Dr.WEB

для файловых серверов UNIX

Руководство администратора

Dr.Web для файловых серверов 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

Условные обозначения и сокращения

В данном руководстве используются следующие условные обозначения:

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

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

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

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

Перечень сокращений приведен в разделе Приложение Ж. Список сокращений.

Введение

Благодарим вас за приобретение программного продукта Dr.Web для файловых серверов 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 файловых серверов UNIX версии 11.0.

Соглашение о путях к файлам продукта

Dr.Web для файловых серверов 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
GNU/Linux, Solaris	*<opt_dir>*	`/opt/drweb.com`
	<etc_dir>	`/etc/opt/drweb.com`
	<var_dir>	`/var/opt/drweb.com`
FreeBSD	*<opt_dir>*	`/usr/local/libexec/drweb.com`
	<etc_dir>	`/usr/local/etc/drweb.com`
	<var_dir>	`/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 файловых серверов UNIX создан для защиты файловых серверов, 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 файловых серверов 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 файловых серверов 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 файловых серверов 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. **Мониторинг обращений к файлам:**

- **В файловой системе ОС.** Отслеживаются обращения к файлам с данными и попытки запуска исполняемых файлов. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках инфицирования ими файловой системы сервера.

  Обратите внимание, что функция мониторинга файловой системы доступна только для ОС семейства **GNU/Linux**. *Для других ОС из списка поддерживаемых компонент, предоставляющий эту возможность, не поставляется.*

- **В разделяемых каталогах Samba.** Отслеживаются обращения локальных и удаленных пользователей файлового сервера к файлам как на запись, так и на чтение. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках сохранения их в хранилище, что предотвращает их дальнейшее распространение по сети.
- **На томах Novell Storage Services.** Отслеживаются обращения пользователей файлового хранилища NSS к файлам на запись. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках сохранения их в хранилище NSS, что предотвращает их дальнейшее распространение по сети.

  Обратите внимание, что функция мониторинга томов **Novell Storage Services** *доступна только для* **Novell Open Enterprise Server** *SP2 на базе операционной системы* **SUSE Linux Enterprise Server** *10 SP3 или старше. Для других ОС из списка поддерживаемых компонент, предоставляющий эту возможность, не поставляется.*

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.
4. **Автоматическое обновление** антивирусного ядра, содержимого вирусных баз 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 файловых серверов UNIX представляет собой программный комплекс, состоящий из набора компонентов, каждый из которых выполняет свой набор функций. Перечень компонентов, входящих в Dr.Web для файловых серверов UNIX, перечислен в таблице ниже.

Компонент	Описание
Dr.Web ConfigD	Демон управления конфигурацией комплекса Dr.Web для файловых серверов UNIX. Решает следующие задачи:

Компонент	Описание
	• 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. Информирует компоненты продукта об изменении состава запущенных компонентов. • Хранит и предоставляет всем компонентам информацию об имеющихся лицензионных ключах и настройках. Принимает изменённые настройки и ключи от уполномоченных компонентов Dr.Web для файловых серверов UNIX. Оповещает компоненты при изменении лицензионных ключей и настроек. Исполняемый файл компонента: **drweb-configd** Внутреннее наименование, выводимое в журнал: `ConfigD`
Dr.Web Virus-Finding Engine	Антивирусное ядро. Является основным компонентом антивирусной защиты. Реализует алгоритмы поиска и распознавания вирусов и вредоносных программ, а также анализа подозрительного поведения (используя сигнатурный и эвристический анализ). Используется всеми компонентами Dr.Web для файловых серверов UNIX через Dr.Web Scanning Engine. Исполняемый файл компонента: **drweb32.dll** Внутреннее наименование, выводимое в журнал: `CoreEngine`
Dr.Web Scanning Engine	Сканирующее ядро. Компонент, отвечающий за загрузку антивирусного ядра Dr.Web Virus-Finding Engine и вирусных баз. Передает антивирусному ядру на проверку содержимое файлов и загрузочных записей дисковых устройств по запросам от других компонентов Dr.Web для файловых серверов 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. Используется всеми компонентами Dr.Web для файловых серверов UNIX для антивирусной проверки. Исполняемый файл компонента: **drweb-se** Внутреннее наименование, выводимое в журнал: `ScanEngine`
Вирусные базы Dr.Web	Автоматически обновляемая база данных сигнатур вирусов и прочих угроз, а также алгоритмов распознавания и нейтрализации вредоносного программного обеспечения. Используется антивирусным ядром Dr.Web Virus-Finding Engine и поставляется совместно с ним.

Компонент	Описание
Dr.Web File Checker	Компонент проверки объектов файловой системы и менеджер карантина. Принимает от других компонентов Dr.Web для файловых серверов 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 каталогами карантина. Организует и содержит в актуальном состоянии кэш, хранящий информацию о ранее проверенных файлах для уменьшения частоты повторных проверок файлов. Используется компонентами, проверяющими объекты файловой системы, такими как SpIDer Guard, SpIDer Guard для SMB, SpIDer Guard для NSS. Исполняемый файл компонента: **drweb-filecheck** Внутреннее наименование, выводимое в журнал: `FileCheck`
SpIDer Guard	Монитор файловой системы Linux. Работает в фоновом режиме и отслеживает операции с файлами (такие как создание, открытие, закрытие и запуск файла) в файловых системах **GNU/Linux**. Посылает компоненту проверки файлов запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ. В зависимости от возможностей ОС использует механизм **fanotify** (API, предоставляемый ОС) или специализированный модуль ядра, разработанный компанией Dr.Web (LKM-модуль, поставляется совместно с SpIDer Guard, в отдельном пакете). Поставляется только в составе дистрибутивов, предназначенных для ОС семейства **GNU/Linux**. Исполняемый файл компонента: **drweb-spider** Внутреннее наименование, выводимое в журнал: `LinuxSpider`
Модуль ядра **GNU/Linux** для SpIDer Guard	Модуль ядра **GNU/Linux** (LKM-модуль), используемый монитором SpIDer Guard для доступа к событиям файловой системы в тех ОС, в которых API **fanotify** недоступен или реализован с ограниченным набором функций (как, например, в системах с мандатной моделью доступа). Компонент поставляется как в скомпилированном виде (для набора ОС, в которых **fanotify** не реализован или недоступен), так и в виде исходных кодов, позволяющих осуществить сборку и

Компонент	Описание
	установку модуля ядра ОС вручную (инструкция по сборке приведена в разделе Сборка модуля ядра для SpIDer Guard). Поставляется только в составе дистрибутивов, предназначенных для ОС семейства **GNU/Linux**. Исполняемый файл компонента: **drweb.ko**
SpIDer Guard для SMB	Монитор разделяемых каталогов **Samba**. Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции чтения и записи) в каталогах, отведенных для файловых хранилищ SMB-сервера **Samba**. Отправляет компоненту проверки файлов содержимое новых и изменившихся файлов на проверку. Для интеграции с файловым сервером использует модули VFS SMB, работающие на стороне сервера **Samba**. Исполняемый файл компонента: **drweb-smbspider-daemon** Внутреннее наименование, выводимое в журнал: `SMBSpider`
SpIDer Guard для NSS	Монитор томов NSS (**Novell Storage Services**). Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции записи) на томах NSS, смонтированных в указанную точку файловой системы. Отправляет содержимое новых и изменившихся файлов на проверку компоненту проверки файлов. Поставляется только в составе дистрибутивов, предназначенных для ОС семейства **GNU/Linux**. Работоспособен только в **Novell Open Enterprise Server** SP2 на базе операционной системы **SUSE Linux Enterprise Server** 10 SP3 или старше. Исполняемый файл компонента: **drweb-nss** Внутреннее наименование, выводимое в журнал: `<% NSSSPIDER_SECTION%>`
Dr.Web ES Agent	Агент централизованной защиты. Обеспечивает работу программного комплекса в централизованном и мобильном режимах. Обеспечивает связь с сервером централизованной защиты, получает от него лицензионный ключевой файл, обновления вирусных баз и антивирусного ядра. Передает на сервер информацию о составе и состоянии компонентов программного комплекса Dr.Web для файловых серверов UNIX и накопленную статистику вирусных инцидентов.

Компонент	Описание
	Исполняемый файл компонента: **drweb-esagent** Внутреннее наименование, выводимое в журнал: `ESAgent`
Dr.Web Network Checker	Агент сетевой проверки данных. Используется для передачи на проверку в сканирующее ядро данных, отправленных компонентами программного комплекса через сеть (это такие компоненты, как Dr.Web ClamD). Кроме этого, позволяет программному комплексу Dr.Web для файловых серверов 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). Для обеспечения безопасности при передаче файлов по сети использует SSL. Исполняемый файл компонента: **drweb-netcheck** Внутреннее наименование, выводимое в журнал: `NetCheck`
Dr.Web HTTPD	Веб-сервер управления компонентами Dr.Web для файловых серверов 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 **Apache HTTP Server**) и утилиты удаленного администрирования наподобие **Webmin**. Для обеспечения безопасности при подключении к веб-интерфейсу управления использует протокол HTTPS. Исполняемый файл компонента: **drweb-httpd** Внутреннее наименование, выводимое в журнал: `HTTPD`
Dr.Web Ctl	Утилита, обеспечивающая интерфейс управления Dr.Web для файловых серверов UNIX из командной строки операционной системы. Позволяет осуществлять запуск проверки файлов, просматривать содержимое карантина и управлять им, запускать обновление вирусных баз, подключать программный комплекс к серверу

Компонент	Описание
	централизованной защиты и отключаться от него, просматривать и изменять значения параметров конфигурации программного комплекса. Исполняемый файл компонента: **drweb-ctl** Внутреннее наименование, выводимое в журнал: `Ctl`
Dr.Web Updater	Компонент обновления. Отвечает за загрузку с серверов обновлений компании «Доктор Веб» обновлений для вирусных баз, антивирусного ядра. Обновления могут загружаться как автоматически, по расписанию, так и непосредственно по команде пользователя (через утилиту Dr.Web Ctl или через веб-интерфейс управления). Исполняемый файл компонента: **drweb-update** Внутреннее наименование, выводимое в журнал: `Update`
Dr.Web SNMPD	Представляет собой SNMP-агент. Предназначен для интеграции программного комплекса Dr.Web для файловых серверов 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. Исполняемый файл компонента: **drweb-snmpd** Внутреннее наименование, выводимое в журнал: `SNMPD`
Dr.Web ClamD	Компонент, эмулирующий интерфейс антивирусного демона **clamd**, являющегося компонентом антивирусного продукта **ClamAV®**. Позволяет прозрачно использовать для антивирусной проверки продукт Dr.Web для файловых серверов UNIX любым приложениям, которые могут использовать антивирусный продукт **ClamAV®**. Исполняемый файл компонента: **drweb-clamd** Внутреннее наименование, выводимое в журнал: `ClamD`
Dr.Web CloudD	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. Исполняемый файл компонента: **drweb-cloudd** Внутреннее наименование, выводимое в журнал: `CloudD`

На рисунке ниже показана структура программного комплекса Dr.Web для файловых серверов UNIX и его взаимодействия с внешними приложениями.

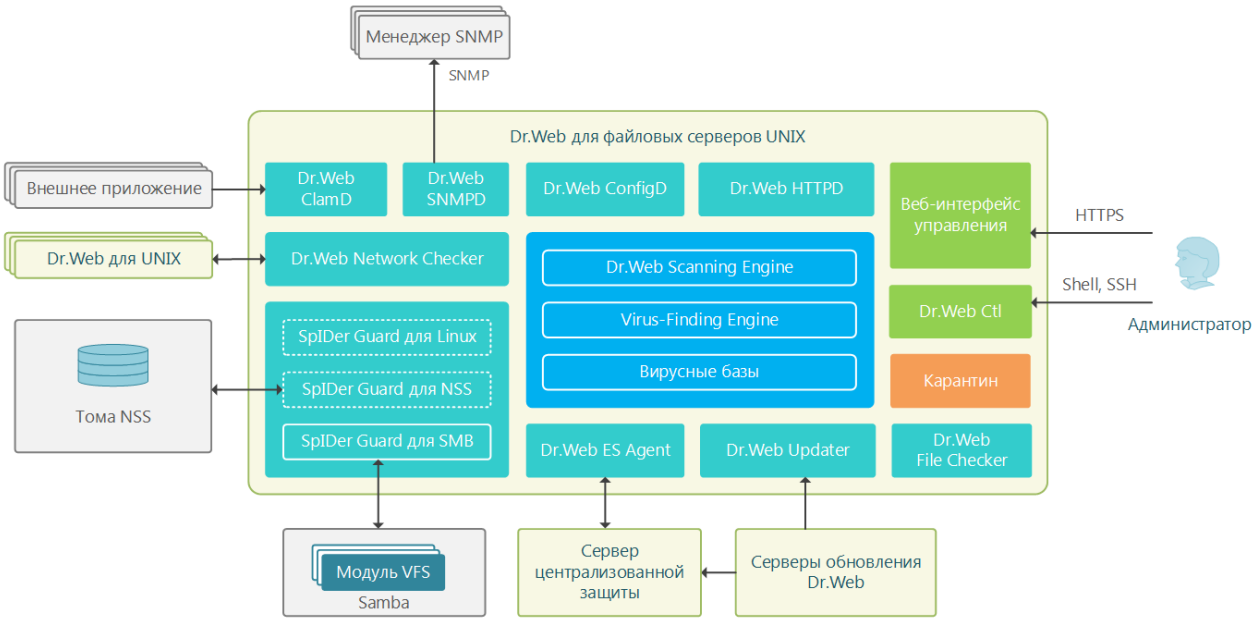

Рисунок 1. Структура программного продукта Dr.Web для файловых серверов UNIX

На приведенном рисунке использованы следующие обозначения:

	– программный комплекс Dr.Web для файловых серверов UNIX в целом и внешние по отношению к нему программные продукты Dr.Web, не входящие непосредственно в его состав.
	– внешние по отношению к Dr.Web для файловых серверов UNIX программы и программные комплексы, с которыми он интегрируется.
	– компоненты, образующие ядро продукта Dr.Web для файловых серверов UNIX. Остальные компоненты продукта используют ядро как сервис, осуществляющий непосредственную антивирусную проверку.
	– сервисные компоненты, решающие конкретные задачи в рамках антивирусной защиты (проверку объектов файловой системы, обновление вирусных баз, подключение к серверам централизованной защиты, общая координация работы и т.д.).
	– компоненты, предоставляющие пользователю интерфейс для управления работой Dr.Web для файловых серверов UNIX.
	– карантин (система каталогов файловой системы, хранящих изолированные файлы с угрозами).

Компоненты, обозначенные пунктирной границей, могут отсутствовать, в зависимости от поставки или сценария использования продукта.

Более подробно компоненты Dr.Web для файловых серверов UNIX описаны в разделе Компоненты программного комплекса.

Каталоги карантина

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

Действие	Требуемые полномочия
	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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

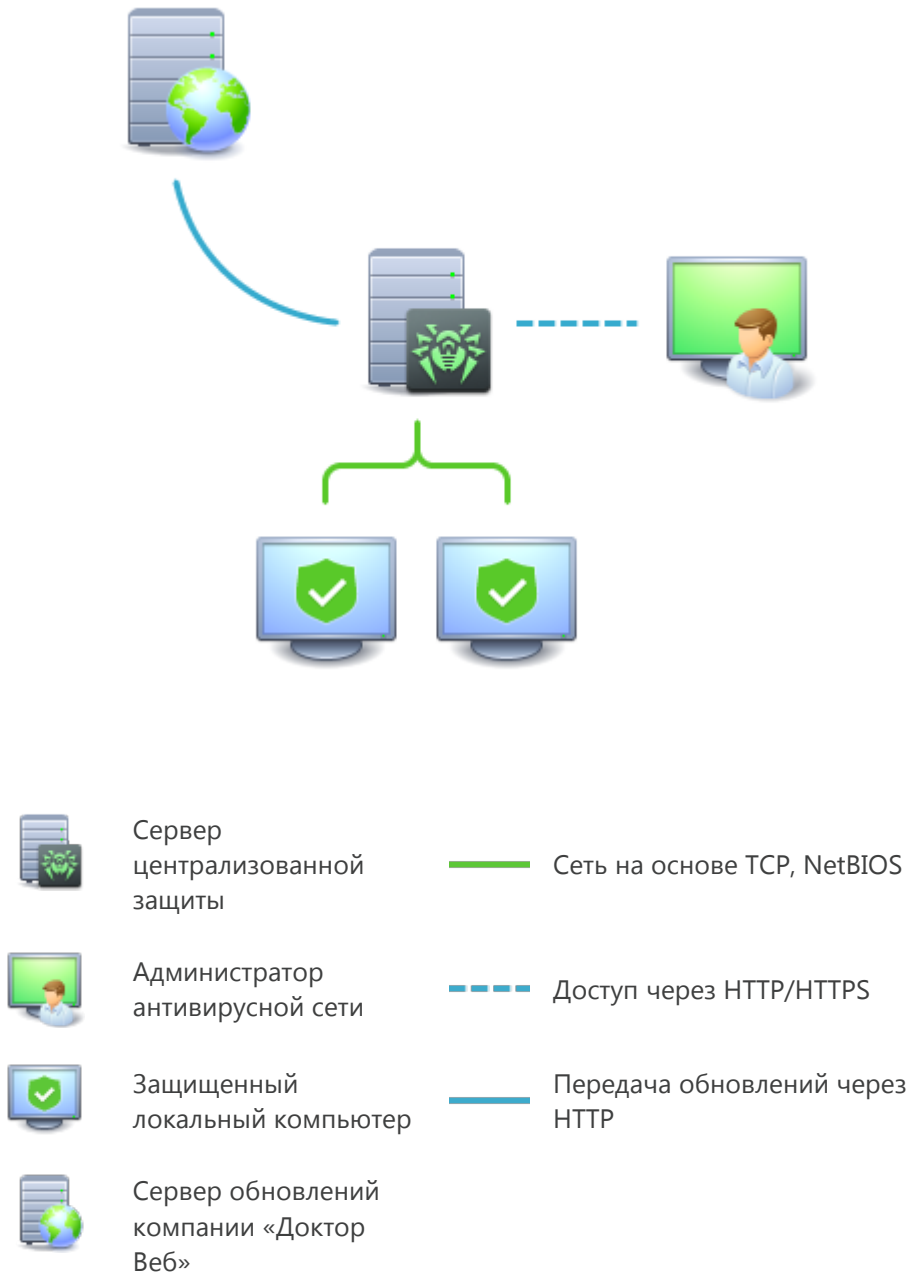

Рисунок 2. Логическая структура антивирусной сети.

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 файловых серверов UNIX реализована *не полностью*: сервер не управляет настройками компонентов программного комплекса.

Подключение к серверу централизованной защиты

Dr.Web для файловых серверов 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 файловых серверов UNIX.

Если Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов UNIX возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
Платформа	Поддерживаются процессоры с архитектурой и системой команд **Intel/AMD**: 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 файловых серверов UNIX.
Операционная система	**GNU/Linux** (на основе ядра с версией не ниже 2.6.37 и использующая библиотеку **glibc** версии 2.13 и выше), **FreeBSD** или **Solaris** для платформ **Intel x86/amd64**. ⚠ В случае использования 64-битной версии операционной системы, должна быть *обязательно* включена поддержка исполнения 32-битных приложений (для этого, возможно, потребуются дополнительные библиотеки, см. ниже). Операционная система должна поддерживать механизм аутентификации **PAM**. Перечень протестированных дистрибутивов ОС перечислен ниже.
Прочее	Наличие сетевого подключения: • Подключение к сети Интернет для обновления вирусных баз и компонентов Dr.Web для файловых серверов UNIX. • При работе в режиме централизованной защиты достаточно только подключения к используемому серверу в рамках локальной сети, доступ в Интернет не требуется.

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

Название дистрибутива Linux	Версии	Платформы
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 файловых серверов 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 файловых серверов 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

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

Поддерживаемые файловые серверы

1. **Файловая служба Samba**

   Для интеграции с файловой службой **Samba** требуется установленный и настроенный сервер **Samba** одной из следующих версий: 3.0.33, 3.0.36, 3.2.0 – 3.6.0, 4.0.0 – 4.8.0.

   Монитор SpIDer Guard для SMB, входящий в состав Dr.Web для файловых серверов UNIX, использует для интеграции с **Samba** специальный модуль VFS SMB. Совместно с компонентом SpIDer Guard для SMB поставляется несколько версий модуля VFS SMB, собранных для различных версий **Samba**, однако они могут оказаться несовместимы с версией **Samba**, установленной на вашем файловом сервере, например, если установленный у вас сервер **Samba** использует опцию `CLUSTER_SUPPORT`.

   В случае несовместимости поставляемых модулей VFS SMB с вашим сервером **Samba**, в процессе установки продукта на экран *будет выдано соответствующее сообщение*. В этом случае перед интеграцией необходимо выполнить процедуру сборки модуля VFS SMB для вашего сервера **Samba**, включая поддержку опции `CLUSTER_SUPPORT`, если это требуется.

   Процедура сборки модуля VFS SMB из исходных кодов описана в разделе Сборка модуля VFS SMB.

2. **Файловая служба NSS**

   Для интеграции с файловой службой **Novell Storage Services (NSS)** требуется **Novell Open Enterprise Server** SP2 на базе операционной системы **SUSE Linux Enterprise Server** 10 SP3 или старше (11 SP1, SP2).

Совместимость с подсистемами безопасности

При настройках по умолчанию Dr.Web для файловых серверов UNIX не совместим с подсистемой улучшения безопасности **SELinux**. Кроме того, по умолчанию Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов UNIX. Подробнее см. в разделе Настройка подсистем безопасности.

Лицензирование

Права пользователя на использование копии программного продукта Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX распространяется в виде инсталляционного файла с именем `drweb-<версия>-av-srv-<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-srv-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 файловых серверов 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. Ознакомиться с текстом Лицензионного соглашения после установки продукта вы можете, прочитав файл `/opt/drweb.com/share/doc/LICENSE`. Расширение файла указывает язык, на котором написан текст Лицензионного соглашения. Файл `LICENSE` без расширения хранит текст Лицензионного соглашения Dr.Web на английском языке. В случае если вы *не согласны* с условиями Лицензионного соглашения, вам следует удалить продукт после установки.
- Запуск программы установки в полностью автоматическом режиме требует наличия прав суперпользователя. Для повышения прав вы можете использовать команды **su** и **sudo**.

Если ваш дистрибутив **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, а также автоматически интегрировать Dr.Web для файловых серверов UNIX с файловым сервером **Samba** и указать перечень разделяемых каталогов, которые должны находиться под наблюдением монитора SpIDer Guard для SMB.

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. Далее необходимо разрешить или запретить модификацию конфигурационного файла `smb.conf` сервера **Samba**, а также подтвердить, что скрипт установки правильно определил путь к демону сервера **Samba**, или указать правильный путь.
4. Далее следует отметить, какие разделяемые каталоги (из управляемых **Samba**) должны быть добавлены под наблюдение монитора SpIDer Guard для SMB. Для этого следуйте инструкциям скрипта:
   - Указание номера разделяемого каталога, не отмеченного символом `[X]`, добавляет его под наблюдение, а в противном случае – удаляет его из-под наблюдения.
   - Ввод *A* или *All* добавляет под наблюдение все доступные разделяемые каталоги, а ввод символа *N* или *None* – удаляет все разделяемые каталоги из-под наблюдения.

   Для завершения выбора и записи внесенных изменений в конфигурационный файл следует ввести *0*, *Q* или *Quit*.
5. После этого все внесенные изменения будут зафиксированы в конфигурационном файле. Дополнительно будет определена требуемая версия библиотеки модуля VFS SMB, и ссылка на него будет добавлена в каталог сервера **Samba**.
6. По окончании внесения изменений необходимо нажать клавишу ENTER для завершения работы скрипта.

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

Установка из репозитория

Нативные пакеты продукта Dr.Web для файловых серверов UNIX находятся в официальном репозитории Dr.Web https://repo.drweb.com/. После добавления репозитория Dr.Web в список репозиториев, используемых менеджером пакетов вашей операционной системы, вы сможете устанавливать его в виде нативных пакетов для операционной системы так же, как и любые другие программы из репозиториев вашей операционной системы. Необходимые зависимости будут разрешаться автоматически.

Все нижеприведенные команды для подключения репозиториев, 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 файловых серверов 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 файловых серверов UNIX из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-file-servers
```

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 файловых серверов UNIX из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-file-servers
```

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 файловых серверов UNIX из репозитория выполните команду:

```
# urpmi drweb-file-servers
```

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 файловых серверов UNIX из репозитория выполните команду:

```
# yum install drweb-file-servers
```

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

```
# dnf install drweb-file-servers
```

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 файловых серверов UNIX из репозитория выполните команды:

```
# zypper refresh
# zypper install drweb-file-servers
```

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

Обновление продукта

Предусмотрено два режима обновления продукта Dr.Web для файловых серверов 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 файловых серверов UNIX следует выполнять тем же способом, каким был установлена версия Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX с версией новее 6.0.2, вы можете воспользоваться командой:

```
$ drweb-ctl appinfo
```

из присутствующей в выводе команды строчки вида

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

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

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

Обновление установкой универсального пакета

Выполните установку Dr.Web для файловых серверов 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 почтовых серверов и Интернет-шлюзов) следует отметить для удаления *только* следующие пакеты:

- `drweb-file-servers-doc`
- `drweb-samba-web`
- `drweb-smbspider`

Обновление из репозитория

Обратите внимание, что вы *не сможете* обновить Dr.Web для файловых серверов 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 файловых серверов UNIX на отдельную машину.

Для обновления текущей версии Dr.Web для файловых серверов 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 репозиториев обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

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

```
# yum update
```

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

```
# dnf update
```

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

- **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 файловых серверов 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 файловых серверов 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.

Пожалуйста, обратите внимание, что после удаления Dr.Web для файловых серверов UNIX, вам необходимо вручную удалить из каталога сервера **Samba** ссылку на модуль VFS SMB Dr.Web и отредактировать файл конфигурации **Samba** (`smb.conf`), удалив из секций параметров разделяемых каталогов строку `vfs objects = smb_spider` (где `smb_spider` – имя символической ссылки на на модуль VFS SMB Dr.Web).

Удаление универсального пакета

Удаление продукта Dr.Web для файловых серверов 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 файловых серверов UNIX, но и *все другие* продукты Dr.Web, установленные на вашем компьютере.

В случае если на вашем компьютере, кроме Dr.Web для файловых серверов UNIX, установлены и другие продукты Dr.Web, для удаления только Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов UNIX выполните команду:

```
# apt-get remove drweb-file-servers
```

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-file-servers`, 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 файловых серверов 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 файловых серверов UNIX.

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

ALT Linux, PCLinuxOS (apt-rpm)

Удаление Dr.Web для файловых серверов 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 файловых серверов UNIX выполните команду:

```
# urpme drweb-file-servers
```

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

```
# urpme --auto-orphans drweb-file-servers
```

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

1. Первый вариант команды удалит только пакет `drweb-file-servers`, 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-file-servers`, 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 файловых серверов UNIX.

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

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

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

```
# yum remove drweb*
```

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

```
# dnf remove drweb*
```

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

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 файловых серверов UNIX.

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

SUSE Linux (zypper)

Для удаления Dr.Web для файловых серверов UNIX выполните команду:

```
# zypper remove drweb-file-servers
```

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-file-servers`, 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 файловых серверов UNIX.

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

Дополнительно

Пакеты и файлы продукта

Пакеты

Продукт Dr.Web для файловых серверов UNIX состоит из следующих пакетов:

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

Пакет	Содержимое
drweb-common	Основной конфигурационный файл drweb.ini, основные библиотеки, документация и структура каталогов продукта. В процессе установки данного пакета также будут созданы пользователь drweb и группа drweb
drweb-configd	Файлы компонентов Dr.Web ConfigD и Dr.Web Ctl
drweb-esagent	Файлы компонента Dr.Web ES Agent
drweb-filecheck	Файлы компонента Dr.Web File Checker
drweb-file-servers-doc	Документация PDF по продукту
drweb-file-servers	Корневой метапакет продукта
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-libs	Файлы основных библиотек продукта *)
drweb-netcheck	Файлы компонента Dr.Web Network Checker
drweb-nss	Файлы компонента SpIDer Guard для NSS
drweb-openssl	Библиотеки **OpenSSL**
drweb-protobuf	Библиотеки **Protobuf**
drweb-se	Файлы компонента Dr.Web Scanning Engine
drweb-smbspider-daemon	Файлы компонента SpIDer Guard для SMB (демон мониторинга SMB)
drweb-smbspider	Файлы компонента SpIDer Guard для SMB
drweb-smbspider-modules	Файлы компонента SpIDer Guard для SMB (модули VFS SMB)
drweb-smbspider-modules-src	Файлы компонента SpIDer Guard для SMB (исходные коды модуля VFS SMB)
drweb-snmpd	Файлы компонента Dr.Web SNMPD
drweb-spider	Файлы компонента SpIDer Guard

Пакет	Содержимое
drweb-spider-kmod	Файлы модуля ядра **GNU/Linux** для работы SpIDer Guard в режиме *LKM*
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 файловых серверов UNIX размещаются в каталогах /opt, /etc и /var дерева файловой системы.

