Dr.WEB®

Антивирус для файловых серверов UNIX

Защити созданное

Руководство администратора

Антивирус Dr.Web для файловых серверов UNIX
Версия 10.1.0
Руководство администратора
03.11.2015

Dr.Web, Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: 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
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов **Dr.Web** или их компонентов.
Зеленое и подчеркнутое начертание	Ссылки на страницы руководства и веб-сайты.
`Моноширинный шрифт`	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением. 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`**.
Курсив	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак плюса (+)	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
Восклицательный знак 	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Далее в данном руководстве следующие термины будут использованы без расшифровки:

Обозначение	Расшифровка
EPM	ESP Package Manager (менеджер пакетов)
FQDN	Fully Qualified Domain Name
GNU	GNU (GNU is Not Unix) project
HTML	HyperText Markup Language
HTTP	HyperText transfer Protocol
HTTPS	HTTP via SSL
ID	Идентификатор
IP	Internet Protocol
LKM	Linux Kernel Module
MBR	Master Boot Record
NSS	Novell Storage Services
OID	(SNMP) Object ID

Обозначение	Расшифровка
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
URL	Unified Resource Locator
VBR	Volume Boot Record
ОС	Операционная система
ФС	Файловая система

Введение

Благодарим вас за приобретение программного продукта **Антивирус Dr.Web для файловых серверов UNIX**. Он позволит вам обеспечить надежную защиту вашего компьютера от компьютерных угроз всех возможных типов, используя наиболее современные технологии обнаружения и обезвреживания угроз.

Данное руководство предназначено для помощи пользователям компьютеров, работающих под управлением операционных систем семейства **GNU/Linux**, а также других UNIX-подобных ОС, таких как **Solaris** и **FreeBSD,** в установке и использовании продукта **Антивирус Dr.Web для файловых серверов UNIX** версии 10.1.0. В дальнейшем будет использовано обозначение **Dr.Web для файловых серверов UNIX**.

Если у вас уже установлен **Dr.Web для файловых серверов UNIX** версии 6.0.2, и вы желаете обновить его до версии 10.1.0, выполните процедуру перехода на новую версию.

Соглашение о путях к файлам продукта

Описываемый в документе программный продукт предназначен для функционирования в среде различных операционных систем семейства UNIX. При этом пути, используемые для размещения компонентов и служебных файлов продукта, зависят от операционной системы. Для удобства обозначения путей к файлам программного комплекса, зависящих 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 условным обозначениям в разных операционных системах, приведены в таблице ниже.

Операционная система	Условное обозначение	Реальный путь
GNU/Linux	**<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
Solaris	**<opt_dir>**	Совпадают с соответствующими путями для **GNU/Linux**.
	<etc_dir>	
	<var_dir>	

Для экономии места, в приводимых в документе 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 ОС.

О продукте

Dr.Web для файловых серверов UNIX создан для защиты 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 угроз, разработанных для различных платформ.

Основные компоненты решения (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 антивирусные решения для операционных систем **IBM OS/2**, **Novell NetWare**, **Macintosh** (**OS X**) и **Microsoft Windows**. Кроме того, созданы антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением операционных систем **Andorid**, **Symbian**, **iOS** и **Microsoft Windows Mobile**.

Компоненты продукта **Dr.Web для файловых серверов UNIX** постоянно обновляются, а вирусные базы **Dr.Web** регулярно дополняются новыми сигнатурами угроз, что обеспечивает актуальный уровень защищенности компьютера, программ и данных пользователей. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре.

Основные функции

Основные функции продукта **Dr.Web для файловых серверов UNIX**:

1. **Поиск и обезвреживание** 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).

   Для обнаружения вредоносных и нежелательных программ используются:

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

   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 **Вирусную лабораторию компании «Доктор Веб»**. Подробнее о методах обезвреживания угроз см. в Приложении 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.

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.

