь <code>/etc/ssl/certs/</code>;</li><li>• Для <b>CentOS и Fedora</b> – путь <code>/etc/pki/tls/certs/ca-bundle.crt</code>.</li><li>• Для других дистрибутивов путь может быть определен через результат вызова команды <b>openssl version -d</b>.</li></ul>



- Если команда недоступна или дистрибутив ОС опознать не удалось, используется значение `/etc/ssl/certs/`.

## Секции источников данных

Кроме основной секции `[LookupD]`, в файле конфигурации также задаются секции, описывающие подключения к серверам **LDAP** и **Active Directory** (по одной на каждое подключение). Эти секции именуются по схеме `[LookupD.<тип>.<имя>]`, где:


- `<тип>` – тип подключения: **LDAP** (для **LDAP**) или **AD** (для **Active Directory**).
- `<имя>` – уникальный идентификатор (тег) подключения для ссылки на него из правил.

Например: `[LookupD.LDAP.auth1]`. Секции, описывающие подключение, содержат набор параметров, зависящих от типа источника. Количество секций не ограничено.

### 1. Параметры секций типа LDAP

<b>url</b>  {строка}	<p>URL, определяющий используемый сервер LDAP и извлекаемые данные. Согласно <a href="#">RFC 4516</a>, URL строится по следующей схеме:</p> <pre>&lt;scheme&gt; : // &lt;host&gt; [ : &lt;port&gt; ] / &lt;dn&gt; [ ? &lt;attrs&gt; [ ? &lt;scope&gt; [ ? &lt;filter&gt; [ ? &lt;extensions&gt; ] ] ] ]</pre> <p>Здесь:</p> <ul style="list-style-type: none"><li><code>&lt;scheme&gt;</code> – способ подключения к серверу (допускаются схемы <code>ldap</code>, <code>ldaps</code> и <code>ldapi</code>);</li><li><code>&lt;host&gt; [ : &lt;port&gt; ]</code> – адрес сервера LDAP, к которому направляется запрос;</li><li><code>&lt;dn&gt;</code> – уникальное имя (distinguished name) объекта, информация о котором получается;</li><li><code>&lt;attrs&gt;</code> – имена атрибутов записей, значения которых должны быть получены в запросе;</li><li><code>&lt;scope&gt;</code> – область поиска (<code>base</code>, <code>one</code>, <code>sub</code>);</li><li><code>&lt;filter&gt;</code> – фильтрующее условие на значения извлекаемых атрибутов.</li><li><code>&lt;extensions&gt;</code> – перечень используемых в запросе расширений LDAP.</li></ul> <p><b>Особенности:</b></p> <ul style="list-style-type: none"><li>• В списке атрибутов <code>&lt;attrs&gt;</code> можно использовать спецсимволы выбора <code>'*'</code>, <code>'+'</code> и <code>'1.1'</code>.</li><li>• В частях URL <code>&lt;dn&gt;</code> и <code>&lt;filter&gt;</code> могут быть использованы следующие автоматически разрешаемые маркеры:<ul style="list-style-type: none"><li>▫ <code>\$u</code> – заменяется на имя пользователя, переданное клиентским компонентом.</li><li>▫ <code>\$d</code> – заменяется на имя домена, переданное клиентским компонентом.</li></ul></li></ul>
----------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



	<ul style="list-style-type: none"><li>▫ \$D – цепочка <code>&lt;subdomain&gt;.&lt;domain&gt;</code>, преобразованная в <code>dc=&lt;subdomain&gt;,dc=&lt;domain&gt;</code>.</li><li>▫ \$\$ – символ '\$'.</li><li>• Если в условии <code>&lt;filter&gt;</code> требуется использовать специальные символы (например: '*', '(', ')', '\', символ с кодом 0) как обычные, то их следует записывать в виде <code>\xx</code>. Кроме того, специальные символы в URL LDAP кодируются с помощью последовательностей <code>%xx</code>. Например, при использовании символа '/' в URL по схеме <code>ldapi</code> в качестве части пути к локальному сокету сервера LDAP, этот символ кодируется как <code>%2f</code>.</li><li>• В качестве допустимых расширений в <code>&lt;extensions&gt;</code> поддерживаются только <code>StartTLS</code> и <code>1.3.6.1.4.1.1466.20037</code>, которые включают использование механизма TLS (т.е. организация защищенного соединения с сервером LDAP, даже если явно не указано использование защищенной схемы <code>ldaps</code>) Если перед именем используемого расширения указан символ '!', то использование TLS <i>обязательно</i>, т.е. в случае невозможности установки безопасного соединения запрос <i>не будет</i> исполнен. В противном случае запрос будет исполнен, даже если безопасное соединение не будет установлено.</li></ul> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> Указанные расширения не могут применяться в случае использования защищенной схемы <code>ldaps</code>. Для получения более подробной информации воспользуйтесь <a href="#">RFC 4516</a> или <code>man ldap_search_ext_s</code>.</div> <p><b>Примеры:</b></p> <pre>"ldaps://ds.example.com:990/\$D?givenName,sn,cn?sub?(uid=\$u)" "ldap://ldap.local/o=org,dc=nodomain?ipNetworkNumber?sub?(objectClass=ipNetwork)?!StartTLS"</pre> <p><b>Значение по умолчанию:</b> <i>(не задано)</i></p>
<b>BindDn</b> <i>{строка}</i>	<p>Объект в каталоге LDAP, связываемый с пользователем для авторизации.</p> <p><b>Пример:</b> <code>"cn=admin,dc=nodomain"</code></p> <p><b>Значение по умолчанию:</b> <i>(не задано)</i></p>
<b>BindPassword</b> <i>{строка}</i>	<p>Пароль для аутентификации доступа к серверу LDAP.</p> <p><b>Значение по умолчанию:</b> <i>(не задано)</i></p>
<b>ChaseReferrals</b>	<p>Следовать ли по отсылкам на другие LDAP-серверы, если текущий сервер LDAP присылает их в ответ на запросы.</p>



{логический}	Значение по умолчанию: No
--------------	---------------------------

## 2. Параметры секции типа AD

<b>Host</b> {строка}	Доменное имя (FQDN) или IP-адрес узла, на котором находится сервер службы <b>Active Directory</b> , к которому необходимо подключиться.  <b>Пример:</b> "win2012.win.local" <b>Значение по умолчанию:</b> (не задано)
<b>Port</b> {целое число}	Порт на узле, прослушиваемый сервером службы <b>Active Directory</b> . <b>Значение по умолчанию:</b> 389
<b>Dn</b> {строка}	DN объекта в каталоге <b>Active Directory</b> (аналог части dn в URL LDAP).  <b>Пример:</b> "dc=win,dc=local" <b>Значение по умолчанию:</b> (не задано)
<b>User</b> {строка}	Полный идентификатор пользователя на сервере для идентификации.  <b>Пример:</b> "Administrator@WIN.LOCAL" <b>Значение по умолчанию:</b> (не задано)
<b>Password</b> {строка}	Пароль для аутентификации доступа к серверу <b>Active Directory</b> . <b>Значение по умолчанию:</b> (не задано)
<b>ChaseReferrals</b> {логический}	Следовать ли по отсылкам на другие LDAP-серверы, если текущий сервер <b>Active Directory</b> присылает их в ответ на запросы. <b>Значение по умолчанию:</b> No
<b>UseSSL</b> {логический}	Использовать SSL/TLS при обращении к серверу <b>Active Directory</b> . <b>Значение по умолчанию:</b> No

## Добавление секций источников данных

Чтобы добавить новую секцию параметров для источника данных некоторого типа с тегом `<имя>` при помощи утилиты [Dr.Web Ctl](#), предназначенной для управления Dr.Web для Интернет-шлюзов UNIX из командной строки (запускается [командой drweb-ctl](#)), достаточно использовать команду:

```
# drweb-ctl cfset LookupD.<mun> -a <имя>
```



Пример:

```
# drweb-ctl cfset LookupD.AD -a WinAD1  
# drweb-ctl cfset LookupD.AD.WinAD1.Host 192.168.0.20
```

Первая команда добавит в файл конфигурации секцию [LookupD.AD.WinAD1], а вторая изменит в ней значение параметра **Host**.

Кроме того, вы можете записать новую секцию непосредственно в [файл конфигурации](#) (например, добавив ее в конец файла):

```
[LookupD.AD.WinAD1]  
Host = 192.168.0.20
```



Оба способа задания настроек приведут к одинаковому результату, но в случае непосредственной правки файла конфигурации необходимо применить измененные настройки, отправив сигнал `SIGHUP` модулю **drweb-configd** (для этого вы можете выполнить [команду](#) **drweb-ctl reload**).





## Приложения

### Приложение А. Виды компьютерных угроз

Под термином «угроза» в данной классификации следует понимать любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они также могут нанести вред пользователю.

#### Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется инфицированием. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Большая часть вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы делят по типу файлов, которые они инфицируют:

- *файловые вирусы* инфицируют файлы операционной системы (обычно исполняемые файлы и динамические библиотеки) и активизируются при обращении к инфицированному файлу;
- *макро-вирусы* инфицируют документы, которые используют программы из пакета **Microsoft® Office** (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). *Макросы* – это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в **Microsoft® Word** макросы могут запускаться при открытии, закрытии или сохранении документа);
- *скрипт-вирусы* пишутся на языках сценариев (скриптов) и в большинстве случаев инфицируют другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях;
- *загрузочные вирусы* инфицируют загрузочные 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 защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- *шифрованные вирусы* шифруют свой код при каждом новом инфицировании, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры;
- *полиморфные вирусы* используют помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур;
- *стелс-вирусы (вирусы-невидимки)* предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишется на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т.д.) и по инфицируемым ими операционным системам.

## Компьютерные черви

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

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

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

В компании «Доктор Веб» червей делят по способу (среде) распространения:

- *сетевые черви* распространяются посредством различных сетевых протоколов и протоколов обмена файлами;



- *почтовые черви* распространяются посредством почтовых протоколов (POP3, SMTP и т.д.);
- *чат-черви* распространяются, используя популярные программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т.д.).

## Троянские программы

Этот тип вредоносных программ не способен к саморепликации. Троянские программы подменяют какую-либо из часто запускаемых программ и выполняют ее функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т.д.), либо делая возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловых сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполнять другие типы угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- *бэкдоры* – это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы; они прописывают себя в реестре, модифицируя ключи;
- *руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (*User Mode Rootkits – UMR*), и руткиты, работающие в режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет обнаружение и обезвреживание) (*Kernel Mode Rootkits – KMR*);
- *клавиатурные перехватчики (кейлоггеры)* используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действия является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т.д.);
- *кликеры* переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь



перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак);

- *прокси-трояны* предоставляют злоумышленнику анонимный выход в сеть Интернет через компьютер жертвы.

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

## Программы взлома

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

## Рекламные программы

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

## Программы-шутки

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

## Программы дозвона

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



## Потенциально опасные программы

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

## Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типом компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать в карантин, а также их следует отправлять на анализ специалистам антивирусной лаборатории «Доктор Веб».



## Приложение Б. Устранение компьютерных угроз

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

Эвристический анализатор также использует технологию FLY-CODE™ – универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчиком продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке запакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, запакованных одинаковым полиморфным упаковщиком.

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

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.



## Действия с угрозами

В продуктах Dr.Web реализована возможность применять определенные действия к обнаруженным объектам для обезвреживания компьютерных угроз. Пользователь может оставить автоматически применяемые к определенным типам угроз действия, заданные по умолчанию, изменить их или выбирать нужные действия для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий:

- *Ignore (Игнорировать)* – Пропустить обнаруженную угрозу, не предпринимая никаких действий.
- *Report (Информировать)* – Уведомить о наличии угрозы, но ничего не делать с инфицированным объектом.
- *Cure (Лечить)* – Попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое. Обратите внимание, что это действие применимо не ко всем видам угроз.
- *Quarantine (Переместить в Карантин, Изолировать)* – Переместить инфицированный объект (если он допускает эту операцию) в специальный каталог карантина с целью его изоляции.
- *Delete (Удалить)* – Безвозвратно удалить инфицированный объект.



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





## Приложение В. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу <https://download.drweb.com/doc/>;
- прочитайте раздел часто задаваемых вопросов по адресу [https://support.drweb.com/show\\_faq/](https://support.drweb.com/show_faq/);
- посетите форумы компании «Доктор Веб» по адресу <https://forum.drweb.com/>.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела <https://support.drweb.com/>;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу <https://company.drweb.com/contacts/offices/>.



## Приложение Г. Конфигурационный файл программного комплекса

Параметрами конфигурации всех компонентов программного комплекса Dr.Web для Интернет-шлюзов UNIX управляет координирующий демон управления конфигурацией Dr.Web ConfigD. Параметры конфигурации всех компонентов хранятся в едином файле `drweb.ini`, который по умолчанию располагается в каталоге `<etc_dir>` (`/etc/opt/drweb.com` для **GNU/Linux**).



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.

Об условных обозначениях путей `<opt_dir>`, `<etc_dir>` и `<var_dir>` см. [Введение](#).

Просмотреть перечень всех параметров, доступных для изменения, включая те, которые отсутствуют в конфигурационном файле, так как имеют значения по умолчанию, можно при помощи команды:

```
$ drweb-ctl cfshow
```

Изменить значение любого параметра можно двумя способами:

1. Задать его в конфигурационном файле (отредактировав файл в любом текстовом редакторе) и отправить сигнал SIGHUP демону управления конфигурацией (модуль **drweb-configd**) для применения внесенных в файл изменений (для этого вы можете выполнить [команду](#) **drweb-ctl reload**).
2. Выполнить в командной строке команду:

```
# drweb-ctl cfset <секция>.<параметр> <новое значение>
```



Обратите внимание, что для выполнения этой команды утилита управления Dr.Web Ctl должна запускаться от имени суперпользователя. Для получения прав суперпользователя используйте команду **su** или **sudo**.