Структура используемых каталогов:

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

Каталог	Содержимое
drweb-spider-kmod/	Файлы модуля ядра для работы компонента SpIDer Guard (исходные коды для ручной сборки).
scripts/	Файлы вспомогательных сценариев.
<var_dir>/	Вспомогательные и временные файлы продукта.
bases/	Файлы вирусных баз Dr.Web (актуальная обновленная версия).
cache/	Кэш обновлений.
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`	• Dr.Web Ctl • Dr.Web ConfigD • Dr.Web Scanning Engine • Dr.Web File Checker • Dr.Web Updater • Вирусные базы
Комплект для мониторинга файловой системы **Linux**	`drweb-spider`	• Dr.Web Ctl • Dr.Web ConfigD • Dr.Web Scanning Engine • Dr.Web File Checker • Dr.Web Updater • SpIDer Guard • Вирусные базы
Комплект для мониторинга разделяемых каталогов **Samba**	`drweb-smbspider`	• Dr.Web Ctl • Dr.Web ConfigD • Dr.Web Scanning Engine • Dr.Web File Checker • Dr.Web Updater • SpIDer Guard для SMB • Вирусные базы
Комплект для мониторинга томов **NSS**	`drweb-nss`	• Dr.Web Ctl • Dr.Web ConfigD • Dr.Web Scanning Engine • Dr.Web File Checker • Dr.Web Updater • SpIDer Guard для NSS • Вирусные базы
Комплект для эмуляции **ClamAV** (**clamd**)	`drweb-clamd`	• Dr.Web Ctl • Dr.Web ConfigD • Dr.Web Scanning Engine • Dr.Web File Checker • Dr.Web Network Checker • Dr.Web Updater • Dr.Web ClamD • Вирусные базы

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 файловых серверов 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 run-файл содержит пакеты всех компонентов, из которых состоит программный комплекс Dr.Web для файловых серверов 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 файловых серверов 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-file-servers
```

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 **МСВС** 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 файловых серверов UNIX при настройках по умолчанию. Для обеспечения корректной работы Dr.Web для файловых серверов UNIX в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web для файловых серверов UNIX.

В этом разделе рассматриваются настройки, обеспечивающие корректную работу Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 зашиты:

- `Permissive` – защита активна, но используется разрешающая стратегия: действия, нарушающие политики безопасности, не запрещаются, а только фиксируются в журнале аудита.

- `Enforced` – защита активна, используется запрещающая стратегия: действия, нарушающие политики безопасности, регистрируются в журнале аудита и блокируются.
- `Disabled` – **SELinux** установлен, но неактивен.

Если **SELinux** работает в режиме *Enforced*, следует временно (на период установки продукта) перевести ее в режим *Permissive*. Для этого выполните 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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX. В случае если это не так, следует или дождаться таких инцидентов в процессе работы продукта Dr.Web для файловых серверов UNIX, или создать разрешающие политики принудительно, воспользовавшись утилитой **policygentool** (см. ниже).

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

Пример использования **audit2allow**:

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

В данном примере утилита **audit2allow** производит поиск в файле `/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 файловых серверов 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 настройки **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, монитор SpIDer Guard в режиме работы по умолчанию (**Mode** = AUTO) не может перехватывать события о доступе к файлам с более высокими уровнями привилегий, нежели уровень привилегий, на котором запущен SpIDer Guard. Кроме того, в случае если пользователь работает на отличном от нуля уровне привилегий, утилита управления Dr.Web для файловых серверов UNIX из командной строки Dr.Web Ctl не может взаимодействовать с монитором SpIDer Guard и 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 SpIDer Guard для перехвата событий доступа к файлам с любым уровнем привилегий

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

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

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

Для получения дополнительной информации используйте команду:

```
$ man drweb-spider
```

Настройка корректного запуска Dr.Web для файловых серверов UNIX на любом уровне привилегий

Чтобы все компоненты Dr.Web для файловых серверов 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 файловых серверов UNIX выполните его активацию, получив и установив ключевой файл.
2. Далее рекомендуется выполнить проверку работоспособности продукта.
3. Интегрируйте Dr.Web для файловых серверов UNIX с требуемыми файловыми службами (см. инструкцию для Samba, см. инструкцию для NSS).
4. При необходимости настройте параметры мониторинга областей файловой системы **Linux**, находящихся вне томов NSS и вне разделяемых каталогов **Samba**.
5. Проверьте состав запущенных компонентов и при необходимости включите дополнительные компоненты, которые по умолчанию отключены, если они необходимы для защиты вашего сервера (например, SpIDer Guard, 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 потребуется 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX. В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.

При работе Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов UNIX установите значение параметра **`KeyPath`** таким образом, чтобы он указывал на ключевой файл.
3. Перезапустите Dr.Web для файловых серверов 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 файловых серверов 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\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

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

В случае корректной работы Dr.Web для файловых серверов 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.

Настройка мониторинга файловой системы

Для настройки мониторинга файловой системы **Linux** монитором SpIDer Guard необходимо задать значения ряда параметров, находящихся в секции настроек `[LinuxSpider]` конфигурационного файла:

- Установите для параметра **`Start`** значение `Yes`, чтобы включить монитор;
- Укажите режим взаимодействия монитора с файловой системой в параметре **`Mode`** (рекомендуется использовать значение `Auto`);
- В параметре **`ExcludedProc`** при необходимости перечислите пути к исполняемым файлам доверенных приложений, то есть приложений, доступ которых к файлам не будет контролироваться монитором;
- В параметрах **`IncludedPath`** и **`ExcludedPath`** определите область наблюдения и область исключения в файловой системе (перечни путей к объектам, подлежащим и не подлежащим контролю монитором). В частности, если некоторые пути находятся под управлением файлового сервера **Samba** или являются томами **NSS**, эти пути следует добавить в область исключения во избежание конфликтов при проверке разными мониторами;
- Задайте параметры проверки файлов и реакции монитора на обнаружение угроз различных типов.

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

Интеграция с файловым сервером Samba

Монитор SpIDer Guard для SMB использует для интеграции с **Samba** специальный модуль VFS SMB. Совместно с монитором SpIDer Guard для SMB поставляется несколько версий модуля VFS SMB, собранных для различных версий **Samba**, однако они могут оказаться несовместимы с версией **Samba**, установленной на вашем файловом сервере, например, если установленный у вас сервер **Samba** использует опцию `CLUSTER_SUPPORT`.

В случае несовместимости поставляемых модулей VFS SMB с вашим сервером **Samba**, в процессе установки продукта на экран *будет выдано соответствующее сообщение*. В этом случае перед интеграцией необходимо выполнить процедуру сборки модуля VFS SMB для вашего сервера **Samba**, включая поддержку опции `CLUSTER_SUPPORT`, если это требуется.

Для получения информации о процедуре сборки модуля VFS SMB из исходных кодов см. в разделе Сборка модуля VFS SMB.

Шаги по интеграции с Samba

Для интеграции SpIDer Guard для SMB с файловым сервером **Samba** необходимо выполнить следующее:

1. В каталоге VFS-модулей сервера **Samba** (по умолчанию для **Linux** – `/usr/lib/samba/vfs`) создать символическую ссылку `smb_spider.so`, указывающую на модуль VFS SMB Dr.Web, соответствующий используемой версии сервера **Samba**.

   Модули VFS SMB, поставляемые Dr.Web, расположены в каталоге с библиотеками продукта:

   - <*opt_dir*>`/lib/samba` – для 32-битной платформы.
   - <*opt_dir*>`/lib64/samba` – для 64-битной платформы.

   Файлы модулей имеют имя вида `libsmb_spider.so.`<*ver*>, где <*ver*> – версия сервера **Samba**, с которой работает данный модуль.

   Например: `/opt/drweb.com/lib/samba/libsmb_spider.so.3.6.0` – модуль VFS SMB для сервера **Samba** версии 3.6.0, работающего на 32-битной платформе в среде ОС **Linux**.

   Данное действие вы можете выполнить, используя сценарий поддержки интеграции `update-links.sh` *(см. ниже).*

2. В файле конфигурации сервера **Samba** `smb.conf` (по умолчанию для **Linux** – в каталоге `/etc/samba`) создать секции для разделяемых каталогов. Секция разделяемого каталога должна иметь вид:

```
[<имя ресурса>]
comment = <комментарий>
path = <путь к защищаемому каталогу>
vfs objects = smb_spider
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

где <*имя ресурса*> – любое имя разделяемого ресурса, а <*комментарий*> – произвольная строка-комментарий (не обязательно). Имя объекта, указанное в параметре `vfs objects`, должно совпадать с именем файла символической ссылки (`smb_spider` в данном случае).

После этого каталог, указанный в параметре `path`, будет находиться под наблюдением монитора SpIDer Guard для SMB. При этом взаимодействие SpIDer Guard для SMB с модулем VFS SMB будет производиться через UNIX-сокет `/<samba chroot path>/var/run/.com.drweb.smb_spider_vfs`. Путь к этому UNIX-сокету по умолчанию задан в настройках SpIDer Guard для SMB, а также модуля VFS SMB.

Подключить SpIDer Guard для SMB к уже настроенным в файле конфигурации сервера **Samba** *разделяемым каталогам вы можете, используя сценарий поддержки интеграции* `drweb_smbspider_configure.sh` *(см. ниже).*

3. Если требуется изменить путь к сокету, то его необходимо задать не только в настройках SpIDer Guard для SMB (параметр **`SmbSocketPath`**), но и в файле конфигурации **Samba** `smb.conf`. Для этого в секцию `[<имя ресурса>]` необходимо добавить строку:

   ```
   smb_spider:socket = <путь к сокету>
   ```

   где <*путь к сокету*> должен быть абсолютным путем к UNIX-сокету, относительно корня, заданного для сервера **Samba** через **chroot** (<*samba chroot path*>).

4. При необходимости, задавая значения параметров **`ExcludedPath`** и **`IncludedPath`**, определите пути к объектам, находящимся в защищаемых разделяемых каталоге, и которые должны быть исключены из проверки и наоборот, проверяться монитором SpIDer Guard для SMB. Допускается указание путей как к каталогам, так и к конкретным файлам. Если указан каталог, то будет пропускаться или проверяться всё содержимое этого каталога. Обратите внимание, что параметр **`IncludedPath`** имеет приоритет над параметром **`ExcludedPath`**, т.е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен.

5. Если требуется задать персональные настройки проверки для данного разделяемого каталога, отличные от настроек по умолчанию (для всех модулей), то необходимо задать тег-идентификатор для модуля VFS SMB, контролирующего этот каталог:

   ```
   smb_spider:tag = <имя ресурса>
   ```

   Далее индивидуальные настройки контроля этого разделяемого каталога задаются в настройках SpIDer Guard для SMB в виде отдельной секции `[SMBSpider.Share.<имя ресурса>]`.

Чтобы добавить новую секцию параметров с тегом <*имя ресурса*> при помощи утилиты управления Dr.Web Ctl, достаточно использовать команду **drweb-ctl** `cfset SmbSpider.Share.`<*имя ресурса*>`.`<*параметр*> <*значение*>, например:

```
# drweb-ctl cfset SmbSpider.Share.UserFiles.OnAdware Quarantine
```

Данная команда добавит в файл конфигурации секцию `[SMBSpider.Share.UserFiles]`. Эта секция будет содержать все параметры проверки каталога, причем значения всех параметров, кроме параметра **OnAdware**, указанного в команде, будут совпадать со значениями параметров из общей секции `[SMBSpider]`.

6. Включите работу SpIDer Guard для SMB, задав для параметра **Start** значение `Yes`.

После внесения изменений в настройки следует перезапустить как сервер **Samba**, так и Dr.Web для файловых серверов UNIX. Для перезапуска Dr.Web для файловых серверов UNIX используйте команду **drweb-ctl** `reload`. Также вы можете выполнить перезапуск демона управления конфигурацией Dr.Web ConfigD (используйте команду **service** `drweb-configd restart`).

Для предотвращения возможных конфликтов между SpIDer Guard для SMB и SpIDer Guard при проверке файлов в разделяемых каталогах **Samba**, рекомендуется дополнительно настроить SpIDer Guard, выполнив одно из следующих действий:

- добавить разделяемые каталоги **Samba** в область исключения (перечислить эти каталоги в параметре **ExcludedPath**);
- добавить процесс **Samba** (**smbd**) в список игнорируемых процессов (указать `smbd` в параметре **ExcludedProc**).

Сценарии поддержки интеграции

Для удобства настройки интеграции SpIDer Guard для SMB с файловым сервером **Samba** поставляются специальные файлы сценариев оболочки для настройки интеграции. Они расположены в каталоге <*opt_dir*>`/share/drweb-smbspider-modules`:

Файл сценария	Назначение
`drweb_smbspider_configure.sh`	Сценарий, вносящий в диалоговом режиме изменения в файл конфигурации сервера **Samba** `smb.conf` (подключающий для наблюдения разделяемые каталоги, описанные в файле).
`update-links.sh`	Сценарий, создающий/обновляющий ссылку на модуль VFS SMB Dr.Web в каталоге сервера **Samba**
`vfs-versions.sh`	Вспомогательный сценарий, определяющий требуемую версию модуля VFS SMB Dr.Web, используется сценарием `update-links.sh`

Сценарий оболочки `update-links.sh` автоматически запускается сразу при установке продукта. При необходимости вы можете запускать его в дальнейшем также вручную. Сценарий `drweb_smbspider_configure.sh` запускается автоматически в случае установки продукта из универсального пакета, его рекомендуется запустить вручную после установки продукта, если продукт был установлен из репозитория, или если вы отказались от его запуска при установке. Он может быть запущен неоднократно, по мере необходимости добавления и удаления каталогов из-под наблюдения. Этот сценарий сохраняет оригинальную (не измененную) копию файла конфигурации сервера **Samba** `smb.conf`, добавляя к его имени расширение `.drwebsave`.

Интеграция с томами NSS

Для интеграции Dr.Web для файловых серверов UNIX с томами **Novell Storage Services** необходимо задать значения ряда параметров, находящихся в секции `[NSS]` конфигурационного файла:

- В параметре **`NssVolumesMountDir`** укажите путь к каталогу файловой системы, в который смонтированы тома файловой системы **NSS** (по умолчанию используется путь `/media/nss`).
- В параметре **`ProtectedVolumes`** перечислите имена томов файловой системы **NSS**, находящихся в каталоге, указанном в параметре **`NssVolumesMountDir`**, и подлежащих защите. Если параметр оставить пустым, то защите будут подлежать все тома, присутствующие в каталоге, указанном в параметре **`NssVolumesMountDir`**.
- При необходимости, задавая значения параметров **`ExcludedPath`** и **`IncludedPath`**, определите пути к объектам, находящимся на защищаемых томах, которые должен быть исключены из проверки и наоборот, проверяться монитором SpIDer Guard для NSS. Допускается указание путей как к каталогам, так и к конкретным файлам. Если указан каталог, то будет пропускаться или проверяться всё содержимое этого каталога. Обратите внимание, что параметр **`IncludedPath`** имеет приоритет над параметром **`ExcludedPath`**, т.е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен. Параметры **`IncludedPath`** и **`ExcludedPath`** допускают использование файловых масок (*wildcards*). Регистрозависимость путей, указываемых в этих параметрах, определяется настройками **NSS**.
- Включите работу SpIDer Guard для NSS, задав для параметра **`Start`** значение `Yes`.

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

Краткие инструкции

Как подключить Dr.Web для файловых серверов UNIX к серверу Samba

Следуйте инструкции, представленной в разделе Интеграция с файловым сервером Samba.

Как подключить Dr.Web для файловых серверов UNIX к Novell Storage Services

Следуйте инструкции, представленной в разделе Интеграция с томами NSS.

Как настроить мониторинг файловой системы GNU/Linux

Следуйте инструкции, представленной в разделе Настройка мониторинга файловой системы.

Как перезапустить программный комплекс Dr.Web для файловых серверов 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 файловых серверов 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
`start`	Запустить Dr.Web ConfigD, если он еще не запущен. При запуске Dr.Web ConfigD запустит все необходимые модули комплекса Dr.Web для файловых серверов UNIX.
`stop`	Завершить работу Dr.Web ConfigD, если он запущен. При завершении работы Dr.Web ConfigD завершит работу всех модулей комплекса Dr.Web для файловых серверов UNIX.
`restart`	Перезапустить (завершить и запустить) Dr.Web ConfigD. Dr.Web ConfigD, соответственно, завершит и запустит все модули комплекса Dr.Web для файловых серверов UNIX. Если Dr.Web ConfigD не был запущен, равносильно start.
`condrestart`	Перезапустить Dr.Web ConfigD только в том случае, если он был запущен.

Параметр	Описание
`reload`	Послать Dr.Web ConfigD сигнал HUP, если он запущен. Dr.Web ConfigD перешлет этот сигнал всем модулям комплекса Dr.Web для файловых серверов UNIX. Используется для инициации процесса перечитывания конфигурации всеми компонентами комплекса.
`status`	Вывести на консоль текущее состояние Dr.Web ConfigD.

Для перезапуска (или запуска, если он не был запущен) программного комплекса Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 добавить новый разделяемый каталог SMB

1. Отредактируйте конфигурационный файл сервера **Samba** `smb.conf`, добавив в него секцию описания разделяемого каталога. Секция разделяемого каталога должна иметь вид:

```
[<имя ресурса>]
comment = <комментарий>
path = <путь к защищаемому каталогу>
vfs objects = smb_spider
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

где *<имя ресурса>* – любое имя разделяемого ресурса, а *<комментарий>* – произвольная строка-комментарий (не обязательно).

2. Если требуется задать для добавленного разделяемого каталога настройки проверки, отличающиеся от заданных для SpIDer Guard для SMB по умолчанию, воспользуйтесь пунктами 3 и 4 инструкции, приведенной в разделе Интеграция с файловым сервером Samba.
3. Перезапустите сервер **Samba** и программный комплекс Dr.Web для файловых серверов UNIX.

Как добавить новый защищаемый том NSS

1. Укажите имя тома, подлежащего защите, в параметре **`ProtectedVolumes`** (находится в секции `[NSS]` конфигурационного файла). Если параметр сделать пустым, то защите будут подлежать все тома, присутствующие в каталоге, указанном в параметре **`NssVolumesMountDir`**.
2. Перезапустите программный комплекс Dr.Web для файловых серверов UNIX.

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

	Аргументы: <*путь к файлу*> – путь к файлу, в котором следует сохранить идентификатор процесса (PID).

Пример:

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

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 файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

`DefaultLogLevel` *{уровень подробности}*	Определяет уровень подробности ведения журнала *для всех* компонентов продукта Dr.Web для файловых серверов UNIX по умолчанию. *Используется, если в конфигурации какого-либо из компонентов не указан свой уровень подробности ведения журнала.* **Значение по умолчанию:** `Notice`
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента Dr.Web ConfigD. **Значение по умолчанию:** `Notice`
`Log` *{тип журнала}*	Метод ведения журнала демона управления конфигурацией, а также метод ведения журнала для тех компонентов, у которых не указан свой собственный метод ведения журнала.

	Обратите внимание, что при начальной загрузке, пока конфигурационный файл еще не прочитан, демон управления конфигурацией будет использовать следующие значения этого параметра: • В режиме демона (если был запущен с параметром `-d`) – `SYSLOG:Daemon` • В ином случае – `Stderr` Если компонент работает в фоновом режиме (запущен с параметром командной строки `-d`), значение `Stderr` *не может* быть использовано для данного параметра. **Значение по умолчанию:** `Syslog:Daemon`
PublicSocketPath *{путь к файлу}*	Путь к сокету, используемому для взаимодействия всех компонентов Dr.Web для файловых серверов UNIX. **Значение по умолчанию:** `/var/run/.com.drweb.public`
AdminSocketPath *{путь к файлу}*	Путь к сокету, используемому для взаимодействия компонентов Dr.Web для файловых серверов UNIX, обладающих повышенными (административными) полномочиями. **Значение по умолчанию:** `/var/run/.com.drweb.admin`
CoreEnginePath *{путь к файлу}*	Путь к динамической библиотеке антивирусного ядра Dr.Web Virus-Finding Engine. **Значение по умолчанию:** <*var_dir*>`/lib/drweb32.dll` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/lib/drweb32.dll` • Для **FreeBSD**: `/var/drweb.com/lib/drweb32.dll`
VirusBaseDir *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы вирусных баз. **Значение по умолчанию:** <*var_dir*>`/bases` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/bases` • Для **FreeBSD**: `/var/drweb.com/bases`
KeyPath *{путь к файлу}*	Путь к ключевому файлу продукта (лицензионному или демонстрационному). **Значение по умолчанию:** <*etc_dir*>`/drweb32.key` • Для **Linux**, **Solaris**: `/etc/opt/drweb.com/drweb32.key` • Для **FreeBSD**: `/usr/local/etc/drweb.com/drweb32.key`
CacheDir *{путь к каталогу}*	Путь к каталогу кэша (используется как для кэша обновлений, так и для кэша проверенных файлов). **Значение по умолчанию:** <*var_dir*>`/cache` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/cache` • Для **FreeBSD**: `/var/drweb.com/cache`

TempDir *{путь к каталогу}*	Путь к каталогу для хранения временных файлов. **Значение по умолчанию:** *Путь, извлеченный из системной переменной окружения* `TMPDIR`, `TMP`, `TEMP` *или* `TEMPDIR` *(переменные перебираются в указанном порядке). Если ни одна из них не обнаружена, то* `/tmp`.
RunDir *{путь к каталогу}*	Путь к каталогу, в котором находятся PID-файлы запущенных компонентов и сокеты, используемые для взаимодействия компонентов продукта. **Значение по умолчанию:** `/var/run`
VarLibDir *{путь к каталогу}*	Путь к каталогу библиотек, используемых компонентами продукта. **Значение по умолчанию:** <*var_dir*>`/lib` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/lib` • Для **FreeBSD**: `/var/drweb.com/lib`
VersionDir *{путь к каталогу}*	Путь к каталогу, в котором хранится информация о текущих версиях используемых компонентов Dr.Web для файловых серверов UNIX. **Значение по умолчанию:** <*var_dir*>`/version` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/version` • Для **FreeBSD**: `/var/drweb.com/version`
DwsDir *{путь к каталогу}*	Параметр не используется. **Значение по умолчанию:** <*var_dir*>`/dws` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/dws` • Для **FreeBSD**: `/var/drweb.com/dws`
AdminGroup *{имя группы | GID}*	Группа пользователей, обладающих административными правами в рамках Dr.Web для файловых серверов UNIX. Данные пользователи наряду с суперпользователем *root* могут повышать полномочия компонентов Dr.Web для файловых серверов UNIX до полномочий суперпользователя. **Значение по умолчанию:** *Определяется автоматически в момент установки продукта.*
TrustedGroup *{имя группы | GID}*	Параметр не используется. **Значение по умолчанию:** `drweb`
DebugIpc *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = `DEBUG`) подробные сообщения IPC (взаимодействие демона управления конфигурацией с другими компонентами). **Значение по умолчанию:** `No`
UseCloud	Использовать обращение к сервису Dr.Web Cloud для получения сведений о вредоносности файлов и URL.

{логический}	**Значение по умолчанию:** `No`
`AntispamCorePath` *{путь к файлу}*	Параметр не используется. **Значение по умолчанию:** <*var_dir*>`/lib/vaderetro.so` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/lib/vaderetro.so` • Для **FreeBSD**: `/var/drweb.com/lib/vaderetro.so`
`VersionNotification` *{логический}*	Уведомлять пользователя о наличии обновлений для обновления текущей установленной версии продукта. **Значение по умолчанию:** `Yes`

Dr.Web Ctl

Программный комплекс Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 команды. Не являются обязательными для запуска.
- <*команда*> – команда, которая должна быть выполнена Dr.Web для файловых серверов 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: `$ drweb-ctl <команда> -h`
`-v, --version`	Вывести на экран версию модуля и завершить работу
`-d, --debug`	Предписывает выводить на экран расширенные диагностические сообщения во время выполнения указанной команды. Не имеет смысла без указания команды. Используйте вызов: `$ drweb-ctl <команда> -d`

3. Команды

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

Команда	Описание
	 При использовании опций `--stdin` и `--stdin0` пути в списке не должны содержать шаблонов. Предпочтительное использование опций `--stdin` и `--stdin0` – обработка в команде `scan` списка путей, сформированного внешней программой, например – **find** (см. Примеры использования). `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--PackerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ArchiveMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MailMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ContainerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MaxCompressionRatio` <*степень*> – установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее *2*. **Значение по умолчанию:** *3000* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** *On*

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

Команда	Описание
`bootscan <устройство> | ALL`	**Назначение:** Инициировать проверку компонентом проверки файлов Dr.Web File Checker загрузочной записи на указанных дисковых устройствах. Проверяются как записи MBR, так и записи VBR. **Аргументы:** <*устройство*> – путь к блочному файлу дискового устройства, загрузочная запись на котором подлежит проверке. Может быть указано несколько дисковых устройств через пробел. Обязательный аргумент. Если вместо файла устройства указано `ALL`, будут проверены все загрузочные записи на всех доступных дисковых устройствах. **Опции:** `-a [--Autonomous]` – запустить отдельную копию Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением. `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** *On* `--Cure` <*Yes*|*No*> – требуется ли делать попытки лечения обнаруженных угроз. Если указано *No*, то производится только информирование об обнаруженной угрозе. **Значение по умолчанию:** *No* `--ShellTrace` – включить вывод дополнительной отладочной информации при проверке загрузочной записи.
`procscan`	**Назначение:** Инициировать проверку компонентом проверки файлов Dr.Web File Checker содержимого исполняемых файлов, содержащих код процессов, запущенных в системе. При обнаружении угрозы выполняется

Команда	Описание
	не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него. **Аргументы:** Нет. **Опции:** `-a [--Autonomous]` – запустить отдельную копию Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если продукт работает под его управлением. `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** *On* `--PackerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--OnKnownVirus` <*действие*> – действие, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза. **Возможные действия:** *REPORT, CURE, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnIncurable` <*действие*> – действие, которое следует выполнить в случае если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnSuspicious` <*действие*> – действие, которое следует выполнить в случае если эвристический анализ обнаружит подозрительный объект. **Возможные действия:** *REPORT, QUARANTINE, DELETE*.

Команда	Описание
	Значение по умолчанию: *REPORT* `--OnAdware` <*действие*> – действие, которое следует выполнить в случае если обнаружена рекламная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnDialers` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа дозвона. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnJokes` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа-шутка. **Возможные действия**: *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnRiskware` <*действие*> – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnHacktools` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа взлома. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* *Обратите внимание, что при обнаружении угроз в исполняемом файле все запущенные из него процессы принудительно завершаются Dr.Web для файловых серверов UNIX.*
`netscan` <*путь*>	**Назначение:** Инициировать распределенную проверку указанного файла или каталога через агент сетевой проверки данных Dr.Web Network Checker. Если настроенные соединения с другими узлами, на которых имеется продукт Dr.Web для UNIX, поддерживающий функцию распределенной проверки, отсутствуют, то будет произведена проверка с использованием сканирующего ядра, доступного локально (аналогично команде `scan`). **Аргументы:** <*путь*> – путь к файлу или каталогу, который нужно проверить. **Опции:** `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет.

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

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

Команда	Описание
	`--OnIncurable` <*действие*> – действие, которое следует выполнить в случае если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnSuspicious` <*действие*> – действие, которое следует выполнить в случае если эвристический анализ обнаружит подозрительный объект. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnAdware` <*действие*> – действие, которое следует выполнить в случае если обнаружена рекламная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnDialers` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа дозвона. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnJokes` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа-шутка. **Возможные действия**: *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnRiskware` <*действие*> – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* `--OnHacktools` <*действие*> – действие, которое следует выполнить в случае если обнаружена программа взлома. **Возможные действия:** *REPORT, QUARANTINE, DELETE*. **Значение по умолчанию:** *REPORT* Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т.п.), вместо удаления (*DELETE*) выполняется перемещение контейнера в карантин (*QUARANTINE*).
`proxyscan` <*путь*>	**Назначение:** Инициировать проверку компонентом проверки файлов Dr.Web File Checker указанного файла или каталога с использованием метода проверки «proxy» (штатно этот метод проверки используется монитором SpIDer Guard для SMB и компонентом Dr.Web ClamD).

Команда	Описание
	 Обратите внимание, что угрозы, обнаруженные этим методом проверки, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). Для проверки файлов и каталогов рекомендуется использовать команду `scan`. **Аргументы:** <*путь*> – путь к файлу или каталогу, который нужно проверить. **Опции:** `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено. **Значение по умолчанию:** *0* `--HeuristicAnalysis` <*On|Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** *On* `--PackerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ArchiveMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MailMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ContainerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены.

Команда	Описание
	Значение по умолчанию: *8* `--MaxCompressionRatio <степень>` – установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее *2*. **Значение по умолчанию:** *3000*
`rawscan <путь>`	**Назначение:** Инициировать «сырую» проверку указанного файла или каталога, с использованием сканирующего ядра Dr.Web Scanning Engine напрямую, без использования компонента проверки файлов Dr.Web File Checker. ⚠ Обратите внимание, что угрозы, обнаруженные при «сыром» сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). 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`. **Аргументы:** `<путь>` – путь к файлу или каталогу, который нужно проверить. **Опции:** `--ScanEngine <путь>` – путь к UNIX-сокету сканирующего ядра Dr.Web Scanning Engine. Если не указан, то для проверки будет запущена автономная копия сканирующего ядра (будет завершена после завершения проверки). `--Report <тип>` – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout <число>` – установить тайм-аут на проверку одного файла в мс. Значение *0* указывает, что время проверки не ограничено.

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

Команда	Описание
	 Обратите внимание, что угрозы, обнаруженные при удаленном сканировании, не будут нейтрализованы, а также они не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). Вы можете использовать эту команду только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров и прочих «умных» устройств вы можете воспользоваться механизмом обновления прошивки, а для вычислительных машин – выполнив подключение к ним (в том числе – в удаленном терминальном режиме) и произведя соответствующие операции в их файловой системе (удаление или перемещение файлов и т.п.) или запустив антивирусное ПО, установленное на них. **Аргументы:** <*узел*> – IP-адрес или доменное имя узла, к которому необходимо подключиться для проверки. <*путь*> – путь к файлу или каталогу, который нужно проверить. **Опции:** `-l [--Login]` <*имя*> – логин (имя пользователя) для авторизации на удаленном узле через SSH. *Если имя пользователя не указано, будет произведена попытка подключиться к удаленному узлу от имени пользователя, запустившего команду.* `-i [--Identity]` <*путь к файлу*> – файл закрытого ключа для аутентификации указанного пользователя через SSH. `-p [--Port]` <*число*> – номер порта на удаленном узле для подключения через SSH. **Значение по умолчанию:** *22* `--Password` <*пароль*> – пароль для аутентификации указанного пользователя через SSH. *Обратите внимание, что пароль передается в открытом виде.* `--Report` <*тип*> – установить тип отчета о проверке. **Возможные значения:** • `BRIEF` – краткий отчет.

Команда	Описание
	• `DEBUG` – подробный отчет. **Значение по умолчанию:** *BRIEF* `--ScanTimeout` <*число*> – установить тайм-аут на проверку одного файла в мс. Значение 0 указывает, что время проверки не ограничено. **Значение по умолчанию:** 0 `--PackerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ArchiveMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MailMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке почтовых файлов (pst, tbb и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--ContainerMaxLevel` <*число*> – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.). Значение *0* указывает, что вложенные объекты будут пропущены. **Значение по умолчанию:** *8* `--MaxCompressionRatio` <*степень*> – установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее *2*. **Значение по умолчанию:** *3000* `--HeuristicAnalysis` <*On*|*Off*> – использовать ли эвристический анализ при проверке. **Значение по умолчанию:** `On`

3.2. Команды управления обновлением и работой в режиме централизованной защиты

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

Команда	Описание
`update`	**Назначение:** Инициировать процесс обновления антивирусных компонентов (вирусных баз и антивирусного ядра, и прочих, в зависимости от поставки) с серверов обновлений компании «Доктор Веб»
`esconnect` <*сервер*>`[:`<*порт*>`]`	**Назначение:** Подключить Dr.Web для файловых серверов UNIX к указанному серверу централизованной защиты (например, Dr.Web Enterprise Server). О режимах работы см. в разделе Режимы работы. **Аргументы:** • <*сервер*> – IP-адрес или имя узла в сети, на котором располагается сервер централизованной защиты. Обязательный аргумент. • <*порт*> – номер порта, используемого сервером централизованной защиты. Необязательный аргумент, указывается только в случае, если сервер централизованной защиты использует нестандартный порт. **Опции:** `--Key` <*путь*> – путь к файлу публичного ключа сервера централизованной защиты, к которому производится подключение. `--Login` <*ID*> – логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты. `--Password` <*пароль*> – пароль для подключения к серверу централизованной защиты. `--Group` <*ID*> – идентификатор группы на сервере, в которую следует поместить рабочую станцию при подключении. `--Rate` <*ID*> – идентификатор тарифной группы, которую следует применить к рабочей станции при ее включении в группу на сервере централизованной защиты (может быть указана только совместно с опцией `--Group`). `--Compress` <*On*|*Off*> – принудительно инициировать сжатие передаваемых данных (*On*) или запретить его (*Off*). Если опция не указана, использование сжатия определяется сервером. `--Encrypt` <*On*|*Off*> – принудительно инициировать шифрование передаваемых данных (*On*) или запретить его (*Off*). Если опция не указана, использование шифрования определяется сервером. `--Newbie` – подключиться как «новичок» (получить новую учетную запись на сервере).

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

3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
`cfset` *<секция>*`.`*<параметр>* *<значение>*	**Назначение:** Изменить активное значение указанного параметра текущей конфигурации. *Обратите внимание, что знак равенства не используется.* **Аргументы:** • *<секция>* – имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент. • *<параметр>* – имя изменяемого параметра. Обязательный аргумент. • *<значение>* – значение, которое следует присвоить изменяемому параметру. Обязательный аргумент. *Для задания значения параметров всегда используется формат <секция>.<параметр> <значение>.*

Команда	Описание
	Обратите внимание, что если вы хотите задать несколько значений параметра, то нужно повторить вызов команды `cfset` *столько раз, сколько значений параметра вы хотите добавить. При этом для добавления нового значения в список значений параметра необходимо использовать опцию* `-a` *(см. ниже). Нельзя использовать вариант команды <параметр> значение1, значение2, так как строка значение1, значение2 будет считаться единым значением параметра.* *Описание конфигурационного файла доступно в разделе* Приложение Г. Конфигурационный файл программного комплекса*, а также в документации* **man** `5 drweb.ini`. **Опции:** `-a [--Add]` – не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). Также эту опцию следует использовать для добавления новых групп параметров с тегом. `-e [--Erase]` – не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). Также эту опцию можно использовать для удаления группы параметров с тегом целиком. `-r [--Reset]` – сбросить параметр в значение по умолчанию. <*значение*> в этом случае в команде не указывается, а если указано – игнорируется. Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе – список значений) заменяется на указанное значение. *Для секций, описывающих индивидуальные параметры точек подключения компонента* Dr.Web ClamD *и разделяемых каталогов для монитора* SpIDer Guard для SMB*, применение опции* `-r` *приводит к замене значения параметра в индивидуальной секции на значение, указанное у соответствующего «родительского» параметра в секции настроек компонента.* Если требуется добавить новую точку подключения <*point*> для Dr.Web ClamD или секцию параметров для разделяемого каталога **Samba** с тегом <*tag*>, используйте команду: `cfset ClamD.Endpoint.<point> -a`, например: `cfset ClamD.Endpoint.point1 -a` `cfset SmbSpider.Share.<tag> -a`, например: `cfset SmbSpider.Share.BuhFiles -a`

Команда	Описание
	Для выполнения этой команды требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды **su** или **sudo**.
`cfshow [<секция>] [.<параметр>]`	**Назначение:** Вывести на экран параметры текущей конфигурации программного комплекса. Для вывода параметров по умолчанию используется формат <*секция*>.<*параметр*> = <*значение*>. Секции и параметры не установленных компонентов по умолчанию не выводятся. **Аргументы:** • <*секция*> – имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла. • <*параметр*> – имя выводимого параметра. Необязательный аргумент. Если не указан, выводятся все параметры указанной секции, в противном случае выводится только этот параметр. Если указан без имени секции, то выводятся все вхождения этого параметра во все секции конфигурационного файла. **Опции:** `--Uncut` – вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. В противном случае выводятся только те параметры, которые используются имеющимися компонентами. `--Changed` – вывести только те параметры, для которых заданы значения, отличающиеся от значений по умолчанию. `--Ini` – вывести значения параметров в формате INI-файла: сначала в отдельной строке выводится имя секции, заключенное в квадратные скобки, после чего параметры, принадлежащие секции, перечисляются в виде пар <*параметр*> = <*значение*> (по одному в строке). `--Value` – вывести только значение указанного параметра. В этом случае аргумент <параметр> обязателен.
`reload`	**Назначение:** Послать сигнал `SIGHUP` демону управления конфигурацией Dr.Web ConfigD. Получив этот сигнал, Dr.Web ConfigD перечитывает конфигурацию и рассылает ее изменения всем компонентам Dr.Web для файловых серверов UNIX; переоткрывает журнал программного комплекса; перезагружает компоненты, использующие вирусные базы (включая антивирусное ядро), а также пытается перезапустить компоненты, работа которых была нештатно завершена.

Команда	Описание
	Аргументы: Нет. **Опции:** Нет.

3.4. Команды управления угрозами и карантином

Доступны следующие команды управления угрозами и карантином:

Команда	Описание
`threats [<действие> <объект>]`	**Назначение:** Выполнить указанное действие с обнаруженными ранее угрозами по их идентификаторам. Тип действия определяется указанной опцией команды. Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. Для каждой угрозы выводится следующая информация: • Идентификатор, присвоенный угрозе (порядковый номер) • Полный путь к инфицированному файлу • Информация об угрозе (имя, тип по классификации компании «Доктор Веб») • Информация о файле: размер, пользователь-владелец, дата последнего изменения • История действий с инфицированным файлом: обнаружение, применявшиеся действия и т.п. **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (CTRL+C прерывает ожидание). *Если эта опция указана совместно с любой из опций-действий, она игнорируется.* `--Cure` <*список угроз*> – выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Quarantine` <*список угроз*> – выполнить перемещение в карантин перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Delete` <*список угроз*> – выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Ignore` <*список угроз*> – игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую).

Команда	Описание
	Если требуется применить данную команду ко всем обнаруженным угрозам, вместо <*список угроз*> следует указать `All`. Например, команда: `$ drweb-ctl threats --Quarantine All` перемещает в карантин все обнаруженные объекты с угрозами.
`quarantine [<действие> <объект>]`	**Назначение:** Применить действие к указанному объекту, находящемуся в карантине. Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине, с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в карантин. Для каждого изолированного объекта выводится следующая информация: • Идентификатор, присвоенный изолированному объекту в карантине • Исходный путь к файлу, перемещенному в карантин • Дата перемещения файла в карантин • Информация о файле: размер, пользователь-владелец, дата последнего изменения • Информация об угрозе (имя, тип по классификации компании «Доктор Веб») **Аргументы:** Нет. **Опции:** `-a [--Autonomous]` – запустить отдельную копию компонента проверки файлов Dr.Web File Checker для выполнения заданного действия с карантином, завершив его работу после окончания действия. *Эта опция может быть применена совместно с любой из опций, указанных ниже.* `--Delete` <*объект*> – удалить указанный объект из карантина. *Обратите внимание, что удаление из карантина – необратимая операция.* `--Cure` <*объект*> – попытаться вылечить указанный объект в карантине. *Обратите внимание, что, даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина следует воспользоваться командой восстановления* `--Restore`. `--Restore` <*объект*> – восстановить указанный объект из карантина в исходное место. *Обратите внимание, что для выполнения этой команды может потребоваться, чтобы* **drweb-ctl** *была запущена от имени*

Команда	Описание
	суперпользователя. Восстановить файл из карантина можно, даже если он инфицирован. `--TargetPath` <*путь*> – восстановить объект из карантина в указанное место: как файл с указанным именем, если <*путь*> – это путь к файлу, или в указанный каталог (если <*путь*> – это путь к каталогу). Применяется только совместно с командой восстановления `--Restore`. В качестве <*объект*> используется идентификатор объекта в карантине. Если требуется применить данную команду ко всем объектам, находящимся в карантине, вместо <*объект*> следует указать `All`. Например, команда: `$ drweb-ctl quarantine --Restore All` восстанавливает из карантина все имеющиеся в нем объекты. *Обратите внимание, что для варианта* `--Restore All` *дополнительная опция* `--TargetPath`*, если указана, должна задавать путь к каталогу, а не к файлу.*
`nss_threats [`<*действие*> <*объект*>`]`	**Назначение:** Выполнить указанное действие с обнаруженными ранее на томах NSS угрозами по их идентификаторам. Тип действия определяется указанной опцией команды. Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. Выводится тот же перечень информации об угрозах, что и в вызове команды `threats` (см. выше), возможно, дополненный или модифицированный с учетом особенностей хранилища NSS. Для выполнения этой команды требуется, чтобы был установлен и запущен SpIDer Guard для NSS. **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (нажатие CTRL+C прерывает ожидание). `--Cure` <*список угроз*> – выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Quarantine` <*список угроз*> – выполнить перемещение в карантин NSS перечисленных угроз (идентификаторы угроз перечисляются через запятую) `--Delete` <*список угроз*> – выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую).

Команда	Описание
	`--Ignore` <*список угроз*> – игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить данную команду ко всем угрозам, обнаруженным на томах NSS, вместо <*список угроз*> следует указать `All`. Например, команда: `$ drweb-ctl nss_threats --Quarantine All` перемещает в карантин NSS все обнаруженные объекты с угрозами.
`nss_quarantine [`<*действие*> <*объект*>`]`	**Назначение:** Применить действие к указанному объекту, находящемуся в карантине на томах NSS. Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине NSS, с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в карантин. Выводится тот же перечень информации, что и в вызове команды `quarantine` (см. выше), возможно, дополненный или модифицированный с учетом особенностей хранилища NSS. Для выполнения этой команды требуется, чтобы был установлен и запущен SpIDer Guard для NSS. **Аргументы:** Нет. **Опции:** `--Delete` <*объект*> – удалить указанный объект из карантина NSS. *Обратите внимание, что удаление из карантина – необратимая операция.* `--Cure` <*объект*> – попытаться вылечить указанный объект в карантине NSS. *Обратите внимание, что, даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина следует воспользоваться командой восстановления* `--Restore`. `--Rescan` <*объект*> – повторно проверить указанный объект в карантине NSS. *Обратите внимание, что, даже если по результатам повторной проверки окажется, что объект не инфицирован, то он все равно останется в карантине. Для извлечения объекта из карантина следует воспользоваться командой восстановления* `--Restore`. `--Restore` <*объект*> – восстановить указанный объект из карантина NSS.

Команда	Описание
	Обратите внимание, что для выполнения этой команды может потребоваться, чтобы **drweb-ctl** *была запущена от имени суперпользователя. Восстановить файл из карантина можно, даже если он инфицирован.* `--TargetPath` <*путь*> – восстановить объект из карантина в указанное место: как файл с указанным именем, если <*путь*> – это путь к файлу, или в указанный каталог (если <*путь*> – это путь к каталогу). *Применяется только совместно с командой восстановления* `--Restore`. В качестве <*объект*> используется идентификатор объекта в карантине NSS. Если требуется применить данную команду ко всем объектам, находящимся в карантине NSS, вместо <*объект*> следует указать `All`. Например, команда: `$ drweb-ctl quarantine --Restore All` восстанавливает из карантина все имеющиеся в нем объекты. *Обратите внимание, что для варианта* `--Restore All` *дополнительная опция* `--TargetPath`*, если указана, должна задавать путь к каталогу, а не к файлу.*

Если в настройках SpIDer Guard для NSS для некоторого типа угроз указано действие *Quarantine*, то при восстановлении угрозы этого типа из карантина на том NSS при помощи команды `nss_quarantine`, она будет снова незамедлительно перемещена в карантин. Например, настройки по умолчанию