- **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 файловой системы доступна только для ОС семейства **GNU/Linux**, а 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. В других ОС из списка поддерживаемых, компоненты, предоставляющие указанные функции, не поставляются.

3. **Надежная изоляция инфицированных или подозрительных объектов** в специальном хранилище – карантине, чтобы они не могли нанести ущерба системе. При перемещении объектов в карантин они специальным образом переименовываются, и могут быть восстановлены в исходное место (в случае необходимости) только по команде пользователя.
4. **Автоматическое обновление** содержимого вирусных баз **Dr.Web** и антивирусного ядра 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 защищаемом компьютере единых политик безопасности, принятых в некоторой сети, в состав которой он входит. Это может быть как сеть некоторого предприятия (корпоративная сеть) или частная сеть VPN, так и сеть, организованная провайдером каких-либо услуг, например, доступа к сети Интернет.

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: • Управление 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. • Единообразное хранение и предоставление другим компонентам комплекса информации об имеющихся лицензионных ключах и настройках. Принимает изменённые настройки и ключи от уполномоченных компонентов **Dr.Web для файловых серверов**

Компонент	Описание
	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). 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. С точки зрения остальных компонентов **Dr.Web для файловых серверов UNIX**, предоставляет сервис антивирусной проверки. Может работать как под управлением демона **Dr.Web ConfigD**, так и в автономном режиме. Исполняемый файл компонента: `drweb-se` Внутреннее наименование, выводимое в журнал: **ScanEngine**
Вирусные базы **Dr.Web**	Автоматически обновляемая база данных, используемая антивирусным ядром для распознавания вредоносных программ и лечения известных вирусов.
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. 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.  Поставляется только в составе дистрибутивов, предназначенных для ОС семейства **GNU/Linux**. Исполняемый файл компонента: `drweb-spider` Внутреннее наименование, выводимое в журнал: **LinuxSpider**

Компонент	Описание
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: **NSS**
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. Исполняемый файл компонента: `drweb-esagent` Внутреннее наименование, выводимое в журнал: **ESAgent**
Dr.Web Network Checker	Агент распределённой проверки файлов. Позволяет принимать на проверку файлы с удаленных узлов сети и передавать локальные файлы на проверку на удаленные узлы сети. Для приёма и передачи файлов на удаленных узлах также должен функционировать антивирусный продукт **Dr.Web** для операционных систем семейства UNIX. 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	Сервер веб-интерфейса управления компонентами **Dr.Web для файловых серверов UNIX**. Веб-интерфейс может быть открыт в браузере на локальном или удаленном компьютере. Наличие

Компонент	Описание
	встроенного сервера веб-интерфейса позволяет продукту не использовать сторонние веб-серверы (такие, например, как **httpd Apache**) и утилиты удаленного администрирования наподобие **Webmin.** Для обеспечения безопасности при передаче данных 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 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 обновлений вирусных баз и антивирусного ядра с серверов обновлений компании **«Доктор Веб»** (как автоматически, по расписанию, так и непосредственно по команде пользователя).
	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**