Подробнее о синтаксисе команд `cfshow` и `cfset` консольной утилиты управления Dr.Web Ctl (модуль **drweb-ctl**) см. в разделе [Dr.Web Ctl](#).



## Структура файла

Файл конфигурации сформирован следующим образом:

- Содержимое файла разбито на последовательность именованных секций. Возможные имена секций жестко заданы и не могут быть произвольными. Имя секции задается в квадратных скобках и совпадает с именем компонента Dr.Web для Интернет-шлюзов UNIX, использующего параметры из этой секции (за исключением секции [Root], в которой хранятся параметры демона управления конфигурацией Dr.Web ConfigD).
- Символы ';' или '#' в строках конфигурационного файла обозначают начало комментария – весь текст, идущий в строке за этими символами, пропускается компонентами Dr.Web для Интернет-шлюзов UNIX при чтении параметров из конфигурационного файла.
- В одной строке файла задается значение только одного параметра конфигурации. Основной формат задания значения параметра (пробелы, окружающие символ '=', если встречаются, игнорируются):

```
<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.
- Порядок, в котором указаны секции в файле и порядок, в котором указаны параметры внутри секции, не имеют значения.
- Значения параметров в конфигурационном файле могут быть заключены в кавычки, и должны быть заключены в кавычки в том случае, если они содержат пробелы.
- Некоторые параметры могут иметь список 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, всё значение необходимо заключить в кавычки.

Примеры задания параметра, имеющего несколько значений:

- 1) Перечисление нескольких значений через запятую:

```
Parameter = Value1, Value2, "Value 3"
```

- 2) Задание тех же значений параметра в разных строках секции конфигурационного файла:

```
Parameter = Value2  
Parameter = Value1  
Parameter = "Value 3"
```

Обратите внимание, что порядок следования значений параметра в списке его значений также несущественен.



Если значения параметра являются путями, то каждое значение параметра в списке должно быть заключено в кавычки, если используется форма перечисления значений через запятую. Например, если в параметре **ExcludedPaths** требуется указать два пути `/etc/file1` и `/etc/file2`, то этот параметр нужно записать в файл конфигурации либо в виде строки

```
ExcludedPaths = "/etc/file1", "/etc/file2"
```

либо в виде двух строк

```
ExcludedPaths = /etc/file1  
ExcludedPaths = /etc/file2
```

В противном случае строка `/etc/file1, /etc/file2` может быть воспринята использующим данный параметр компонентом как один путь.

- Возможность присвоения параметру нескольких значений указывается явно. Если для некоторого параметра в данном документе или в комментариях в файле конфигурации явно не указано, что ему можно присвоить несколько значений, то параметр может обладать только одним значением.

Описание секций конфигурационного файла приведено в описании использующих его компонентов Dr.Web для Интернет-шлюзов UNIX.

## Типы параметров

Параметры конфигурации могут быть следующих типов:

- *адрес* – Адрес сетевого соединения в виде пары `<IP-адрес>:<порт>`. В некоторых случаях порт может быть опущен (в каждом случае это указывается в описании параметра).
- *логический* – Параметр-флаг. В качестве значений параметра могут быть использованы только значения `Yes` и `No`.
- *целое число* – В качестве значения параметра может быть указано неотрицательное целое число.
- *дробное число* – В качестве значения параметра может быть указано неотрицательное число, содержащее дробную часть.
- *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 следующие суффиксы, задающие единицы измерения:
  - `w` – недели (`1w = 7d`);
  - `d` – сутки (`1d = 24h`);
  - `h` – часы (`1h = 60m`);
  - `m` – минуты (`1m = 60s`);
  - `s` – секунды.



Если суффикс опущен, считается, что задан интервал времени в секундах. Для интервала, заданного в секундах, можно после точки указать миллисекунды (не более трех знаков после запятой, 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  $N_1, \dots, N_6$  – 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:

1. В файле конфигурации:

```
UpdateInterval = 30m2.5s
```

2. С использованием [команды drweb-ctl](#) cfset:

```
# drweb-ctl cfset Update.UpdateInterval 1802.5s
```

3. Задание через параметр командной строки (например, для сканирующего ядра [Аргументы командной строки](#)):

```
$ drweb-se --WatchdogInterval 1802.5
```

- *размер* – В качестве значения параметра указывается размер некоторого объекта (файла, буфера, кэша и т.п.), состоящий из целого неотрицательного числа и суффикса, указывающего заданную единицу измерения. Могут быть использованы следующие суффиксы, задающие единицы размера:

- 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 (в реальности в параметрах конфигурации размер всегда сохраняется в байтах).

- *путь к каталогу (файлу)* – В качестве значения параметра выступает строка, содержащая допустимый путь к каталогу (файлу). Обратите внимание, что 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 (? , \*).



- *уровень подробности* – Параметр задает уровень подробности записи в журнал для компонента Dr.Web для Интернет-шлюзов UNIX. Параметр этого типа может принимать следующие 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.
- *тип журнала* – Параметр определяет способ ведения журнала компонентом Dr.Web для Интернет-шлюзов UNIX. Параметр этого типа может принимать следующие 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>` – Сообщения будут сохраняться компонентом непосредственно в указанный файл журнала.

Примеры задания параметра:

1. В файле конфигурации:

```
Log = Stderr:ShowTimestamp
```

2. С использованием [команды](#) `drweb-ctl cfset:`



```
# drweb-ctl cfset Root.Log /var/opt/drweb.com/log/general.log
```

3. Задание через параметр командной строки (например, для сканирующего ядра [Аргументы командной строки](#)):

```
$ drweb-se --Log Syslog:DAEMON
```

- *действие* – Действие, которое необходимо совершить компоненту Dr.Web для Интернет-шлюзов UNIX в случае обнаружения угроз некоторого типа или при возникновении некоторого другого события. Возможные значения:
  - Report – Только сформировать уведомление об угрозе, не предпринимать более никаких действий.
  - Cure – Попытаться выполнить лечение (удалить из тела файла только вредоносное содержимое).
  - Quarantine – Переместить инфицированный файл в карантин.
  - 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.

## Правила проверки трафика

Правила представляют собой цепочку продукций вида ЕСЛИ *<условная часть>* ТО *<часть действий>*. При этом в части *<условная часть>* перечисляются проверки вида «Переменная (не) имеет заданное значение» или «Значение переменной (не) входит в указанное множество», а в *<часть действий>* содержит набор (не менее одного) действий, каждое из которых представляет собой *конечную резолюцию* (пропустить или заблокировать проверяемый объект) или *модифицирующее действие* вида «Изменить свойства проверяемого объекта», «Присвоить указанной переменной заданное значение» или «Добавить заданное значение к множеству значений указанной переменной».

Часть действий правила выполняется, только если истинна условная часть. Если условная часть правила ложна, то действия, указанные в этом правиле, не выполняются и осуществляется переход к следующему правилу. Правила перебираются сверху вниз до тех пор, пока не сработает какая-либо конечная резолюция. После этого все нижележащие правила (если имеются) игнорируются. Важно, что действия в *<части действий>* при срабатывании правила выполняются в порядке их перечисления слева направо, при этом, если в цепочке действий встречается конечная резолюция, прерывающая обработку правил, оставшаяся часть действий, указанная в *<части действий>*, не выполняется.



## Формат правил


Формат продукции правила имеет вид:

```
[<условие>[, <условие>[, ...]]] : <действие>[, <действие>[, ...]]
```

Условная часть правила (перед символом ':') может отсутствовать, в этом случае часть действий выполняется безусловно. Если условная часть правила отсутствует, то разделитель ':' может быть опущен. Запятая между условиями в условной части и действиями в части действий играет роль конъюнкции (т.е. логического «И»): условная часть считается истинной, только если истинны все перечисленные в ней условия, а все действия, указанные в части действий, выполняются в порядке их перечисления слева направо до момента встречи конечной резолюции, прерывающая обработку правил. Ключевые слова, имена переменных и параметров из конфигурации в правилах не чувствительны к регистру.

## Условия

В условной части правил могут встречаться следующие типы условий:

Условие	Смысл условия
<code>&lt;переменная&gt; &lt;значение&gt;</code>	Значение указанной переменной совпадает с заданным.  <i>Может быть использовано только для переменных, которые не могут принимать множества значений.</i>
<code>&lt;переменная&gt; [not] in &lt;множество значений&gt;</code>	Значение указанной переменной содержится в указанном множестве значений (для <i>not</i> – не совпадает ни с одним из значений указанного множества).
<code>&lt;переменная&gt; [not] match &lt;множество значений&gt;</code>	Значение указанной переменной соответствует любому регулярному выражению из указанного набора (для <i>not</i> – не соответствует ни одному из выражений в указанном наборе). <div> Регулярные выражения записываются с использованием синтаксиса POSIX (BRE, ERE) или Perl (PCRE, PCRE2).</div>
<code>&lt;переменная&gt; [not] gt &lt;значение&gt;</code>	Значение указанной переменной (не) больше заданного.





Условие	Смысл условия
	<i>Может быть использовано только для переменных, которые принимают единственное числовое значение.</i>
<code>&lt;переменная&gt; [not] lt &lt;значение&gt;</code>	<p>Значение указанной переменной (не) меньше заданного.</p> <p><i>Может быть использовано только для переменных, которые принимают единственное числовое значение.</i></p>

\*) Необязательное ключевое слово `not` обозначает отрицание.


Часть *<множество значений>*, с которым сравнивается переменная, может быть указано следующим способом:

Запись	Смысл
<code>(&lt;значение 1&gt;[, &lt;значение 2&gt;[, ...]])</code>	В скобках перечисляется непосредственно множество проверяемых значений (не менее одного). Для случая с одним значением и использованием условия <code>in</code> скобки можно опустить (получится случай <code>&lt;переменная&gt; &lt;значение&gt;</code> ).
<code>"&lt;секция&gt; . &lt;параметр&gt;"</code>	<p>Множество значений некоторого параметра конфигурации, где в кавычках указывается имя параметра из конфигурации (с указанием содержащей его секции), значение (или набор значений) которого проверяется.</p> <p>Перечни параметров, которые можно использовать в условии, зависят от компонента, для которого заданы правила, и приведены ниже.</p>
<code>file("&lt;имя файла&gt;")</code>	Перечень значений считывается из текстового файла <i>&lt;имя файла&gt;</i> (одна строка файла – один элемент списка, ведущие и завершающие пробелы в строках не учитываются). Путь к файлу должен быть абсолютным. Кавычки и апострофы, если они встречаются в <i>&lt;имя файла&gt;</i> , необходимо экранировать символом кривой черты <code>'\'</code> .



Запись	Смысл
	<div data-bbox="916 255 1449 1460"><p>Размер файла не должен быть больше 64 МБ.</p><p>Содержимое файла считывается и подставляется в правила один раз – при загрузке <u>файла конфигурации</u>. Если указанный файл отсутствует или его размер слишком велик, при загрузке настроек будет выдана <u>ошибка</u> x102.</p><p>В случае если содержимое файла изменено в процессе работы программного комплекса, для применения внесенных изменений необходимо после сохранения файла перезагрузить программный комплекс, используя <u>команду</u> <b>drweb-ctl reload</b>.</p><p>Не для всех переменных можно получать множество значений из файла. Для каждой переменной ниже указывается, можно ли использовать для проверки ее значений множество значений, получаемые из файла.</p></div>
<mun_LOOKUP_запроса>@<тег> [ @<значение> ]	<p>Множество значений запрашивается через Dr.Web LookupD у внешнего источника данных (LDAP, ActiveDirectory), где &lt;mun_LOOKUP_запроса&gt; – это тип источника (LDAP или AD); &lt;тег&gt; – это имя секции, описывающей подключение для выборки проверяемого параметра, а необязательное &lt;значение&gt; – значение, которое должно находиться в множестве значений, извлеченных из источника данных.</p>



Запись	Смысл
	<div><p>Не для всех переменных можно получать значения через Dr.Web LookupD. Также не для всех переменных используется условие <i>&lt;проверка&gt;</i>. Для каждой переменной ниже указывается, можно ли использовать для проверки ее значений значения, получаемые через Dr.Web LookupD.</p></div>

Если переменная имеет множественное значение, то условие *<переменная> in <множество значений>* истинно, если пересечение множества текущих значений указанной переменной *<переменная>* с указанным множеством *<множество значений>* не пусто. Условие *not in* истинно в противоположном случае. Например, пусть *X* – переменная, текущее значение которой – множество, содержащее значения *a, b, c*. Тогда:

- *X in (a, b)* – истинно, так как значения *a* и *b* встречаются в обоих множествах;
- *X in (a, d, e)* – истинно, так как значение *a* встречается в обоих множествах;
- *X in (d, e)* – ложно, так как ни одно из значений переменной (*a, b, c*) не встречается в множестве (*d, e*).
- *X in ()* – ложно, так как множество значений переменной не пусто.
- *X not in ()* – истинно, множество значений переменной не пусто.
- *X not in (d, e)* – истинно, так как ни одно из значений переменной (*a, b, c*) не встречается в множестве (*d, e*).
- *X not in (a, d, e)* – ложно, так как значение *a* встречается в обоих множествах.

В описании переменных ниже для каждой переменной указано, может ли она принимать множество значений.



## Действия

Действия делятся на *конечные резолюции*, определяющие запрет или разрешение на пропуск объекта и *действия, изменяющие значения некоторой переменной*, что может быть использовано при проверке условий в нижележащих правилах.

### Конечные резолюции

Резолюция	Описание (смысл)
<b>Общие резолюции</b>	
PASS	<p>Пропустить трафик (разрешить создать соединение, передать объект получателю). Последующие правила (если имеются) не используются.</p> <p>Для правил обработки почты имеет смысл команды пропуска письма к получателю, применив к нему все накопленные изменения (т.е. все сработавшие действия REPACK, ADD_HEADER, CHANGE_HEADER, см. ниже).</p>
BLOCK as <reason>	<p>Заблокировать трафик (отказать в создании соединения, передаче объекта получателю). Последующие правила (если имеются) не используются..</p> <p>В журнале фиксируется, что блокировка случилась по причине &lt;reason&gt;. Эта же причина используется для определения, какую страницу с уведомлением показать пользователю в браузере. В качестве &lt;reason&gt; для BLOCK может быть использовано две стандартные причины:</p> <ul style="list-style-type: none"><li>• BlackList – считается, что данные заблокированы по причине попадания в черный список пользователя.</li><li>• _match – причиной блокировки является попадание веб-ресурса или файла с угрозой в категорию, из-за которой сработало правило (для условий *_category in (...)). Переменная _match хранит список блокируемых <a href="#">категорий</a>, для которых сработало соответствие.</li></ul>

Особенности обработки конечных резолюций:

- BLOCK as BlackList всегда отрабатывает как «*попал в черный список*» (вне зависимости от того, что за условие указано в правиле с данной резолюцией).
- BLOCK as \_match, если в \_match не пусто, отрабатывает как «*попал в \_match категорию(u)*».
- BLOCK as \_match, если в \_match пусто, отрабатывает как «*попал в черный список*» (вне зависимости от того, что за условие указано в правиле с данной резолюцией).



- Если были просмотрены все правила, а ни одно правило с резолюцией не сработало (или резолюции отсутствуют в правилах), то это равносильно применению к соединению действия PASS.



Для правил SpIDer Gate, управляющих не почтовыми соединениями, срабатывание почтовой резолюции равносильно BLOCK as BlackList (дополнительно в журнале будет зафиксировано сообщение о применении неизвестного действия).

В правилах для Dr.Web ICAPD почтовые резолюции не имеют смысла: правила, содержащие почтовые резолюции, игнорируются без какой-либо реакции.

## Изменение значения переменной

Для изменения значения переменной используется инструкция