```
NSS.OnKnownVirus = Cure
NSS.OnIncurable = Quarantine
```

помещают все неизлечимые объекты в карантин. Поэтому, при восстановлении неизлечимого объекта из карантина на том NSS при помощи команды `nss_quarantine`, он будет снова незамедлительно перемещен в карантин.

3.5. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	**Назначение:** Вывести на экран информацию о работающих компонентах Dr.Web для файловых серверов UNIX. Для каждого запущенного компонента выводится следующая информация:

Команда	Описание
	• Внутреннее имя • Идентификатор процесса **GNU/Linux** (PID) • Состояние (запущен, остановлен и т.п.) • Код ошибки, если работа компонента завершена вследствие ошибки • Дополнительная информация (опционально). Для демона управления конфигурацией Dr.Web ConfigD в качестве дополнительной информации выводятся: • Перечень установленных компонентов – *Installed* • Перечень компонентов, запуск которых должен быть обеспечен демоном – *Should run*. **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об изменении состояния компонентов и выводить их на экран сразу, как только они будут поступать (нажатие CTRL+C прерывает ожидание).
`baseinfo`	**Назначение:** Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз. Выводится следующая информация: • Версия антивирусного ядра • Дата и время выпуска используемых вирусных баз • Число доступных вирусных записей • Момент последнего успешного обновления вирусных баз и антивирусного ядра • Момент следующего запланированного автоматического обновления **Аргументы:** Нет. **Опции:** Нет.
`certificate`	**Назначение:** Вывести на экран содержимое доверенного сертификата Dr.Web, который используется Dr.Web для файловых серверов UNIX. Для сохранения сертификата в файл <*cert_name*>`.pem` вы можете использовать команду: `$ drweb-ctl certificate > <cert_name>.pem` **Аргументы:** Нет. **Опции:** Нет.
`idpass` <*идентификатор*>	**Назначение:** Вывести на экран пароль, который был сгенерирован компонентом проверки сообщений электронной почты Dr.Web MailD для

Команда	Описание
	почтового сообщения с указанным идентификатором и использован для защиты вложенного архива с угрозами, вырезанными из письма (т.е. если в настройках компонента параметр **RepackPassword** был установлен в значение `HMAC(<secret>)`). **Аргументы:** • *<идентификатор>* – идентификатор сообщения электронной почты. **Опции:** `-s [--Secret]` *<secret>* – Секретное слово, использованное для генерации пароля архива. *Если секретное слово не указано при вызове команды, будет использовано текущее секретное слово <secret>, указанное в настройках Dr.Web MailD. Если при этом параметр* **RepackPassword** *отсутствует или установлен в значение, отличное от* `HMAC(<secret>)`*, команда вернет ошибку.*
`license`	**Назначение:** Вывести на экран информацию об активной лицензии, получить демонстрационную лицензию или получить ключевой файл для уже зарегистрированной лицензии (например – на сайте компании). Если не указана ни одна опция, то выводится следующая информация (если используется лицензия для одиночного режима работы): • Номер лицензии • Дата и время окончания действия лицензии Если используется лицензия, выданная сервером централизованной защиты (для работы в режиме централизованной защиты или в мобильном режиме), выводится соответствующая информация. **Аргументы:** Нет. **Опции:** `--GetRegistered` *<серийный номер>* – получить лицензионный ключевой файл для указанного серийного номера, если не нарушены условия получения нового ключевого файла (например, программа не находится в режиме централизованной защиты, когда лицензией управляет сервер централизованной защиты). *Если серийный номер не является серийным номером демонстрационного периода, то он должен быть предварительно зарегистрирован на сайте компании.* Подробнее о лицензировании продуктов Dr.Web см. раздел Лицензирование. Для регистрации серийного номера требуется наличие подключения к сети Интернет.

Команда	Описание
`stat`	**Назначение:** Вывести на экран статистику работы компонентов, обрабатывающих файлы (нажатие CTRL+C или Q прерывает отображение статистики) или агента сетевой проверки данных Dr.Web Network Checker. В статистике отображается: • имя компонента, инициировавшего проверку файлов. • PID компонента. • усреднённое количество файлов, обрабатываемых в секунду за последнюю минуту, 5 минут, 15 минут. • процент использования кэша проверенных файлов. • среднее количество ошибок проверки в секунду. Для агента распределенной проверки на экран выводится: • перечень локальных клиентов, инициировавших сканирование. • перечень удаленных узлов, которым переданы файлы на сканирование. • перечень удаленных узлов, от которых получены файлы на сканирование. Для локальных клиентов агента распределенной проверки указывается имя и PID, а для удаленных – адрес и порт узла. Для каждого клиента, как локального, так и удаленного выводится: • среднее за секунду количество проверенных файлов. • среднее за секунду количество переданных и полученных байт. • среднее за секунду количество ошибок. **Аргументы:** Нет. **Опции:** `-n [--netcheck]` – Вывести на экран статистику работы агента сетевой проверки данных.

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 файлова передается команде **drweb-ctl** `scan` с параметром `--stdin` или `--stdin0`.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.3. Проверка дополнительных объектов

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

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

2. 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 файловых серверов UNIX. Она использует параметры, указанные в секции `[Root]`.

Веб-интерфейс управления Dr.Web

Веб-интерфейс управления Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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 компонентов, включенных в состав Dr.Web для файловых серверов 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 файловых серверов 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 (актуально только для файловых хранилищ, контролируемых SpIDer Guard для SMB).
- **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.

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 файловых серверов 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.
- Имя удаленного пользователя, поместившего файл в хранилище (актуально только для файловых хранилищ, контролируемых SpIDer Guard для SMB).
- 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.
	– Применить некоторое дополнительное действие к отмеченным файлам (выбирается из выпадающего списка). Доступны следующие дополнительные действия: • **В карантин** – Переместить файлы с угрозами в карантин • **Вылечить** – Попытаться вылечить угрозы • **Игнорировать** – Игнорировать угрозы, обнаруженные в отмеченных файлах, и удалить их из списка обнаруженных угроз

Обратите внимание, что для работами с угрозами, обнаруженными на томах NSS, требуется, чтобы был установлен и запущен SpIDer Guard для NSS.

Если в настройках монитора SpIDer Guard для NSS для некоторого типа угроз указано действие *Quarantine*, то при восстановлении угрозы этого типа из карантина на том NSS, она будет снова незамедлительно перемещена в карантин. Например, настройки монитора по умолчанию помещают все неизлечимые объекты в карантин. Поэтому, при восстановлении неизлечимого объекта из карантина на том NSS, он будет снова незамедлительно перемещен в карантин.

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 файловых серверов 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.

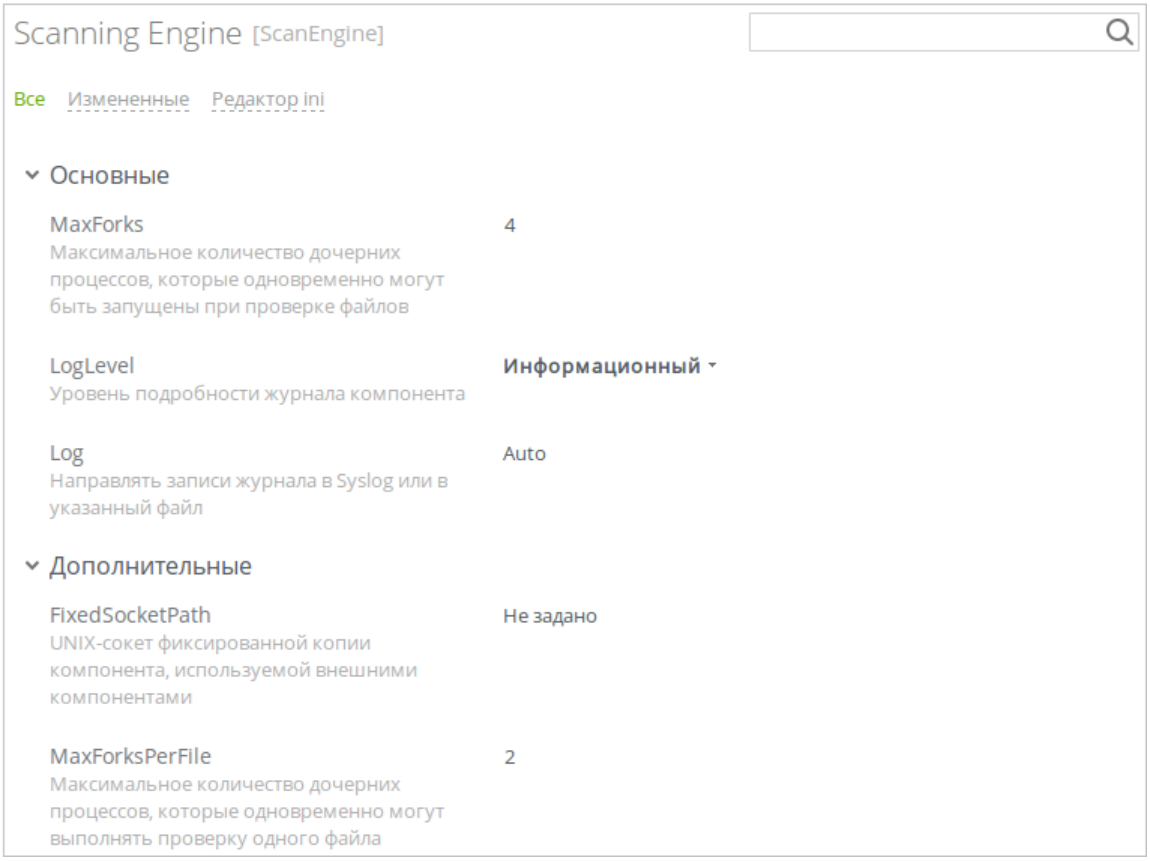

Рисунок 3. Представление настроек компонента в табличной форме

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.

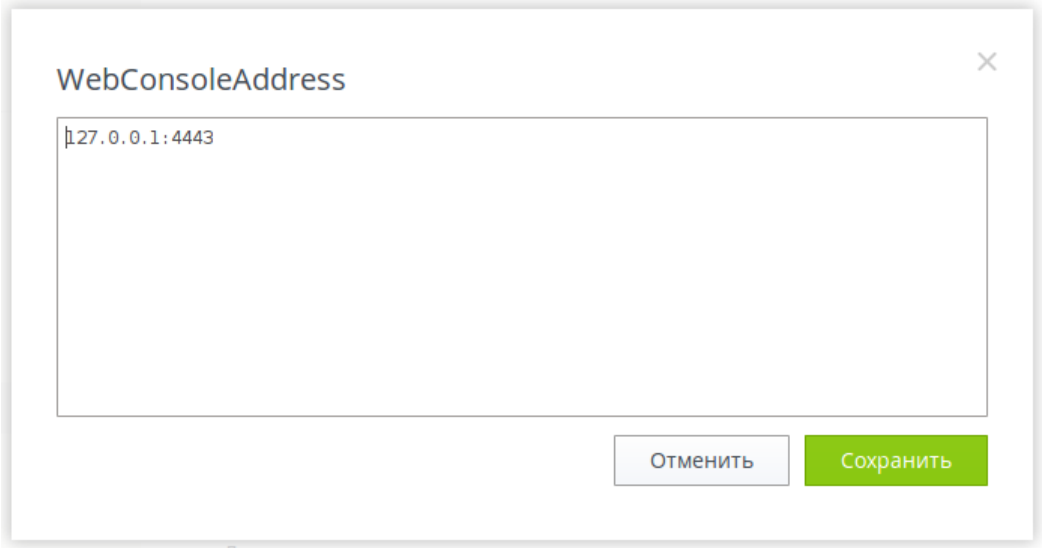

Рисунок 4. Редактирование списка значений

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 ✕ 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.

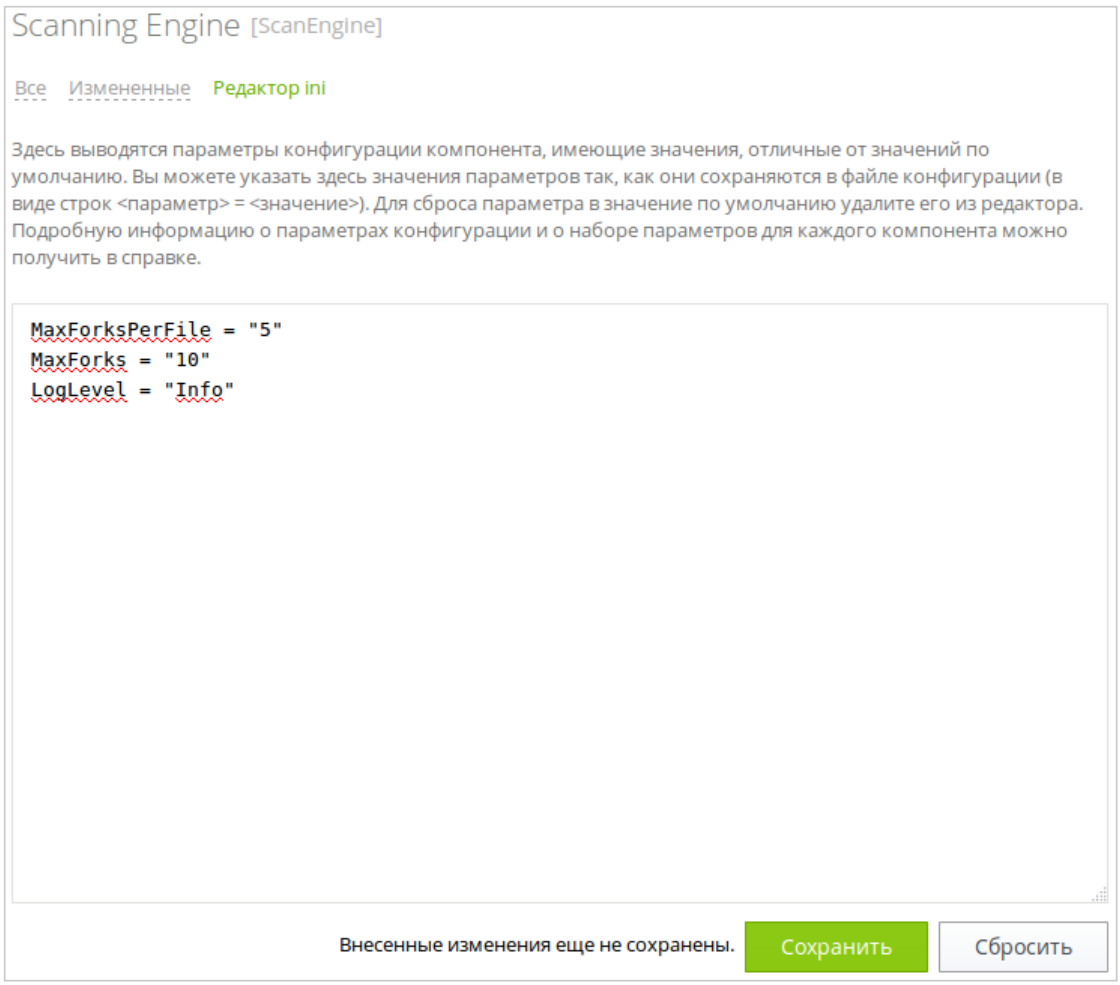

Рисунок 5. Редактор настроек для простого вида

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 SpIDer Guard.
- Параметры конфигурации компонента SpIDer Guard для NSS.
- Параметры конфигурации компонента SpIDer Guard для SMB.
- 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.
- Управление централизованной защитой.

Управление централизованной защитой

Вы можете подключить Dr.Web для файловых серверов 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 файловых серверов 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.

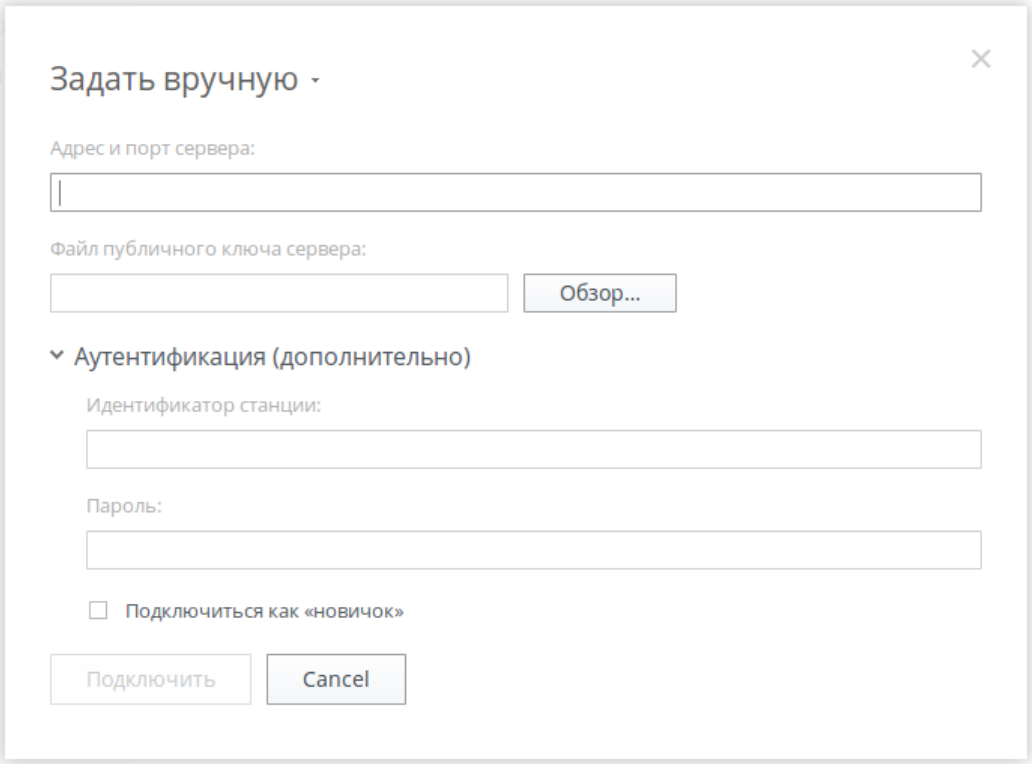

Рисунок 6. Окно подключения к серверу централизованной защиты

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 файловых серверов 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 файловых серверов 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.

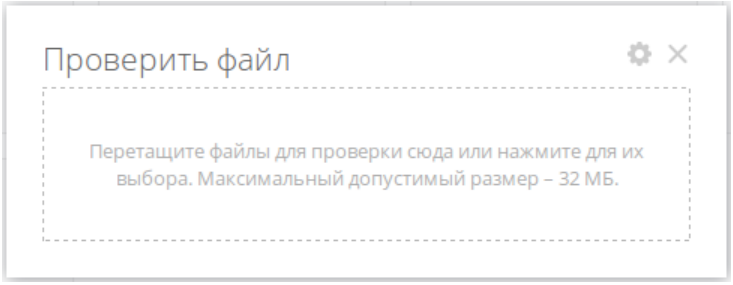

Рисунок 7. Панель проверки локальных файлов

Для закрытия панели следует нажать значок ✕ 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 север 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).

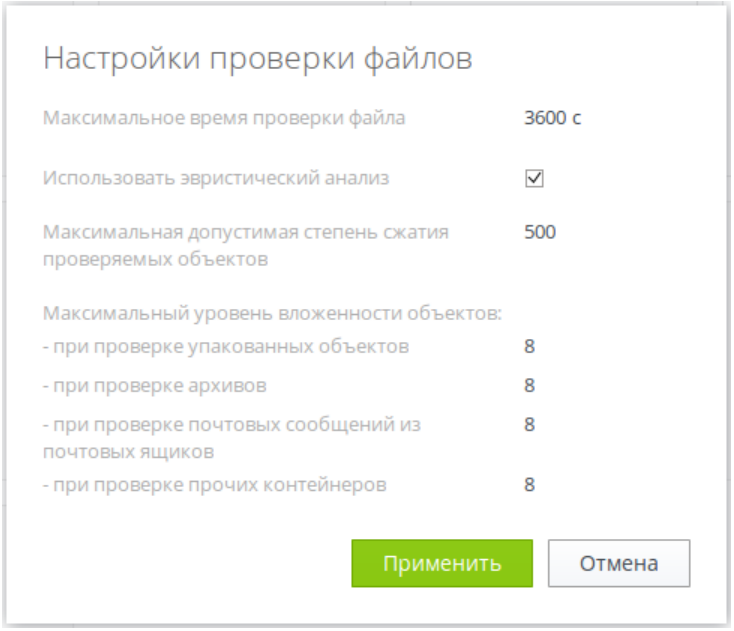

Рисунок 8. Настройка параметров проверки локальных файлов

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 файловых серверов UNIX и проверка по мере загрузки. В процессе загрузки и проверки файлов панель проверки отображает общий прогресс процесса проверки.

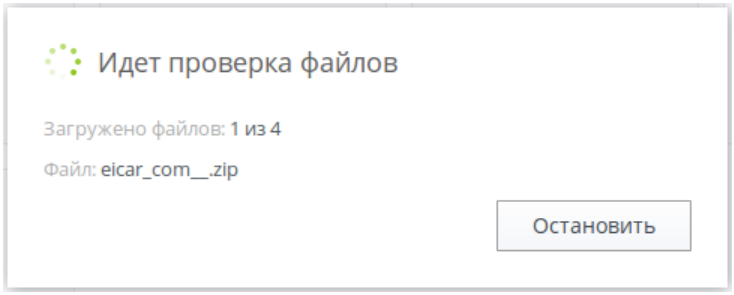

Рисунок 9. Прогресс проверки локальных файлов

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

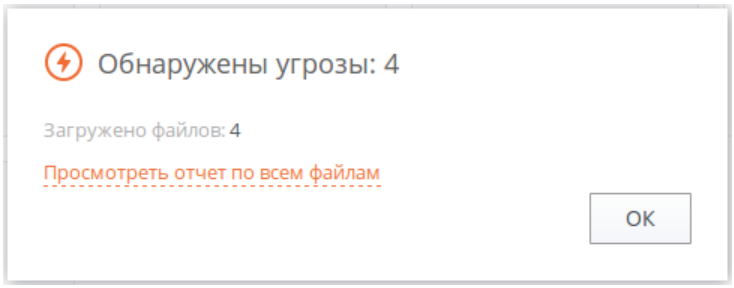

Рисунок 10. Результат проверки локальных файлов

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

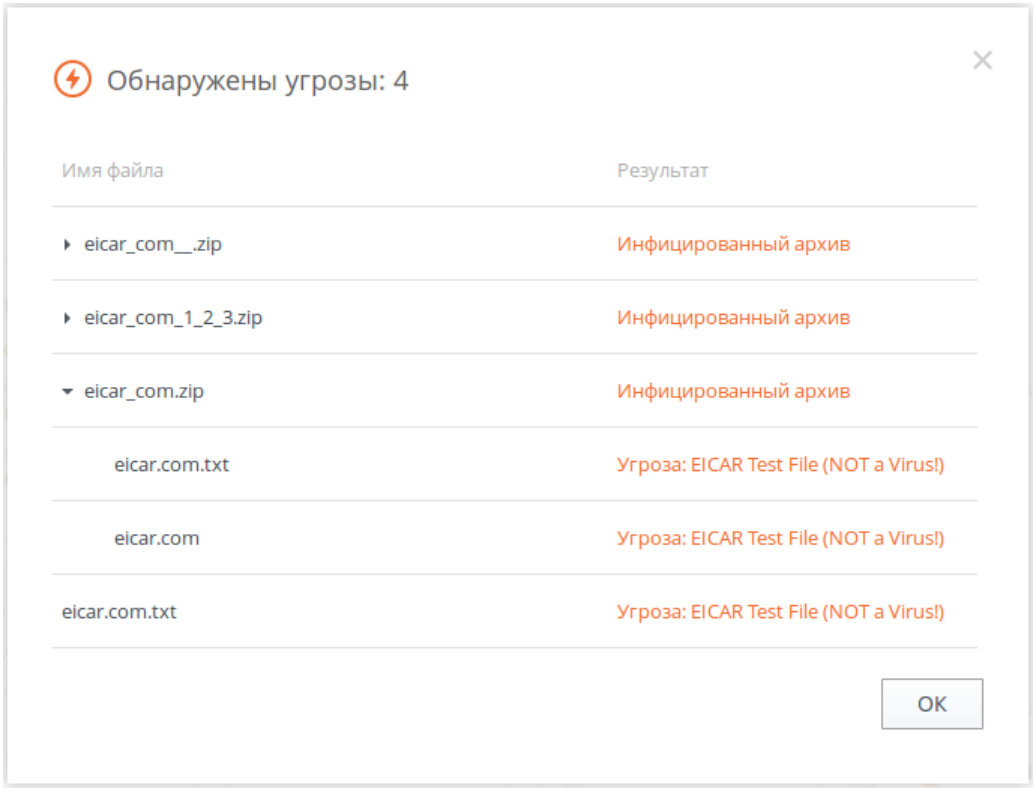

Рисунок 11. Расширенный отчет о проверке локальных файлов

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

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.

SpIDer Guard

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

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

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

Принципы работы

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

> Для ряда ОС модуль ядра поставляется совместно с SpIDer Guard уже в скомпилированном виде. В случае если для ОС, в которой используется SpIDer Guard, модуль ядра не поставляется в скомпилированном виде, используйте исходные коды модуля, предоставляемые компанией «Доктор Веб» для сборки и установки модуля ядра вручную (инструкция по сборке приведена в разделе Сборка модуля ядра для SpIDer Guard).

При обнаружении новых или измененных файлов монитор отправляет задание на их проверку компоненту проверки файлов Dr.Web File Checker, который, в свою очередь, инициирует их проверку сканирующим ядром Dr.Web Scanning Engine. Схема работы монитора показана на рисунке ниже.

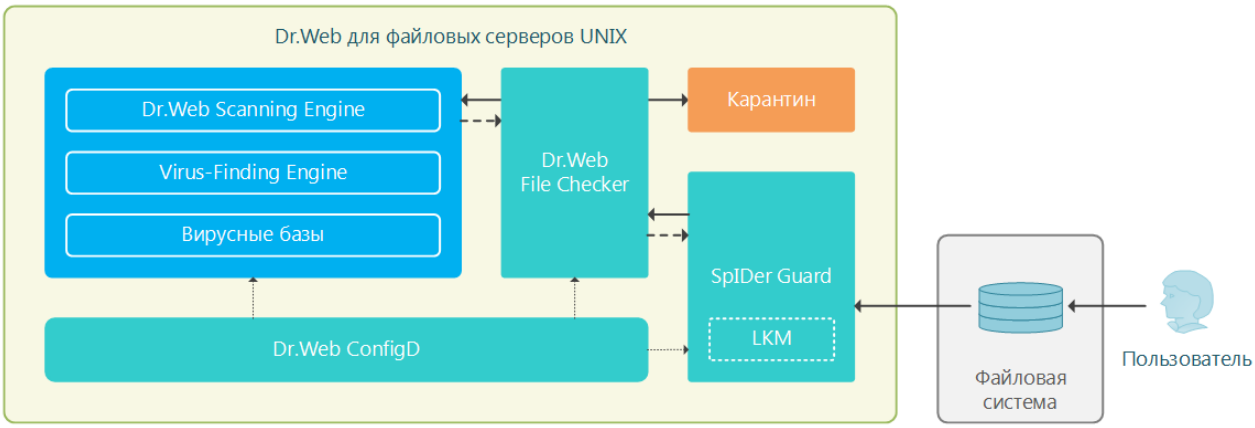

Рисунок 12. Схема работы компонента

Для определения областей файловой системы, подлежащих наблюдению, монитор файловой системы SpIDer Guard использует два параметра конфигурации:

- **`IncludedPath`** – содержит список путей, подлежащих мониторингу (*область наблюдения*).
- **`ExcludedPath`** – содержит список путей, которые требуется исключить из мониторинга (*область исключения*).

Таким образом, наблюдению подвергаются только те файлы, пути к которым принадлежат области наблюдения, определяемой списком **`IncludedPath`**, но не принадлежат области исключения, определяемой списком **`ExcludedPath`**. При этом, если один и тот же путь указан в обоих списках, то параметр **`IncludedPath`** имеет приоритет: объекты, расположенные по данному пути, будут находиться под контролем монитора файловой системы SpIDer Guard (подробнее об алгоритме определения принадлежности объекта области наблюдения или исключения см. ниже).

Пример:

Пусть в списках указаны следующие пути в файловой системе:

```
IncludedPath = /a, /b/c, /d/file1
ExcludedPath = /b, /d/file1, /b/c/file2
```

Тогда монитор файловой системы SpIDer Guard будет контролировать доступ:

- Ко всем файлам в каталоге `/a`.
- Ко всем файлам в каталоге `/b/c`, за исключением файла `file2`.
- К файлу `/d/file1`.

Файловые операции с остальными файлами в файловой системе монитор при данных настройках контролировать не будет.

Обратите внимание, что указание пути `/b` в списке **`ExcludedPath`** синтаксически корректно, но не имеет смысла: файлы по данному пути и так не будут находиться под наблюдением, потому что этот путь не входит в область наблюдения, задаваемую списком **`IncludedPath`**.

Использование исключений (включение объектов в список **ExcludedPath**) бывает необходимо, например, в случае если некоторые файлы часто изменяются, что порождает их постоянную перепроверку и тем самым нагружает систему. Если точно известно, что частое изменение файлов в некотором каталоге не является следствием вредоносной активности, а следствием работы некоторой доверенной программы, то можно добавить путь к этому каталогу, или изменяемым файлам в нем, в список исключений. В этом случае монитор файловой системы SpIDer Guard не будет реагировать на изменения этих файлов, даже если они принадлежат области наблюдения. Кроме того, имеется возможность указать и саму программу, работающую с файлами, в списке доверенных программ (параметр конфигурации **ExcludedProc**), тогда файловые операции, производимые этой программой, также не будут приводить к проверкам файлов, даже если эти файлы находятся в области наблюдения.

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

Определение принадлежности объекта области наблюдения

Для определения, подлежит некоторый объект файловой системы контролю или нет, монитор файловой системы SpIDer Guard, при обнаружении файловой операции, выполняет следующие действия:

1. Получает информацию о процессе, осуществившем операцию с файлом. Если исполняемый путь этого процесса (имя исполняемого файла с полным путем к нему) присутствует в списке **ExcludedProc**, то измененный объект не подлежит проверке, конец.
2. Иначе монитор получает полный путь к измененному объекту.
3. Полученный путь проверяется на совпадение с элементами списков **IncludedPath** и **ExcludedPath**.
4. Если путь совпадает с одним из элементов списка **IncludedPath**, то объект подлежит проверке, конец.
5. Если путь совпадает с одним из элементов списка **ExcludedPath**, то объект не подлежит проверке и операция с ним должна быть проигнорирована, конец.
6. Если путь не был найден ни в одном из списков, то он усекается «от конца к началу», т.е. производится подъем на один уровень выше к корню файловой системы.
7. Если полученный путь пуст, то конец, иначе возврат к пункту 3.

Это продолжается до тех пор, пока путь, полученный на очередной итерации, не совпадет с одним из элементов списков **IncludedPath** или **ExcludedPath**, либо пока не будет достигнут корень файловой системы.

Аргументы командной строки

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

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

SpIDer Guard допускает использование следующих параметров:

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

Пример:

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

Данная команда выведет на экран краткую справку компонента SpIDer Guard.

Замечания о запуске

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 пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой **drweb-ctl**).

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

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[LinuxSpider]` объединенного конфигурационного файла продукта Dr.Web для файловых серверов UNIX.

В секции представлены следующие параметры:

LogLevel *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **DefaultLogLevel** из секции [Root]. **Значение по умолчанию:** Notice
Log *{тип журнала}*	Метод ведения журнала
ExePath *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>/bin/drweb-spider • Для **Linux**: /opt/drweb.com/bin/drweb-spider
Start *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в Yes предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение No – немедленно завершить работу компонента. **Значение по умолчанию:** *Зависит от того, в составе какого продукта работает компонент.*
Mode *{LKM | FANOTIFY | AUTO}*	Определяет режим работы монитора файловой системы SpIDer Guard. **Возможные значения:** • LKM – Работа через LKM-модуль Dr.Web, установленный в ядро операционной системы (*LKM* – **Linux** *kernel module*). • FANOTIFY – Работа через системный механизм **fanotify**. • AUTO – Автоматическое определение оптимального режима работы.

	 Изменение значения этого параметра следует производить с крайней осторожностью, поскольку ядра различных ОС **GNU/Linux** в разной мере поддерживают тот и другой режим работы. Настоятельно рекомендуется оставлять этот параметр в значении `AUTO`, чтобы при запуске был выбран оптимальный режим интеграции с диспетчером файловой системы. При этом компонент сначала пытается использовать режим `FANOTIFY`, потом, в случае неудачи – `LKM`. Если не удалось использовать ни один из режимов, работа компонента завершается. При необходимости вы можете собрать LKM-модуль Dr.Web из исходных кодов и установить его в систему, следуя инструкции в разделе Сборка модуля ядра для SpIDer Guard. **Значение по умолчанию:** `AUTO`
`DebugAccess` *{логический}*	Включать или нет в журнал на отладочном уровне (при **`LogLevel`** = `DEBUG`) подробные сообщения о доступе к файлам. **Значение по умолчанию:** `No`
`ExcludedProc` *{путь к файлу}*	Определяет список процессов, файловая активность которых не контролируется. Если файловая операция была совершена любым из процессов, перечисленных здесь, то измененный или созданный файл не будет проверяться. *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 процессы **wget** и **curl**. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[LinuxSpider]` ` ExcludedProc = "/usr/bin/wget",` `"/usr/bin/curl"` • Две строки (по одному значению в строке) `[LinuxSpider]` ` ExcludedProc = /usr/bin/wget` ` ExcludedProc = /usr/bin/curl`

	2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/wget` `# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/curl` **Значение по умолчанию:** *(не задано)*
ExcludedPath *{путь к файлу или каталогу}*	Определяет путь к объекту, который должен быть пропущен при мониторинге файловых операций. Допускается указание пути как к каталогу, так и к конкретному файлу. Если указан каталог, то будут исключены из наблюдения все файлы этого каталога. *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 `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[LinuxSpider]` `ExcludedPath = "/etc/file1", "/usr/bin"` • Две строки (по одному значению в строке) `[LinuxSpider]` `ExcludedPath = /etc/file1` `ExcludedPath = /usr/bin` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset LinuxSpider.ExcludedPath -a /etc/file1` `# drweb-ctl cfset LinuxSpider.ExcludedPath -a /usr/bin` *Обратите внимание, что не имеет смысла указывать здесь пути к символическим ссылкам, поскольку при проверке файла всегда анализируется прямой путь к нему, поэтому указанные здесь символические ссылки не будут иметь никакого эффекта.* **Значение по умолчанию:** `/proc, /sys`
IncludedPath *{путь к файлу или каталогу}*	Определяет путь к объекту, который должен находиться под наблюдением и проверяться при совершении с ним файловых операций. Допускается указание пути как к каталогу, так и к конкретному файлу. Если указан каталог, то будут проверены все файлы и подкаталоги этого каталога, пути к которым отсутствуют в списке **ExcludedPath**.

	Этот параметр имеет приоритет над параметром **ExcludedPath** в этой же секции: если путь к одному и тому же объекту указан в обоих списках, то объект будет проверяться при совершении с ним файловых операций. *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 `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[LinuxSpider]` ` IncludedPath = "/etc/file1", "/usr/bin"` • Две строки (по одному значению в строке) `[LinuxSpider]` ` IncludedPath = /etc/file1` ` IncludedPath = /usr/bin` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset LinuxSpider.IncludedPath -a /etc/file1` `# drweb-ctl cfset LinuxSpider.IncludedPath -a /usr/bin` *Обратите внимание, что не имеет смысла указывать здесь пути к символическим ссылкам, поскольку при проверке файла всегда анализируется прямой путь к нему, поэтому указанные здесь символические ссылки не будут иметь никакого эффекта.* **Значение по умолчанию:** `/`
OnKnownVirus *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле известной угрозы (вируса и т.д.), обнаруженной методом сигнатурного анализа, при проверке файла, инициированной по запросу SpIDer Guard. **Возможные значения:** *Cure, Quarantine, Delete* **Значение по умолчанию:** `Cure`
OnIncurable *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на неудачу излечения угрозы (т.е. применение действия *Cure* закончилось неудачей) при проверке файла, инициированной по запросу SpIDer Guard.

	Возможные значения: *Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
`OnSuspicious` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле неизвестной угрозы (или подозрения на угрозу) методом эвристического анализа, при проверке файла, инициированной по запросу SpIDer Guard. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
`OnAdware` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле рекламной программы при проверке файла, инициированной по запросу SpIDer Guard. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
`OnDialers` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле программы автоматического дозвона при проверке файла, инициированной по запросу SpIDer Guard. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
`OnJokes` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле программы-шутки при проверке файла, инициированной по запросу SpIDer Guard. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`OnRiskware` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле условно-вредоносной («рискованной») программы при проверке файла, инициированной по запросу SpIDer Guard. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`OnHacktools` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле хакерской программы (средство удаленного доступа или управления, троянская программа и т.п.) при проверке файла, инициированной по запросу SpIDer Guard. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`

ScanTimeout *{интервал времени}*	Устанавливает тайм-аут на проверку одного файла по запросу SpIDer Guard. *Может быть указано значение в диапазоне от 1s до 1h.* **Значение по умолчанию:** `30s`
HeuristicAnalysis *{On | Off}*	Определяет, использовать ли эвристический анализ для поиска возможных неизвестных угроз при проверке файла, инициированной по запросу SpIDer Guard. Использование эвристического анализа повышает надежность проверки, но увеличивает её длительность. *Реакция на срабатывание эвристического анализа задается в параметре* **OnSuspicious**. **Возможные значения:** • `On` – Использовать эвристический анализ при проверке. • `Off` – Не использовать эвристический анализ. **Значение по умолчанию:** `On`
PackerMaxLevel *{целое число}*	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 Guard. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`
ArchiveMaxLevel *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке архивов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке файла, инициированной по запросу SpIDer Guard. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `0`
MailMaxLevel *{целое число}*	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 Guard. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `0`

ContainerMaxLevel *{целое число}*	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 Guard. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`
MaxCompressionRatio *{целое число}*	Устанавливает максимальную допустимую степень сжатия проверяемых объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке файла, инициированной по запросу SpIDer Guard. *Величина степени сжатия должна быть не менее 2.* **Значение по умолчанию:** `500`

Настройка мониторинга файловой системы

Инструкцию по настройке мониторинга файловой системы см. в разделе Настройка мониторинга файловой системы.

Использование модуля ядра для SpIDer Guard

Если операционная система не предоставляет механизм **fanotify**, используемый SpIDer Guard для мониторинга действий с объектами файловой системы, он может использовать специальный загружаемый LKM-модуль, работающий в пространстве ядра (кроме того, модуль ядра может использоваться в тех случаях, когда механизм **fanotify** реализован с ограничениями по доступу к файловой системе, как, например, в системах с мандатной моделью доступа).

По умолчанию в составе SpIDer Guard поставляется скомпилированный модуль ядра для всех ОС, указанных в разделе Системные требования. Кроме этого совместно с компонентом SpIDer Guard поставляется архив в формате `tar.bz2`, содержащий исходные файлы загружаемого модуля ядра, чтобы его можно было собрать вручную.

> Загружаемый модуль ядра, используемый SpIDer Guard, предназначен для работы с ядрами **GNU/Linux** версий 2.6.* и новее.

Архив с исходными кодами загружаемого модуля ядра располагается в каталоге основных файлов Dr.Web для файловых серверов UNIX <*opt_dir*> (для **Linux** – `/opt/drweb.com`), в подкаталоге `share/drweb-spider-kmod/src/`, и имеет имя вида `drweb-spider-kmod-`<*версия*>`-`<*дата*>`.tar.bz2`.

Также в каталоге `drweb-spider-kmod` имеется файл сценария `check-kmod-install.sh`, исполнив который, вы получите информацию, поддерживает ли используемая вами операционная система предварительно скомпилированные версии ядра, уже включенные в состав продукта. В случае если нет, на экран будет выведена рекомендация выполнить ручную сборку.

В случае отсутствия каталога `drweb-spider-kmod` по указанному пути, выполните установку пакета `drweb-spider-kmod` (из репозитория или выборочной установкой из универсального пакета, в зависимости от способа, которым установлен продукт).

Для выполнения ручной сборки загружаемого модуля ядра из исходных кодов необходимо обладать правами суперпользователя (*root*). Для получения прав суперпользователя при сборке воспользуйтесь командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

Инструкция по сборке модуля ядра

1. Распакуйте архив с исходными кодами в любой каталог. Например, команда

   ```
   # tar -xf drweb-spider-kmod-<версия>-<дата>.tar.bz2
   ```

   распакует архив непосредственно в каталог, содержащий сам архив, создав в нем подкаталог с именем файла архива.

2. Перейдите в созданный каталог с исходными кодами и выполните команду:

   ```
   # make
   ```

   В случае возникновения ошибок на этапе **make** следует их устранить (см. ниже) и выполнить компиляцию повторно.

3. После успешного окончания этапа **make** выполните следующие команды:

   ```
   # make install
   # depmod
   ```

4. После успешной сборки модуля ядра и его регистрации в системе, выполните дополнительно настройку SpIDer Guard, указав ему режим работы с модулем ядра, выполнив команду

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

   Также допускается установка значения `AUTO` вместо значения `LKM`. В этом случае SpIDer Guard будет пробовать использовать не только модуль ядра, но и системный механизм **fanotify**. Для получения дополнительной информации используйте команду:

   ```
   $ man 1 drweb-spider
   ```

Возможные ошибки сборки

На этапе выполнения сборки **make** могут возникать ошибки. В случае возникновения ошибок проверьте следующее:

- Для успешной сборки требуется наличие **Perl** и компилятора **GCC**. Если они отсутствуют, установите их.
- В некоторых ОС может потребоваться предварительная установка пакета `kernel-devel`.
- В некоторых ОС сборка может завершиться ошибкой из-за неправильно определенного пути к каталогу исходных кодов ядра. В этом случае используйте команду **make** с параметром `KDIR=`<*путь к исходным кодам ядра*>. Обычно они размещаются в каталоге `/usr/src/kernels/`<*версия ядра*>.

Версия ядра, выдаваемая командой **uname** `-r`, может не совпадать с именем каталога <*версия ядра*>.

SpIDer Guard для SMB

Компонент SpIDer Guard для SMB – это монитор каталогов файловой системы, используемых как разделяемые каталоги файловым SMB-сервером **Samba**. Этот компонент предназначен для мониторинга действий с файлами в разделяемых каталогах **Samba**. Он работает в режиме резидентного монитора и контролирует основные действия в файловой системе, относящиеся к файлам и каталогам (создание, открытие, закрытие, а также операции чтения и записи), содержащимся в защищаемых каталогах. Когда компонент перехватывает такое событие, он проверяет, был ли файл изменен, и если да, то он создает задачу на проверку этого файла, которую отправляет компоненту проверки файлов Dr.Web File Checker. В случае если запрашиваемый файл действительно требует проверки, Dr.Web File Checker, в свою очередь, инициирует проверку содержимого файла сканирующим ядром Dr.Web Scanning Engine. В случае если в файле обнаружена угроза, файл блокируется для доступа на период, указанный в настройках, до момента применения к нему действия по нейтрализации угрозы. Также в настройках компонента может быть задано предписание блокировать файл в случае ошибки его проверки (в том числе если отсутствует действующая лицензия).

Для предотвращения возможных конфликтов между SpIDer Guard и SpIDer Guard для SMB при проверке файлов в разделяемых каталогах **Samba**, рекомендуется дополнительно настроить SpIDer Guard, выполнив одно из следующих действий:

- Добавить разделяемые каталоги **Samba** в область исключения (перечислить эти каталоги в параметре **`ExcludedPath`**).
- Добавить процесс **Samba** (**smbd**) в список игнорируемых процессов (указать значение `smbd` в параметре **`ExcludedProc`**).

Монитор SpIDer Guard для SMB использует для интеграции с **Samba** специальный модуль VFS SMB. Совместно с монитором SpIDer Guard для SMB поставляется несколько версий модуля VFS SMB, собранных для различных версий **Samba**, однако они могут оказаться несовместимы с версией **Samba**, установленной на вашем файловом сервере, например, если установленный у вас сервер **Samba** использует опцию `CLUSTER_SUPPORT`.

В случае несовместимости поставляемых модулей VFS SMB с вашим сервером **Samba** необходимо выполнить сборку модуля VFS SMB для вашего сервера **Samba**, включая поддержку опции `CLUSTER_SUPPORT`, если это требуется. Процедура сборки модуля VFS SMB из исходных кодов описана в разделе Сборка модуля VFS SMB.

Принципы работы

Монитор SpIDer Guard для SMB работает в режиме демона (обычно запускается демоном управления конфигурацией Dr.Web ConfigD при запуске системы). После запуска он

работает в качестве сервера, к которому подключаются специальные плагины (модули VFS SMB), работающие на стороне сервера **Samba** и контролирующие активность пользователей в разделяемых каталогах. При обнаружении новых или измененных файлов монитор запрашивает их проверку компонентом проверки файлов Dr.Web File Checker. Схема работы монитора показана на рисунке ниже.

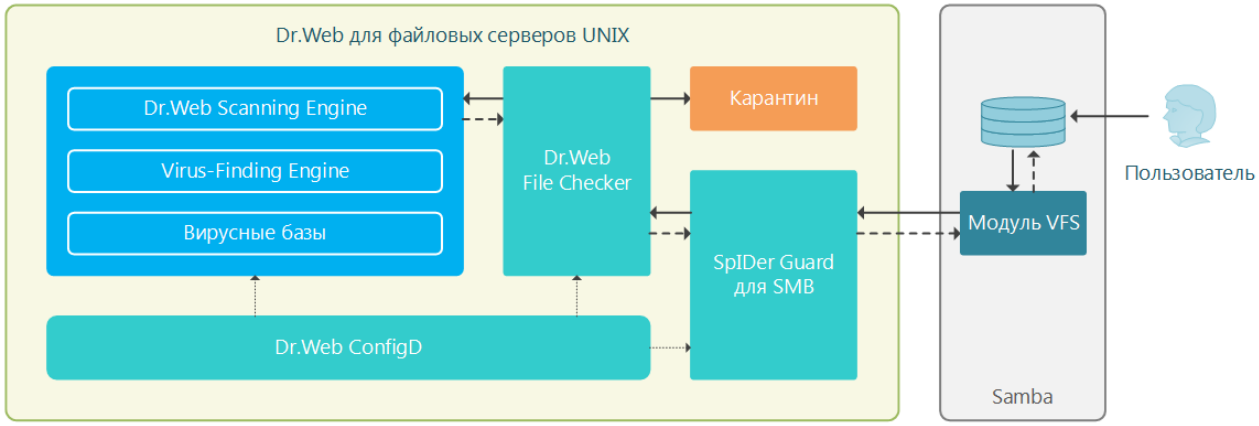

Рисунок 13. Схема работы компонента

Когда в файле, проверенном по запросу от монитора, обнаруживается неизлечимая угроза, или если для данного типа угрозы в настройках было указано действие «Блокировать» (*Block*) монитор дает команду модулю VFS SMB, контролирующему разделяемый каталог, блокировать этот файл для пользователей (т.е. запретить чтение файла, запись в него и его исполнение). Также, если это не отключено в настройках, рядом с заблокированным файлом создается специальный текстовый файл, содержащий описание причины блокировки файла. Это делается для того, чтобы предотвратить для пользователя эффект «неожиданного исчезновения файла», который мог бы возникать в случае, если к файлу было автоматически применено действие «Удалить» (*Delete*) или «Переместить в карантин» (*Quarantine*). Это позволяет предотвратить множественные попытки пользователя (или программы-червя, заразившей компьютер пользователя) заново создать перемещенный или удаленный файл. Кроме того, это действие является способом проинформировать пользователя, что его компьютер, возможно, инфицирован какой-либо вредоносной программой. Получив такую информацию, пользователь может выполнить антивирусную проверку своего компьютера, обнаружить и обезвредить свои локальные угрозы. Дополнительно файл (в зависимости от значения соответствующего параметра конфигурации) может быть заблокирован при ошибке проверки, в том числе, если отсутствует активная лицензия, обеспечивающая работу SpIDer Guard для SMB.

Имеется возможность запретить компоненту наблюдать за указанными каталогами и файлами, находящимися внутри контролируемых разделяемых каталогов сервера **Samba**. Это может быть необходимо, если некоторые файлы изменяются слишком часто, что заставляет монитор столь же часто их проверять. Частая проверка файлов в хранилище может привести к большой нагрузке на систему. Если при этом точно известно, что для некоторых файлов в хранилище частое изменение – это нормальное поведение, то рекомендуется исключить такие файлы из-под наблюдения монитора. В этом случае он не будет реагировать на их изменение и не будет инициировать их проверку компонентом проверки файлов.

Для определения каталогов, подлежащих и не подлежащих наблюдению, монитор файловых хранилищ **Samba** SpIDer Guard для SMB использует два параметра конфигурации:

- **`IncludedPath`** – содержит список путей, подлежащих мониторингу («область наблюдения»).
- **`ExcludedPath`** – содержит список путей, которые требуется исключить из мониторинга («область исключения»).

Стандартно в качестве области наблюдения рассматривается весь разделяемый каталог. В случае указания областей наблюдения и исключения, наблюдению подвергаются только те файлы из разделяемого каталога, пути к которым не принадлежат исключения, определяемой списком **`ExcludedPath`**, или принадлежат области наблюдения, определяемой списком **`IncludedPath`**. При этом, если один и тот же путь указан в обоих списках, то параметр **`IncludedPath`** имеет приоритет: объекты, расположенные по данному пути, будут находиться под контролем монитора SpIDer Guard для SMB. Таким образом, параметр **`IncludedPath`** имеет смысл использовать для включения в область наблюдения отдельных каталогов и файлов, находящихся внутри области исключения.

Имеется возможность задать различные параметры защиты для различных разделяемых каталогов **Samba**, находящихся под защитой монитора SpIDer Guard для SMB, включая различные области наблюдения и исключения, а также реакции на обнаруженные угрозы. Это достигается заданием в секции конфигурации монитора SpIDer Guard для SMB индивидуальных настроек для модулей VFS SMB, контролирующих эти разделяемые каталоги.

Аргументы командной строки

Для запуска компонента SpIDer Guard для SMB из командной строки операционной системы используется следующая команда:

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

SpIDer Guard для SMB допускает использование следующих параметров:

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

Пример:

```
$ /opt/drweb.com/bin/drweb-smbspider-daemon --help
```

Данная команда выведет на экран краткую справку компонента SpIDer Guard для SMB.

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 пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой **drweb-ctl**).

Для получения справки о компоненте из командной строки используйте команду **man** `1 drweb-smbspider-daemon`

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[SMBSpider]` объединенного Приложение Г. Конфигурационный файл программного комплекса продукта Dr.Web для файловых серверов UNIX.

В секции представлены следующие параметры:

LogLevel *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **DefaultLogLevel** из секции [Root]. **Значение по умолчанию:** Notice
Log *{тип журнала}*	Метод ведения журнала
ExePath *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>/bin/drweb-smbspider-daemon • Для **Linux**, **Solaris**: /opt/drweb.com/bin/drweb-smbspider-daemon • Для **FreeBSD**: /usr/local/libexec/drweb.com/bin/drweb-smbspider-daemon
Start *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. *Установка данного параметра в* Yes *предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение* No *– немедленно завершить работу компонента.* **Значение по умолчанию:** No
SambaChrootDir *{путь к каталогу}*	Определяет путь к корневому каталогу файлового хранилища SMB (переопределяется через **chroot** файловым сервером). Используется как префикс, подставляемый в начало всех путей к файлам и каталогам, находящимся в файловом хранилище, и описывает путь к ним относительно корня локальной файловой системы. *Если этот путь не указан, используется путь к корню файловой системы* /. **Значение по умолчанию:** *(не задано)*
SmbSocketPath *{путь к файлу}*	Определяет путь к файлу сокета для взаимодействия SpIDer Guard для SMB с модулям VFS SMB. *Этот путь всегда является относительным и дополняет путь, указанный в значении параметра* **SambaChrootDir** *(если параметр* **SambaChrootDir** *пуст, то дополняется путь к корню файловой системы* /*).*

	Значение по умолчанию: `var/run/.com.drweb.smb_spider_vfs`
ActionDelay *{интервал времени}*	Определяет величину задержки, которую SpIDer Guard для SMB нужно выдержать между моментом обнаружения угрозы и применением действия к инфицированному объекту. В течение этого периода файл будет блокирован. **Значение по умолчанию:** `24h`
MaxCacheSize *{размер}*	Определяет размер кэша, отводимого модулям VFS SMB на хранение информации о проверенных файлах в контролируемых ими каталогах SMB. *Если указано 0, то кэш не используется.* **Значение по умолчанию:** `10mb`
`[*]` **ExcludedPath** *{путь к файлу или каталогу}*	Определяет путь к объекту внутри разделяемого каталога, который должен быть пропущен при проверке. Допускается указание пути как к каталогу, так и к конкретному файлу. Допускается использовать файловые маски (содержащие символы '`?`' и '`*`', а также символьные классы '`[ ]`', '`[! ]`', '`[^ ]`'). *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 `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[SMBSpider]` `ExcludedPath = "/etc/file1", "/usr/bin"` • Две строки (по одному значению в строке) `[SMBSpider]` `ExcludedPath = /etc/file1` `ExcludedPath = /usr/bin` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset SMBSpider.ExcludedPath -a /etc/file1` `# drweb-ctl cfset SMBSpider.ExcludedPath -a /usr/bin` *Если указан каталог, то будет пропущено всё содержимое этого каталога.* **Значение по умолчанию:** *(не задано)*

`[*]` **IncludedPath** *{путь к файлу или каталогу}*	Определяет путь к объекту внутри разделяемого каталога, который должен обязательно проверяться. Допускается указание пути как к каталогу, так и к конкретному файлу. Допускается использовать файловые маски (содержащие символы '`?`' и '`*`', а также символьные классы '`[ ]`', '`[! ]`', '`[^ ]`'). *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 `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[SMBSpider]` `IncludedPath = "/etc/file1", "/usr/bin"` • Две строки (по одному значению в строке) `[SMBSpider]` `IncludedPath = /etc/file1` `IncludedPath = /usr/bin` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset SMBSpider.IncludedPath -a /etc/file1` `# drweb-ctl cfset SMBSpider.IncludedPath -a /usr/bin` *Если указан каталог, то будут проверены все содержащиеся в этом каталоге файлы и подкаталоги.* *Обратите внимание, что этот параметр имеет приоритет над параметром* **ExcludedPath** *(см. выше), т.е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен.* **Значение по умолчанию:** *(не задано)*
`[*]` **AlertFiles** *{логический}*	Определяет, создавать ли рядом с файлом, заблокированным монитором каталогов SMB из-за обнаружения угрозы, текстовый файл с описанием причины блокировки. Создаваемый файл будет иметь имя *<имя заблокированного файла>*`.drweb.alert.txt`. **Возможные значения:** • `Yes` – Создавать файлы причин блокировки. • `No` – Не создавать. **Значение по умолчанию:** `Yes`

[*] **OnKnownVirus** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле известной угрозы (вируса и т.д.), обнаруженной методом сигнатурного анализа, при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Block, Cure, Quarantine, Delete* **Значение по умолчанию:** `Cure`
[*] **OnIncurable** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на неудачу излечения угрозы (т.е. применение действия Cure закончилось неудачей) при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Block, Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
[*] **OnSuspicious** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле неизвестной угрозы (или подозрения на угрозу) методом эвристического анализа при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Pass, Block, Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
[*] **OnAdware** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле рекламной программы при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Pass, Block, Quarantine, Delete* **Значение по умолчанию:** `Pass`
[*] **OnDialers** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле программы автоматического дозвона при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Pass, Block, Quarantine, Delete* **Значение по умолчанию:** `Pass`
[*] **OnJokes** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле программы-шутки при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Pass, Block, Quarantine, Delete* **Значение по умолчанию:** `Pass`

[*] **OnRiskware** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле условно-вредоносной («рискованной») программы при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Pass, Block, Quarantine, Delete* **Значение по умолчанию:** `Pass`
[*] **OnHacktools** *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле хакерской программы (средство удаленного доступа или управления, троянская программа и т.п.) при проверке файла, инициированной по запросу SpIDer Guard для SMB. **Возможные значения:** *Pass, Block, Quarantine, Delete* **Значение по умолчанию:** `Pass`
[*] **BlockOnError** *{логический}*	Определяет, следует ли SpIDer Guard для SMB блокировать файл для доступа, если в процессе его проверки произошла ошибка, либо если отсутствует действующая лицензия, разрешающая проверку файлов монитором SpIDer Guard для SMB. При отсутствии действующей лицензии, если этот параметр установлен в значение `Yes`, SpIDer Guard для SMB будет блокировать все файлы, помещаемые в защищаемый им разделяемый каталог. **Возможные значения:** • `Yes` – Блокировать доступ к файлу. • `No` – Не блокировать. **Значение по умолчанию:** `Yes`
[*] **ScanTimeout** *{интервал времени}*	Устанавливает тайм-аут на проверку одного файла по запросу от SpIDer Guard для SMB. *Может быть указано значение в диапазоне от 1s до 1h.* **Значение по умолчанию:** `30s`
[*] **HeuristicAnalysis** *{On | Off}*	Определяет, использовать ли эвристический анализ для поиска возможных неизвестных угроз при проверке по запросу от SpIDer Guard для SMB. Использование эвристического анализа повышает надежность проверки, но увеличивает её длительность. *Реакция на срабатывание эвристического анализа задается в параметре* **OnSuspicious**.

	Возможные значения: • `On` – Использовать эвристический анализ при проверке. • `Off` – Не использовать эвристический анализ. **Значение по умолчанию:** `On`
`[*]` **`PackerMaxLevel`** *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке запакованных объектов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу SpIDer Guard для SMB. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`
`[*]` **`ArchiveMaxLevel`** *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке архивов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу SpIDer Guard для SMB. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `0`
`[*]` **`MailMaxLevel`** *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке почтовых сообщений и почтовых ящиков (mailboxes). Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу SpIDer Guard для SMB. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`
`[*]` **`ContainerMaxLevel`** *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке прочих контейнеров (таких, как HTML-страницы). Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу SpIDer Guard для SMB. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`
`[*]` **`MaxCompressionRatio`** *{целое число}*	Устанавливает максимальную допустимую степень сжатия проверяемых объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке, инициированной по запросу SpIDer Guard для SMB.

	Величина степени сжатия должна быть не менее 2. **Значение по умолчанию:** `500`

Настройка индивидуальных параметров мониторинга

Имеется возможность в конфигурационном файле SMB-сервера **Samba** (обычно это файл `smb.conf`) задать уникальный тег для каждого модуля VFS SMB, контролирующего каждый разделяемый каталог (хранилище). Уникальные теги для модулей VFS SMB в файле `smb.conf` задаются строкой вида:

```
smb_spider:tag = <имя>
```

где <*имя*> – это уникальный тег (имя), присвоенный сервером **Samba** модулю VFS SMB, контролирующему некоторый разделяемый каталог.

Если для некоторого модуля VFS SMB определен уникальный тег <*имя*>, то имеется возможность добавить в конфигурационный файл Dr.Web для файловых серверов UNIX, наряду с секцией `[SMBSpider]`, хранящей все параметры работы с SMB, отдельную секцию, регулирующую только параметры проверки конкретного хранилища, защищаемого модулем VFS SMB, имеющим присвоенный тег. Эта секция должна иметь имя вида `[SMBSpider.Share.<имя>]`.

Индивидуальные секции для модулей VFS SMB могут включать в себя список параметров, отмеченных символом "`[*]`" в таблице выше. Остальные параметры не могут быть указаны в индивидуальных секциях, поскольку они всегда определяются сразу для всех модулей VFS SMB, с которыми работает монитор каталогов SMB SpIDer Guard для SMB.

Для всех параметров, которые не указаны в индивидуальной секции `[SMBSpider.Share.<имя>]`, использующий ее модуль VFS SMB будет брать соответствующих параметров из общей секции `[SMBSpider]`. Таким образом, если вовсе не задавать индивидуальных секций, помеченных тегами, то все модули VFS SMB будут использовать одинаковые настройки защиты контролируемых разделяемых каталогов. При этом, если из секции `[SMBSpider.Share.<имя>]` удалить некоторый параметр, то для этой секции (и соответствующего каталога с тегом <*имя*>) будет применяться не значение параметра по умолчанию, а значение, указанное в соответствующем одноименном «родительском» параметре (из общей секции `[SMBSpider]`).

Чтобы добавить новую секцию параметров для разделяемого каталога **Samba** с тегом <*имя*> при помощи утилиты управления продуктом Dr.Web для файловых серверов UNIX из командной строки Dr.Web Ctl (запускается командой **drweb-ctl**), достаточно использовать команду:

```
# drweb-ctl cfset SmbSpider.Share -a <имя>
```

Пример:

```
# drweb-ctl cfset SmbSpider.Share -a BuhFiles
# drweb-ctl cfset SmbSpider.Share.BuhFiles.OnAdware Quarantine
```

Первая команда добавит в файл конфигурации секцию `[SMBSpider.Share.BuhFiles]`, а вторая изменит в ней значение параметра **OnAdware**. Таким образом, добавленная секция будет содержать все параметры, отмеченные символом "`[*]`" в таблице выше, причем значения всех параметров, кроме параметра **OnAdware**, указанного в команде, будут совпадать со значениями параметров из общей секции `[SMBSpider]`.

Интеграция с файловым сервером Samba

Инструкцию по интеграции с файловым сервером **Samba** см. в разделе Интеграция с файловым сервером Samba.

Сборка модуля VFS SMB

Если в процессе установки Dr.Web для файловых серверов UNIX было установлено, что версия **Samba**, установленного на вашем файловом сервере, не совместима ни с одной из поставляемых в составе продукта версий вспомогательного модуля VFS SMB, используемого монитором SpIDer Guard для SMB, вам необходимо выполнить ручную сборку этого модуля из исходных кодов.

Исходные коды вспомогательного модуля VFS SMB, используемого SpIDer Guard для SMB, поставляются в отдельном пакете `drweb-smbspider-modules-src` и запакованы в архив формата `tar.gz`. При установке пакета `drweb-smbspider-modules-src` архив с исходными кодами располагается в каталоге `/usr/src/` и имеет имя `drweb-smbspider-11.0.src.tar.gz`. В случае отсутствия этого архива по указанному пути выполните установку пакета (из репозитория или выборочной установкой из универсального пакета, в зависимости от способа, которым установлен продукт).

Кроме исходных кодов модуля VFS SMB, используемого SpIDer Guard для SMB, вам потребуются также исходные коды используемой вами версии сервера **Samba**. В случае их отсутствия загрузите их, например, воспользовавшись источником https://www.samba.org/samba/download/. Для определения, какая версия **Samba** у вас используется, введите команду:

```
$ smbd -V
```

Вспомогательный модуль VFS SMB, используемый SpIDer Guard для SMB, должен быть собран с использованием исходных кодов той версии **Samba**, которая работает на вашем файловом сервере, в противном случае работоспособность SpIDer Guard для SMB не гарантируется.

Для выполнения сборки из исходных кодов необходимо обладать правами суперпользователя. Для получения прав суперпользователя при сборке воспользуйтесь командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

Инструкция по сборке модуля VFS SMB

1. Распакуйте архив с исходными кодами модуля в любой каталог. Например, команда

   ```
   # tar -xf drweb-smbspider-11.0.src.tar.gz
   ```

   распакует архив непосредственно в каталог, содержащий сам архив, создав в нем подкаталог с именем файла архива.
2. Уточните версию используемого вами сервера **Samba** и загрузите его исходные коды, если этого еще не было сделано.
3. Уточните, использует ли установленный у вас сервер **Samba** опцию `CLUSTER_SUPPORT`, выполнив команду:

   ```
   $ smbd -b | grep CLUSTER_SUPPORT
   ```

   Если опция `CLUSTER_SUPPORT` используется установленным у вас сервером **Samba**, в результате выполнения указанной команды на экран будет выдана строка `CLUSTER_SUPPORT`.
4. Перейдите в каталог с исходными кодами **Samba** и выполните конфигурирование (`./configure`) и сборку (**make**) сервера. При конфигурировании укажите актуальное значение опции, отвечающей за использование `CLUSTER_SUPPORT`. В случае проблем с конфигурированием и сборкой исходных кодов **Samba**, обратитесь к документации разработчика, например, перейдя по ссылке https://www.samba.org/samba/docs/.

   Сборка **Samba** из исходных кодов нужна только для последующей правильной сборки модуля VFS SMB, используемого SpIDer Guard для SMB. Замены установленного у вас сервера **Samba** на собранный из исходных кодов не потребуется.

5. После успешного окончания сборки **Samba** перейдите в каталог с исходными кодами модуля VFS SMB и выполните команду:

   ```
   # ./configure --with-samba-source=<путь к каталогу исходных кодов Samba> && make
   ```

где <*путь к каталогу исходных кодов Samba*> – это путь к каталогу, в котором производилась сборка **Samba** на предыдущем шаге.

6. После успешной сборки модуля VFS SMB, скопируйте полученный файл `libsmb_spider.so` из созданного в результате сборки подкаталога `.libs` в каталог VFS-модулей сервера **Samba** (по умолчанию для **GNU/Linux** – `/usr/lib/samba/vfs`) с переименованием файла в `smb_spider.so`, выполнив, например, команду:

   ```
   # cp ./.libs/libsmb_spider.so /usr/lib/samba/vfs/smb_spider.so
   ```

7. После копирования собранного модуля VFS SMB, каталоги, в которых производилась сборка модуля и сервера **Samba**, можно удалить.

Далее необходимо выполнить интеграцию Dr.Web для файловых серверов UNIX с сервером **Samba**, как это описано в соответствующем разделе Руководства администратора (обратите внимание, что на первом шаге интеграции в данном случае не требуется создавать символической ссылки `smb_spider.so` в каталоге VFS-модулей сервера **Samba**).

SpIDer Guard для NSS

> ⚠ Компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства **GNU/Linux**. Работоспособен только в **Novell Open Enterprise Server** SP2 на базе операционной системы **SUSE Linux Enterprise Server** 10 SP3 или старше.

Монитор томов NSS SpIDer Guard для NSS предназначен для мониторинга файловой активности на томах файловой системы NSS (**Novell Storage Services**). Компонент работает в режиме резидентного монитора и отслеживает основные события файловой системы, связанные с изменением файлов (создание, открытие, закрытие). При перехвате этих событий монитор проверяет, было ли изменено содержимое файла, и если да, то монитор формирует задание компоненту проверки файлов Dr.Web File Checker на проверку содержимого измененного файла.

Принципы работы

Монитор SpIDer Guard для NSS работает в режиме демона (обычно запускается демоном управления конфигурацией Dr.Web ConfigD при запуске системы). Он выполняет наблюдение только тех томов файловой системы NSS, которые указаны в настройках монитора (параметры **`NssVolumesMountDir`** и **`ProtectedVolumes`**). Автоматической корректировки списка наблюдаемых томов NSS по мере их монтирования или отмонтирования не производится. При обнаружении новых или измененных файлов на томах NSS монитор отправляет их на проверку сканирующему ядру Dr.Web Scanning Engine. Также особенностью монитора SpIDer Guard для NSS является то, что он ведет собственный карантин угроз, обнаруженных на томах NSS. Схема работы монитора показана на рисунке ниже.

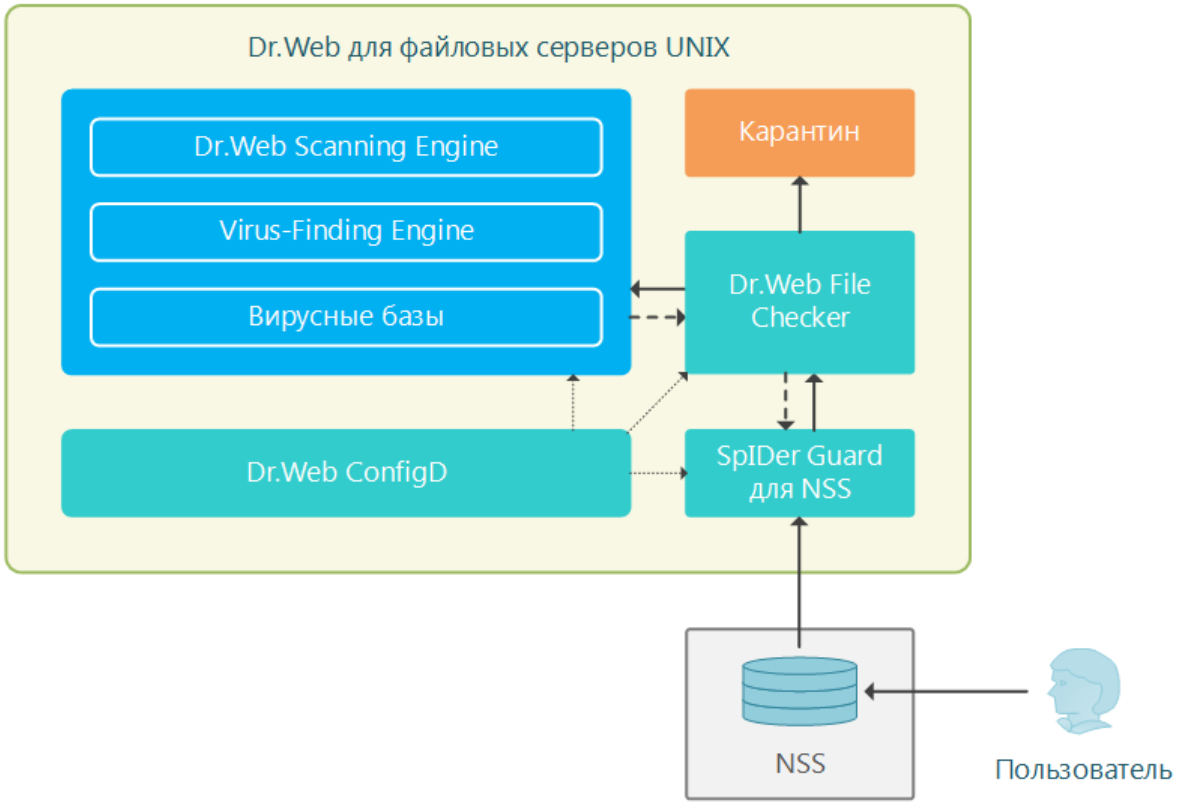

Рисунок 14. Схема работы компонента

Особенностью работы монитора томов NSS является то, что если угроза обнаруживается в файле при его копировании (как на защищаемый том, так и внутри тома NSS), то SpIDer Guard для NSS отметит наличие угрозы только в файле-копии, но оставит не обнаруженной угрозу в файле-источнике. Файл-источник в этом случае будет считаться безопасным до тех пор, пока к нему не будет осуществлена отдельная попытка доступа, причем, если он расположен на томе NSS, то проверен он будет только в случае его изменения.

Если в настройках монитора томов NSS для некоторого типа угроз указано действие *Quarantine*, то при восстановлении угрозы этого типа из карантина на том NSS, она будет снова незамедлительно перемещена в карантин. Например, настройки по умолчанию

```
NSS.OnKnownVirus = Cure
NSS.OnIncurable = Quarantine
```

помещают все неизлечимые объекты в карантин. Поэтому, при восстановлении неизлечимого объекта из карантина на том NSS, он будет снова незамедлительно перемещен в карантин.

Задание путей к проверяемым объектам

Монитор томов NSS SpIDer Guard для NSS будет проверять только те объекты файловой системы, которые находятся на защищаемых томах (параметры **NssVolumesMountDir** и

ProtectedVolumes) и пути к которым на этих томах не соответствуют путям, указанным в параметре **ExcludedPath**, или соответствуют путям, указанным в параметре **IncludedPath**. При этом параметр **IncludedPath** имеет приоритет над параметром **ExcludedPath**: если путь к объекту содержится в обоих этих параметрах, то он проверяется. Использование исключений может быть необходимо, если файлы в некотором каталоге часто изменяются, что порождает их постоянную перепроверку и тем самым нагружает систему. Если точно известно, что частое изменение файлов в некотором каталоге не является следствием вирусной активности, а следствием работы некоторой доверенной программы, то можно добавить путь к этому каталогу или файлам в список исключений. В этом случае монитор томов NSS SpIDer Guard для NSS не будет реагировать на изменения этих файлов. Параметр **IncludedPath** разумно использовать, если нужно обеспечить проверку некоторых объектов, находящихся внутри пути, указанном в параметре **ExcludedPath**.

Рассмотрим пример настроек:

```
NssVolumesMountDir = /media/nss
ProtectedVolumes =
ExcludedPath = vol1/path1, vol1/path2, vol2/sys
IncludedPath = vol1/path1, vol1/path2/incl, vol2/doc
```

При указанных настройках монитор будет проверять все файлы на томе `vol3` (не наложено никаких ограничений на проверку), все файлы на томе `vol2`, за исключением файлов, находящихся в каталоге `/sys` (и всех его подкаталогах); на томе `vol1` не будут проверяться только файлы в каталоге `/path2`, но при этом будут проверяться файлы во всех прочих каталогах этого тома, не находящихся в каталоге `/path2`, а также содержимое каталога `/path2/incl`. Обратите внимание, что указание одного и того же пути (в данном примере – `vol1/path`) в обоих списках бессмысленно, поскольку это равносильно отсутствию ограничений на проверку этого пути. Кроме того, указание пути `vol2/doc` в параметре **IncludedPath** также бессмысленно, поскольку этот каталог не находится в зоне исключений, заданной для тома `vol2` (она содержит только каталог `/sys`).

Аргументы командной строки

Для запуска компонента SpIDer Guard для NSS из командной строки операционной системы используется следующая команда:

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

SpIDer Guard для NSS допускает использование следующих параметров:

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

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

Пример:

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

Данная команда выведет на экран краткую справку компонента SpIDer Guard для NSS.

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 пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой **drweb-ctl**).

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

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[NSS]` объединенного конфигурационного файла продукта Dr.Web для файловых серверов UNIX.

В секции представлены следующие параметры:

`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **`DefaultLogLevel`** из секции `[Root]`. **Значение по умолчанию:** `Notice`
`Log` *{тип журнала}*	Метод ведения журнала
`LogProtocol` *{логический}*	Определяет, следует ли сохранять в журнал монитора томов NSS SpIDer Guard для NSS также и сообщения протокола. **Возможные значения:** • `Yes` – Сохранять.

	• `No` – Не сохранять. **Значение по умолчанию:** `No`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>`/bin/drweb-nss` • Для **Linux**: `/opt/drweb.com/bin/drweb-nss`
`Start` *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. *Установка данного параметра в* `Yes` *предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение* `No` *– немедленно завершить работу компонента.* **Значение по умолчанию:** `No`
`NssVolumesMountDir` *{путь к каталогу}*	Указывает путь к каталогу файловой системы, в который смонтированы тома файловой системы NSS. **Значение по умолчанию:** `/media/nss`
`ProtectedVolumes` *{имя тома}*	Имена томов файловой системы NSS, находящихся в точке монтирования **`NssVolumesMountDir`** и подлежащих защите. Если параметр пуст, защите подлежат все тома, присутствующие в точке монтирования **`NssVolumesMountDir`**. *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 тома `vol1` и `vol2`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[<%NSSSPIDER_SECTION%>]` ` ProtectedVolumes = "vol1", "vol2"` • Две строки (по одному значению в строке) `[<%NSSSPIDER_SECTION%>]` ` ProtectedVolumes = vol1` ` ProtectedVolumes = vol2` 2. Добавление значений через команду **`drweb-ctl`** `cfset`. `# drweb-ctl cfset <%NSSSPIDER_SECTION%>.ProtectedVolumes -a vol1` `# drweb-ctl cfset <%NSSSPIDER_SECTION%>.ProtectedVolumes -a vol2`

	Значение по умолчанию: *(не задано)*
ExcludedPath *{путь к файлу или каталогу}*	Определяет путь к объекту, который должен быть пропущен при проверке. Допускается указание пути как к каталогу, так и к конкретному файлу. Если указан каталог, то будет пропущено всё содержимое этого каталога, включая подкаталоги, за исключением объектов, пути к которым указаны в параметре **IncludedPath**: эти объекты *будут проверяться*. *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 `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[<%NSSSPIDER_SECTION%>]` ` ExcludedPath = "/etc/file1", "/usr/bin"` • Две строки (по одному значению в строке) `[<%NSSSPIDER_SECTION%>]` ` ExcludedPath = /etc/file1` ` ExcludedPath = /usr/bin` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset <%NSSSPIDER_SECTION%>.ExcludedPath -a /etc/file1` `# drweb-ctl cfset <%NSSSPIDER_SECTION%>.ExcludedPath -a /usr/bin` *Пути в списке указываются относительными – относительно пути, указанного в* **NssVolumesMountDir**. **Значение по умолчанию:** *(не задано)*
IncludedPath *{путь к файлу или каталогу}*	Определяет путь к объекту, который должен быть обязательно проверен. Допускается указание пути как к каталогу, так и к конкретному файлу. Если указан каталог, то будут проверены все содержащиеся в этом каталоге файлы и подкаталоги. Этот параметр имеет смысл использовать только для разрешения проверки отдельных объектов (файлов или подкаталогов), путь к которым указан в параметре **ExcludedPath**. Кроме того, этот параметр имеет приоритет над параметром **ExcludedPath**: если путь к одному и тому же объекту (файлу или каталогу) включен в оба параметра, то этот объект будет проверен.

	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 `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[<%NSSSPIDER_SECTION%>]` ` IncludedPath = "/etc/file1", "/usr/bin"` • Две строки (по одному значению в строке) `[<%NSSSPIDER_SECTION%>]` ` IncludedPath = /etc/file1` ` IncludedPath = /usr/bin` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset <%NSSSPIDER_SECTION%>.IncludedPath -a /etc/file1` `# drweb-ctl cfset <%NSSSPIDER_SECTION%>.IncludedPath -a /usr/bin` *Пути в списке указываются относительными – относительно пути, указанного в* **`NssVolumesMountDir`**. **Значение по умолчанию:** *(не задано)*
`OnKnownVirus` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле известной угрозы (вируса и т.д.), обнаруженной методом сигнатурного анализа, при проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Cure, Quarantine, Delete* **Значение по умолчанию:** `Cure`
`OnIncurable` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на неудачу излечения угрозы (т.е. применение действия *Cure* закончилось неудачей) при проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
`OnSuspicious` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле неизвестной угрозы (или подозрения на угрозу) методом эвристического анализа при

	проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Quarantine`
`OnAdware` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле рекламной программы при проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`OnDialers` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле программы автоматического дозвона при проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`OnJokes` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле программы-шутки при проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`OnRiskware` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле условно-вредоносной («рискованной») программы при проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`OnHacktools` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на обнаружение в проверяемом файле хакерской программы (средство удаленного доступа или управления, троянская программа и т.п.) при проверке файла, инициированной по запросу монитора томов NSS. **Возможные значения:** *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`OnError` *{действие}*	Определяет реакцию Dr.Web для файловых серверов UNIX на случай если произойдет ошибка при проверке файла, инициированной по запросу монитора томов NSS.

	Возможные значения: *Report, Quarantine, Delete* **Значение по умолчанию:** `Report`
`ScanTimeout` *{интервал времени}*	Устанавливает тайм-аут на проверку одного файла по запросу от монитора томов NSS. *Может быть указано значение в диапазоне от 1s до 1h.* **Значение по умолчанию:** `30s`
`HeuristicAnalysis` *{On | Off}*	Определяет, использовать ли эвристический анализ для поиска возможных неизвестных угроз при проверке по запросу от монитора томов NSS. Использование эвристического анализа повышает надежность проверки, но увеличивает её длительность. *Реакция на срабатывание эвристического анализа задается в параметре* **`OnSuspicious`**. **Возможные значения:** • `On` – Использовать эвристический анализ при проверке. • `Off` – Не использовать эвристический анализ. **Значение по умолчанию:** `On`
`PackerMaxLevel` *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке запакованных объектов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу монитора томов NSS. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`
`ArchiveMaxLevel` *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке архивов. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу монитора томов NSS. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `0`
`MailMaxLevel` *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке почтовых сообщений и почтовых ящиков (mailboxes). Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу монитора томов NSS. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`

ContainerMaxLevel *{целое число}*	Устанавливает максимальный уровень вложенности объектов при проверке прочих контейнеров. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу монитора томов NSS. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* **Значение по умолчанию:** `8`
MaxCompressionRatio *{целое число}*	Устанавливает максимальную допустимую степень сжатия проверяемых объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке, инициированной по запросу монитора томов NSS. *Величина степени сжатия должна быть не менее 2.* **Значение по умолчанию:** `500`

Если в настройках монитора томов NSS для некоторого типа угроз указано действие *Quarantine*, то при восстановлении угрозы этого типа из карантина на том NSS, она будет снова незамедлительно перемещена в карантин. Например, настройки по умолчанию

```
NSS.OnKnownVirus = Cure
NSS.OnIncurable = Quarantine
```

помещают все неизлечимые объекты в карантин. Поэтому, при восстановлении неизлечимого объекта из карантина на том NSS, он будет снова незамедлительно перемещен в карантин.

Интеграция с томами NSS

Инструкцию по интеграции с томами NSS см. в разделе Интеграция с томами NSS.

Dr.Web ClamD

Компонент Dr.Web ClamD выполняет эмуляцию продуктом Dr.Web для файловых серверов 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 файловых серверов 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 отрытый 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.

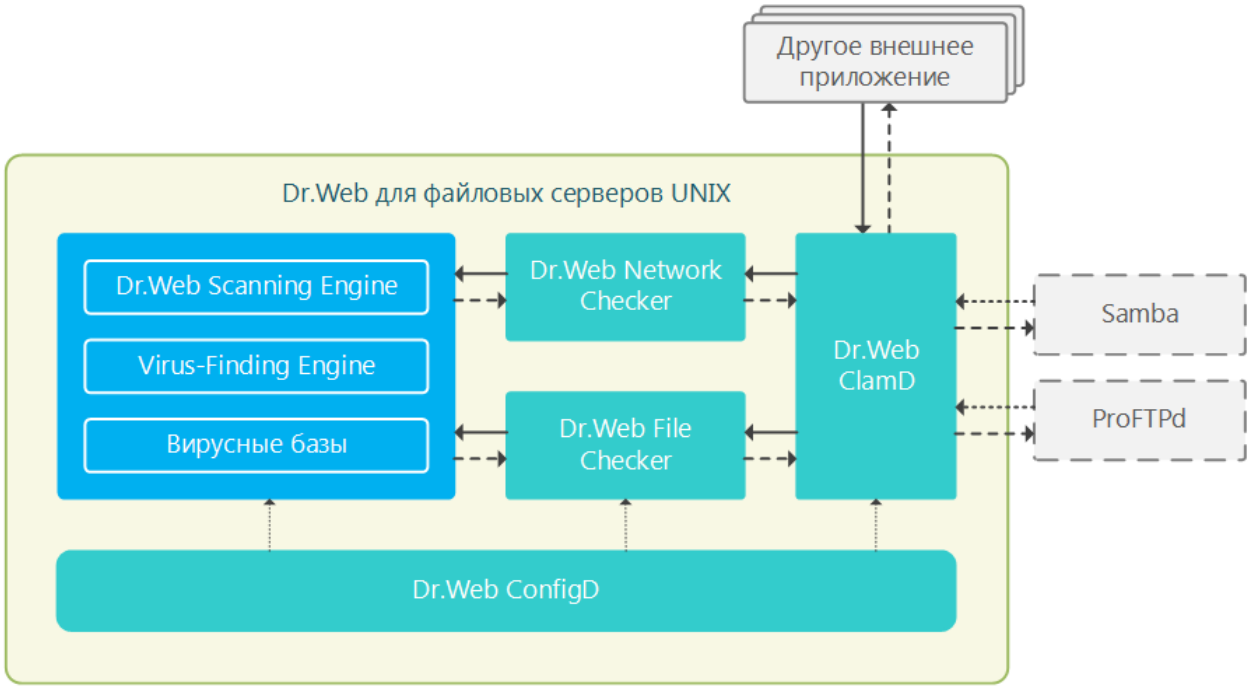

Рисунок 15. Схема работы компонента

По умолчанию компонент не запускается автоматически при старте программного комплекса Dr.Web для файловых серверов 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 серверы файловых служб (такие, как **Samba** и **ProFTPd**), если они оснащены модулем интеграции с **clamd**. Подробнее см. в разделе Интеграция с внешними приложениями.

Обнаруженные угрозы *не нейтрализуются* средствами Dr.Web для файловых серверов 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`	**Назначение:** Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. **Краткий вариант:** `-h` **Аргументы:** Нет.
`--version`	**Назначение:** Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. **Краткий вариант:** `-v` **Аргументы:** Нет.

Пример:

```
$ /opt/drweb.com/bin/drweb-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 файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **`DefaultLogLevel`** из секции `[Root]`. **Значение по умолчанию:** `Notice`
`Log` *{тип журнала}*	Метод ведения журнала
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** *<opt_dir>*`/bin/drweb-clamd` • Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-clamd` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-clamd`
`Start` *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления

	конфигурацией немедленно попытаться запустить компонент, а установка его в значение `No` – немедленно завершить работу компонента. **Значение по умолчанию:** `No`
`Endpoint.<тег>.`**`ClamdSocket`** *{IP-адрес | UNIX-сокет}*	Определяет точку подключения с именем *<тег>* и сокет (адрес IPv4 или адрес сокета UNIX) для клиентов, желающих проверять файлы на наличие угроз. *Для одной точки <тег> может быть задан только один сокет.* **Значение по умолчанию:** *(не задано)*
`[Endpoint.<тег>.]`**`DetectSuspicious`** *{логический}*	Сообщать о подозрительных файлах, обнаруженных эвристическим анализатором. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `Yes`
`[Endpoint.<тег>.]`**`DetectAdware`** *{логический}*	Сообщать о файлах, содержащих рекламные программы. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `Yes`
`[Endpoint.<тег>.]`**`DetectDialers`** *{логический}*	Сообщать о файлах, содержащих программы дозвона. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `Yes`
`[Endpoint.<тег>.]`**`DetectJokes`** *{логический}*	Сообщать о файлах, содержащих программы-шутки. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех*

	точек, у которых значение этого параметра не задано. **Значение по умолчанию:** `No`
`[Endpoint.<тег>.]`**`DetectRiskware`** *{логический}*	Сообщать о файлах, содержащих потенциально опасные программы. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `No`
`[Endpoint.<тег>.]`**`DetectHacktools`** *{логический}*	Сообщать о файлах, содержащих программы взлома. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `No`
`[Endpoint.<тег>.]`**`ReadTimeout`** *{интервал времени}*	Определяет тайм-аут на ожидание данных от клиента. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `5s`
`[Endpoint.<тег>.]`**`StreamMaxLength`** *{размер}*	Определяет максимальный размер данных, которые могут быть получены от клиента (при передаче данных для проверки в виде потока байтов). *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `25mb`
`[Endpoint.<тег>.]`**`ScanTimeout`** *{интервал времени}*	Определяет таймаут на проверку одного файла (или одной порции данных), поступившего от клиента.

	Может быть указано значение в диапазоне от 1s до 1h. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `3m`
`[Endpoint.<тег>.]`**`HeuristicAnalysis`** *{On | Off}*	Определяет, следует ли использовать эвристический анализ при проверке. *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `On`
`[Endpoint.<тег>.]`**`PackerMaxLevel`** *{целое число}*	Определяет максимальный уровень вложенности для проверки запакованных объектов. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `8`
`[Endpoint.<тег>.]`**`ArchiveMaxLevel`** *{целое число}*	Определяет максимальный уровень вложенности для проверки архивов. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `8`
`[Endpoint.<тег>.]`**`MailMaxLevel`**	Определяет максимальный уровень вложенности для проверки почтовых файлов.

{целое число}	*Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `8`
`[Endpoint.<тег>.]`**`ContainerMaxLevel`** *{целое число}*	Определяет максимальный уровень вложенности для проверки объектов, находящихся в контейнерах. *Может быть указано значение в диапазоне от 0 до 60. Значение 0 указывает, что вложенные объекты не проверяются.* *Если указан префикс* `Endpoint.<тег>`*, то значение параметра определено только для точки <тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано.* **Значение по умолчанию:** `8`
`[Endpoint.<тег>.]`**`MaxCompressionRatio`** *{целое число}*	Устанавливает максимальную допустимую степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке. *Величина степени сжатия должна быть не менее 2.* **Значение по умолчанию:** `500`

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 **ClamdSocket** должен обязательно задаваться с префиксом `Endpoint.<имя>`, 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]
ClamdSocket = /tmp/srv1.socket

[ClamD.Endpoint.servers2]
ClamdSocket = 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.ClamdSocket /tmp/srv1.socket
# drweb-ctl cfset ClamD.Endpoint.servers2.ClamdSocket 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**
Файловые службы	
FTP-сервер **ProFTPd**	**Использование clamd:** Проверка файлов, загружаемых на сервер по протоколу FTP. **Требование для интеграции:** Сборка **ProFTPd** с дополнительным модулем `mod_clamav`. **Ссылки на документацию:** Документация по продукту **ProFTPd**: http://www.proftpd.org/docs/ Описание и исходные коды модуля `mod_clamav`: https://github.com/jbenden/mod_clamav

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 **ProFTPd** к Dr.Web ClamD:

1. Настройка Dr.Web ClamD:

```
[ClamD]
Start = yes

[ClamD.Endpoint.ftps]
ClamdSocket = 127.0.0.1:3310
```

2. Настройка **ProFTPd**:

```
ClamAV on
ClamServer 127.0.0.1
ClamPort 3310
```

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 файловых серверов 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.