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

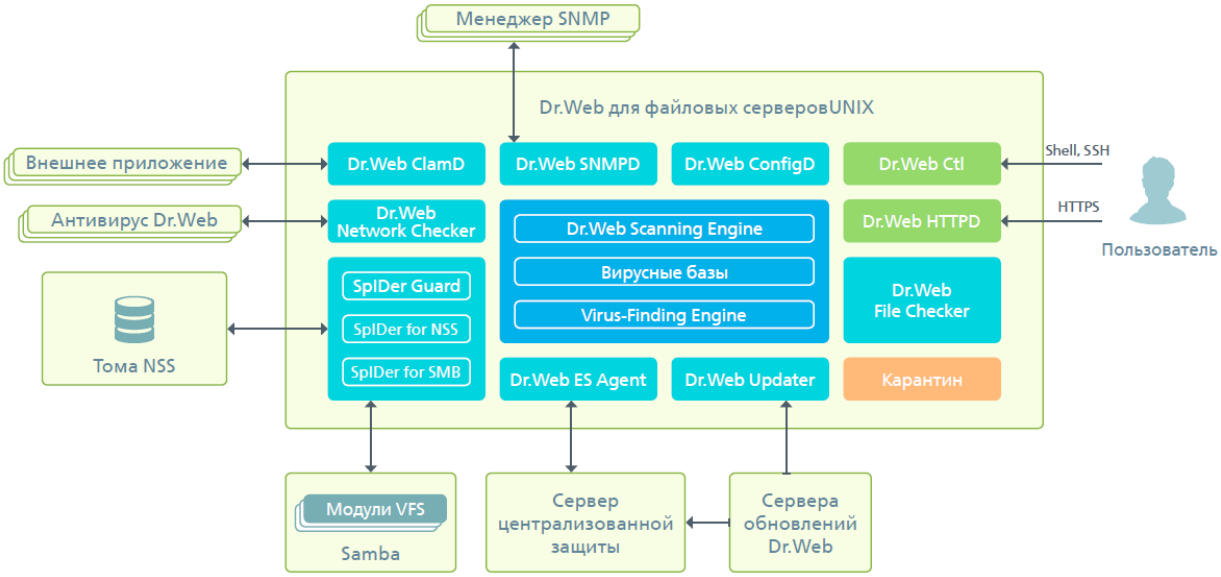

Рисунок 1. Структура программного продукта Dr.Web для файловых серверов UNIX

На приведенном рисунке использованы следующие обозначения:

- – программный комплекс **Dr.Web для файловых серверов UNIX** в целом и внешние по отношению к нему программные комплексы и смежные системы, не входящие непосредственно в его состав.
- – 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).

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

Пользователь может управлять содержимым карантина из командной строки, используя утилиту **Dr.Web Ctl**. При этом всегда обрабатывается консолидированный карантин, объединяющий в себе все каталоги с изолированными объектами, доступные в данный момент.

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

Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз **Dr.Web для файловых серверов UNIX** (точнее, пользователь, от имени которого он запущен) должен обладать следующими полномочиями:

Действие	Требуемые полономочия
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.

Действие	Требуемые полономочия
Лечение файлов	Без ограничений. После выполнения лечения остается вылеченный файл с исходными правами доступа и владельцем. Обратите внимание, что файл может быть даже удален, если удаление является методом лечения обнаруженной в нем угрозы.
Восстановление файла из карантина	Пользователь должен иметь разрешение на чтение восстанавливаемого файла и иметь разрешение выполнять запись в каталог восстановления.
Удаление файла из карантина	Пользователь должен иметь разрешение на запись в исходный файл, который был перемещен в карантин.

Для запуска утилиты управления из командной строки с правами суперпользователя 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 **Антивирус 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 автономном 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 **Антивируса**, 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.