```
SET <переменная> = ([<значение 1>[, <значение 2>[, ...]]])
```

Если скобки пустые – это означает очистку списка значений переменной. Для случая с одним значением скобки необходимо опустить, т.е. использовать синтаксис

```
SET <переменная> = <значение>
```

## Переменные, используемые в правилах

При указании переменных в правилах регистр символов не учитывается. Переменные, название которых состоит из нескольких слов, могут быть записаны с использованием подчеркивания для разделения слов, или записаны без подчёркивания. Таким образом, записи `variable_name`, `VariableName` и `variablename` представляют одну и ту же переменную. В данном разделе все переменные записаны с использованием подчеркивания (т.е. используется вариант написания `variable_name`).

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
<code>protocol</code>	<p>Тип сетевого протокола, используемого соединением.</p> <p><i>Переменная может принимать множество значений.</i></p> <p><b>Возможные значения:</b> HTTP, SMTP, IMAP, POP3.</p>	Да	Нет



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	<p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.</li><li>• В правилах для Dr.Web ICAPD не имеет смысл указывать значение, отличное от HTTP: для него протокол может быть только HTTP.</li><li>• Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>protocol in (HTTP, SMTP) protocol in (POP3) protocol in file("/etc/file")</pre>		
sni_host	<p>SNI (адрес) узла, с которым устанавливается соединение через SSL/TLS.</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>• Если SSL не используется, то значение переменной не определено, условие будет ложным.</li><li>• Не имеет смысла использовать в правилах для Dr.Web ICAPD (он не обрабатывает SSL, поэтому условие всегда будет ложным).</li><li>• Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>sni_host not in ('vk.com', 'ya.ru') sni_host in "LinuxFirewall.BlackList" sni_host in file("/etc/file")</pre>	Да	Нет



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
sni_category	<p>Список <a href="#">категорий</a>, к которым в базах категорий веб-ресурсов относится узел (определенный по SNI), с которым устанавливается соединение через SSL/TLS (<i>AdultContent</i>, и т.п.).</p> <p><i>Переменная может принимать множество значений.</i></p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>• Если SSL не используется, то значение переменной не определено, условие будет ложным.</li><li>• Не имеет смысл использовать в правилах для Dr.Web ICAPD (он не обрабатывает SSL, поэтому условие всегда будет ложным).</li><li>• Для правил, используемых компонентами Dr.Web MailD и Dr.Web ICAPD, условие <code>c not in</code> будет <i>истинным</i>, даже если по результатам проверки узел не принадлежит никакой из предопределенных категорий («безопасный» узел). Для правил компонента Dr.Web Firewall для Linux (SpIDer Gate) условие в этом случае будет <i>ложным</i>.</li><li>• Если базы данных категорий веб-ресурсов не установлены, то переменную нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке <a href="#">x112</a>).</li><li>• Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>sni_category not in (AdultContent, Chats) sni_category in "LinuxFirewall.BlockCategory" sni_category in (FreeEmail)</pre>	Да	Нет



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	<code>sni_category not in file("/etc/file")</code>		
<code>url</code>	<p>URL, запрошенный клиентом. Может быть сравнен с указанной строкой или регулярным выражением.</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>• Можно использовать только в правилах для Dr.Web ICAPD.</li><li>• Для проверки значения переменной можно использовать Dr.Web LookupD.</li><li>• Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>url match ("drweb.com", "example\..*", "aaa.ru/") url match "ICAPD.Adlist" url not match LDAP@BadURLs url match file("/etc/file")</pre>	Да	Нет
<code>url_host</code>	<p>URL/узел, с которым устанавливается соединение.</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.</li><li>• Для проверки значения переменной можно использовать Dr.Web LookupD.</li><li>• Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>url_host in ('vk.com', 'ya.ru') url_host not in "ICAPD.Whitelist" url_host in LDAP@hosts url_host not in file("/etc/file")</pre>	Да	Нет





Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
url_category	<p>Список <a href="#">категорий</a>, к которым (по базам категорий веб-ресурсов или по ответу из Dr.Web Cloud) относится URL/узел, с которым установлено соединение.</p> <p><i>Переменная может принимать множество значений.</i></p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.</li><li>Для правил, используемых компонентами Dr.Web MailD и Dr.Web ICAPD, условие с <code>not in</code> будет <i>истинным</i>, даже если по результатам проверки URL/узел не принадлежит никакой из predeterminedных категорий («безопасный» URL/узел). Для правил компонента Dr.Web Firewall для Linux (SpIDer Gate) условие в этом случае будет <i>ложным</i>.</li><li>Если базы данных категорий веб-ресурсов не установлены, то переменную нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке <a href="#">x112</a>).</li><li>Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>url_category not in (AdultContent, Chats) url_category in "LinuxFirewall.BlockCategory" url_category in (FreeEmail) url_category in file("/etc/file")</pre>	Да	Нет
threat_category	Список <a href="#">категорий</a> , к которым по информации из вирусных баз относится	Да	Нет



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	<p>угроза, обнаруженная в передаваемых данных.</p> <p><i>Переменная может принимать множество значений.</i></p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.</li><li>Для правил, используемых компонентами Dr.Web MailD и Dr.Web ICAPD, условие <code>c not in</code> будет <i>истинным</i>, даже если по результатам проверки объект не содержит угроз ни из одной из predeterminedных категорий («безопасный» объект). Для правил компонента Dr.Web Firewall для Linux (SpIDer Gate) условие в этом случае будет <i>ложным</i>.</li><li>Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>threat_category in "LinuxFirewall.BlockThreat" threat_category not in (Joke) threat_category in file("/etc/file")</pre>		
user	<p>Имя пользователя, с правами которого запущен процесс-отправитель (или получатель) трафика.</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>В правилах для Dr.Web ICAPD имеет смысл имени пользователя, прошедшего аутентификацию на прокси-сервере (если прокси-сервер поддерживает аутентификацию). Если прокси-сервер не аутентифицирует пользователей, переменная имеет пустое значение.</li></ul>	Да	Нет



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	<ul style="list-style-type: none"><li>Для проверки значения переменной можно использовать Dr.Web LookupD.</li><li>Если требуется проверить вхождение пользователя в некоторую группу пользователей, используйте источник данных LDAP или Active Directory, возвращающий перечень групп. Также запрос должен содержать условие сравнения имени группы, которой принадлежит пользователь, с требуемым (используйте формат <i>&lt;тип источника LookupD&gt;@&lt;источник групп&gt;@&lt;требуемая группа&gt;</i>). Запросы к Active Directory (AD@) возвращают только перечни групп, поэтому для них использование части <i>@&lt;требуемая группа&gt;</i> обязательно.</li><li>Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>user in ('user1', 'user2') user in AD@Winusergroups@Admins user in LDAP@AllowedUsers user not in file("/etc/file")</pre>		
src_ip	<p>IP-адрес узла, со стороны которого следует соединение.</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>Для проверки значения переменной можно использовать Dr.Web LookupD.</li><li>Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>src_ip not in (127.0.0.1, 10.20.30.41, 198.126.10.0/24) src_ip in LDAP@AllowedAddresses</pre>	Да	Нет



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	<code>src_ip not in file("/etc/file")</code>		
<code>proc</code>	<p>Процесс, устанавливающий соединение (полный путь к исполняемому файлу).</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>• Не имеет смысла использовать в правилах для Dr.Web ICAPD (он не имеет информации о процессах, поэтому условие всегда будет ложным).</li><li>• Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>proc in ('/usr/bin/lis') proc not in ('/home/user/myapp', '/bin/bin1') proc in "LinuxFirewall.ExcludedProc" proc in file("/etc/file")</pre>	Да	Нет
<code>direction</code>	<p>Тип трафика, идущего по соединению.</p> <p><b>Возможные значения:</b> <code>request</code> (клиентский запрос), <code>response</code> (ответ сервера).</p> <p><i>Переменная не может иметь множества значений, условия типа <code>match u in</code> неприменимы.</i></p> <p><b>Примеры:</b></p> <pre>direction request direction not response</pre>	Да	Нет
<code>divert</code>	<p>Направление соединения.</p> <p><b>Возможные значения:</b> <code>input</code> (входящее – создано/инициировано извне локального узла), <code>output</code> (исходящее – создано/инициировано на локальном узле).</p>	Да	Нет



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	<p><i>Переменная не может иметь множества значений, условия типа match и in неприменимы.</i></p> <p><b>Примеры:</b></p> <pre>divert input divert not output</pre>		
content_type	<p>MIME-тип данных, передающихся по соединению.</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"><li>• Может быть определен, только если не используется SSL/TLS или было разрешено вскрытие SSL.</li><li>• Выражению "*"/*" соответствуют данные любого MIME-типа, а также HTTP-ответы без заголовка Content-Type.</li><li>• Для проверки значения переменной можно использовать Dr.Web LookupD.</li><li>• Множество значений для проверки значения переменной можно получать из файла.</li></ul> <p><b>Примеры:</b></p> <pre>content_type in ("multipart/byteranges", "application/octet-stream") content_type not in ("text/*", "image/*") content_type not in ("audio/*") content_type in ("*/*") content_type in LDAP@BlockedContent content_type not in file("/etc/file")</pre>	Да	Нет
unwrap_ssl	<p>Используется ли раскрытие защищенного трафика, передаваемого через SSL/TLS.</p> <p><b>Возможные значения:</b> true, false.</p>	Нет	Да



Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	<p><b>Особенности использования:</b></p> <ul style="list-style-type: none"> <li>Переменная не может не иметь значения, т.е. инструкция <code>SET unwrap_ssl = ()</code> недопустима.</li> <li>Переменная не может использоваться в условиях, а нужна только для управления вскрытием SSL (например, чтобы продемонстрировать пользователю веб-страницу с уведомлением о блокировке от нашего имени).</li> <li>Не имеет смысла использовать в правилах для Dr.Web ICAPD (он не обрабатывает SSL, изменение значения переменной никак не влияет на обработку правил).</li> </ul> <p><b>Примеры:</b></p> <pre>SET unwrap_ssl = TRUE set Unwrap_SSL = false</pre>		
<code>http_templates_dir</code>	<p>Путь к каталогу, из которого брать шаблон страницы уведомления о блокировке HTTP-запроса/ответа.</p> <p>Если путь начинается с / – это абсолютный путь, если с любого другого символа – то это относительный путь. Корнем при этом считается путь из параметра <b>TemplatesDir</b>.</p> <p><b>Особенности использования:</b></p> <ul style="list-style-type: none"> <li>Имеет смысл только для протокола HTTP(S).</li> </ul> <p><b>Примеры:</b></p> <pre>SET http_templates_dir = "/etc/mytemplates" set http_templates_dir = "templates_for_my_site"</pre>	Нет	Да

## Категории нежелательных веб-сайтов и угроз

1. Категории нежелательных веб-сайтов (для переменных `sni_category`, `url_category`)



Обозначение	Категория веб-сайтов
<i>InfectionSource</i>	Сайты, содержащие вредоносное ПО («источники распространения вирусов»).
<i>NotRecommended</i>	Сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению.
<i>AdultContent</i>	Сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.
<i>Violence</i>	Сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
<i>Weapons</i>	Сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
<i>Gambling</i>	Сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.
<i>Drugs</i>	Сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
<i>ObsceneLanguage</i>	Сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
<i>Chats</i>	Сайты для обмена сообщениями в режиме реального времени.
<i>Terrorism</i>	Сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
<i>FreeEmail</i>	Сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика.
<i>SocialNetworks</i>	Социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств.
<i>DueToCopyrightNotice</i>	Сайты, ссылки на которые указаны правообладателями некоторого произведения, защищенного авторскими правами (кинофильмы, музыкальные произведения и т. д.).

В качестве значения переменных `sni_category` и `url_category` можно также использовать имена параметров, управляющих блокировкой (см. ниже).

## 2. Категории угроз (для переменной `threat_category`)

Обозначение	Категория угроз
<i>KnownVirus</i>	Известная угроза (вирус).
<i>VirusModification</i>	Модификация известной угрозы (вируса).



Обозначение	Категория угроз
<i>UnknownVirus</i>	Неизвестная угроза, подозрительный объект.
<i>Adware</i>	Рекламная программа.
<i>Dialer</i>	Программа дозвона.
<i>Joke</i>	Программа-шутка.
<i>Riskware</i>	Потенциально опасная программа.
<i>Hacktool</i>	Программа взлома.

В качестве значения переменной `threat_category` можно также использовать имена параметров, управляющих блокировкой (см. ниже).

## Параметры конфигурации, которые можно использовать в условиях правил

Параметры, используемые в правилах компонента Dr.Web Firewall для Linux (указываются с префиксом `LinuxFirewall.`):

Параметр	Описание и пример использования
<code>Whitelist</code>	<p>Белый список. Хранит перечень доменов, доступ к которым разрешается, даже если эти домены находятся в базе категорий.</p> <p><b>Примеры:</b></p> <pre>sni_host in "LinuxFirewall.Whitelist" : PASS url_host not in "LinuxFirewall.Whitelist" : BLOCK as _match</pre>
<code>Blacklist</code>	<p>Черный список. Хранит перечень доменов, доступ к которым запрещен самим пользователем (или администратором).</p> <p><b>Примеры:</b></p> <pre>sni_host in "LinuxFirewall.Blacklist" : SET Unwrap_SSL = FALSE url_host in "LinuxFirewall.Blacklist" : BLOCK as BlackList</pre>
<code>BlockCategory</code>	<p>«Мета-параметр»: Его значениями является список названий категорий (<i>Chats</i>, <i>AdultContent</i> и т.д.), для которых соответствующие параметры <b>Block*</b> в секции <code>[LinuxFirewall]</code> установлены в <code>Yes</code>.</p> <p><b>Примеры:</b></p> <pre>url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match</pre>





Параметр	Описание и пример использования
	<code>sni_category in "LinuxFirewall.BlockCategory" : BLOCK as BlackList</code>
BlockThreat	«Мета-параметр»: Его значениями является список названий типов угроз ( <i>KnownVirus</i> , <i>Joke</i> и т.д.), для которых соответствующие параметры <b>Block*</b> в секции [LinuxFirewall] установлены в Yes.  <b>Примеры:</b> <code>threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match</code>
ExcludedProc	Перечень доверенных процессов, трафик которых не должен проверяться.  <b>Примеры:</b> <code>proc in "LinuxFirewall.ExcludedProc" : PASS</code>

Параметры, используемые в правилах компонента Dr.Web ICAPD (указываются с префиксом ICAPD.):

Параметр	Описание и пример использования
Whitelist	Белый список. Хранит перечень доменов, доступ к которым разрешается, даже если эти домены находятся в базе категорий.  <b>Примеры:</b> <code>url_host not in "ICAPD.Whitelist" : BLOCK as BlackList</code>
Blacklist	Черный список. Хранит перечень доменов, доступ к которым запрещен самим пользователем (или администратором).  <b>Примеры:</b> <code>url_host in "ICAPD.Blacklist" : BLOCK as BlackList</code>
Adlist	Рекламный список. Хранит перечень регулярных выражений, которые описывают рекламные сайты. Задается самим пользователем (или администратором).  <b>Примеры:</b> <code>url match "ICAPD.Adlist" : BLOCK as BlackList</code>
BlockCategory	«Мета-параметр»: Его значениями является список названий категорий ( <i>Chats</i> , <i>AdultContent</i> и т.д.), для которых соответствующие параметры <b>Block*</b> в секции [ICAPD] установлены в Yes.  <b>Примеры:</b> <code>url_category in "ICAPD.BlockCategory" : BLOCK as _match</code>



Параметр	Описание и пример использования
BlockThreat	<p>«Мета-параметр»: его значениями является список названий типов угроз (<i>KnownVirus</i>, <i>Joke</i> и т.д.), для которых соответствующие параметры <b>Block*</b> в секции [ICAPD] установлены в Yes.</p> <p><b>Примеры:</b></p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre>

## Особенности сохранения правил в файл конфигурации

- В файле конфигурации, в секциях настроек компонентов, использующих правила, правила хранятся в переменных типа **RuleSet**, каждая из которых представляет собой набор (последовательность), состоящий из неограниченного числа правил. При этом правила в каждом наборе перебираются последовательно (сверху вниз) до момента достижения конечной резолюции.
- При записи в файл конфигурации безусловного правила (правила, содержащего только действия и не содержащего условной части), к нему будет добавлена пустая условная часть и знак разделителя ':'.

Например, следующее правило, не содержащее условной части, и состоящее только из действия:

```
BLOCK as _match
```

будет записано в файл конфигурации в следующем виде:

```
: BLOCK as _match
```

- При записи в файл конфигурации правило, содержащее в части действий набор из нескольких действий, будет записано в виде последовательности правил с одинаковой условной частью и одним действием в части действий в том же порядке, в каком перечислены действия.

Например, следующее правило, содержащее два действия в части действий:

```
user in ('user1', 'user2') : SET http_templates_dir = "/etc/mytemplates",  
BLOCK as _match
```

будет записано в файл конфигурации в виде последовательности двух правил:

```
user in ('user1', 'user2') : SET http_templates_dir = "/etc/mytemplates"  
user in ('user1', 'user2') : BLOCK as _match
```

- Так как в записи правил не предусмотрено дизъюнкции (логическое «ИЛИ») условий в условной части, для реализации логического «ИЛИ» следует записать цепочку правил, в условии каждого из которых будет указано единственное условие-дизъюнкт. Например, следующие два правила эквивалентны правилу «Осуществить блокировку, если обнаружен вредоносный объект типа *KnownVirus* или URL из категории *Terrorism*»:



```
threat_category in (KnownVirus) : BLOCK as _match  
url_category in (Terrorism) : BLOCK as _match
```

так как следующие записи логически эквивалентны:  $(a \rightarrow x, b \rightarrow x); ((a \rightarrow x) \wedge (b \rightarrow x)); ((a \vee b) \rightarrow x)$ .

Как и для любого параметра конфигурации, значения параметров типа **RuleSet** (т.е. правила) могут быть просмотрены и изменены при помощи команд `cfshow` и `cfset` утилиты управления Dr.Web Ctl (модуль **drweb-ctl**). Подробнее о синтаксисе команд `cfshow` и `cfset` консольной утилиты управления Dr.Web Ctl (модуль **drweb-ctl**) см. в разделе [Dr.Web Ctl](#).



## Приложение Д. Генерация сертификатов SSL

Для компонентов программного комплекса Dr.Web для Интернет-шлюзов UNIX, 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 программного продукта. 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 (CA) 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 CA.

### Генерация закрытого ключа SSL и сертификата

Генерация состоит из двух шагов:

1. Генерация закрытого ключа (алгоритм RSA, длина ключа – 2048 бит):

```
$ 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 можно использовать команду:

```
$ openssl rsa -noout -text -in keyfile.key
```

2. Генерация сертификата на указанный срок на основании имеющегося закрытого ключа (в данном примере – на 365 суток)

```
$ openssl req -new -x509 -days 365 -key keyfile.key -out certificate.crt
```

Обратите внимание, что данная 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 можно воспользоваться следующей командой:

```
$ openssl x509 -noout -text -in certificate.crt
```



## Регистрация сертификата в качестве доверенного сертификата СА

Если имеется сертификат, который нужно зарегистрировать в системном списке доверенных сертификатов центров сертификации (например, такой сертификат мог быть сгенерирован на предыдущем шаге), необходимо выполнить следующие действия:

1. Переместить или скопировать файл сертификата в системный каталог доверенных сертификатов (в **Debian/Ubuntu** – `/etc/ssl/certs/`).
2. Создать в каталоге доверенных сертификатов символическую ссылку на сертификат именем которой будет являться хэш сертификата.
3. Переиндексировать содержимое системного каталога сертификатов.

Приведенный ниже пример выполняет все эти три действия. Предполагается, что 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/
```

## Создание подписанного сертификата

Для создания подписанного сертификата необходимо выполнить следующие шаги:

1. Сгенерировать файл-запрос на подписание сертификата (*Certificate Signing Request – CSR*) на основании имеющегося закрытого ключа. Если ключа не имеется, его предварительно следует сгенерировать. Запрос на подписание создается следующей 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 можно воспользоваться командой:

```
$ openssl req -noout -text -in request.csr
```

2. На основании запроса и имеющегося сертификата СА создать подписанный сертификат. Создание подписанного сертификата производится следующей командой:

```
$ openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set_serial 01 -in request.csr -out sigcert.crt
```

Обратите внимание, что для создания подписанного сертификата нужно иметь три файла: файл корневого сертификата `ca.crt` и его закрытый ключ `ca.key`, а также файл запроса на подписание сертификата `request.csr`. Созданный подписанный сертификат будет сохранен в файл `sigcert.crt`.



Для проверки результата можно воспользоваться командой:

```
$ openssl x509 -noout -text -in sigcert.crt
```

Процедуру создания ключа и сертификата (или подписанного сертификата, в зависимости от необходимости) следует повторить столько раз, сколько уникальных сертификатов необходимо создать. 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.



## Приложение Е. Описание известных ошибок

В данном разделе представлены:

- Описание ошибок, [определяемых по коду ошибки](#).
- Описание ошибок, не имеющих кода, но [определяемых по симптомам их проявления](#).
- [Каталог](#), связывающий коды ошибок, сообщения об ошибке и их внутреннее обозначение.



Если описание возникшей у вас ошибки отсутствует в данном разделе, рекомендуется обратиться в [техническую поддержку](#), сообщив код ошибки и описав обстоятельства ее появления.

Для облегчения идентификации ошибки рекомендуется настроить вывод журнала в отдельный файл и разрешить вывод расширенной отладочной информации. Для этого выполните следующие [команды](#):

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

Для возврата настроек ведения журнала по умолчанию выполните следующие команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

### Ошибки, определяемые по коду

Если вместо текстового сообщения или числового кода ошибки вы получили внутренний код ошибки вида EC\_XXX (например, EC\_APP\_TERMINATED), то установить числовой код и описание ошибки, приведенное в данном разделе, вы можете, воспользовавшись таблицей внутреннего [каталога ошибок](#).

**Сообщение об ошибке:** Ошибка связи с монитором

**Код ошибки:** x1

**Описание:** Ошибка связи некоторого компонента с демоном управления конфигурацией [Dr.Web ConfigD](#).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Перезапустите демон управления конфигурацией, выполнив команду

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

2. Проверьте, что в системе установлен, настроен и корректно функционирует механизм аутентификации **PAM**. Если это не так, установите и настройте его (за подробностями обратитесь к руководствам по администрированию вашего дистрибутива ОС).
3. Если перезапуск демона управления конфигурацией при корректно настроенном **PAM** не помогает, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии [файла конфигурации](#)), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией.

4. Если демон управления конфигурацией запустить не удастся, попробуйте переустановить пакет `drweb-configd`.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Операция уже выполняется.*

**Код ошибки:** x2

**Описание:** Операция, запрошенная пользователем, в данный момент уже выполняется.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Подождите завершения выполняющейся операции и при необходимости повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Операция ожидает выполнения.*

**Код ошибки:** x3

**Описание:** Операция, запрошенная пользователем, в данный момент ожидает выполнения (возможно, производится установление сетевого соединения или осуществляется загрузка и инициализация какого-либо компонента программного комплекса, требующая продолжительного времени).





Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Подождите начала выполнения операции и при необходимости повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Прервано пользователем.*

**Код ошибки:** x4

**Описание:** Выполнявшееся действие было прервано пользователем (возможно, оно выполнялось слишком долго).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Операция отменена.*

**Код ошибки:** x5

**Описание:** Выполнявшееся действие было отменено (возможно, оно выполнялось слишком долго).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите требуемое действие снова.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Соединение IPC разорвано.*

**Код ошибки:** x6

**Описание:** IPC-соединение с некоторым компонентом программного комплекса разорвано (скорее всего, компонент завершил свою работу из-за простоя или вследствие команды пользователя).



Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Если выполнявшаяся операция не была завершена, то повторите ее запуск снова. В противном случае разрыв соединения не является ошибкой.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Недопустимый размер сообщения IPC.*

**Код ошибки:** x7

**Описание:** В процессе обмена данными между компонентами получено сообщение недопустимого размера.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Перезапустите программный комплекс, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Недопустимый формат сообщения IPC.*

**Код ошибки:** x8

**Описание:** В процессе обмена данными между компонентами получено сообщение недопустимого формата.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Перезапустите программный комплекс, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Не готов.*



**Код ошибки:** x9

**Описание:** Требуемое действие не может быть выполнено, потому что запрошенный компонент или устройство еще не инициализированы.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Компонент не установлен.*

**Код ошибки:** x10

**Описание:** Компонент, который необходим для выполнения некоторой функции, не установлен.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Установите или переустановите требуемый компонент. Если имя компонента неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Если установка или переустановка требуемого компонента не помогла, попробуйте переустановить весь программный комплекс целиком.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Неожиданное сообщение IPC.*

**Код ошибки:** x11

**Описание:** В процессе обмена данными между компонентами получено недопустимое сообщение.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Перезапустите программный комплекс, выполнив команду:

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



Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Нарушение протокола IPC.*

**Код ошибки:** x12

**Описание:** В процессе обмена данными между компонентами произошло нарушение протокола обмена данными.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Перезапустите программный комплекс, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Неизвестное состояние подсистемы.*

**Код ошибки:** x13

**Описание:** Обнаружено, что некоторая подсистема программного комплекса, требуемая для выполнения операции, находится в неизвестном состоянии.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите операцию.
2. При повторении ошибки перезапустите программный комплекс, выполнив команду:

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

после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Путь должен быть абсолютным.*

**Код ошибки:** x20

**Описание:** Требуется абсолютный (т.е. начинающийся от корня файловой системы) путь к файлу или каталогу, а указан относительный путь.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала



программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Измените путь к файлу или каталогу таким образом, чтобы он был абсолютным, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Недостаточно памяти для завершения операции.*

**Код ошибки:** `x21`

**Описание:** Для выполнения требуемой операции не хватает памяти (например, попытка распаковать слишком большой файл).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Попробуйте увеличить объем памяти, доступной процессам программного комплекса (например, изменив лимиты при помощи команды **ulimit**), перезапустить программный комплекс и повторить операцию.

Обратите внимание, что 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** вы можете ознакомиться в документации **man systemd.exec**.

Для перезапуска Dr.Web для Интернет-шлюзов UNIX выполните команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Ошибка ввода-вывода.*

**Код ошибки:** `x22`

**Описание:** Произошла ошибка ввода/вывода (например, дисковое устройство еще не инициализировано или раздел файловой системы более недоступен).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog`



или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте доступность требуемого устройства ввода/вывода или раздела файловой системы. При необходимости выполните его монтирование и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Нет такого файла или каталога.*

**Код ошибки:** `x23`

**Описание:** Указанный объект файловой системы (файл или каталог) отсутствует, возможно, он был удален.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного пути. При необходимости исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Доступ запрещён.*

**Код ошибки:** `x24`

**Описание:** Недостаточно прав для доступа к указанному объекту файловой системы (файлу или каталогу).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного пути и наличие необходимых прав у компонента. При необходимости доступа к объекту, измените права доступа к нему или повысьте права компонента и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Не каталог.*

**Код ошибки:** `x25`

**Описание:** Ожидался путь к каталогу, однако указанный объект файловой системы не является каталогом.



Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Файл данных повреждён.*

**Код ошибки:** `x26`

**Описание:** Данные, к которым производится обращение, повреждены.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите операцию.
2. При повторении ошибки перезапустите программный комплекс, выполнив команду

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

после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Файл уже существует.*

**Код ошибки:** `x27`

**Описание:** При попытке создать файл было обнаружено, что файл с таким именем уже существует.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Файловая система только для чтения.*

**Код ошибки:** `x28`



**Описание:** При попытке создать или изменить объект файловой системы (каталог, файл или сокет) было обнаружено, что файловая система доступна только для чтения.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного пути. Исправьте путь так, чтобы он вел на раздел файловой системы, доступный для записи, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Ошибка сети.*

**Код ошибки:** `x29`

**Описание:** Произошла сетевая ошибка (возможно, внезапно перестал отвечать удаленный узел или не удастся установить требуемое соединение).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Не дисковое устройство.*

**Код ошибки:** `x30`

**Описание:** Производится попытка обращения к устройству ввода/вывода, которое не является дисковым устройством.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного имени устройства. Исправьте путь так, чтобы он вел к дисковому устройству, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Неожиданный конец файла.*





**Код ошибки:** x31

**Описание:** При чтении данных неожиданно был достигнут конец файла.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к правильному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Файл был изменён.*

**Код ошибки:** x32

**Описание:** При сканировании файла было обнаружено, что он был изменен.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите операцию сканирования.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Специальный файл.*

**Код ошибки:** x33

**Описание:** При доступе к объекту файловой системы было обнаружено, что это не регулярный файл (т.е. это каталог, сокет или иной объект файловой системы).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к регулярному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Имя уже используется.*

**Код ошибки:** x34



**Описание:** При попытке создать объект файловой системы (каталог, файл или сокет) было обнаружено, что объект с таким именем уже существует.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Хост отключен.*

**Код ошибки:** x35

**Описание:** Обнаружено, что удаленный узел недоступен по сети.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте доступность требуемого узла сети. При необходимости исправьте адрес узла сети и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Достигнут предел использования ресурса.*

**Код ошибки:** x36

**Описание:** Достигнут предел использования некоторого ресурса.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте доступность требуемого ресурса. При необходимости увеличьте лимит на использование ресурса и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Различные точки монтирования.*

**Код ошибки:** x37

**Описание:** Производится попытка выполнить восстановление файла, требующая его



перемещение между каталогами файловой системы, принадлежащим различным точкам монтирования.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Выберите другой путь для восстановления файла и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Ошибка распаковки.

**Код ошибки:** x38

**Описание:** Не удалось распаковать архив (возможно, он защищен паролем или поврежден).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Убедитесь что файл не поврежден. Если архив защищен паролем, снимите защиту, указав правильный пароль, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Вирусная база повреждена.

**Код ошибки:** x40

**Описание:** Обнаружено, что повреждены вирусные базы.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в [секции](#) [Root] [файла конфигурации](#)).

Для просмотра и исправления пути перейдите на страницу **Общих настроек веб-интерфейса** управления (если он установлен).

Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```



Для установки нового значения параметра введите команду:

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

Для сброса значения параметра в значение по умолчанию введите команду:

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

2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Не поддерживаемая версия вирусных баз.*

**Код ошибки:** x41

**Описание:** Обнаружено, имеющиеся вирусные базы предназначены для старой версии программы.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в [секции](#) [Root] [файла конфигурации](#)).

Для просмотра и исправления пути перейдите на страницу **Общих настроек** [веб-интерфейса](#) управления (если он установлен).

Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

Для установки нового значения параметра введите команду:

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

Для сброса значения параметра в значение по умолчанию введите команду:

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

2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.



- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Вирусная база пуста.

**Код ошибки:** x42

**Описание:** Обнаружено, что вирусные базы пусты.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в [секции](#) [Root] [файла конфигурации](#)).

- Для просмотра и исправления пути перейдите на страницу **Общих настроек веб-интерфейса** управления (если он установлен).
- Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

Для установки нового значения параметра введите команду:

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

Для сброса значения параметра в значение по умолчанию введите команду:

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

2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Объект не может быть вылечен.

**Код ошибки:** x43

**Описание:** Попытка применить действие «Лечить» к неизлечимому объекту при нейтрализации



угрозы.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Выберите действие, допустимое для данного объекта и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Не поддерживаемая комбинация вирусных баз.*

**Код ошибки:** `x44`

**Описание:** Обнаружено, что имеющийся набор вирусных баз несовместим.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в [секции](#) `[Root]` [файла конфигурации](#)).
  - Для просмотра и исправления пути перейдите на страницу **Общих настроек веб-интерфейса** управления (если он установлен).
  - Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

Для установки нового значения параметра введите команду:

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

Для сброса значения параметра в значение по умолчанию введите команду:

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

2. Обновите вирусные базы:
  - Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
  - Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.



**Сообщение об ошибке:** *Достигнут предел проверки.*

**Код ошибки:** x45

**Описание:** При сканировании объекта превышены заданные ограничения (например, на величину распакованного файла, на глубину уровней вложенности и т.п.).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Измените ограничения для сканирования объектов (в настройках соответствующего компонента) любым удобным вам способом:
  - Используя страницу настроек этого компонента в [веб-интерфейсе](#) управления (если он установлен).
  - При помощи [команд](#) `drweb-ctl cfshow` и `drweb-ctl cfset`.
2. После изменения настроек повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Неверные учетные данные пользователя.*

**Код ошибки:** x47

**Описание:** Попытка пройти аутентификацию с неверными учетными данными пользователя.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Пользователь не имеет требуемых прав.*

**Код ошибки:** x48

**Описание:** Попытка пройти авторизацию с учетными данными пользователя, не имеющего требуемых прав.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимый токен доступа.

**Код ошибки:** x49

**Описание:** Компонент программного комплекса предъявил некорректный токен авторизации при попытке получения доступа к операции, требующей повышенные права.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Пройдите аутентификацию, указав правильные учетные данные пользователя, имеющего необходимые полномочия, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимый аргумент.

**Код ошибки:** x60

**Описание:** При попытке исполнить некоторую команду был указан недопустимый аргумент.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повторите требуемое действие снова, указав допустимый аргумент.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимая операция.

**Код ошибки:** x61

**Описание:** Совершена попытка выполнить недопустимую команду.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).



**Устранение ошибки:**

1. Повторите требуемое действие снова, указав допустимую команду.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Требуются полномочия суперпользователя.*

**Код ошибки:** x62

**Описание:** Требуемое действие может быть выполнено только пользователем, обладающим полномочиями суперпользователя.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Повысьте свои права до суперпользователя и повторите требуемое действие снова. Для повышения прав вы можете воспользоваться командами **su** и **sudo**.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Не разрешено в режиме централизованной защиты.*

**Код ошибки:** x63

**Описание:** Требуемое действие может быть выполнено только при работе программного комплекса в одиночном (standalone) [режиме](#).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Переведите программный комплекс в одиночный режим и повторите операцию снова.
2. Для перевода программного комплекса в одиночный режим:
  - Сбросьте флажок **Включить режим централизованной защиты** на странице настроек **Централизованная защита веб-интерфейса** управления, если он установлен.
  - Или выполните [команду](#):

```
# drweb-ctl esdisconnect
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.



**Сообщение об ошибке:** *Не поддерживаемая ОС.*

**Код ошибки:** x64

**Описание:** Операционная система, установленная на узле, не поддерживается программным комплексом.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Установите операционную систему из списка, указанного в [системных требованиях](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Функция не реализована.*

**Код ошибки:** x65

**Описание:** Производятся попытки использования функций некоторого компонента, которые не реализованы в текущей версии.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Попробуйте сбросить настройки программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии [файла конфигурации](#)), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите программный комплекс, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Неизвестный параметр.*

**Код ошибки:** x66

**Описание:** [Файл конфигурации](#) содержит параметры, неизвестные или не поддерживаемые в текущей версии программного комплекса.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала



программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Откройте файл `<etc_dir>/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 программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

#### Сообщение об ошибке: *Неизвестная секция.*

**Код ошибки:** `x67`

**Описание:** [Файл конфигурации](#) содержит секции, неизвестные или не поддерживаемые в текущей версии программного комплекса.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Откройте файл `<etc_dir>/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 программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией.



Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимое значение параметра.

**Код ошибки:** x68

**Описание:** Некоторый параметр в [файле конфигурации](#) имеет недопустимое для этого параметра значение.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Измените значение параметра любым удобным для вас способом:

- Используя страницу настроек этого компонента в [веб-интерфейсе](#) управления (если он установлен).
- При помощи [команд](#) `drweb-ctl cfshow` и `drweb-ctl cfset`.

Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту, использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.

2. Также вы можете отредактировать непосредственно файл конфигурации `<etc_dir>/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 программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимое состояние.

**Код ошибки:** x69

**Описание:** Некоторый компонент или весь программный комплекс находятся в недопустимом состоянии для выполнения запрошенной операции.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog`



или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Повторите требуемое действие через некоторое время.
2. При повторении ошибки перезапустите программный комплекс, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Разрешено только одно значение.*

**Код ошибки:** `x70`

**Описание:** Некоторый параметр в [файле конфигурации](#) имеет список значений, что недопустимо для этого параметра.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Измените значение параметра любым удобным для вас способом:
  - Используя страницу настроек этого компонента в [веб-интерфейсе](#) управления (если он установлен).
  - При помощи [команд](#) `drweb-ctl cfshow` и `drweb-ctl cfset`.

Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту, использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.

2. Также вы можете отредактировать непосредственно файл конфигурации `<etc_dir>/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 программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимое имя тега.**Код ошибки:** x71

**Описание:** Некоторая секция в [файле конфигурации](#), в имя которой включен уникальный идентификатор-тег, имеет недопустимое значение тега.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Если ошибка произошла при попытке создания секции в [веб-интерфейсе](#) управления или при использовании [команды](#)

```
# drweb-ctl cfset <секция>.<параметр> <новое значение>
```

то повторите сохранение, задав для тега допустимое значение.

2. Если секция сохранена непосредственно в файл конфигурации `<etc_dir>/drweb.ini`, то отредактируйте его. Для этого откройте его в любом текстовом редакторе, найдите заголовок секции, содержащий недопустимое значение тега, задайте для тега допустимое значение, сохраните файл и перезапустите демон управления конфигурацией [Dr.Web ConfigD](#), выполнив команду:

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

3. Если вышеприведенные шаги не помогут, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Запись не найдена.**Код ошибки:** x80

**Описание:** При попытке обратиться к информации о найденной угрозе было обнаружено, что информация о ней отсутствует (возможно, угроза уже была обработана другим компонентом программного комплекса).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Запись обрабатывается в данный момент.*

**Код ошибки:** x81

**Описание:** При попытке обратиться к информации о найденной угрозе было обнаружено, что в данный момент времени она уже обрабатывается другим компонентом программного комплекса.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Файл уже находится в карантине.*

**Код ошибки:** x82

**Описание:** При попытке перемещения файла с найденной угрозой в карантин было обнаружено, что он уже в карантине (скорее всего, угроза уже была обработана другим компонентом программного комплекса).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Не удалось сохранить резервную копию перед обновлением.*

**Код ошибки:** x89

**Описание:** Перед началом загрузки обновлений с сервера обновлений не удалось выполнить сохранение резервной копии обновляемых файлов.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**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 перейдите на страницу настроек **Updater** [веб-интерфейса](#) управления (если он установлен).
- Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Update.BackupDir
```

Для установки нового значения параметра введите команду:

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

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Update.BackupDir -r
```

2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или 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, попробуйте переустановить пакет drweb-update.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимый DRL-файл.