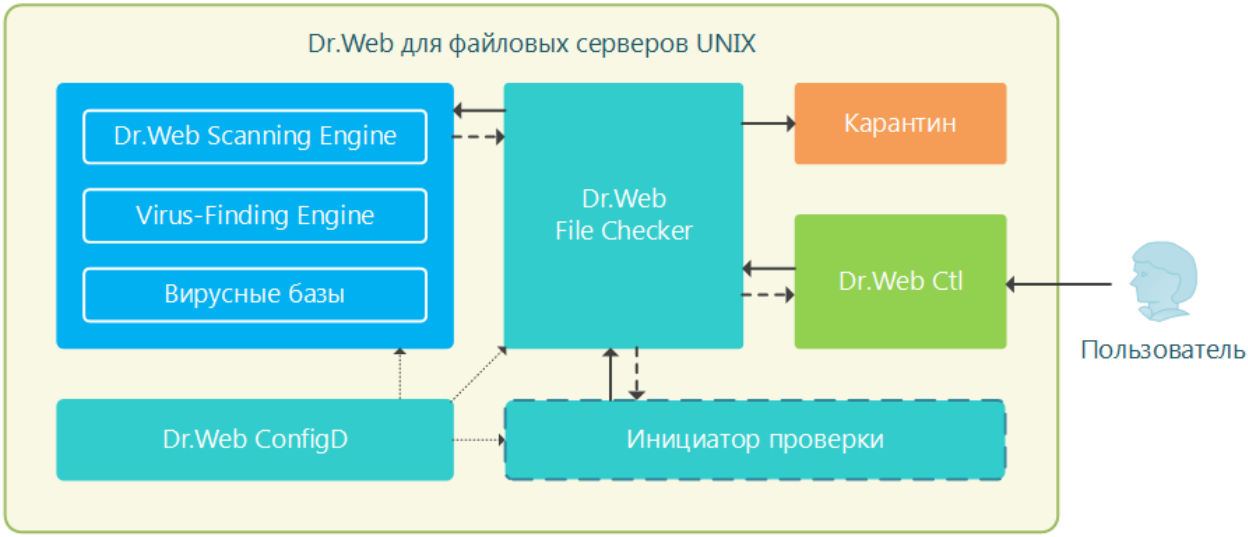

Рисунок 16. Схема работы компонента

При поступлении запросов на проверку объектов файловой системы от компонентов программного комплекса Dr.Web для файловых серверов 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 (например, монитор SpIDer Guard для SMB).

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. Этот метод проверки используется монитором SpIDer Guard.
- *Метод «proxy»* – метод проверки файлов, заключающийся в том, что компонент проверки файлов выполняет только проверку файлов на наличие угроз, не применяя к ним никаких действий, в том числе не выполняя регистрацию обнаруженных угроз (эти действия целиком возлагаются на компонент, инициировавший проверку). Этот метод проверки используется монитором SpIDer Guard для SMB и 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
`--help`	**Назначение:** Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. **Краткий вариант:** `-h` **Аргументы:** Нет.
`--version`	**Назначение:** Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. **Краткий вариант:** `-v`

	Аргументы: Нет.

Пример:

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

Данная команда выведет на экран краткую справку компонента Dr.Web File Checker.

Замечания о запуске

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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX.

Эта секция хранит следующие параметры:

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

	• Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-filecheck` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-filecheck`
DebugClientIpc *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = DEBUG) подробные сообщения IPC. **Значение по умолчанию:** No
DebugScan *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = DEBUG) подробные сообщения, поступающие в процессе проверки файлов. **Значение по умолчанию:** No
DebugFlowScan *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = DEBUG) подробные сообщения о проверке файлов методом *«flow»*. (Обычно метод *«flow»* используется монитором SpIDer Guard). **Значение по умолчанию:** No
DebugProxyScan *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = DEBUG) подробные сообщения о проверке файлов методом *«proxy»*. (Обычно метод *«proxy»* используется монитором SpIDer Guard для SMB и компонентом Dr.Web ClamD). **Значение по умолчанию:** No
DebugCache *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = DEBUG) подробные сообщения о состоянии кэша проверенных файлов. **Значение по умолчанию:** No
MaxCacheSize *{размер}*	Максимальный разрешенный размер кэша для хранения информации о проверенных файлах. *Если указано 0 – кэширование отключено.* **Значение по умолчанию:** 50mb
RescanInterval *{интервал времени}*	Длительность интервала, в течение которого не производится повторная проверка содержимого файлов, информация о предыдущей проверке которых имеется в кэше (период актуальности кэшированной информации). *Допустимо значение от* 0s *до* 1m *(включительно). Если указан интервал менее* 1s *– задержка отсутствует, файл будет проверяться при любом запросе.* **Значение по умолчанию:** 1s
IdleTimeLimit *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. *Допустимо значение от* 10s *до* 30d *(включительно).*

	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 файловых серверов 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 (SpIDer Gate, 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 файловых серверов 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 файловых серверов UNIX с заданным набором узлов в сети с установленным на них продуктом Dr.Web для файловых серверов 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 позволять 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, дожидающихся проверки на каждом используемом узле. Данные, принятые по сети для проверки, передаются сканирующему ядру Dr.Web Scanning Engine, как показано на рисунке ниже.

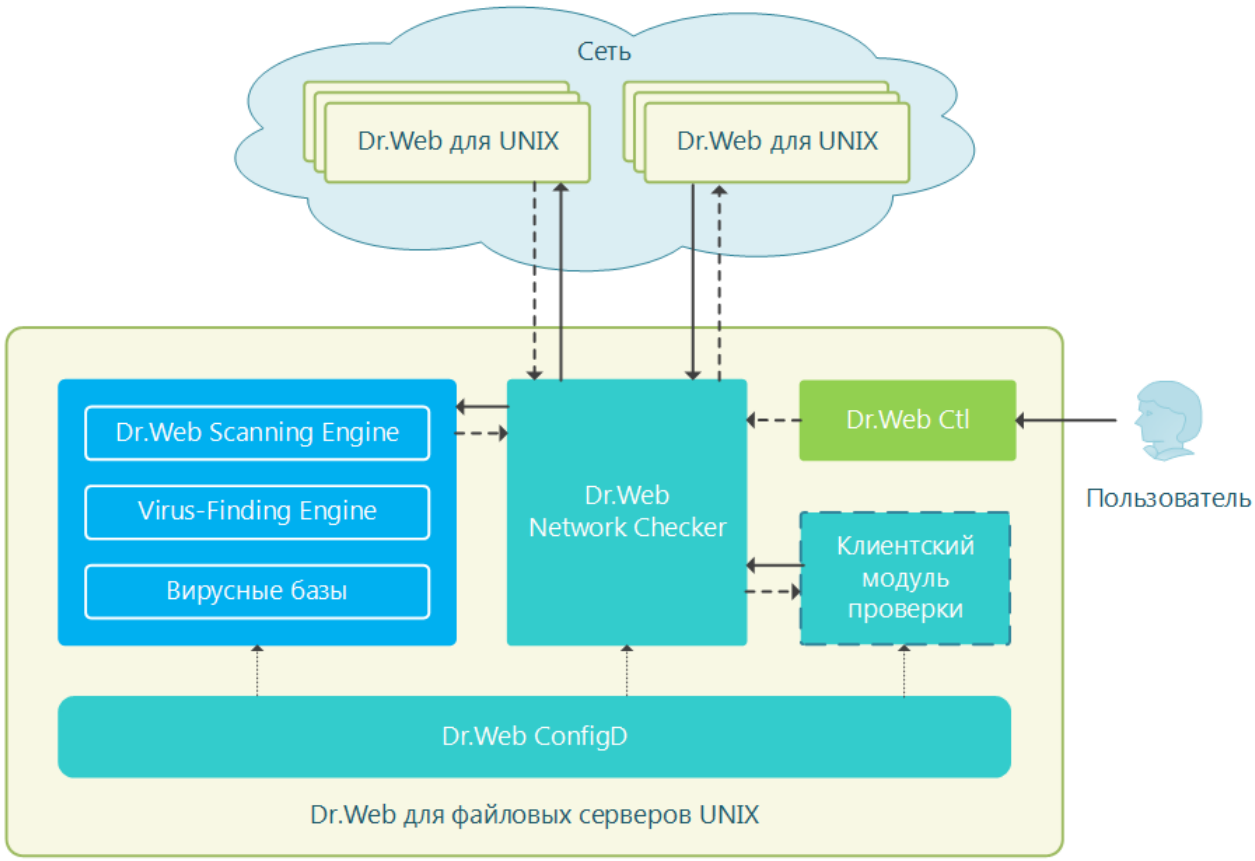

Рисунок 17. Схема работы компонента

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

Пример:

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

Данная команда выведет на экран краткую справку компонента Dr.Web Network Checker.

Замечания о запуске

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 файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

LogLevel *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **DefaultLogLevel** из секции `[Root]`. **Значение по умолчанию:** `Notice`
Log *{тип журнала}*	Метод ведения журнала
ExePath *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>`/bin/drweb-netcheck` • Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-netcheck` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-netcheck`
FixedSocketPath *{путь к файлу}*	Путь к файлу UNIX-сокета фиксированной копии агента Dr.Web Network Checker.

	При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелась запущенная копия агента распределенной проверки файлов, доступная клиентам через этот сокет. **Значение по умолчанию:** *(не задано)*
RunAsUser *{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: **RunAsUser** `= name:123456`. *Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.* **Значение по умолчанию:** `drweb`
IdleTimeLimit *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Минимальное значение – `10s`. *Если задано значение параметра* **LoadBalanceAllowFrom** *или* **FixedSocketPath**, *то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя).* **Значение по умолчанию:** `30s`
LoadBalanceUseSsl *{логический}*	Флаг, определяющий использование для соединения с другими узлами безопасного соединения SSL/TLS. **Возможные значения:** • `Yes` – Использовать SSL/TLS. • `No` – Не использовать SSL/TLS. *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* **LoadBalanceSslCertificate** *и* **LoadBalanceSslKey**). **Значение по умолчанию:** `No`
LoadBalanceSslCertificate *{путь к файлу}*	Путь к файлу сертификата SSL, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS. *Обратите внимание, что файл сертификата и файл закрытого ключа (определяется следующим параметром) должны соответствовать друг другу.*

	Значение по умолчанию: *(не задано)*
LoadBalanceSslKey *{путь к файлу}*	Путь к файлу закрытого ключа, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS. *Обратите внимание, что файл сертификата и файл закрытого ключа (определяется предыдущим параметром) должны соответствовать друг другу.* **Значение по умолчанию:** *(не задано)*
LoadBalanceSslCa *{путь}*	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. *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.* **Значение по умолчанию:** *(не задано)*
LoadBalanceServerSocket *{адрес}*	Сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web Network Checker на данном узле для получения файлов на проверку от удаленных узлов (если она может работать как сервер сетевого сканирования). **Значение по умолчанию:** *(не задано)*
LoadBalanceAllowFrom *{IP-адрес}*	IP-адрес удаленного узла сети, от которого Dr.Web Network Checker на данном узле может принимать файлы на проверку (как сервер сетевого сканирования). *Может иметь список значений. Значения в списке указываются через запятую (каждое значение – в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).* **Пример:** Добавить в список адреса узлов 192.168.0.1 и 10.20.30.45. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[NetCheck]` ` LoadBalanceAllowFrom = "192.168.0.1", "10.20.30.45"`

	• Две строки (по одному значению в строке) `[NetCheck]` ` LoadBalanceAllowFrom = 192.168.0.1` ` LoadBalanceAllowFrom = 10.20.30.45` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 192.168.0.1` `# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 10.20.30.45` *Если параметр пуст, удаленные файлы на проверку не принимаются (узел не работает в режиме сервера).* **Значение по умолчанию:** *(не задано)*
LoadBalanceSourceAddress *{IP-адрес}*	IP-адрес сетевого интерфейса, используемого Dr.Web Network Checker на данном узле для передачи файлов на удаленную проверку, если узел работает как клиент сетевого сканирования и если на узле доступно несколько сетевых интерфейсов. *Если указать пустое значение, то используемый сетевой интерфейс будет автоматически выбран ядром ОС.* **Значение по умолчанию:** *(не задано)*
LoadBalanceTo *{адрес}*	Сокет (IP-адрес и порт) удаленного узла, на который Dr.Web Network Checker на данном узле может отправлять файлы на удаленную проверку (как клиент сетевого сканирования). *Может иметь список значений. Значения в списке указываются через запятую (каждое значение – в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).* **Пример:** Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[NetCheck]` ` LoadBalanceTo = "192.168.0.1:1234", "10.20.30.45:5678"` • Две строки (по одному значению в строке) `[NetCheck]` ` LoadBalanceTo = 192.168.0.1:1234` ` LoadBalanceTo = 10.20.30.45:5678`

	2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset NetCheck.LoadBalanceTo -a 192.168.0.1:1234` `# drweb-ctl cfset NetCheck.LoadBalanceTo -a 10.20.30.45:5678` *Если параметр пуст, локальные файлы не передаются на удаленную проверку (узел не работает в режиме клиента сетевого сканирования).* **Значение по умолчанию:** *(не задано)*
LoadBalanceStatusInterval *{интервал времени}*	Интервал времени между рассылками данным узлом информации о своей загруженности для всех агентов распределенной проверки, перечисленных в параметре **LoadBalanceAllowFrom**. **Значение по умолчанию:** `1s`
SpoolDir *{путь к каталогу}*	Каталог в локальной файловой системе, используемый для хранения файлов, принятых Dr.Web Network Checker по сети от клиентов сканирования для проверки. **Значение по умолчанию:** `/tmp/netcheck`
LocalScanPreference *{дробное число}*	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. Минимальное значение – `1`. **Значение по умолчанию:** `1`

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 файловых серверов 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 файловых серверов 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.

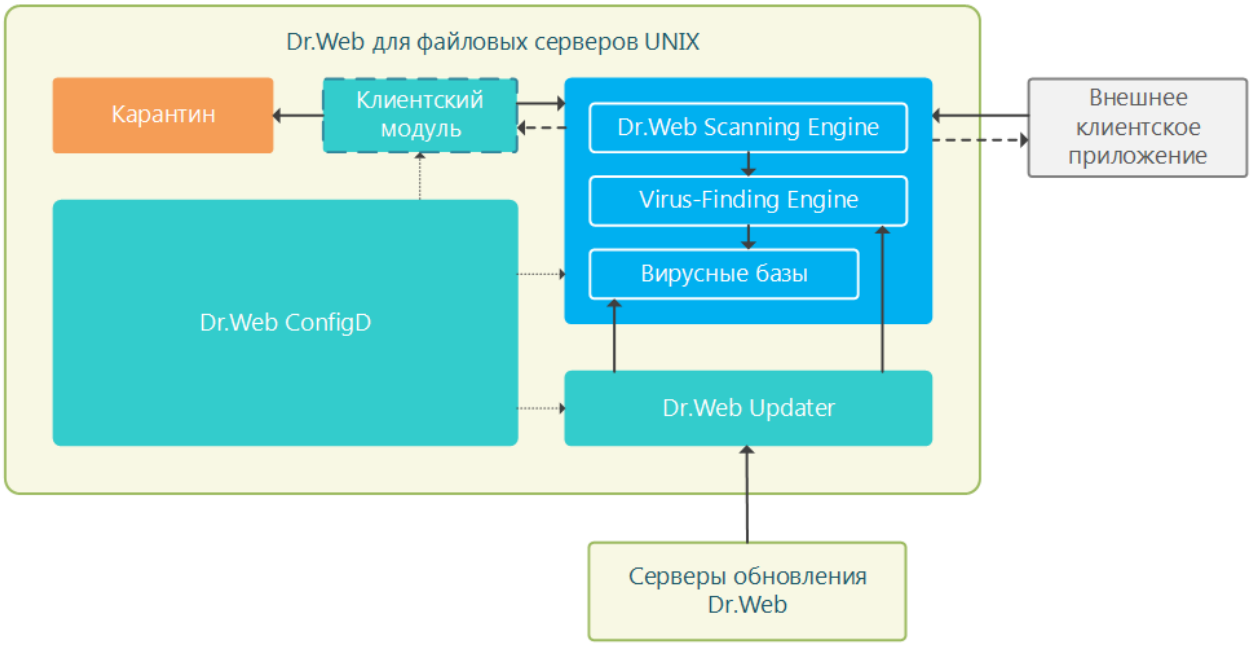

Рисунок 18. Схема работы компонента

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 файловых серверов 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 файловых серверов 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 <сокет> [<параметры>]
```

где обязательный аргумент <*сокет*> указывает адрес сокета, используемого Dr.Web Scanning Engine для обслуживания запросов клиентских компонентов. Может задаваться только в виде пути к файлу (сокет UNIX).

Dr.Web Scanning Engine допускает использование следующих параметров:

Параметр	Описание
`--help`	**Назначение:** Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. **Краткий вариант:** `-h` **Аргументы:** Нет.
`--version`	**Назначение:** Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. **Краткий вариант:** `-v` **Аргументы:** Нет.
Дополнительные параметры запуска (совпадают с параметрами из конфигурационного файла и замещают их при необходимости):	

`--EnginePath`	**Назначение:** Указать путь к файлу библиотеки антивирусного ядра Dr.Web Virus-Finding Engine. **Краткий вариант:** Нет. **Аргументы:** <*путь к файлу*> – полный путь к файлу используемой библиотеки.
`--VirusBaseDir`	**Назначение:** Указать путь к каталогу, содержащему файлы вирусных баз. **Краткий вариант:** Нет. **Аргументы:** <*путь к каталогу*> – полный путь к каталогу вирусных баз.
`--TempDir`	**Назначение:** Указать путь к каталогу временных файлов. **Краткий вариант:** Нет. **Аргументы:** <*путь к каталогу*> – полный путь к каталогу временных файлов.
`--Key`	**Назначение:** Указать путь к используемому ключевому файлу. **Краткий вариант:** Нет. **Аргументы:** <*путь к файлу*> – полный путь к ключевому файлу.
`--MaxForks`	**Назначение:** Определить максимальное разрешенное число дочерних процессов, которые Dr.Web Scanning Engine может породить в процессе проверки. **Краткий вариант:** Нет. **Аргументы:** <*число*> – максимальное разрешенное число дочерних процессов.
`--MaxForksPerFile`	**Назначение:** Определить максимальное разрешенное число дочерних процессов, которые Dr.Web Scanning Engine может использовать при проверке одного составного файла (архива, контейнера и т.п.). **Краткий вариант:** Нет. **Аргументы:** <*число*> – максимальное разрешенное число дочерних процессов. Не может быть меньше 1 и не может быть больше значения параметра `--MaxForks`.
`--WatchdogInterval`	**Назначение:** Установить периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность дочерних процессов, занимающихся проверкой содержимого файлов, для остановки зависших при проверке. **Краткий вариант:** Нет. **Аргументы:** <*интервал времени*> – периодичность проверки дочерних процессов.
`--Shelltrace`	**Назначение:** Включить отслеживание оболочки (вывод в журнал расширенной информации о проверке файлов ядром Dr.Web Virus-Finding Engine). **Краткий вариант:** Нет. **Аргументы:** Нет.
`--LogLevel`	**Назначение:** Задать уровень подробности ведения журнала ядром Dr.Web Scanning Engine в процессе работы. **Краткий вариант:** Нет.

	Аргументы: <*уровень подробности*>. Возможные значения: • DEBUG – Самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация. • INFO – Выводятся все сообщения. • NOTICE – Выводятся сообщения об ошибках, предупреждения, уведомления. • WARNING – Выводятся сообщения об ошибках и предупреждения. • ERROR – Выводятся только сообщения об ошибках.
`--Log`	**Назначение:** Задать способ ведения журнала сообщений компонента. **Краткий вариант:** Нет. **Аргументы:** <*тип журнала*>. Возможные значения: • `Stderr[:ShowTimestamp]` – Сообщения будут выводиться в стандартный поток ошибок *stderr*. Дополнительная опция `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени. • `Syslog[:`<*facility*>`]` – Сообщения будут передаваться системной службе журналирования **syslog**. Дополнительная метка <*facility*> используется для указания типа журнала, в котором **syslog** будет сохранять сообщения. Возможные значения: ○ `DAEMON` – сообщения демонов; ○ `USER` – сообщения пользовательских процессов; ○ `MAIL` – сообщения почтовых программ; ○ `LOCAL0` – сообщения локальных процессов 0; ... ○ `LOCAL7` – сообщения локальных процессов 7. • <*path*> – Путь к файлу, в который будут сохраняться сообщения журнала. **Примеры:** `--Log /var/opt/drweb.com/log/se.log` `--Log Stderr:ShowTimestamp` `--Log Syslog:DAEMON`

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-сокет `/tmp/drweb.ipc/.se` и порождать 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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX.

Эта секция хранит следующие параметры:

LogLevel *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **DefaultLogLevel** из секции `[Root]`. **Значение по умолчанию:** `Notice`
Log *{тип журнала}*	Метод ведения журнала
ExePath *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>`/bin/drweb-se` • Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-se` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-se`

FixedSocketPath *{путь к файлу}*	Путь к файлу UNIX-сокета фиксированной копии сканирующего ядра Dr.Web Scanning Engine. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелась запущенная копия сканирующего ядра, доступная клиентам через этот сокет. **Значение по умолчанию:** *(не задано)*
IdleTimeLimit *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Минимальное значение – `10s`. *Если задано значение параметра* **FixedSocketPath***, то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя).* **Значение по умолчанию:** `30s`
MaxForks *{целое число}*	Определяет максимальное разрешенное количество копий дочерних сканирующих процессов, порождаемых сканирующим ядром Dr.Web Scanning Engine, которые одновременно могут быть запущены. **Значение по умолчанию:** *Автоматически определяется при старте, как удвоенное число доступных процессорных ядер, или 4, если полученное число меньше 4.*
MaxForksPerFile *{целое число}*	Определяет максимальное разрешенное количество копий дочерних сканирующих процессов, которые одновременно могут быть запущены Dr.Web Scanning Engine при проверке файлов-контейнеров (таких как архивы). Не может быть меньше `1` и не может быть больше значения, указанного в параметре **MaxForks**. **Значение по умолчанию:** *Автоматически определяется при старте, как величина* `MaxForks/2`.
BufferedIo *{On | Off}*	Использовать буферизованный ввод-вывод при проверке файлов. *Использование буферизованного ввода-вывода в ОС* **FreeBSD** *и* **Linux** *может увеличить скорость проверки файлов, расположенных на медленных дисковых устройствах.* **Значение по умолчанию:** `Off`
WatchdogInterval *{интервал времени}*	Определяет периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность порожденных им дочерних сканирующих процессов для обнаружения зависаний при проверке («сторожевой таймер»). **Значение по умолчанию:** `1.5s`

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 файловых серверов UNIX работает в режиме централизованной защиты, то в качестве источника обновлений используется сервер централизованной защиты (например, Dr.Web Enterprise Server), причем все обновления получаются 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 . 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.

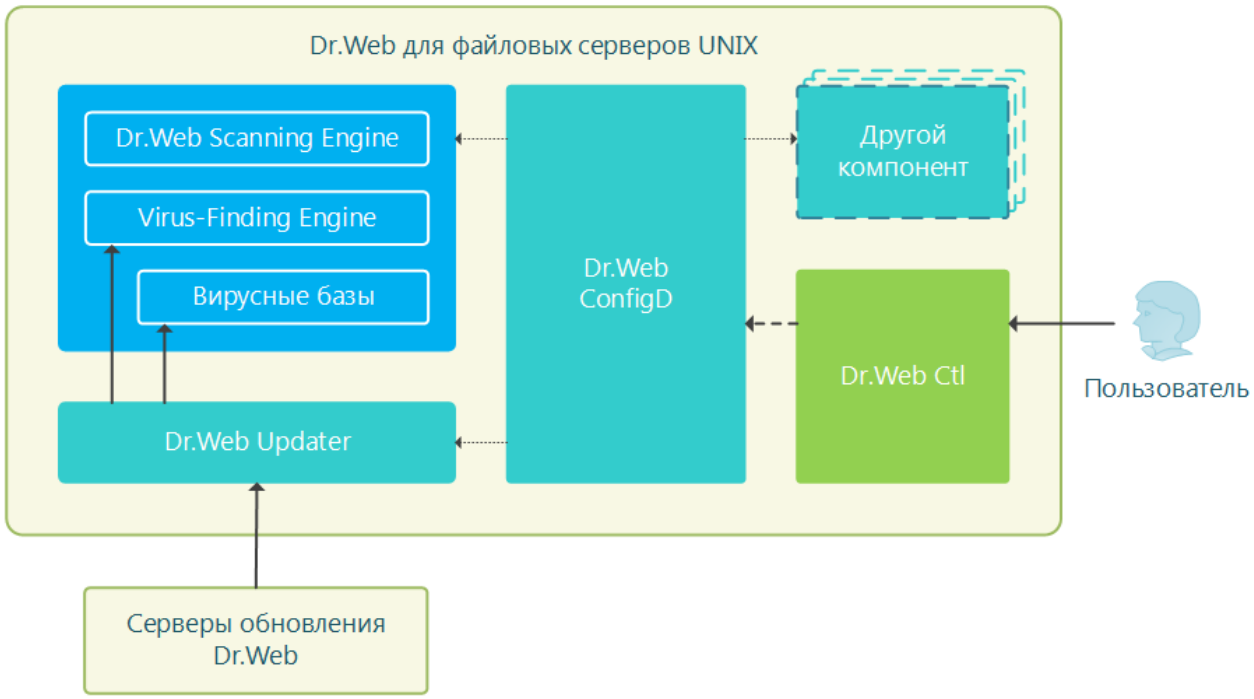

Рисунок 19. Схема работы компонента

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 файловых серверов 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 ***DrlDir**. 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 ***CustomDrlDir**. 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 ***CustomDrlDir** в настройках компонента.

Содержимое файлов списков серверов подписано для невозможности их модификации. Если вам необходимо создать особый перечень серверов обновления, обратитесь в техническую поддержку.

Компонент может выполнять сохранение резервных копий обновляемых файлов для последующего отката обновлений по команде пользователя. Место сохранения резервных копий и глубина хранимой истории обновлений задаются в настройках компонента. Откат обновлений выполняется через утилиту управления продуктом Dr.Web для файловых серверов 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
--help	**Назначение:** Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. **Краткий вариант:** -h **Аргументы:** Нет.
--version	**Назначение:** Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. **Краткий вариант:** -v

	Аргументы: Нет.

Пример:

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

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

Замечания о запуске

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 файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **`DefaultLogLevel`** из секции `[Root]`. **Значение по умолчанию:** `Notice`
`Log` `{тип журнала}`	Метод ведения журнала
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>`/bin/drweb-update` • Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-update` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-update`
`RunAsUser` *{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: **`RunAsUser`** `= name:123456`. *Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.* **Значение по умолчанию:** `drweb`
`UpdateInterval` *{интервал времени}*	Частота проверки наличия обновлений на серверах обновления Dr.Web, т.е. период времени, который должен пройти от предыдущей успешной попытки подключения к серверам обновления (автоматического или инициированного пользователем) до следующей попытки выполнить обновление. **Значение по умолчанию:** `30m`
`RetryInterval` *{интервал времени}*	Частота повторных попыток выполнить обновление с серверов обновления в случае если очередная попытка выполнить обновление завершилось неудачей. Параметр может принимать значение от `1m` до `30m` включительно. **Значение по умолчанию:** `3m`
`MaxRetries` *{целое число}*	Количество повторных попыток выполнить обновление с серверов обновления Dr.Web (предпринимаемых через промежутки времени, указанные в параметре **`RetryInterval`**), если предыдущая попытка выполнить обновление с серверов обновления окончилась неудачей. *Если значение параметра – 0, повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени, указанный в параметре* **`UpdateInterval`***).* **Значение по умолчанию:** `3`
`Proxy` *{строка подключения}*	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). Если значение параметра не задано, прокси-сервер не используется. **Возможные значения:** <*строка подключения*> – Строка подключения к прокси-серверу. Имеет следующий формат (URL): `[`<*protocol*>`://[`<*user*>`:`<*password*>`@]`<*proxyhost*>`:`<*port*> где: • <*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>) содержит 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 значением 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`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке

	`` [Update] ExcludedFiles = "123.vdb", "456.dws" ``` • Две строки (по одному значению в строке) ``` [Update] ExcludedFiles = 123.vdb ExcludedFiles = 456.dws ``` 2. Добавление значений через команду **drweb-ctl** `cfset`. ``` # drweb-ctl cfset Update.ExcludedFiles -a 123.vdb # drweb-ctl cfset Update.ExcludedFiles -a 456.dws ``` **Значение по умолчанию:** `drweb32.lst`
`NetworkTimeout` *{интервал времени}*	Тайм-аут на сетевые операции компонента обновления при выполнении обновлений с серверов обновления Dr.Web. Используется для ожидания продолжения обновления в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то обновление будет продолжено. *Не имеет смысла указывать величину тайм-аута более* `75s`, *т.к. за это время соединение закроется по тайм-ауту TCP. Минимально допустимое значение* – `5s`. **Значение по умолчанию:** `60s`
`BaseDrlPath` *{путь к файлу}*	Определяет путь к подписанному файлу списка серверов стандартной зоны обновления, используемых компонентом обновлений для обновления вирусных баз и антивирусного ядра. **Значение по умолчанию:** <*var_dir*>`/drl/bases/update.drl` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/drl/bases/update.drl` • Для **FreeBSD**: `/var/drweb.com/drl/bases/update.drl`
`BaseCustomDrlPath` *{путь к файлу}*	Определяет путь к подписанному файлу списка серверов особой зоны обновления, используемых компонентом обновлений для обновления вирусных баз и антивирусного ядра. *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.* **Значение по умолчанию:** <*var_dir*>`/drl/bases/custom.drl` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/drl/bases/custom.drl`

	• Для **FreeBSD**: `/var/drweb.com/drl/bases/custom.drl`
BaseUpdateEnabled *{логический}*	Флаг, указывающий, разрешено или запрещено обновление вирусных баз и антивирусного ядра. **Возможные значения:** • `Yes` – Обновление разрешено и будет производиться. • `No` – Обновление не разрешено и не будет производиться. **Значение по умолчанию:** `Yes`
VersionDrlPath *{путь к файлу}*	Определяет путь к подписанному файлу списка серверов зоны обновления, используемых компонентом обновлений для обновления версий компонентов Dr.Web для файловых серверов UNIX. **Значение по умолчанию:** <*var_dir*>`/drl/version/update.drl` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/drl/version/update.drl` • Для **FreeBSD**: `/var/drweb.com/drl/version/update.drl`
VersionUpdateEnabled *{логический}*	Флаг, указывающий, разрешено или запрещено обновление версий компонентов Dr.Web для файловых серверов UNIX. **Возможные значения:** • `Yes` – Обновление разрешено и будет производиться. • `No` – Обновление не разрешено и не будет производиться. **Значение по умолчанию:** `Yes`
DwsDrlPath *{путь к файлу}*	Параметр не используется. **Значение по умолчанию:** <*var_dir*>`/drl/dws/update.drl` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/drl/dws/update.drl` • Для **FreeBSD**: `/var/drweb.com/drl/dws/update.drl`
DwsCustomDrlPath *{путь к файлу}*	Параметр не используется. **Значение по умолчанию:** <*var_dir*>`/drl/dws/custom.drl` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/drl/dws/custom.drl` • Для **FreeBSD**: `/var/drweb.com/drl/dws/custom.drl`
DwsUpdateEnabled *{логический}*	Параметр не используется. **Значение по умолчанию:** `Yes`
AntispamDrlPath *{путь к файлу}*	Параметр не используется. **Значение по умолчанию:** <*var_dir*>`/drl/antispam/update.drl`

	• Для **Linux**, **Solaris**: `/var/opt/drweb.com/drl/antispam/update.drl` • Для **FreeBSD**: `/var/drweb.com/drl/antispam/update.drl`
AntispamCustomDrlPath *{путь к файлу}*	Параметр не используется. **Значение по умолчанию:** <*var_dir*>`/drl/antispam/custom.drl` • Для **Linux**, **Solaris**: `/var/opt/drweb.com/drl/antispam/custom.drl` • Для **FreeBSD**: `/var/drweb.com/drl/antispam/custom.drl`
AntispamUpdateEnabled *{логический}*	Параметр не используется. **Значение по умолчанию:** `No`
BackupDir *{путь к каталогу}*	Определяет путь к каталогу, в который сохраняются старые версии обновляемых файлов для возможности отката обновлений. При каждом обновлении сохраняются резервные копии только обновленных файлов. **Значение по умолчанию:** `/tmp/update-backup`
MaxBackups *{целое число}*	Максимальное количество сохраняемых предыдущих версий обновляемых файлов. При превышении этой величины самая старая копия удаляется при очередном обновлении. *Если значение параметра – 0, то предыдущие версии файлов для восстановления не сохраняются.* **Значение по умолчанию:** `0`

Dr.Web ES Agent

Агент централизованной защиты Dr.Web ES Agent предназначен для подключения программного комплекса Dr.Web для файловых серверов UNIX к серверу централизованной защиты (например, к Dr.Web Enterprise Server).

Когда Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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.

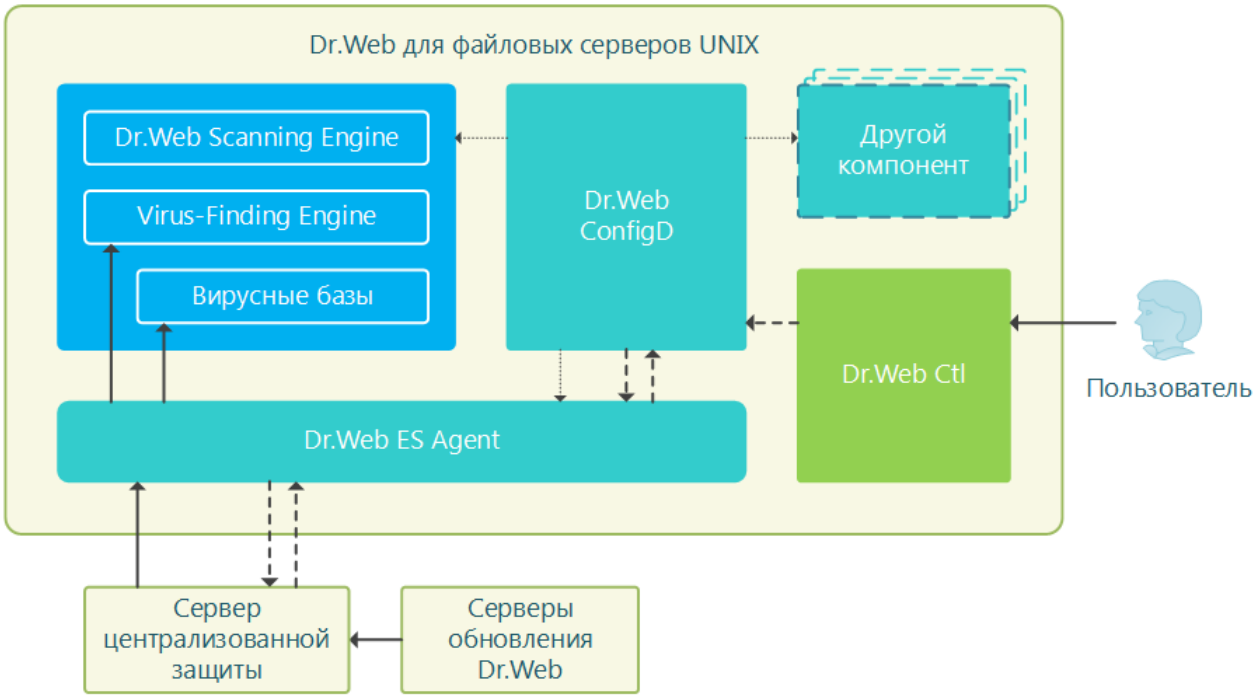

Рисунок 20. Схема работы компонента

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

Пример:

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

Данная команда выведет на экран краткую справку компонента Dr.Web ES Agent.

Замечания о запуске

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 файловых серверов UNIX к серверу централизованной защиты пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

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

ExePath *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>/bin/drweb-esagent • Для **Linux**, **Solaris**: /opt/drweb.com/bin/drweb-esagent • Для **FreeBSD**: /usr/local/libexec/drweb.com/bin/drweb-esagent
DebugIpc *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = DEBUG) подробные сообщения IPC (взаимодействие Dr.Web ES Agent и демона управления конфигурацией Dr.Web ConfigD). **Значение по умолчанию:** No
MobileMode *{On | Off | Auto}*	Определяет возможность программного комплекса, при подключении к серверу централизованной защиты, работать в мобильном режиме. **Возможные значения:** • On – Использовать мобильный режим, если он разрешен сервером централизованной защиты (выполнять обновления с серверов обновлений компании «Доктор Веб» через Dr.Web Updater). • Off – Не использовать мобильный режим, оставаться в режиме централизованной защиты (обновления всегда получаются только с сервера централизованной защиты). • 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. *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.* **Значение по умолчанию:** Auto
Discovery *{On | Off}*	Разрешает или запрещает агенту принимать *discovery*-запросы от инспектора сети, встроенного в сервер централизованной защиты (*discovery*-запросы используются инспектором для проверки структуры и состояния антивирусной сети). **Возможные значения:** • On – Разрешать агенту принимать и обрабатывать *discovery*-запросы. • Off – Не разрешать агенту принимать и обрабатывать *discovery*-запросы. *Обратите внимание, что параметр имеет приоритет выше, чем настройки сервера централизованной защиты: если указано значение Off, агент не будет принимать discovery-запросы, даже если эта функция включена на сервере.* **Значение по умолчанию:** On

`UpdatePlatform` *{название платформы}*	Указывает агенту получать с сервера централизованной защиты обновления для антивирусного ядра, разработанного для указанной платформы, где *название платформы* – строка, содержащая название платформы. **Возможные значения:** • **GNU/Linux:** `unix-linux-32`, `unix-linux-64`, `unix-linux-mips` • **FreeBSD:** `unix-freebsd-32`, `unix-freebsd-64` • **Solaris:** `unix-solaris-32`, `unix-solaris-64` • **Darwin:** `unix-darwin-32`, `unix-darwin-64`  Настоятельно не рекомендуется изменять значение параметра, если вы не уверены, что это действительно необходимо. **Значение по умолчанию:** *Зависит от текущей используемой платформы*

Dr.Web HTTPD

Компонент Dr.Web HTTPD обеспечивает инфраструктуру для локального или удаленного взаимодействия с Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов UNIX по протоколу HTTPS. Данная возможность позволяет разработать для Dr.Web для файловых серверов 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 файловых серверов 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.

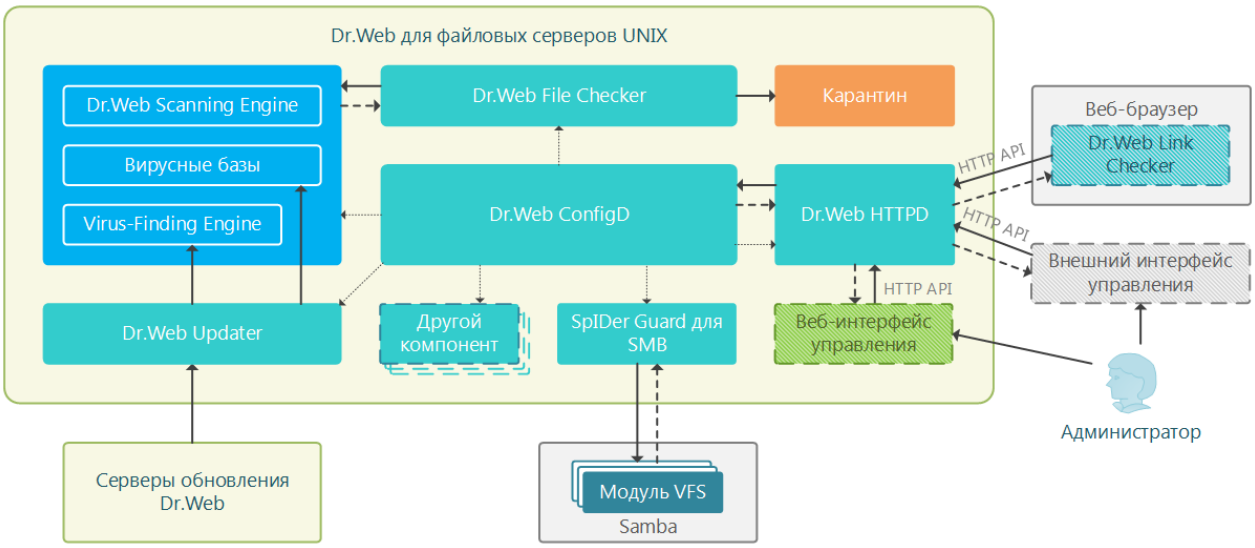

Рисунок 21. Схема работы компонента

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 файловых серверов UNIX, компоненту проверки файлов Dr.Web File Checker и монитору SpIDer Guard для NSS, 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 файловых серверов 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`	**Назначение:** Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. **Краткий вариант:** `-h` **Аргументы:** Нет.
`--version`	**Назначение:** Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. **Краткий вариант:** `-v` **Аргументы:** Нет.

Пример:

```
$ /opt/drweb.com/bin/drweb-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 файловых серверов 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 файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **`DefaultLogLevel`** из секции `[Root]`. **Значение по умолчанию:** `Notice`
`Log` *{тип журнала}*	Метод ведения журнала
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** *<opt_dir>*`/bin/drweb-httpd` • Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-httpd` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-httpd`
`Start` *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение `No` – немедленно завершить работу компонента. **Значение по умолчанию:** *Зависит от того, установлен ли веб-интерфейс управления продуктом.*
`WebConsoleAddress` *{адрес, ...}*	Определяет список сетевых сокетов (каждый сетевой сокет определяется парой *<IP-адрес>:<порт>*), прослушиваемых Dr.Web HTTPD в ожидании подключений к веб-интерфейсу 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.* **Значение по умолчанию:** `127.0.0.1:4443`
`LinkCheckerAddress` *{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.

	Может иметь список значений. Значения в списке указываются через запятую (каждое значение – в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). **Пример:** Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[<%HTTPD_SECTION%>]` ` LinkCheckerAddress = "192.168.0.1:1234", "10.20.30.45:5678"` • Две строки (по одному значению в строке) `[<%HTTPD_SECTION%>]` ` LinkCheckerAddress = 192.168.0.1:1234` ` LinkCheckerAddress = 10.20.30.45:5678` 2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset <%HTTPD_SECTION%>.LinkCheckerAddress -a 192.168.0.1:1234` `# drweb-ctl cfset <%HTTPD_SECTION%>.LinkCheckerAddress -a 10.20.30.45:5678` *Если не указано ни одного значения, то использование расширения Dr.Web Link Checker невозможно. Подключиться к веб-интерфейсу управления продуктом, используя данные адреса, невозможно.* **Значение по умолчанию:** *(не задано)*
`ServerSslCertificate` *{путь к файлу}*	Определяет путь к файлу серверного сертификата, используемого сервером веб-интерфейса управления для взаимодействия с клиентами по протоколу HTTPS. *Данный файл генерируется автоматически при установке компонента.* *Обратите внимание, что файл сертификата и файл закрытого ключа (определяется следующим параметром) должны соответствовать друг другу.* **Значение по умолчанию:** `<etc_dir>/certs/serv.crt` • Для **Linux**, **Solaris**: `/etc/opt/drweb.com/certs/serv.crt` • Для **FreeBSD**: `/usr/local/etc/drweb.com/certs/serv.crt`
`ServerSslKey` *{путь к файлу}*	Определяет путь к файлу закрытого ключа, используемого сервером веб-интерфейса управления для взаимодействия с клиентами по протоколу HTTPS.

	Данный файл генерируется автоматически при установке компонента. *Обратите внимание, что файл сертификата (определяется предыдущим параметром) и файл закрытого ключа должны соответствовать друг другу.* **Значение по умолчанию:** <*etc_dir*>`/certs/serv.key` • Для **Linux**, **Solaris**: `/etc/opt/drweb.com/certs/serv.key` • Для **FreeBSD**: `/usr/local/etc/drweb.com/certs/serv.key`
`WebconsoleRoot` *{путь к каталогу}*	Определяет путь к каталогу, в котором хранятся файлы, используемые веб-интерфейсом управления, если он установлен (аналог каталога `htdocs` для **Apache HTTP Server**). **Значение по умолчанию:** <*opt_dir*>`/share/drweb-httpd/webconsole` • Для **Linux**, **Solaris**: `/opt/drweb.com/share/drweb-httpd/webconsole` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/share/drweb-httpd/webconsole`
`LinkcheckerRoot` *{путь к каталогу}*	Определяет путь к каталогу, в котором хранятся файлы, используемые расширением для веб-браузеров Dr.Web Link Checker. **Значение по умолчанию:** <*opt_dir*>`/share/drweb-httpd/linkchecker` • Для **Linux**, **Solaris**: `/opt/drweb.com/share/drweb-httpd/linkchecker` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/share/drweb-httpd/linkchecker`
`AccessLogPath` *{путь к файлу}*	Определяет путь к файлу, хранящему журнал всех запросов HTTP/HTTPS, поступающих от клиентов к серверу веб-интерфейса управления. *Если параметр не задан, журнал HTTP/HTTPS-запросов сервером не ведется.* **Значение по умолчанию:** *(не задано)*

Dr.Web SNMPD

SNMP-агент Dr.Web Dr.Web SNMPD предназначен для интеграции программного комплекса Dr.Web для файловых серверов UNIX с системами мониторинга посредством протокола SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов Dr.Web для файловых серверов 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 2c 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 файловых серверов 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.

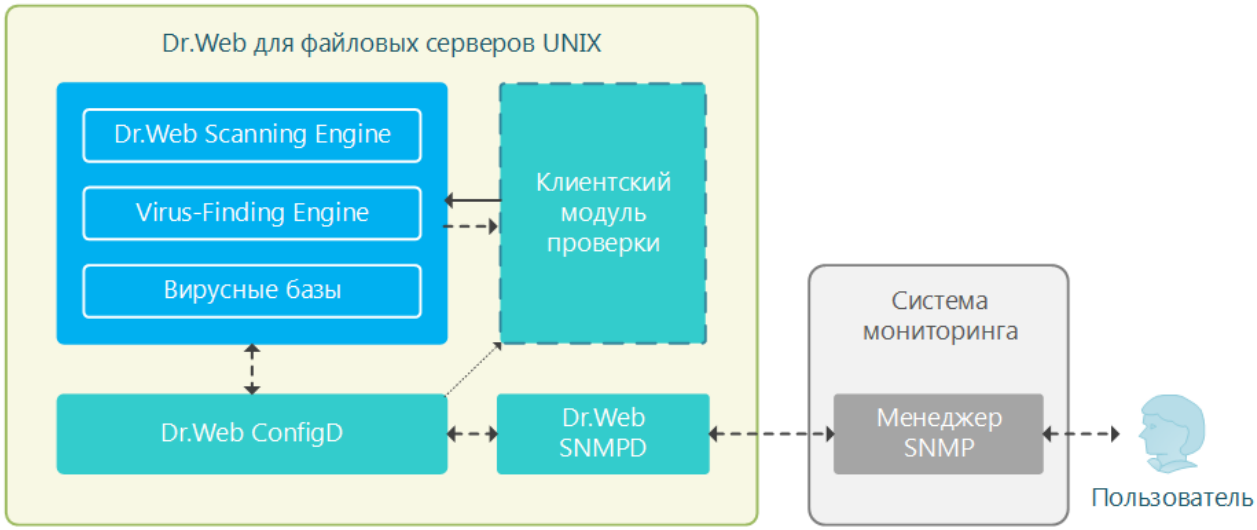

Рисунок 22. Схема работы компонента

Обнаружение угроз сканирующим ядром может происходить при проверках файлов, производящихся по запросам от различных компонентов Dr.Web для файловых серверов 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 файловых серверов 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 (`2c`, `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	**Назначение:** Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. **Краткий вариант:** -h **Аргументы:** Нет.
--version	**Назначение:** Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. **Краткий вариант:** -v **Аргументы:** Нет.

Пример:

```
$ /opt/drweb.com/bin/drweb-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 файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

LogLevel *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **DefaultLogLevel** из секции `[Root]`. **Значение по умолчанию:** `Notice`
Log *{тип журнала}*	Метод ведения журнала
ExePath *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>`/bin/drweb-snmpd` • Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-snmpd` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-snmpd`
Start *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение `No` – немедленно завершить работу компонента. **Значение по умолчанию:** `No`
RunAsUser *{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: **RunAsUser** `= name:123456`.

	Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска. **Значение по умолчанию:** `drweb`
`ListenAddress` *{адрес}*	Адрес (IP-адрес и порт), прослушиваемый агентом Dr.Web SNMPD в ожидании подключений от клиентов (менеджеров SNMP). *Обратите внимание, что для совместной работы с* **snmpd** *необходимо указать порт, отличный от стандартного (161), а кроме того, у* **snmpd** *необходимо настроить проксирование.* **Значение по умолчанию:** `127.0.0.1:161`
`SnmpVersion` *{V2c | V3}*	Используемая версия протокола SNMP (*SNMPv2c* или *SNMPv3*). **Значение по умолчанию:** `V2c`
`V3EngineId` *{строка}*	Строка-идентификатор *Engine ID* для *SNMPv3* (согласно RFC 3411). **Значение по умолчанию:** `800073FA044452574542`
`TrapReceiver` *{список адресов}*	Список адресов (IP-адрес и порт), на которые Dr.Web SNMPD будет отправлять уведомления *SNMP trap* при обнаружении угроз компонентами Dr.Web для файловых серверов UNIX. *Может иметь список значений. Значения в списке указываются через запятую (каждое значение – в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).* **Пример:** Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678. 1. Добавление значений в файл конфигурации. • Два значения в одной строке `[SNMPD]` ` TrapReceiver = "192.168.0.1:1234", "10.20.30.45:5678"` • Две строки (по одному значению в строке) `[SNMPD]` ` TrapReceiver = 192.168.0.1:1234` ` TrapReceiver = 10.20.30.45:5678`

	2. Добавление значений через команду **drweb-ctl** `cfset`. `# drweb-ctl cfset SNMPD.TrapReceiver -a 192.168.0.1:1234` `# drweb-ctl cfset SNMPD.TrapReceiver -a 10.20.30.45:5678` **Значение по умолчанию:** *(не задан)*
V2cCommunity *{строка}*	Строка «SNMP read community» для аутентификации менеджеров SNMP (протокол *SNMPv2c*) при доступе к переменным MIB Dr.Web для чтения. *Параметр используется в случае если задано* **SnmpVersion** = `V2c`. **Значение по умолчанию:** `public`
V3UserName *{строка}*	Имя пользователя для аутентификации менеджеров SNMP (протокол *SNMPv3*) для доступа к переменным MIB Dr.Web. *Параметр используется в случае если задано* **SnmpVersion** = `V3`. **Значение по умолчанию:** `noAuthUser`
V3Auth *{SHA(<pwd>) | MD5(<pwd>) | None}*	Метод аутентификации менеджеров SNMP (протокол *SNMPv3*) для доступа к переменным MIB Dr.Web. **Возможные значения:** • `SHA(<PWD>)` – используется SHA-хэш пароля (строки <*PWD*>). • `MD5(<PWD>)` – используется MD5-хэш пароля (строки <*PWD*>). • `None` – аутентификация не производится. где <*PWD*> – пароль в открытом виде (*plain text*). При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа `\`. **Примеры:** 1. Значение параметра в файле конфигурации: **V3Auth** = `MD5(123456)` 2. Задание этого же значения из командной строки с использованием команды **drweb-ctl** `cfset`: **drweb-ctl** `cfset SNMPD.V3Auth MD5\(123456\)`

	Параметр используется в случае если задано **SnmpVersion** = V3. **Значение по умолчанию:** None
V3Privacy *{DES(<secret>) | AES128(<secret>) | None}*	Метод шифрования содержимого SNMP-сообщений (протокол *SNMPv3*). **Возможные значения:** • DES(<*secret*>) – используется алгоритм шифрования DES. • AES128(<*secret*>) – используется алгоритм шифрования AES128. • None – шифрование содержимого SNMP-сообщений не производится. где <*secret*> – секрет, разделяемый менеджером и агентом (*plain text*). При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа \. **Примеры:** 1. Значение параметра в файле конфигурации: **V3Privacy** = AES128(supersecret) 2. Задание этого же значения из командной строки с использованием команды **drweb-ctl** cfset: **drweb-ctl** cfset SNMPD.V3Privacy AES128\(supersecret\) *Параметр используется в случае если задано* **SnmpVersion** = V3. **Значение по умолчанию:** None

Интеграция с системами мониторинга

SNMP-агент Dr.Web может выступать поставщиком данных для любой системы мониторинга, использующей протокол SNMP версии *2c* 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, 2c и 3. На основе этих шаблонных модулей можно создать любые подключаемые модули, опрашивающие состояние программного комплекса Dr.Web для файловых серверов UNIX через Dr.Web SNMPD.

В каталоге <*opt_dir*>/share/drweb-snmpd/connectors/munin поставляются следующие файлы.

Файл	Описание
plugins/snmp__drweb_malware	Подключаемый модуль **munin-node** для опроса Dr.Web SNMPD через SNMP с целью получения количества угроз, обнаруженных продуктом Dr.Web на узле.
plugins/snmp__drweb_filecheck	Подключаемый модуль **munin-node** для опроса Dr.Web SNMPD через SNMP с целью получения статистики проверки файлов продуктом Dr.Web на узле.
plugins/snmp__drweb_maild_multi	Подключаемый модуль **munin-node** 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 *multigraph* – особенность, реализованная в **Munin** версий старше 1.4.
`plugin-conf.d/drweb.cfg`	Пример конфигурации в **munin-node** 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 2c. 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
`zbx_drweb.xml`	Шаблон описания наблюдаемого узла с установленным антивирусным продуктом Dr.Web
`snmptt.drweb.zabbix.conf`	Настройки утилиты **snmptt** – приемника уведомлений *SNMP trap*

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 файловых серверов 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-snmpd/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-snmpd** 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 формировать 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-snmpd/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
nagiosgraph/rrdopts.conf-sample	Пример конфигурационного файла RRD
objects/drweb.cfg	Конфигурационный файл, описывающий объекты *drweb*
objects/nagiosgraph.cfg	Конфигурационный файл компонента построения графиков **Nagiosgraph**, используемого **Nagios**
plugins/check_drweb	Сценарий сбора данных от узла с продуктом Dr.Web
plugins/eventhandlers/submit_check_result	Сценарий обработки уведомлений *SNMP trap*
snmp/snmptt.drweb.nagios.conf	Настройки утилиты **snmptt** – приемника уведомлений *SNMP trap*

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 файловых серверов UNIX угроз на защищаемом сервере), на сервере мониторинга также должен быть установлен пакет net-snmp (используются стандартные утилиты **snmptt** 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 **snmplwalk**:

   ```
   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_perfdata_file=/usr/nagiosgraph/var/rrd/perfdata.log
service_perfdata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDE
SC$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=30
service_perfdata_file_processing_command=process-service-perfdata-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-snmpd/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 файловых серверов 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`		
alert	**Асинхронные уведомления о событиях (SNMP trap)**	
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
threatActionErrorAlertErrorCode	.1.2.6	Код ошибки (целое число, соответствует кодам из таблицы каталога ошибок)
threatActionErrorAlertAction	.1.2.7	Действие, попытка совершить которое привела к ошибке (целое число: 1 – лечить; 2 – переместить в карантин; 3 – удалить; 4 – информировать; 5 – игнорировать)
componentFailureAlert	.1.3	Уведомление о сбое в работе компонента
componentFailureAlertName	.1.3.1	Идентификатор компонента (целое число***)
componentFailureAlertExitCodeDescription	.1.3.2	Описание кода завершения компонента (строка)
componentFailureAlertExitCode	.1.3.3	Код завершения компонента (целое число, соответствует кодам из таблицы каталога ошибок)
infectedUrlAlert	.1.4	Уведомление о блокировании доступа к веб-ресурсу, содержащему угрозу (для соединений HTTP/HTTPS)
infectedUrlAlertUrl	.1.4.1	Заблокированный URL (строка)
infectedUrlAlertDirection	.1.4.2	Направление HTTP-сообщения (целое число: 1 – запрос, 2 – ответ)
infectedUrlAlertType	.1.4.3	Тип угрозы (целое число *)
infectedUrlAlertName	.1.4.4	Название угрозы (строка)
infectedUrlAlertOrigin	.1.4.5	Идентификатор компонента, обнаружившего угрозу (целое число***)
infectedUrlAlertSrcIp	.1.4.6	IP-адрес источника соединения (строка)
infectedUrlAlertSrcPort	.1.4.7	Порт источника соединения (целое число)

Имя параметра	OID параметра	Тип и описание параметра
infectedUrlAlertDstIp	.1.4.8	IP-адрес точки назначения соединения (строка)
infectedUrlAlertDstPort	.1.4.9	Порт точки назначения соединения (целое число)
infectedUrlAlertSniHost	.1.4.10	SNI точки назначения соединения (для SSL-соединений) (строка)
infectedUrlAlertExePath	.1.4.11	Исполняемый путь программы-инициатора соединения (строка)
infectedUrlAlertUserName	.1.4.12	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
infectedAttachmentAlert	.1.5	Уведомление об обнаружении вредоносного вложения в сообщении электронной почты
infectedAttachmentAlertType	.1.5.1	Тип угрозы (целое число *)
infectedAttachmentAlertName	.1.5.2	Название угрозы (строка)
infectedAttachmentAlertOrigin	.1.5.3	Идентификатор компонента, обнаружившего угрозу (целое число***)
infectedEmailAttachmentAlertSocket	.1.5.4	IP-адрес, с которого было получено сообщение электронной почты (строка)
infectedEmailAttachmentAlertMailFrom	.1.5.5	Отправитель сообщения электронной почты (строка)
infectedEmailAttachmentAlertRcptTo	.1.5.6	Список получателей сообщения электронной почты (строка)
infectedEmailAttachmentAlertMessageId	.1.5.7	Значение заголовка `Message-ID` сообщения электронной почты (строка)
infectedEmailAttachmentAlertAction	.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
		перепаковано; 2 – отклонено; 3 – отброшено; 4 – вылечено; 5 – перемещено в карантин, 6 – удалено)
infectedEmailAttachmentAlertDivert	.1.5.9	Направление движения сообщения электронной почты (целое число: 1 – входящее; 2 – исходящее)
infectedEmailAttachmentAlertSrcIp	.1.5.10	IP-адрес источника соединения (строка)
infectedEmailAttachmentAlertSrcPort	.1.5.11	Порт источника соединения (целое число)
infectedEmailAttachmentAlertDstIp	.1.5.12	IP-адрес точки назначения соединения (строка)
infectedEmailAttachmentAlertDstPort	.1.5.13	Порт точки назначения соединения (целое число)
infectedEmailAttachmentAlertSniHost	.1.5.14	SNI точки назначения соединения (для SSL-соединений) (строка)
infectedEmailAttachmentAlertProtocol	.1.5.15	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
infectedEmailAttachmentAlertExePath	.1.5.16	Исполняемый путь программы-инициатора соединения (строка)
infectedEmailAttachmentAlertUserName	.1.5.17	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
categoryUrlAlert	.1.6	Уведомление о блокировании доступа к веб-ресурсу, входящему в нежелательную категорию
categoryUrlAlertUrl	.1.6.1	Заблокированный URL (строка)
categoryUrlAlertCategory	.1.6.2	Категория веб-ресурсов, к которой относится URL (целое число**)

Имя параметра	OID параметра	Тип и описание параметра
categoryUrlAlertOrigin	.1.6.3	Идентификатор компонента, обнаружившего угрозу (целое число***)
categoryUrlAlertSrcIp	.1.6.4	IP-адрес источника соединения (строка)
categoryUrlAlertSrcPort	.1.6.5	Порт источника соединения (целое число)
categoryUrlAlertDstIp	.1.6.6	IP-адрес точки назначения соединения (строка)
categoryUrlAlertDstPort	.1.6.7	Порт точки назначения соединения (целое число)
categoryUrlAlertSniHost	.1.6.8	SNI точки назначения соединения (для SSL-соединений) (строка)
categoryUrlAlertExePath	.1.6.9	Исполняемый путь программы-инициатора соединения (строка)
categoryUrlAlertUserName	.1.6.10	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
categoryUrlEmailAttachmentAlert	.1.7	Уведомление об обнаружении нежелательного URL в сообщении электронной почты
categoryUrlEmailAttachmentAlertType	.1.7.1	Категория веб-ресурсов, к которой относится URL (целое число**)
categoryUrlEmailAttachmentAlertOrigin	.1.7.2	Идентификатор компонента, обнаружившего угрозу (целое число***)
categoryUrlEmailAttachmentAlertSocket	.1.7.3	IP-адрес, с которого было получено сообщение электронной почты (строка)
categoryUrlEmailAttachmentAlertMailFrom	.1.7.4	Отправитель сообщения электронной почты (строка)

Имя параметра	OID параметра	Тип и описание параметра
categoryUrlEmailAttachmentAlertRcptTo	.1.7.5	Список получателей сообщения электронной почты (строка)
categoryUrlEmailAttachmentAlertMessageId	.1.7.6	Значение заголовка `Message-ID` сообщения электронной почты (строка)
categoryUrlEmailAttachmentAlertAction	.1.7.7	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)
categoryUrlEmailAttachmentAlertDivert	.1.7.8	Направление движения сообщения электронной почты (целое число: 1 – входящее; 2 – исходящее)
categoryUrlEmailAttachmentAlertSrcIp	.1.7.9	IP-адрес источника соединения (строка)
categoryUrlEmailAttachmentAlertSrcPort	.1.7.10	Порт источника соединения (целое число)
categoryUrlEmailAttachmentAlertDstIp	.1.7.11	IP-адрес точки назначения соединения (строка)
categoryUrlEmailAttachmentAlertDstPort	.1.7.12	Порт точки назначения соединения (целое число)
categoryUrlEmailAttachmentAlertSniHost	.1.7.13	SNI точки назначения соединения (для SSL-соединений) (строка)
categoryUrlEmailAttachmentAlertProtocol	.1.7.14	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
categoryUrlEmailAttachmentAlertExePath	.1.7.15	Исполняемый путь программы-инициатора соединения (строка)
categoryUrlEmailAttachmentAlertUserName	.1.7.16	Имя пользователя, с правами которого исполняется 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)
spamEmailAlertProtocol	.1.8.13	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
spamEmailAlertExePath	.1.8.14	Исполняемый путь программы-инициатора соединения (строка)
spamEmailAlertUserName	.1.8.15	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
blockedConnectionAlert	.1.9	Уведомление о блокировке сетевого соединения
blockedConnectionAlertOrigin	.1.9.1	Идентификатор компонента, обнаружившего угрозу (целое число***)
blockedConnectionAlertDivert	.1.9.2	Направление соединения (целое число: 1 – входящее; 2 – исходящее)
blockedConnectionAlertSrcIp	.1.9.3	IP-адрес источника соединения (строка)
blockedConnectionAlertSrcPort	.1.9.4	Порт источника соединения (целое число)
blockedConnectionAlertDstIp	.1.9.5	IP-адрес точки назначения соединения (строка)
blockedConnectionAlertDstPort	.1.9.6	Порт точки назначения соединения (целое число)
blockedConnectionAlertSniHost	.1.9.7	SNI точки назначения соединения (для SSL-соединений) (строка)
blockedConnectionAlertProtocol	.1.9.8	Тип протокола (целое число: 1 – SMTP; 2 – POP3; 3 – IMAP; 4 – HTTP)
blockedConnectionAlertExePath	.1.9.9	Исполняемый путь программы-инициатора соединения (строка)

Имя параметра	OID параметра	Тип и описание параметра
blockedConnectionAlertUserName	.1.9.10	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
stat	**Статистические показатели работы программного комплекса**	
threatCounters	.2.1	Счетчики обнаруженных угроз
knownVirus	.2.1.1	Число обнаруженных известных вирусов (счетчик; целое число)
suspicious	.2.1.2	Число обнаруженных подозрительных объектов (счетчик; целое число)
adware	.2.1.3	Число обнаруженных рекламных программ (счетчик; целое число)
dialers	.2.1.4	Число обнаруженных программ дозвона (счетчик; целое число)
joke	.2.1.5	Число обнаруженных шуточных программ (счетчик; целое число)
riskware	.2.1.6	Число обнаруженных потенциально опасных программ (счетчик; целое число)
hacktool	.2.1.7	Число обнаруженных программ взлома (счетчик; целое число)
scanErrors	.2.2	Счетчики произошедших ошибок проверки файлов
sePathNotAbsolute	.2.2.1	Количество возникновений ошибки «Не абсолютный путь» (счетчик; целое число)
seFileNotFound	.2.2.2	Количество возникновений ошибки «Файл не найден» (счетчик; целое число)
seFileNotRegular	.2.2.3	Количество возникновений ошибки «Специальный (не