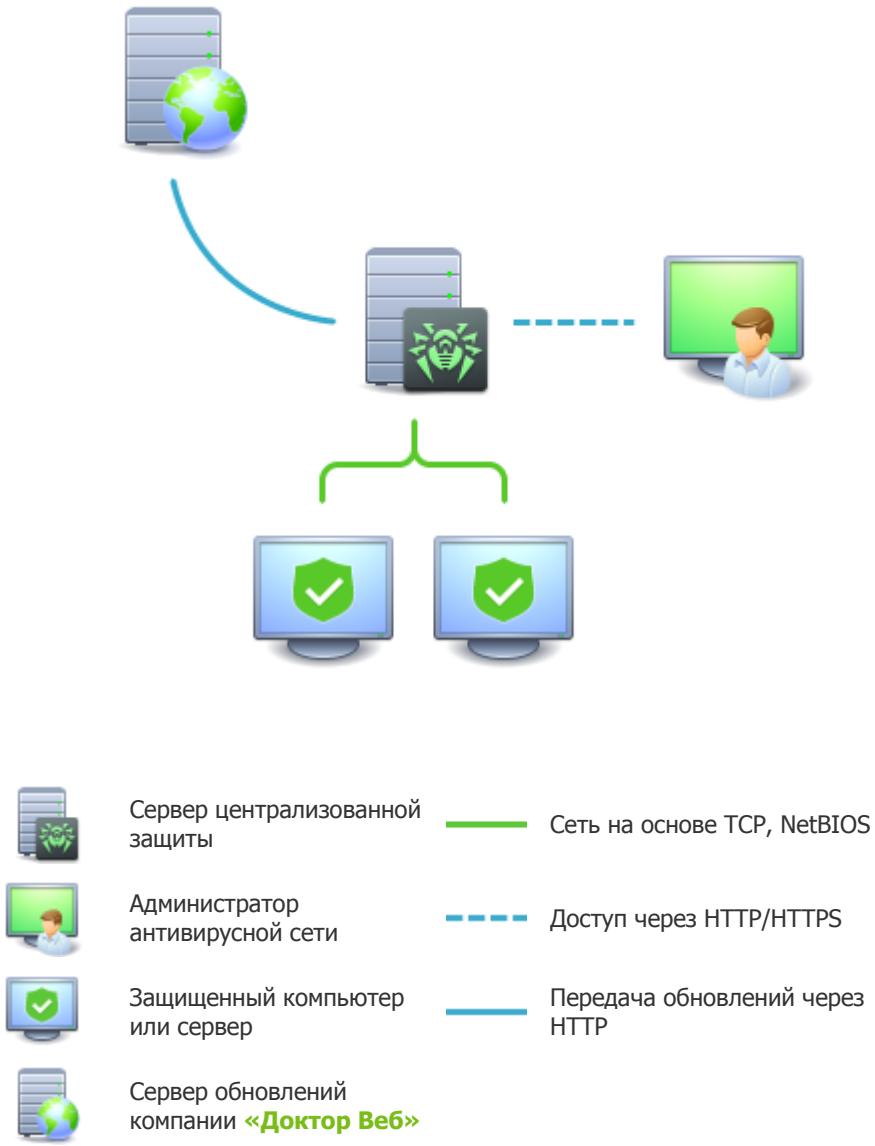

Рисунок 2. Логическая структура антивирусной сети.

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 и не управляет заданиями на проверку объектов файловой системы.

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 **Антивирусом** 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**. Обратите внимание, что 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 **Антивирусом** из командной строки **Dr.Web Ctl**.

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**/**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!)**.

Системные требования

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

Компонент	Требование
Платформа	Поддерживаются 32-битная **(IA-32, x86)** и 64-битная **(x86-64, x64, amd64)** платформы **Intel.**
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**. Система должна использовать механизм аутентификации PAM. 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). 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** (для 32- и 64-битной платформ):

Название дистрибутива Linux	Версии	Требуемые дополнительные библиотеки для 64-битной версии ОС
Debian	7.8, 8.0, 8.1	**libc6-i386**
Fedora	20, 21	**glibc.i686**
Ubuntu	12.04, 14.04, 14.10, 15.04	**libc6-i386**
CentOS	5.11, 6.6, 7.1	**glibc.i686**
Red Hat Enterprise Linux	5.11, 6.6, 7.1	**glibc.i686**
SUSE Linux Enterprise Server	11 SP3, 12	–

  Прочие дистрибутивы ОС **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: http://support.drweb.com/request/.

- **FreeBSD:**

Версии	Требуемые дополнительные библиотеки для 64-битной версии ОС
9.3, 10.1	–

- **Solaris:**

Версии	Требуемые дополнительные библиотеки для 64-битной версии ОС
10 u11	–

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

Компоненты **SpIDer Guard** и **SpIDer Guard для NSS** присутствуют только в дистрибутиве для ОС семейства **GNU/Linux**.