**Код ошибки:** x90

**Описание:** Обнаружено, что нарушена структура одного из файлов списков серверов обновлений.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).



**Устранение ошибки:**

1. Проверьте правильность пути к файлу списка серверов и при необходимости исправьте его (параметры с именем вида **\*DrlPath** в [секции](#) [Update] [файла конфигурации](#)).

- Для просмотра и исправления пути перейдите на страницу настроек **Updater** [веб-интерфейса](#) управления (если он установлен).
- Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду (<**\*DrlPath**> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значение всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

```
$ drweb-ctl cfshow Update[.<*DrlPath>]
```

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

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

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

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

2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

3. Если ошибка повторяется, попробуйте переустановить пакет drweb-update.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимый LST-файл.

**Код ошибки:** x91

**Описание:** Обнаружено, что нарушена структура файла, содержащего перечень обновляемых вирусных баз.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Обновите вирусные базы повторно через некоторое время:



- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

2. Если ошибка повторяется, попробуйте переустановить пакет drweb-update.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Недопустимый сжатый файл.*

**Код ошибки:** x92

**Описание:** Обнаружено, что нарушена структура загруженного файла, содержащего обновления.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Обновите вирусные базы повторно через некоторое время:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Ошибка аутентификации на прокси-сервере.*

**Код ошибки:** x93

**Описание:** Не удалось подключиться к серверам обновлений через прокси-сервер, заданный в настройках.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность параметров подключения к прокси-серверу (задаются в параметре с именем **Proxy** в [секции](#) [Update] [файла конфигурации](#)).
  - Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** [веб-интерфейса](#) управления (если он установлен).



- Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Update.Proxy
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Update.Proxy <новые параметры>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Update.Proxy -r
```

## 2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Нет доступных серверов обновлений.*

**Код ошибки:** x94

**Описание:** Не удалось подключиться ни к одному из серверов обновлений.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

### 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](#)).
  - Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** [веб-интерфейса](#) управления (если он установлен).
  - Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Update.Proxy
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Update.Proxy <новые параметры>
```

Для сброса значения параметра в значение по умолчанию введите команду:



```
# drweb-ctl cfset Update.Proxy -r
```

3. Если параметры сетевого подключения (в том числе – используемого прокси-сервера) правильные, а ошибка происходит, убедитесь в том, что вы используете доступный список серверов обновления. Перечень используемых серверов обновления указывается в параметрах вида **\*DrlPath** в секции [Update] файла конфигурации. Обратите внимание, что если параметры вида **\*CustomDrlPath** указывают на существующий корректный файл списка серверов, то указанные там серверы будут использоваться вместо серверов стандартной зоны обновления (значение, указанное в соответствующем параметре **\*DrlPath**, игнорируется).

- Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater веб-интерфейса** управления (если он установлен).
- Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду (<*\*DrlPath*> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значение всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

```
$ drweb-ctl cfshow Update[.<*DrlPath>]
```

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

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

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

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

4. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимый формат ключевого файла.

**Код ошибки:** x95

**Описание:** Нарушен формат ключевого файла.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте наличие ключевого файла и правильности пути к нему. Путь к ключевому файлу задается в параметре **KeyPath** в [секции](#) [Root] [файла конфигурации](#).
  - Для просмотра и задания пути к ключевому файлу перейдите на страницу **Общих настроек веб-интерфейса** управления (если он установлен).
  - Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.KeyPath
```

Для установки нового значения параметра введите команду:

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

Для сброса значения параметра в значение по умолчанию введите команду:

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

2. Если у вас отсутствует ключевой файл, или используемый ключевой файл поврежден, приобретите и установите его. Описание ключевого файла, способы приобретения и установки описаны в разделе [Лицензирование](#).
3. Для установки имеющегося у вас ключевого файла вы можете воспользоваться также формой активации лицензии, расположенной в нижней части **Главной** страницы [веб-интерфейса](#) управления (если он установлен).
4. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке <https://support.drweb.com/get+cabinet+link/>.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Срок действия лицензии истек.*

**Код ошибки:** x96

**Описание:** Срок действия имеющейся у вас лицензии истёк.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе [Лицензирование](#).
2. Для установки приобретенного ключевого файла вы можете воспользоваться также формой активации лицензии, расположенной в нижней части **Главной** страницы [веб-интерфейса](#) управления (если он установлен).
3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке <https://support.drweb.com/get+cabinet+link/>.



Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Истек тайм-аут сетевой операции.*

**Код ошибки:** x97

**Описание:** Истекло время на ожидание завершения сетевой операции (возможно, внезапно перестал отвечать удаленный узел или не удается установить требуемое соединение).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Недопустимая контрольная сумма.*

**Код ошибки:** x98

**Описание:** Обнаружено, что нарушена контрольная сумма загруженного файла, содержащего обновления.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Обновите вирусные базы повторно через некоторое время:
  - Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
  - Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Недопустимый демонстрационный ключевой файл.*

**Код ошибки:** x99

**Описание:** Используемый демонстрационный ключевой файл недействителен (например, он был получен для другого компьютера).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала



программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Запросите новый демонстрационный период для данного компьютера, или приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе [Лицензирование](#).
2. Для установки приобретенного ключевого файла вы можете воспользоваться также формой активации лицензии, расположенной в нижней части **Главной** страницы [веб-интерфейса](#) управления (если он установлен).
3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке <https://support.drweb.com/get+cabinet+link/>.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Лицензионный ключевой файл заблокирован.*

**Код ошибки:** x100

**Описание:** Используемая вами лицензия была заблокирована (возможно, нарушены условия лицензионного соглашения на использование программного продукта Dr.Web).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе [Лицензирование](#).
2. Для установки приобретенного ключевого файла вы можете воспользоваться формой активации лицензии, расположенной в нижней части **Главной** страницы [веб-интерфейса](#) управления (если он установлен).
3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке <https://support.drweb.com/get+cabinet+link/>.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Недопустимая лицензия.*

**Код ошибки:** x101

**Описание:** Используемая вами лицензия предназначена для другого программного продукта или не содержит необходимых разрешений для работы компонентов установленного у вас продукта.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе [Лицензирование](#).
2. Для установки приобретенного ключевого файла вы можете воспользоваться формой активации лицензии, расположенной в нижней части **Главной** страницы [веб-интерфейса](#) управления (если он установлен).
3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке <https://support.drweb.com/get+cabinet+link/>.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Недопустимая конфигурация.

**Код ошибки:** x102

**Описание:** Некоторый компонент программного комплекса не может функционировать из-за неправильных настроек конфигурации.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Если имя компонента, вызвавшего ошибку, неизвестно, попробуйте его определить, ознакомившись с содержимым журнала.
2. Если ошибка вызвана компонентом Dr.Web Firewall для Linux, то скорее 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 программный комплекс, выполнив команду

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

или

```
# drweb-ctl reload
```



Обратите внимание, что 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).

3. Если ошибка вызвана другим компонентом, то попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:





- Используя страницу настроек этого компонента в [веб-интерфейсе](#) управления (если он установлен).
- При помощи [команд](#) **drweb-ctl** cfshow и **drweb-ctl** cfset.
- Отредактировав вручную [файл конфигурации](#) (удалив все параметры из секции компонента).

4. Если предыдущие шаги не помогли, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите программный комплекс, выполнив команду

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

#### Сообщение об ошибке: Недопустимый исполняемый файл.

**Код ошибки:** x104

**Описание:** Не запускается некоторый компонент программного комплекса, потому что неправильно указан путь к его исполняемому файлу или содержимое файла испорчено.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Проверьте значение пути к исполняемому файлу компонента в конфигурации программного комплекса (параметр **ExePath** в секции компонента), выполнив [команду](#) (замените *<секция компонента>* на название соответствующей секции [файла конфигурации](#))

```
$ drweb-ctl cfshow <секция компонента>.ExePath
```

3. Попробуйте сбросить путь в значение по умолчанию, выполнив команду (замените *<секция компонента>* на название соответствующей секции файла конфигурации)

```
# drweb-ctl cfset <секция компонента>.ExePath -r
```

4. Если предыдущие шаги не помогли, попробуйте переустановить пакет соответствующего компонента.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).



Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Ядро Virus-Finding Engine недоступно.

**Код ошибки:** x105

**Описание:** Отсутствует или недоступен файл антивирусного ядра Dr.Web Virus-Finding Engine (требуется для поиска угроз).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к файлу антивирусного ядра **drweb32.dll** и при необходимости исправьте его (параметр **CoreEnginePath** в [секции](#) [Root] [файла конфигурации](#)).

- Для просмотра и исправления пути перейдите на страницу **Общих настроек веб-интерфейса** управления (если он установлен).
- Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду

```
$ drweb-ctl cfshow Root.CoreEnginePath
```

Для установки нового значения параметра введите команду

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

Для сброса значения параметра в значение по умолчанию введите команду

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

2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или 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 продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Вирусные базы отсутствуют.

**Код ошибки:** x106



**Описание:** Обнаружено, что вирусные базы отсутствуют.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр **VirusBaseDir** в [секции](#) [Root] [файла конфигурации](#)).

- Для просмотра и исправления пути перейдите на страницу **Общих настроек веб-интерфейса** управления (если он установлен).
- Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

Для установки нового значения параметра введите команду

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

Для сброса значения параметра в значение по умолчанию введите команду

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

2. Обновите вирусные базы:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Процесс завершен по сигналу.*

**Код ошибки:** x107

**Описание:** Компонент завершил свою работу (возможно, из-за простоя или вследствие команды пользователя).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**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:

- Используя страницу настроек этого компонента в [веб-интерфейсе](#) управления (если он установлен).
- При помощи [команд](#) **drweb-ctl** cfshow и **drweb-ctl** cfset.
- Отредактировав вручную [файл конфигурации](#) (удалив все параметры из секции компонента).

3. Если это не помогло, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите программный комплекс, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

#### Сообщение об ошибке: Непредвиденное завершение процесса.

**Код ошибки:** x108

**Описание:** Компонент неожиданно завершил свою работу вследствие сбоя.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Попробуйте повторить выполнявшуюся операцию.
2. Если компонент постоянно аварийно завершает свою работу, попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:
  - Используя страницу настроек этого компонента в [веб-интерфейсе](#) управления (если он установлен).
  - При помощи [команд](#) **drweb-ctl** cfshow и **drweb-ctl** cfset.
  - Отредактировав вручную [файл конфигурации](#) (удалив все параметры из секции компонента).
3. Если это не помогло, попробуйте сбросить настройки программного комплекса в значения по умолчанию.

Для этого очистите содержимое файла `<etc_dir>/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```



После очистки файла конфигурации перезапустите программный комплекс, выполнив команду:

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

4. Если ошибка повторяется после сброса настроек программного комплекса, попробуйте переустановить пакет компонента.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** Обнаружено несовместимое ПО.

**Код ошибки:** x109

**Описание:** Компонент программного комплекса не может функционировать, поскольку обнаружено программное обеспечение, препятствующее его корректной работе.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Если ошибка вызвана компонентом SpIDer Gate, то скорее всего проблема в том, что в системе присутствует программное обеспечение, формирующее для системного брандмауэра **NetFilter** правила, препятствующие корректной работе SpIDer Gate. Например, это может быть **Shorewall** или **SuseFirewall2** (в ОС **SUSE Linux**). Основная причина конфликта SpIDer Gate с другими приложениями, настраивающими системный брандмауэр **NetFilter**, в том, что они периодически выполняют проверку целостности заданной ими системы правил и перезаписывают ее.

Настройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе SpIDer Gate. Если не удастся настроить конфликтующее приложение таким образом, чтобы оно не мешало работе SpIDer Gate, отключите это приложение с запретом его запуска при последующих загрузках ОС. Приложение **SuseFirewall2** (в ОС **SUSE Linux**) можно попытаться настроить следующим образом:

- 1) Откройте файл конфигурации **SuseFirewall2** (по умолчанию это файл `/etc/sysconfig/SuSEfirewall2`).
- 2) Найдите в файле блок текста:

```
## Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

- 3) Установите значение параметра в "no":



```
FW_LO_NOTRACK="no"
```

4) Перезапустите **SuseFirewall2**. Для этого используйте следующую команду:

```
# rcSuSEfirewall12 restart
```



Если в настройках **SuseFirewall2** параметр `FW_LO_NOTRACK` отсутствует, то для устранения конфликта необходимо отключить приложение с запретом его запуска при последующих загрузках ОС (например, это необходимо сделать в ОС **SUSE Linux Enterprise Server 11**).

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 для Интернет-шлюзов UNIX.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

#### Сообщение об ошибке: Базы категорий веб-ресурсов отсутствуют

**Код ошибки:** x112

**Описание:** Обнаружено, что базы категорий веб-ресурсов отсутствуют.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Проверьте правильность пути к каталогу базы данных категорий веб-ресурсов и при необходимости исправьте его (параметр **DwsDir** в [секции](#) [Root] [файла конфигурации](#)).
  - Для просмотра и исправления пути перейдите на страницу **Общих настроек веб-интерфейса** управления (если он установлен).
  - Также вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду

```
$ drweb-ctl cfshow Root.DwsDir
```

Для установки нового значения параметра введите команду

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

Для сброса значения параметра в значение по умолчанию введите команду



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

2. Обновите базы категорий веб-ресурсов:

- Нажмите кнопку **Обновить** на **Главной** странице [веб-интерфейса](#) управления, если он установлен.
- Или выполните [команду](#):

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Компонент LookupD недоступен.*

**Код ошибки:** x115

**Описание:** Отсутствует компонент Dr.Web LookupD (требуется для выбора данных из внешних источников)

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к исполняемому файлу **drweb-lookupd** и при необходимости исправьте его (параметр **ExePath** в [секции](#) [LookupD] [файла конфигурации](#)).

Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow LookupD.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset LookupD.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset LookupD.ExePath -r
```

2. При отсутствии настроек компонента Dr.Web LookupD в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-lookupd`.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.



**Сообщение об ошибке:** *SpIDer Gate недоступен.*

**Код ошибки:** x117

**Описание:** Отсутствует компонент SpIDer Gate (требуется для проверки сетевых соединений).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к исполняемому файлу **drweb-gated** и при необходимости исправьте его (параметр **ExePath** в [секции](#) [GateD] [файла конфигурации](#)).

Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow GateD.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset GateD.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset GateD.ExePath -r
```

2. При отсутствии настроек компонента SpIDer Gate в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-gated`.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Scanning Engine недоступен.*

**Код ошибки:** x119

**Описание:** Отсутствует (или не может быть запущен) компонент Dr.Web Scanning Engine (требуется для поиска угроз).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к исполняемому файлу **drweb-se** и при необходимости исправьте его (параметр **ExePath** в [секции](#) [ScanEngine] [файла конфигурации](#)).

Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:





```
$ drweb-ctl cfshow ScanEngine.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset ScanEngine.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset ScanEngine.ExePath -r
```

2. В случае возникновения ошибки при указании правильного пути:

- Выполните команду

```
$ drweb-ctl rawscan /
```

если в выводе на экран присутствует строка `Error: No valid license provided`, то это означает, что отсутствует действующий ключевой файл. Зарегистрируйте продукт и получите лицензию. Если лицензия вами получена, то проверьте наличие [ключевого файла](#) и установите его при необходимости.

- Если вы используете 64-битную версию ОС, убедитесь, что у вас установлены библиотеки поддержки 32-битных приложений (см. раздел [Системные требования](#)), и установите их в случае необходимости. После установки библиотеки поддержки 32-битных приложений перезапустите Dr.Web для Интернет-шлюзов UNIX, выполнив команду

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

- Если ваша ОС использует подсистему безопасности **SELinux**, настройте политику безопасности для модуля **drweb-se** (см. раздел [Настройка политик безопасности SELinux](#)).

3. При отсутствии настроек компонента Dr.Web Scanning Engine в конфигурации, или в случае если предыдущие шаги не помогли, установите или переустановите пакет **drweb-se**.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *File Checker недоступен.*

**Код ошибки:** x120

**Описание:** Отсутствует (или не может быть запущен) компонент Dr.Web File Checker (требуется для поиска угроз).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к исполняемому файлу **drweb-filecheck** и при необходимости исправьте его (параметр **ExePath** в [секции](#) [FileCheck] [файла конфигурации](#)).



Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow FileCheck.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset FileCheck.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset FileCheck.ExePath -r
```

2. В случае возникновения ошибки при указании правильного пути:

- Если вы используете 64-битную версию ОС, убедитесь, что у вас установлены библиотеки поддержки 32-битных приложений (см. раздел [Системные требования](#)), и установите их в случае необходимости. После установки библиотеки поддержки 32-битных приложений перезапустите Dr.Web для Интернет-шлюзов UNIX, выполнив команду:

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

- Если ваша ОС использует подсистему безопасности **SELinux**, настройте политику безопасности для модуля **drweb-filecheck** (см. раздел [Настройка политик безопасности SELinux](#)).

3. При отсутствии настроек компонента Dr.Web File Checker в конфигурации, или в случае если предыдущие шаги не помогли, установите или переустановите пакет **drweb-filecheck**.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *ES Agent недоступен.*

**Код ошибки:** x121

**Описание:** Отсутствует компонент Dr.Web ES Agent (требуется для подключения к серверу централизованной защиты).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к исполняемому файлу **drweb-esagent** и при необходимости исправьте его (параметр **ExePath** в [секции](#) [ESAgent] [файла конфигурации](#)).

Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:



```
$ drweb-ctl cfshow ESAgent.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset ESAgent.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset ESAgent.ExePath -r
```

2. При отсутствии настроек компонента 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 продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Компонент Firewall для Linux недоступен.*

**Код ошибки:** `x122`

**Описание:** Отсутствует компонент Dr.Web Firewall для Linux (требуется для проверки сетевых соединений).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к исполняемому файлу **drweb-firewall** и при необходимости исправьте его (параметр **ExePath** в [секции](#) `[LinuxFirewall]` [файла конфигурации](#)).

Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow LinuxFirewall.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset LinuxFirewall.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset LinuxFirewall.ExePath -r
```

2. При отсутствии настроек компонента Dr.Web Firewall для Linux в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-firewall`.



Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Network Checker недоступен.*

**Код ошибки:** x123

**Описание:** Отсутствует компонент Dr.Web Network Checker (требуется для проверки файлов по сети).

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

**Устранение ошибки:**

1. Проверьте правильность пути к исполняемому файлу **drweb-netcheck** и при необходимости исправьте его (параметр **ExePath** в [секции](#) [Netcheck] [файла конфигурации](#)).

Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Netcheck.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Netcheck.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Netcheck.ExePath -r
```

2. При отсутствии настроек компонента 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 продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

**Сообщение об ошибке:** *Компонент CloudD недоступен.*

**Код ошибки:** x124

**Описание:** Отсутствует компонент Dr.Web CloudD (требуется для обращения к облаку Dr.Web Cloud).



Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Проверьте правильность пути к исполняемому файлу **drweb-cloudd** и при необходимости исправьте его (параметр **ExePath** в [секции](#) [CloudD] [файла конфигурации](#)).

Вы можете воспользоваться [командами](#) утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow CloudD.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset CloudD.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset CloudD.ExePath -r
```

2. При отсутствии настроек компонента 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 продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.

#### Сообщение об ошибке: Непредвиденная ошибка.

**Код ошибки:** x125

**Описание:** Возникла непредвиденная ошибка в работе некоторого компонента.

Для уточнения места и причины возникновения ошибки ознакомьтесь с содержимым журнала программного комплекса (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС).

#### Устранение ошибки:

1. Попробуйте перезапустить программный комплекс, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#), сообщив код ошибки.



## Ошибки, не имеющие кодов

<b>Симптомы:</b>	Dr.Web MailD, SpiDer Gate, Dr.Web ICAPD (перечень указанных компонентов зависит от установленного продукта) не проверяют сообщения, в журнале Dr.Web для Интернет-шлюзов UNIX наблюдаются сообщения Too many open files.
<b>Описание:</b>	В связи большой загрузкой по проверке данных компонент Dr.Web Network Checker исчерпал доступный лимит на число доступных файловых дескрипторов.
<b>Устранение ошибки:</b>	
<p>1. Увеличьте лимит на число открытых файловых дескрипторов, доступных приложению, используя команду <b>ulimit -n</b> (по умолчанию лимит на число дескрипторов для Dr.Web для Интернет-шлюзов UNIX составляет 16384).</p> <p>Обратите внимание, что в некоторых случаях системный сервис <b>systemd</b> может игнорировать заданные изменения лимита. В этом случае отредактируйте (или создайте, при его отсутствии) файл <code>/etc/systemd/system/drweb-configd.service.d/limits.conf</code>, указав в нем измененное значение лимита:</p> <pre>[Service] LimitNOFILE=16384</pre> <p>С перечнем доступных лимитов <b>systemd</b> вы можете ознакомиться в документации <b>man systemd.exec</b>.</p>	
<p>2. После изменения лимита перезапустите Dr.Web для Интернет-шлюзов UNIX, выполнив команду</p> <pre># service drweb-configd restart</pre>	
Если устранить ошибку не удастся, обратитесь в <a href="#">техническую поддержку</a> .	

<b>Симптомы:</b>	<p>Не удается установить соединение с веб-интерфейсом управления Dr.Web в браузере, компоненты Dr.Web отсутствуют в перечне запущенных процессов (<b>ps ax   grep drweb</b>), выполнение любой команды <b>drweb-ctl &lt;команда&gt;</b>, за исключением команды <b>drweb-ctl rawscan</b>, выводит сообщение об ошибке</p> <pre>Error: connect: No such file or directory: "&lt;нуть&gt;/ .com.drweb.public"</pre> <p>или</p> <pre>Error: connect: Connection refused: "&lt;нуть&gt;/ .com.drweb.public".</pre>
<b>Описание:</b>	Dr.Web для Интернет-шлюзов UNIX 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 для Интернет-шлюзов UNIX в целом.

2. Если эта команда вернет ошибку или не даст никакого эффекта, выполните отдельную установку пакета `drweb-configd`.

Обратите внимание, что 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 продукта невозможна.

3. Если и после этого ошибка повторится, удалите продукт Dr.Web для Интернет-шлюзов UNIX целиком, после чего установите его повторно.

Инструкции по установке и удалению продукта и его компонентов см. в разделах [Установка продукта](#) и [Удаление продукта](#).

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#).

**Симптомы:**

1. После отключения SpIDer Gate перестают работать сетевые соединения (как исходящие, так, возможно, и входящие – по протоколам SSH, FTP);
2. Поиск в правилах **NetFilter (iptables)** с использованием команды

```
# iptables-save | grep "comment --comment --comment"
```

выдает непустой результат.

**Описание:**

Данная ошибка связана с некорректной работой **NetFilter (iptables)** версии младше 1.4.15, заключающейся в том, что правила с уникальной меткой (комментарием) добавляются некорректно, вследствие чего SpIDer Gate при завершении своей работы не может удалить добавленные им правила перенаправления сетевых соединений.

**Устранение ошибки:**

1. Повторно включите SpIDer Gate, чтобы он выполнял проверку.
2. Если SpIDer Gate требуется оставить выключенным, удалите некорректные правила **NetFilter (iptables)**, выполнив команду:

```
# iptables-save | grep -v "comment --comment --comment" | iptables-restore
```

Обратите внимание, что вызов команд **iptables-save** и **iptables-restore** требует наличия прав суперпользователя. Для получения прав суперпользователя вы можете воспользоваться командами **su** и **sudo**. Также обратите внимание, что указанная команда удалит из перечня правил все правила с некорректно добавленным комментарием, например, добавленные другими приложениями, выполняющими корректировку маршрутизации соединений.

**Дополнительная информация:**

- Для предотвращения возникновения данной ошибки в дальнейшем рекомендуется обновить операционную систему (или, как минимум, **NetFilter** до версии 1.4.15 или новее).
- Кроме этого вы можете включить ручной режим перенаправления соединений для SpIDer Gate, задавая требуемые правила вручную при помощи утилиты **iptables** (не рекомендуется).
- Дополнительные сведения см. в справке **man: drweb-firewall(1), drweb-gated(1), iptables(8)**.

Если устранить ошибку не удастся, обратитесь в [техническую поддержку](#).

## Внутренний каталог ошибок

Код ошибок	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
0	EC_OK	Success	Не является ошибкой
1	EC_MONITOR_IPC_ERROR	Error on monitor channel	<a href="#">Ошибка x1</a>
2	EC_ALREADY_IN_PROGRESS	Operation is already in progress	<a href="#">Ошибка x2</a>
3	EC_IN_PENDING_STATE	Operation is in pending state	<a href="#">Ошибка x3</a>
4	EC_INTERRUPTED_BY_USER	Interrupted by user	<a href="#">Ошибка x4</a>
5	EC_CANCELED	Operation canceled	<a href="#">Ошибка x5</a>
6	EC_LINK_DISCONNECTED	Link disconnected	<a href="#">Ошибка x6</a>
7	EC_BAD_MESSAGE_SIZE	Invalid IPC message size	<a href="#">Ошибка x7</a>
8	EC_BAD_MESSAGE_FORMAT	Invalid IPC message format	<a href="#">Ошибка x8</a>
9	EC_NOT_READY	Not ready	<a href="#">Ошибка x9</a>
10	EC_NOT_INSTALLED	Component is not installed	<a href="#">Ошибка x10</a>
11	EC_UNEXPECTED_MESSAGE	Unexpected IPC message	<a href="#">Ошибка x11</a>
12	EC_PROTOCOL_VIOLATION	Protocol violation	<a href="#">Ошибка x12</a>
13	EC_UNKNOWN_STATE	Subsystem state is unknown	<a href="#">Ошибка x13</a>
20	EC_NOT_ABSOLUTE_PATH	Path must be absolute	<a href="#">Ошибка x20</a>