Имя параметра	OID параметра	Тип и описание параметра
		регулярный) файл» (счетчик; целое число)
seFileNotBlockDevice	.2.2.4	Количество возникновений ошибки «Файл – не блочное устройство» (счетчик; целое число)
seNameTooLong	.2.2.5	Количество возникновений ошибки «Слишком длинный путь или имя файла» (счетчик; целое число)
seNoAccess	.2.2.6	Количество возникновений ошибки «Доступ запрещен» (счетчик; целое число)
seReadError	.2.2.7	Количество возникновений ошибки «Ошибка чтения» (счетчик; целое число)
seWriteError	.2.2.8	Количество возникновений ошибки «Ошибка записи» (счетчик; целое число)
seFileTooLarge	.2.2.9	Количество возникновений ошибки «Файл слишком большой» (счетчик; целое число)
seFileBusy	.2.2.10	Количество возникновений ошибки «Файл занят» (счетчик; целое число)
seUnpackingError	.2.2.20	Количество возникновений ошибки «Ошибка распаковки» (счетчик; целое число)
sePasswordProtecetd	.2.2.21	Количество возникновений ошибки «Защищено паролем» (счетчик; целое число)
seArchCrcError	.2.2.22	Количество возникновений ошибки «Ошибка контрольной суммы архива» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
seArchInvalidHeader	.2.2.23	Количество возникновений ошибки «Недопустимый заголовок архива» (счетчик; целое число)
seArchNoMemory	.2.2.24	Количество возникновений ошибки «Недостаточно памяти для обработки архива» (счетчик; целое число)
seArchIncomplete	.2.2.25	Количество возникновений ошибки «Неожиданный конец архива» (счетчик; целое число)
seCanNotBeCured	.2.2.26	Количество возникновений ошибки «Объект не может быть вылечен» (счетчик; целое число)
sePackerLevelLimit	.2.2.30	Количество возникновений ошибки «Превышение допустимого уровня вложенности для запакованных объектов» (счетчик; целое число)
seArchiveLevelLimit	.2.2.31	Количество возникновений ошибки «Превышение допустимого уровня вложенности для архивов» (счетчик; целое число)
seMailLevelLimit	.2.2.32	Количество возникновений ошибки «Превышение допустимого уровня вложенности для почтовых файлов» (счетчик; целое число)
seContainerLevelLimit	.2.2.33	Количество возникновений ошибки «Превышение допустимого уровня вложенности для контейнеров» (счетчик; целое число)
seCompressionLimit	.2.2.34	Количество возникновений ошибки «Превышение допустимой величины

Имя параметра	OID параметра	Тип и описание параметра
		коэффициента сжатия» (счетчик; целое число)
seReportSizeLimit	.2.2.35	Количество возникновений ошибки «Превышение допустимого размера отчета о проверке» (счетчик; целое число)
seScanTimeout	.2.2.40	Количество возникновений ошибки «Истекло время на проверку файла» (счетчик; целое число)
seEngineCrash	.2.2.41	Количество возникновений ошибки «Обнаружен сбой сканирующего ядра» (счетчик; целое число)
seEngineHangup	.2.2.42	Количество возникновений ошибки «Перестало отвечать сканирующее ядро» (счетчик; целое число)
seEngineError	.2.2.44	Количество возникновений ошибки «Внутренняя ошибка сканирующего ядра» (счетчик; целое число)
seNoLicense	.2.2.45	Количество возникновений ошибки «Не найдена действующая лицензия» (счетчик; целое число)
seNonSupportedDisk	.2.2.50	Количество возникновений ошибки «Не поддерживаемый диск» (счетчик; целое число)
seUnexpectedError	.2.2.100	Количество возникновений ошибки «Неожиданная ошибка» (счетчик; целое число)
scanLoadAverage	.2.3	Показатели нагрузки проверки файлов
filesScannedTable	.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
markedAsSpam	.2.4.1	Число сообщений электронной почты, отмеченных, как спам (счетчик; целое число)
blockedInfectionSource	.2.4.101	Число заблокированных URL из категории «Источники распространения вирусов» (счетчик; целое число)
blockedNotRecommended	.2.4.102	Число заблокированных URL из категории «Нерекомендуемые» (счетчик; целое число)
blockedAdultContent	.2.4.103	Число заблокированных URL из категории «Сайты для взрослых» (счетчик; целое число)
blockedViolence	.2.4.104	Число заблокированных URL из категории «Насилие» (счетчик; целое число)
blockedWeapons	.2.4.105	Число заблокированных URL из категории «Оружие» (счетчик; целое число)
blockedGambling	.2.4.106	Число заблокированных URL из категории «Азартные игры» (счетчик; целое число)
blockedDrugs	.2.4.107	Число заблокированных URL из категории «Наркотики» (счетчик; целое число)
blockedObsceneLanguage	.2.4.108	Число заблокированных URL из категории «Нецензурная лексика» (счетчик; целое число)
blockedChats	.2.4.109	Число заблокированных URL из категории «Чаты» (счетчик; целое число)
blockedTerrorism	.2.4.110	Число заблокированных URL из категории «Терроризм» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
blockedFreeEmail	.2.4.111	Число заблокированных URL из категории «Бесплатная электронная почта» (счетчик; целое число)
blockedSocialNetworks	.2.4.112	Число заблокированных URL из категории «Социальные сети» (счетчик; целое число)
blockedOwnersNotice	.2.4.113	Число заблокированных URL из категории «По обращению правообладателя» (счетчик; целое число)
blockedBlackList	.2.4.120	Число заблокированных URL из пользовательского черного списка (счетчик; целое число)
info	**Информация о состоянии программного комплекса**	
components	.3.1	Состояние компонентов программного комплекса
configd	.3.1.1	Данные о компоненте **drweb-configd**
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 (*UNIX time*)
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 (*UNIX time*)
configdAppIniSection	.3.1.1.101.1.5	Имя секции с параметрами компонента в конфигурационном файле (строка)
scanEngine	.3.1.2	Данные о компоненте **drweb-se**
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 (*UNIX time*)
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 (*UNIX time*)

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)
fileCheck	.3.1.3	Данные о компоненте **drweb-filecheck**
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 **drweb-update**
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)
esagent	.3.1.5	Данные о компоненте **drweb-esagent**
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 (*UNIX time*)
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)
netcheck	.3.1.6	Данные о компоненте **drweb-netcheck**
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 (*UNIX time*)
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 **drweb-httpd**

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*)
snmpd	.3.1.8	Данные о компоненте **drweb-snmpd**
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*)
clamd	.3.1.20	Данные о компоненте **drweb-clamd**
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*)
icapd	.3.1.21	Данные о компоненте **drweb-icapd**
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 (*UNIX time*)
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 *OPTIONS* (счетчик; целое число)
icapdReqmod	.3.1.21.104	Число запросов *REQMOD* (счетчик; целое число)
icapdRespmod	.3.1.21.105	Число запросов *RESPMOD* (счетчик; целое число)
icapdBad	.3.1.21.106	Число некорректных запросов (счетчик; целое число)
smbspider	.3.1.40	Данные о компоненте **drweb-smbspider-daemon**
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 (*UNIX time*)
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 **Samba**
smbspiderShareEntry	.3.1.40.103.1	Информация о защищаемом ресурсе **Samba** (строка

Имя параметра	OID параметра	Тип и описание параметра
		таблицы; запись)
smbspiderShareIndex	.3.1.40.103.1.1	Индекс (номер) защищаемого ресурса **Samba** (целое число)
smbspiderSharePath	.3.1.40.103.1.2	Путь к защищаемому ресурсу **Samba** (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)
gated	.3.1.41	Данные о компоненте **drweb-gated**
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 (*UNIX time*)
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)
maild	.3.1.42	Данные о компоненте **drweb-maild**
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 **drweb-maild**
maildStatNative	.3.1.42.4.1	Статистика проверки сообщений электронной почты через внутренний интерфейс компонента **drweb-maild** (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 *Milter* компонента **drweb-maild**
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 *Spamd* компонента **drweb-maild**
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 *Rspamd* компонента **drweb-maild**
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)
lookupd	.3.1.43	Данные о компоненте **drweb-lookupd**
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*)
cloudd	.3.1.50	Данные о компоненте **drweb-cloudd**
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*)
vpnd	.3.1.51	Данные о компоненте **drweb-vpnd**
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 (*UNIX time*)
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)
meshd	.3.1.52	Данные о компоненте **drweb-meshd**
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 (*UNIX time*)
lotus	.3.1.60	Данные о компоненте **drweb-lotus**
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 (*UNIX time*)

Имя параметра	OID параметра	Тип и описание параметра
macgui	.3.1.100	Данные о компоненте **drweb-gui** (для **OS X**)
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 (*UNIX time*)
macspider	.3.1.102	Данные о компоненте **drweb-spider** (для **OS X**)
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 (*UNIX time*)
macspiderWorkStatus	.3.1.102.101	Режим работы компонента (целое число: 0 – не задан, 1 – загружается, 2 – запущен)
macfirewall	.3.1.103	Данные о компоненте **drweb-firewall** (для **OS X**)
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 (*UNIX time*)
linuxgui	.3.1.200	Данные о компоненте **drweb-gui** (для **Linux**)

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*)
linuxspider	.3.1.201	Данные о компоненте **drweb-spider** (для **Linux**)
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 **fanotify**, 3 – LKM)
linuxnss	.3.1.202	Данные о компоненте **drweb-nss** (для **Linux**)
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 **drweb-firewall** (для **Linux**)
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 (*UNIX time*)
ctl	.3.1.300	Данные о компоненте **drweb-ctl**
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 (*UNIX time*)
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 (*UNIX time*)
licenseExpires	.3.2.5	Дата прекращения действия лицензии (*UNIX time*)

*) Типы угроз:

Код	Тип угрозы
1	Известный вирус (*known virus*)
2	Подозрительный объект (*suspicious*)
3	Рекламная программа (*adware*)
4	Программа дозвона (*dialer*)
5	Программа-шутка (*joke program*)
6	Потенциально опасная программа (*riskware*)
7	Программа взлома (*hacktool*)

**) Категории URL:

Код	Тип угрозы
1	Источник распространения вирусов (*infectionSource*)
2	Не рекомендуемый (*notRecommended*)
3	Сайты для взрослых (*adultContent*)
4	Насилие (*violence*)
5	Оружие (*weapons*)
6	Азартные игры (*gambling*)
7	Наркотики (*drugs*)
8	Нецензурная лексика (*obsceneLanguage*)
9	Чаты (*chats*)
10	Терроризм (*terrorism*)
11	Бесплатная электронная почта (*freeEmail*)
12	Социальные сети (*socialNetworks*)
13	Добавленные по обращению правообладателя (*ownerNotice*)
14	Черный список (*blackList*)

***) Коды компонентов Dr.Web:

Код	Компонент
1	Dr.Web ConfigD (**drweb-configd**)
2	Dr.Web Scanning Engine (**drweb-se**)
3	Dr.Web File Checker (**drweb-filecheck**)
4	Dr.Web Updater (**drweb-update**)
5	Dr.Web ES Agent (**drweb-esagent**)
6	Dr.Web Network Checker (**drweb-netcheck**)
7	Dr.Web HTTPD (**drweb-httpd**)
8	Dr.Web SNMPD (**drweb-snmpd**)
20	Dr.Web ClamD (**drweb-clamd**)
21	Dr.Web ICAPD (**drweb-icapd**)
40	SpIDer Guard для SMB (**drweb-smbspider-daemon**)
41	SpIDer Gate (**drweb-gated**)
42	Dr.Web MailD (**drweb-maild**)
43	Dr.Web LookupD (**drweb-lookupd**)
50	Dr.Web CloudD (**drweb-cloudd**)
51	Dr.Web VPND (**drweb-vpnd**)
52	Dr.Web MeshD (**drweb-meshd**)
60	Dr.Web для Lotus
100	**drweb-gui** для **macOS**
102	SpIDer Guard для **macOC**
103	Dr.Web Firewall для Linux для **macOS**
200	**drweb-gui** для **Linux**
201	SpIDer Guard (**drweb-spider**)
202	SpIDer Guard для NSS (**drweb-nss**)
203	Dr.Web Firewall для Linux (**drweb-firewall**) для **Linux**

Код	Компонент
300	Dr.Web Ctl (**drweb-ctl**)
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.

Принципы работы

Компонент предназначен 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 предопределенных 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 файловых серверов UNIX. Схема работы компонента показана на рисунке ниже.

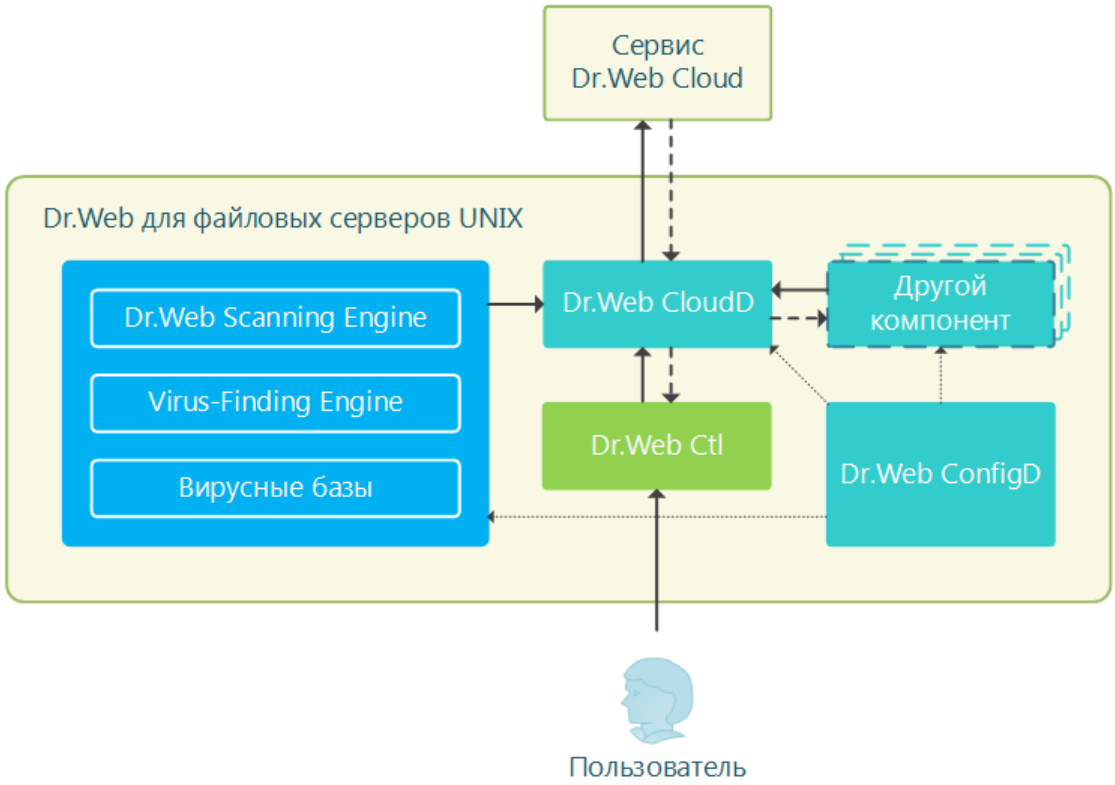

Рисунок 23. Схема работы компонента

Запросы к облачному сервису Dr.Web (на проверку URL или файлов) через данный компонент могут отправлять различные компоненты программного комплекса Dr.Web для файловых серверов UNIX, отмеченные на схеме как «Другой компонент» (в зависимости от состава продукта).

Кроме того, компонент используется при проверке файлов по команде от утилиты управления продуктом Dr.Web для файловых серверов 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`	**Назначение:** Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. **Краткий вариант:** `-h` **Аргументы:** Нет.
`--version`	**Назначение:** Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. **Краткий вариант:** `-v` **Аргументы:** Нет.

Пример:

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

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 файловых серверов 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 файловых серверов UNIX.

В секции представлены следующие параметры:

`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра **`DefaultLogLevel`** из секции `[Root]`. **Значение по умолчанию:** `Notice`
`Log` *{тип журнала}*	Метод ведения журнала
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. **Значение по умолчанию:** <*opt_dir*>`/bin/drweb-cloudd` • Для **Linux**, **Solaris**: `/opt/drweb.com/bin/drweb-cloudd` • Для **FreeBSD**: `/usr/local/libexec/drweb.com/bin/drweb-cloudd`
`RunAsUser` *{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: **`RunAsUser`** `= name:123456`. *Если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.* **Значение по умолчанию:** `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Минимальное значение – `10s`. **Значение по умолчанию:** `30s`
`PersistentCache` *{On | Off}*	Включать или нет сохранение на диск кэша ответов, получаемых от Dr.Web Cloud. **Значение по умолчанию:** `Off`

DebugSdk *{логический}*	Включать или нет в журнал на отладочном уровне (при **LogLevel** = DEBUG) подробные сообщения от Dr.Web Cloud. **Значение по умолчанию:** No

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 пишутся на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т.д.) и по инфицируемым ими операционным системам.

Компьютерные черви

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

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

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

В компании «Доктор Веб» червей делят по способу (среде) распространения:

- *сетевые черви* распространяются посредством различных сетевых протоколов и протоколов обмена файлами;

- *почтовые черви* распространяются посредством почтовых протоколов (POP3, SMTP и т.д.);
- *чат-черви* распространяются, используя популярные программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т.д.).

Троянские программы

Этот тип вредоносных программ не способен к саморепликации. Троянские программы подменяют какую-либо из часто запускаемых программ и выполняют ее функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т.д.), либо делая возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловых сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполнять другие типы угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- *бэкдоры* – это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы; они прописывают себя в реестре, модифицируя ключи;
- *руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (*User Mode Rootkits – UMR*), и руткиты, работающие в режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет обнаружение и обезвреживание) (*Kernel Mode Rootkits – KMR*);
- *клавиатурные перехватчики (кейлоггеры)* используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действия является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т.д.);
- *кликеры* переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь

перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак);

- *прокси-трояны* предоставляют злоумышленнику анонимный выход в сеть Интернет через компьютер жертвы.

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

Программы взлома

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

Рекламные программы

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

Программы-шутки

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

Программы дозвона

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

Потенциально опасные программы

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

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типов компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать в карантин, а также 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 разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке запакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, запакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

Действия с угрозами

В продуктах Dr.Web реализована возможность применять определенные действия к обнаруженным объектам для обезвреживания компьютерных угроз. Пользователь может оставить автоматически применяемые к определенным типам угроз действия, заданные по умолчанию, изменить их или выбирать нужное действия для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий:

- *Ignore (Игнорировать)* – Пропустить обнаруженную угрозу, не предпринимая никаких действий.
- *Report (Информировать)* – Уведомить о наличии угрозы, но ничего не делать с инфицированным объектом.
- *Block (Блокировать)* – Заблокировать все виды доступа к инфицированному файлу (действие может быть доступно не для всех компонентов).
- *Cure (Лечить)* – Попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое. Обратите внимание, что это действие применимо не ко всем видам угроз.
- *Quarantine (Переместить в Карантин, Изолировать)* – Переместить инфицированный объект (если он допускает эту операцию) в специальный каталог карантина с целью его изоляции.
- *Delete (Удалить)* – Безвозвратно удалить инфицированный объект.

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

Приложение В. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.

Приложение Г. Конфигурационный файл программного комплекса

Параметрами конфигурации всех компонентов программного комплекса Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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 файловых серверов 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, ..., 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 операционным 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 файловых серверов 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 файловых серверов 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 файловых серверов 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.
  - `Block` – Оставить файл неизменным, но заблокировать все виды доступа к нему (действие может быть доступно не для всех компонентов).
  - `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.

Приложение Д. Генерация сертификатов SSL

Для компонентов программного комплекса Dr.Web для файловых серверов 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 CA

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 CA 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 удается, 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 файловых серверов 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 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: *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, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Если ошибка вызвана компонентом SpIDer Guard, то скорее всего задан способ работы компонента, который не поддерживается операционной системой. Проверьте установленный режим работы компонента и при необходимости исправьте его, указав значение `AUTO` (параметр **`Mode`** в секции `[LinuxSpider]` файла конфигурации).
   - Для просмотра и исправления режима перейдите на страницу настроек **SpIDer Guard** веб-интерфейса управления (если он установлен).
   - Также вы можете воспользоваться командами утилиты управления из командной строки.

   Для установки значения `AUTO` введите команду

   ```
   # Dr.Web Ctl cfset LinuxSpider.Mode AUTO
   ```

   Для сброса значения параметра в значение по умолчанию введите команду

   ```
   # Dr.Web Ctl cfset LinuxSpider.Mode -r
   ```

   - Если ошибка повторится, выполните ручную сборку и установку загружаемого модуля ядра для компонента SpIDer Guard.

   

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

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).

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 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, препятствующие 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. Отключите или перенастройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе Dr.Web для файловых серверов UNIX.

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

Сообщение об ошибке: *Недоступен модуль ядра Linux для SpIDer Guard.*

Код ошибки: `x113`

Описание: SpIDer Guard для работы требуется модуль ядра **Linux**, который отсутствует.

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 установленный режим работы компонента и при необходимости исправьте его, указав значение `AUTO` (параметр **`Mode`** в секции `[LinuxSpider]` файла конфигурации).
   - Для просмотра и исправления режима перейдите на страницу настроек SpIDer Guard веб-

интерфейса управления (если он установлен).

- Также вы можете воспользоваться командами утилиты управления из командной строки.

Для установки значения `AUTO` введите команду

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

Для сброса значения параметра в значение по умолчанию введите команду

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

2. Если ошибка повторится, выполните ручную сборку и установку загружаемого модуля ядра для компонента SpIDer Guard.

> ⚠ Работа компонента SpIDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список протестированных дистрибутивов **UNIX** (см. раздел Системные требования).

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 файловых серверов 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 файловых серверов 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: *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

Симптомы	После установки модуля ядра SpIDer Guard работа операционной системы аварийно завершается с ошибкой ядра «*Kernel panic*»
Описание	Работа модуля ядра SpIDer Guard невозможна в среде исполнения ядра ОС (например, ОС работает в среде гипервизора **Xen**).

Устранение ошибки:

1. Отмените загрузку модуля ядра SpIDer Guard (модуль ядра имеет имя `drweb`), добавив в загрузчике **grub** строку

   ```
   drweb.blacklist=yes
   ```

   в строку параметров загрузки ядра ОС.
2. После загрузки ОС удалите модуль `drweb.ko` из каталога дополнительных модулей `/lib/modules/`uname -r`/extra`.
3. Установите для SpIDer Guard режим работы *AUTO*, выполнив команды:

   ```
   # drweb-ctl cfset LinuxSpider.Mode Auto
   # drweb-ctl reload
   ```
4. Если используемая вами ОС не поддерживает механизм **fanotify**, или использование этого режима не позволяет использовать SpIDer Guard для полноценного контроля файловой системы (актуально для систем **GNU/Linux** с мандатными моделями доступа, например – **Astra Linux**), и, таким образом, использование режима *LKM* является обязательным для контроля файловой системы, то откажитесь от использования гипервизора **Xen**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы:	Dr.Web MailD, SpIDer Gate, Dr.Web ICAPD (перечень указанных компонентов зависит от установленного продукта) не проверяют сообщения, в журнале Dr.Web для файловых серверов UNIX наблюдаются сообщения `Too many open files`.
Описание:	В связи большой загрузкой по проверке данных компонент Dr.Web Network Checker исчерпал доступный лимит на число доступных файловых дескрипторов.

Устранение ошибки:

1. Увеличьте лимит на число открытых файловых дескрипторов, доступных приложению, используя команду **ulimit** `-n` (по умолчанию лимит на число дескрипторов для Dr.Web для файловых серверов UNIX составляет 16384).

   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:

```
[Service]
LimitNOFILE=16384
```

С перечнем доступных лимитов **systemd** вы можете ознакомиться в документации **man** `systemd.exec`.

2. После изменения лимита перезапустите Dr.Web для файловых серверов UNIX, выполнив команду

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы:	Не удается установить соединение с веб-интерфейсом управления Dr.Web в браузере, компоненты Dr.Web отсутствуют в перечне запущенных процессов (**ps** `ax | grep drweb`), выполнение любой команды **drweb-ctl** *<команда>*, за исключением команды **drweb-ctl** `rawscan`, выводит сообщение об ошибке `Error: connect: No such file or directory: "<путь>/.com.drweb.public"` или `Error: connect: Connection refused: "<путь>/.com.drweb.public".`
Описание:	Dr.Web для файловых серверов 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 файловых серверов 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 файловых серверов 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.

Внутренний каталог ошибок

Код ошибки	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
0	EC_OK	*Success*	Не является ошибкой
1	EC_MONITOR_IPC_ERROR	*Error on monitor channel*	Ошибка x1
2	EC_ALREADY_IN_PROGRESS	*Operation is already in progress*	Ошибка x2
3	EC_IN_PENDING_STATE	*Operation is in pending state*	Ошибка x3
4	EC_INTERRUPTED_BY_USER	*Interrupted by user*	Ошибка x4
5	EC_CANCELED	*Operation canceled*	Ошибка x5
6	EC_LINK_DISCONNECTED	*Link disconnected*	Ошибка x6
7	EC_BAD_MESSAGE_SIZE	*Invalid IPC message size*	Ошибка x7
8	EC_BAD_MESSAGE_FORMAT	*Invalid IPC message format*	Ошибка x8
9	EC_NOT_READY	*Not ready*	Ошибка x9
10	EC_NOT_INSTALLED	*Component is not installed*	Ошибка x10
11	EC_UNEXPECTED_MESSAGE	*Unexpected IPC message*	Ошибка x11
12	EC_PROTOCOL_VIOLATION	*Protocol violation*	Ошибка x12
13	EC_UNKNOWN_STATE	*Subsystem state is unknown*	Ошибка x13
20	EC_NOT_ABSOLUTE_PATH	*Path must be absolute*	Ошибка x20
21	EC_NO_MEMORY	*Not enough memory*	Ошибка x21
22	EC_IO_ERROR	*IO error*	Ошибка x22
23	EC_NO_SUCH_ENTRY	*No such file or directory*	Ошибка x23
24	EC_PERMISSION_DENIED	*Permission denied*	Ошибка x24
25	EC_NOT_A_DIRECTORY	*Not a directory*	Ошибка x25
26	EC_DATA_CORRUPTED	*Data file corrupted*	Ошибка x26
27	EC_FILE_EXISTS	*File already exists*	Ошибка x27

Код ошибки	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
28	EC_READ_ONLY_FS	*Read-only file system*	Ошибка x28
29	EC_NETWORK_ERROR	*Network error*	Ошибка x29
30	EC_NOT_A_DRIVE	*Not a drive*	Ошибка x30
31	EC_UNEXPECTED_EOF	*Unexpected EOF*	Ошибка x31
32	EC_FILE_WAS_CHANGED	*File was changed*	Ошибка x32
33	EC_NOT_A_REGULAR_FILE	*Not a regular file*	Ошибка x33
34	EC_NAME_ALREADY_IN_USE	*Name already in use*	Ошибка x34
35	EC_HOST_OFFLINE	*Host is offline*	Ошибка x35
36	EC_LIMIT_REACHED	*Resource limit reached*	Ошибка x36
37	EC_CROSS_DEVICE_LINK	*Mounting points are different*	Ошибка x37
38	EC_UNPACKING_ERROR	*Unpacking error*	Ошибка x38
40	EC_BASE_CORRUPTED	*Virus base corrupted*	Ошибка x40
41	EC_OLD_BASE_VERSION	*Non-supported virus database version*	Ошибка x41
42	EC_EMPTY_BASE	*Empty virus database*	Ошибка x42
43	EC_CAN_NOT_BE_CURED	*Object cannot be cured*	Ошибка x43
44	EC_INVALID_BASE_SET	*Non-supported virus database combination*	Ошибка x44
45	EC_SCAN_LIMIT_REACHED	*Scan limit reached*	Ошибка x45
47	EC_AUTH_FAILED	*Authentication failed*	Ошибка x47
48	EC_NOT_AUTHORIZED	*Authorization failed*	Ошибка x48
49	EC_INVALID_TOKEN	*Access token is invalid*	Ошибка x49
60	EC_INVALID_ARGUMENT	*Invalid argument*	Ошибка x60
61	EC_INVALID_OPERATION	*Invalid operation*	Ошибка x61
62	EC_ROOT_ONLY	*Superuser privileges required*	Ошибка x62
63	EC_STANDALONE_MODE_ONLY	*Not allowed in central protection mode*	Ошибка x63

Код ошибки	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
64	EC_NON_SUPPORTED_OS	*Non-supported OS*	Ошибка x64
65	EC_NOT_IMPLEMENTED	*Feature not implemented*	Ошибка x65
66	EC_UNKNOWN_OPTION	*Unknown option*	Ошибка x66
67	EC_UNKNOWN_SECTION	*Unknown section*	Ошибка x67
68	EC_INVALID_OPTION_VALUE	*Invalid option value*	Ошибка x68
69	EC_INVALID_STATE	*Invalid state*	Ошибка x69
70	EC_NOT_LIST_OPTION	*Only one value allowed*	Ошибка x70
71	EC_INVALID_TAG	*Tag value is invalid*	Ошибка x71
80	EC_RECORD_NOT_FOUND	*Record not found*	Ошибка x80
81	EC_RECORD_BUSY	*Record is in process now*	Ошибка x81
82	EC_QUARANTINED_FILE	*File has already been quarantined*	Ошибка x82
89	EC_BACKUP_FAILED	*Cannot backup before update*	Ошибка x89
90	EC_BAD_DRL_FILE	*Invalid DRL file*	Ошибка x90
91	EC_BAD_LST_FILE	*Invalid LST file*	Ошибка x91
92	EC_BAD_LZMA_FILE	*Invalid compressed file*	Ошибка x92
93	EC_PROXY_AUTH_ERROR	*Proxy authentication error*	Ошибка x93
94	EC_NO_UPDATE_SERVERS	*No update servers available*	Ошибка x94
95	EC_BAD_KEY_FORMAT	*Invalid key file format*	Ошибка x95
96	EC_EXPIRED_KEY	*License is already expired*	Ошибка x96
97	EC_NETWORK_TIMEDOUT	*Network operation timed out*	Ошибка x97
98	EC_BAD_CHECKSUM	*Invalid checksum*	Ошибка x98
99	EC_BAD_TRIAL_KEY	*Invalid trial license*	Ошибка x99
100	EC_BLOCKED_LICENSE	*Blocked license key*	Ошибка x100
101	EC_BAD_LICENSE	*Invalid license*	Ошибка x101

Код ошибки	Символическое обозначение	Внутреннее сообщение об ошибке	Описание
102	EC_BAD_CONFIG	*Invalid configuration*	Ошибка x102
104	EC_BAD_EXECUTABLE	*Invalid executable file*	Ошибка x104
105	EC_NO_CORE_ENGINE	*Core engine is not available*	Ошибка x105
106	EC_NO_VIRUS_BASES	*No virus databases*	Ошибка x106
107	EC_APP_TERMINATED	*Process terminated by signal*	Ошибка x107
108	EC_APP_CRASHED	*Unexpected process termination*	Ошибка x108
109	EC_INCOMPATIBLE	*Incompatible software detected*	Ошибка x109
113	EC_NO_KERNEL_MODULE	*Kernel module is not available*	Ошибка x113
119	EC_NO_SCAN_ENGINE	*ScanEngine is not available*	Ошибка x119
120	EC_NO_FILE_CHECK	*FileCheck is not available*	Ошибка x120
121	EC_NO_ESAGENT	*ESAgent is not available*	Ошибка x121
123	EC_NO_NET_CHECK	*NetCheck is not available*	Ошибка x123
124	EC_NO_CLOUDD	*CloudD is not available*	Ошибка x124
125	EC_UNEXPECTED_ERROR	*Unexpected error*	Ошибка x125

Приложение Ж. Список сокращений

В данном руководстве следующие термины использованы без расшифровки:

Обозначение	Расшифровка
EPM	ESP Package Manager (менеджер пакетов)
FQDN	Fully Qualified Domain Name
GID	Group ID (системный идентификатор группы пользователей)
GNU	Проект GNU (GNU is Not Unix)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol

Обозначение	Расшифровка
HTTPS	HyperText Transfer Protocol Secure (через SSL/TLS)
ID	Идентификатор
IP	Internet Protocol
LKM	Linux Kernel Module
MBR	Master Boot Record
NSS	Novell Storage Services
OID	(SNMP) Object ID
PID	Process ID (системный идентификатор процесса)
PAM	Pluggable Authentication Modules
RPM	Red Hat Package Manager (менеджер пакетов)
RRA	Round-Robin Archive
RRD	Round-Robin Database
SMB	Server Message Block (протокол доступа к файлам)
SNMP	Simple Network Management Protocol
SP	Service Pack
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User ID (системный идентификатор пользователя)
URL	Unified Resource Locator
VBR	Volume Boot Record
ОС	Операционная система
ФС	Файловая система

Предметный указатель

Предметный указатель

Предметный указатель

Т

У

Ф

Ц