Код ошибок	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
21	EC_NO_MEMORY	<i>Not enough memory</i>	<a href="#">Ошибка x21</a>
22	EC_IO_ERROR	<i>IO error</i>	<a href="#">Ошибка x22</a>
23	EC_NO_SUCH_ENTRY	<i>No such file or directory</i>	<a href="#">Ошибка x23</a>
24	EC_PERMISSION_DENIED	<i>Permission denied</i>	<a href="#">Ошибка x24</a>
25	EC_NOT_A_DIRECTORY	<i>Not a directory</i>	<a href="#">Ошибка x25</a>
26	EC_DATA_CORRUPTED	<i>Data file corrupted</i>	<a href="#">Ошибка x26</a>
27	EC_FILE_EXISTS	<i>File already exists</i>	<a href="#">Ошибка x27</a>
28	EC_READ_ONLY_FS	<i>Read-only file system</i>	<a href="#">Ошибка x28</a>
29	EC_NETWORK_ERROR	<i>Network error</i>	<a href="#">Ошибка x29</a>
30	EC_NOT_A_DRIVE	<i>Not a drive</i>	<a href="#">Ошибка x30</a>
31	EC_UNEXPECTED_EOF	<i>Unexpected EOF</i>	<a href="#">Ошибка x31</a>
32	EC_FILE_WAS_CHANGED	<i>File was changed</i>	<a href="#">Ошибка x32</a>
33	EC_NOT_A_REGULAR_FILE	<i>Not a regular file</i>	<a href="#">Ошибка x33</a>
34	EC_NAME_ALREADY_IN_USE	<i>Name already in use</i>	<a href="#">Ошибка x34</a>
35	EC_HOST_OFFLINE	<i>Host is offline</i>	<a href="#">Ошибка x35</a>
36	EC_LIMIT_REACHED	<i>Resource limit reached</i>	<a href="#">Ошибка x36</a>
37	EC_CROSS_DEVICE_LINK	<i>Mounting points are different</i>	<a href="#">Ошибка x37</a>
38	EC_UNPACKING_ERROR	<i>Unpacking error</i>	<a href="#">Ошибка x38</a>
40	EC_BASE_CORRUPTED	<i>Virus base corrupted</i>	<a href="#">Ошибка x40</a>
41	EC_OLD_BASE_VERSION	<i>Non-supported virus database version</i>	<a href="#">Ошибка x41</a>
42	EC_EMPTY_BASE	<i>Empty virus database</i>	<a href="#">Ошибка x42</a>
43	EC_CAN_NOT_BE_CURED	<i>Object cannot be cured</i>	<a href="#">Ошибка x43</a>
44	EC_INVALID_BASE_SET	<i>Non-supported virus database combination</i>	<a href="#">Ошибка x44</a>
45	EC_SCAN_LIMIT_REACHED	<i>Scan limit reached</i>	<a href="#">Ошибка x45</a>



Код ошибок	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
47	EC_AUTH_FAILED	Authentication failed	<a href="#">Ошибка x47</a>
48	EC_NOT_AUTHORIZED	Authorization failed	<a href="#">Ошибка x48</a>
49	EC_INVALID_TOKEN	Access token is invalid	<a href="#">Ошибка x49</a>
60	EC_INVALID_ARGUMENT	Invalid argument	<a href="#">Ошибка x60</a>
61	EC_INVALID_OPERATION	Invalid operation	<a href="#">Ошибка x61</a>
62	EC_ROOT_ONLY	Superuser privileges required	<a href="#">Ошибка x62</a>
63	EC_STANDALONE_MODE_ONLY	Not allowed in central protection mode	<a href="#">Ошибка x63</a>
64	EC_NON_SUPPORTED_OS	Non-supported OS	<a href="#">Ошибка x64</a>
65	EC_NOT_IMPLEMENTED	Feature not implemented	<a href="#">Ошибка x65</a>
66	EC_UNKNOWN_OPTION	Unknown option	<a href="#">Ошибка x66</a>
67	EC_UNKNOWN_SECTION	Unknown section	<a href="#">Ошибка x67</a>
68	EC_INVALID_OPTION_VALUE	Invalid option value	<a href="#">Ошибка x68</a>
69	EC_INVALID_STATE	Invalid state	<a href="#">Ошибка x69</a>
70	EC_NOT_LIST_OPTION	Only one value allowed	<a href="#">Ошибка x70</a>
71	EC_INVALID_TAG	Tag value is invalid	<a href="#">Ошибка x71</a>
80	EC_RECORD_NOT_FOUND	Record not found	<a href="#">Ошибка x80</a>
81	EC_RECORD_BUSY	Record is in process now	<a href="#">Ошибка x81</a>
82	EC_QUARANTINED_FILE	File has already been quarantined	<a href="#">Ошибка x82</a>
89	EC_BACKUP_FAILED	Cannot backup before update	<a href="#">Ошибка x89</a>
90	EC_BAD_DRL_FILE	Invalid DRL file	<a href="#">Ошибка x90</a>
91	EC_BAD_LST_FILE	Invalid LST file	<a href="#">Ошибка x91</a>
92	EC_BAD_LZMA_FILE	Invalid compressed file	<a href="#">Ошибка x92</a>
93	EC_PROXY_AUTH_ERROR	Proxy authentication error	<a href="#">Ошибка x93</a>
94	EC_NO_UPDATE_SERVERS	No update servers available	<a href="#">Ошибка x94</a>



Код ошибок	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
95	EC_BAD_KEY_FORMAT	<i>Invalid key file format</i>	<a href="#">Ошибка x95</a>
96	EC_EXPIRED_KEY	<i>License is already expired</i>	<a href="#">Ошибка x96</a>
97	EC_NETWORK_TIMEOUT	<i>Network operation timed out</i>	<a href="#">Ошибка x97</a>
98	EC_BAD_CHECKSUM	<i>Invalid checksum</i>	<a href="#">Ошибка x98</a>
99	EC_BAD_TRIAL_KEY	<i>Invalid trial license</i>	<a href="#">Ошибка x99</a>
100	EC_BLOCKED_LICENSE	<i>Blocked license key</i>	<a href="#">Ошибка x100</a>
101	EC_BAD_LICENSE	<i>Invalid license</i>	<a href="#">Ошибка x101</a>
102	EC_BAD_CONFIG	<i>Invalid configuration</i>	<a href="#">Ошибка x102</a>
104	EC_BAD_EXECUTABLE	<i>Invalid executable file</i>	<a href="#">Ошибка x104</a>
105	EC_NO_CORE_ENGINE	<i>Core engine is not available</i>	<a href="#">Ошибка x105</a>
106	EC_NO_VIRUS_BASES	<i>No virus databases</i>	<a href="#">Ошибка x106</a>
107	EC_APP_TERMINATED	<i>Process terminated by signal</i>	<a href="#">Ошибка x107</a>
108	EC_APP_CRASHED	<i>Unexpected process termination</i>	<a href="#">Ошибка x108</a>
109	EC_INCOMPATIBLE	<i>Incompatible software detected</i>	<a href="#">Ошибка x109</a>
112	EC_NO_DWS_BASES	<i>No web resource databases</i>	<a href="#">Ошибка x112</a>
115	EC_NO_LOOKUPD	<i>LookupD is not available</i>	<a href="#">Ошибка x115</a>
117	EC_NO_GATED	<i>GateD is not available</i>	<a href="#">Ошибка x117</a>
119	EC_NO_SCAN_ENGINE	<i>ScanEngine is not available</i>	<a href="#">Ошибка x119</a>
120	EC_NO_FILE_CHECK	<i>FileCheck is not available</i>	<a href="#">Ошибка x120</a>
121	EC_NO_ESAGENT	<i>ESAgent is not available</i>	<a href="#">Ошибка x121</a>
122	EC_NO_FIREWALL	<i>Firewall is not available</i>	<a href="#">Ошибка x122</a>
123	EC_NO_NET_CHECK	<i>NetCheck is not available</i>	<a href="#">Ошибка x123</a>
124	EC_NO_CLOUDD	<i>CloudD is not available</i>	<a href="#">Ошибка x124</a>
125	EC_UNEXPECTED_ERROR	<i>Unexpected error</i>	<a href="#">Ошибка x125</a>



## Приложение Ж. Список сокращений

В данном руководстве следующие термины использованы без расшифровки:

Обозначение	Расшифровка
<i>AD</i>	Microsoft Active Directory
<i>DN</i>	(LDAP) Distinguished Name
<i>EPM</i>	ESP Package Manager (менеджер пакетов)
<i>FQDN</i>	Fully Qualified Domain Name
<i>GID</i>	Group ID (системный идентификатор группы пользователей)
<i>GNU</i>	Проект GNU (GNU is Not Unix)
<i>HTML</i>	HyperText Markup Language
<i>HTTP</i>	HyperText Transfer Protocol
<i>HTTPS</i>	HyperText Transfer Protocol Secure (через SSL/TLS)
<i>ICAP</i>	Internet Content Adaptation Protocol
<i>ID</i>	Идентификатор
<i>IP</i>	Internet Protocol
<i>LDAP</i>	Lightweight Directory Access Protocol
<i>MBR</i>	Master Boot Record
<i>OID</i>	(SNMP) Object ID
<i>PID</i>	Process ID (системный идентификатор процесса)
<i>PAM</i>	Pluggable Authentication Modules
<i>RPM</i>	Red Hat Package Manager (менеджер пакетов)
<i>RRA</i>	Round-Robin Archive
<i>RRD</i>	Round-Robin Database
<i>SNI</i>	Server Name Indication
<i>SNMP</i>	Simple Network Management Protocol
<i>SP</i>	Service Pack



Обозначение	Расшифровка
<i>SSH</i>	Secure Shell
<i>SSL</i>	Secure Sockets Layer
<i>TCP</i>	Transmission Control Protocol
<i>TLS</i>	Transport Layer Security
<i>UID</i>	User ID (системный идентификатор пользователя)
<i>URL</i>	Unified Resource Locator
<i>VBR</i>	Volume Boot Record
ОС	Операционная система
ФС	Файловая система



## Предметный указатель

### С

ClamD: конфигурация 179  
CloudD: конфигурация 278  
ConfigD: конфигурация 79

### Д

Dr.Web ClamD 177  
Dr.Web CloudD 277  
Dr.Web ConfigD 76  
Dr.Web Ctl 83  
Dr.Web ES Agent 215  
Dr.Web File Checker 187  
Dr.Web Firewall для Linux 155  
Dr.Web HTTPD 220  
Dr.Web ICAPD 129  
Dr.Web LookupD 280  
Dr.Web Network Checker 192  
Dr.Web Scanning Engine 200  
Dr.Web SNMP MIB 242  
Dr.Web SNMPD 226  
Dr.Web Updater 207  
drweb-clamd 177  
drweb-cloudd 277  
drweb-configd 76  
drweb-ctl 83  
drweb-esagent 215  
drweb-filecheck 187  
drweb-firewall 155  
drweb-gated 149  
drweb-httpd 220  
drweb-icapd 129  
drweb-lookupd 280  
drweb-netcheck 192  
drweb-se 200  
drweb-snmpd 226  
drweb-update 207

### Е

EICAR 64  
ESAgent: конфигурация 217

### Ф

FileCheck: конфигурация 189

### Г

GateD: конфигурация 152

### Н

HTTPD: конфигурация 223

### И

ICAPD: конфигурация 133

### Л

LinuxFirewall: конфигурация 156  
LookupD: конфигурация 282

### Н

NetCheck: конфигурация 195

### С

ScanEngine: конфигурация 205  
SNMPD: конфигурация 229  
SpiDer Gate 149  
SSL CA 324

### У

Update: конфигурация 209

### А

Активация 61

### Б

Безопасность SELinux 56

### В

Введение 9  
Веб-интерфейс 114  
Выборочная установка 49

### Г

Генерация сертификатов 324

### Д

Деинсталляция продукта 42

### З

Задачи 10  
Закрытые ключи SSL 324



## Предметный указатель

Запуск деинсталлятора 42  
Запуск утилиты командной строки 85  
Защита веб-сервера 70

### И

Известные ошибки 327  
Изоляция 18  
Инсталляция продукта 31  
Интеграция Dr.Web ICAPD и Squid 148  
Интеграция продукта со Squid 66  
Интеграция с клиентами ClamAV clamd 184  
Интеграция с системами мониторинга 232

### К

Как защитить сервер 72  
Как изменить настройки 72  
Как обновить продукт 72  
Как подключиться к серверу централизованной защиты 72  
Как просмотреть журнал 72  
Как просмотреть настройки 72  
Как установить ключ 72  
Карантин 18  
Каталог Карантина 18  
Ключевой файл 61  
Компоненты 13  
компьютерные угрозы 289  
Консольный деинсталлятор 43  
Консольный инсталлятор 34  
Конфигурационный файл 298  
Краткие инструкции 72

### Л

Лицензионный ключевой файл 61  
Лицензирование 29  
Лицензия Dr.Web 29

### М

Мобильный режим 20  
Модули 13  
Мониторинг SNMP 232

### Н

Настройка PARSEC 59  
Настройка SELinux 56  
Настройка подсистем безопасности 55  
Начало работы 61

### О

Об антивирусе 10  
Обновление компонентов 38  
Обновление продукта 38  
Обозначения 8  
Общая конфигурация 79  
Одиночный режим 20  
Операционные системы 25

### П

Пакеты продукта 46  
Параметры конфигурации 298  
Переход на новую версию 39  
Права на доступ к файлам 19  
Правила проверки трафика 303  
приложение  
    виды компьютерных угроз 289  
    устранение компьютерных угроз 294  
Приложения 289  
Примеры вызова drweb-ctl 109  
Проблемы SELinux 56  
Проверка антивируса 64

### Р

Работа из командной строки 83  
Регистрация 61  
Режимы работы 20

### С

Секция [ClamD] 179  
Секция [CloudD] 278  
Секция [ESAgent] 217  
Секция [FileCheck] 189  
Секция [GateD] 152  
Секция [HTTPD] 223  
Секция [ICAPD] 133  
Секция [LinuxFirewall] 156  
Секция [LookupD] 282  
Секция [NetCheck] 195  
Секция [Root] 79  
Секция [ScanEngine] 205  
Секция [SNMPD] 229  
Секция [Update] 209  
Сертификаты SSL 324  
Системные требования 25



## Предметный указатель

Системы мониторинга 232

Сокращения 380

Способы установки 31

Структура продукта 13

### Т

Техническая поддержка 297

### У

Удаление антивируса 30

Удаление дистрибутива 42

Удаление из репозитория 43

Удаление нативных пакетов 43

Удаление продукта 42

Установка антивируса 30

Установка из .gip пакета 32

Установка из дистрибутива 32

Установка из нативных пакетов 35

Установка из репозитория 35

Установка из универсальных пакетов 32

Установка продукта 31

устранение компьютерных угроз 294

### Ф

Файловые полномочия 19

Файлы продукта 46

Функции 10

### Ц

Централизованная защита 20