В ОС **Debian, Fedora, Mint** и **Ubuntu** компонент **SpIDer Guard** по умолчанию работает через системный механизм `fanotify`, а для ОС **CentOS** и **Red Hat Enterprise Linux** – через специальный загружаемый модуль ядра, поставляемый в собранном виде.

В случае необходимости имеется возможность собрать загружаемый модуль ядра вручную из поставляемых исходных кодов для любой ОС семейства **GNU/Linux,** использующей ядро версии `2.6.x` и новее.

Дополнительные пакеты

- **X Window System** и любой менеджер окон – для запуска в оконных программ установки и удаления продукта из универсального пакета.
- Эмулятор терминала **xterm** или **xvt** – для запуска в графическом режиме программ установки и удаления продукта из универсального пакета, рассчитанных на режим командной строки, а также для автоматического запуска интерактивного скрипта настройки из оконной программы установки.
- Для корректной работы с правами пользователя необходимо, чтобы в системе использовался механизм аутентификации PAM.

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.

Поддерживаемые файловые серверы

Файловая служба Samba

Для интеграции с файловой службой **Samba** требуется установленный и настроенный сервер **Samba** версии не ниже 3.0.

Монитор **SpIDer Guard для SMB**, входящий в состав **Dr.Web для файловых серверов UNIX**, использует для интеграции с **Samba** специальный модуль **VFS SMB**. Совместно со **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 Приложении Ж настоящего Руководства.

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).

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

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 Dr.Web**, 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 и не управляет заданиями на проверку объектов файловой системы.

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»** http://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 http://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.ru/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.

Повторная регистрация

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

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

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

Ключевой файл

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

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

- срок действия лицензии или демонстрационного периода, которым он соответствует, не истек;
- разрешение, определяемое лицензией или активным демонстрационным периодом, распространяется на все используемые модули;
- целостность файла не нарушена.

При нарушении любого из этих условий ключевой файл становится недействительным.

При работе **Dr.Web для файловых серверов UNIX** ключевой файл по умолчанию должен находиться в каталоге `<etc_dir>` (`etc/opt/drweb.com` для **Linux**) и иметь имя **`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.

Установка ключевого файла

В случае если уже имеется ключевой файл, соответствующий действующей лицензии на этот продукт (например, он был получен от продавца по электронной почте после регистрации или **Dr.Web 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 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. При необходимости перезапустите компонент **`drweb-configd`**, отправив ему сигнал `SIGHUP`.

Вы можете также воспользоваться командой:

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

В последнем случае ключевой файл не будет скопирован в каталог <etc_dir>.

Об условных обозначениях путей <opt_dir>, <etc_dir> и <var_dir> см. во Введении.

Установка и удаление продукта

Ниже описывается процедура установки и удаления программного комплекса **Dr.Web для файловых серверов UNIX** версии 10.1.0. Также в этом разделе рассмотрена процедура перехода на новую версию, если на вашем компьютере уже установлен **Dr.Web для файловых серверов UNIX** версии 6.0.2.

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`**.

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

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 `<opt_dir>/bin/` на наличие скрипта удаления **`remove.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.

Об условных обозначениях путей `<opt_dir>`, `<etc_dir>` и `<var_dir>` см. во Введении.

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 10.1.0. Для дополнительной информации обратитесь к Руководству пользователя установленной у вас версии **Dr.Web для файловых серверов UNIX**.

Обновление установкой универсального пакета

Выполните установку **Dr.Web для файловых серверов UNIX** версии 10.1.0 из универсального пакета. В процессе установки вам будет предложено автоматически удалить имеющиеся компоненты старой версии продукта.

В случае если на вашем сервере **одновременно** установлено несколько серверных продуктов **Dr.Web** версии 6.0.2 (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 10.1.0 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:

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

  1. Удалите все пакеты текущего дистрибутива командой

     ```
     # yum remove drweb*
     ```

     Если требуется экранирование символа `'*'`, то следует указать `drweb\*`. Эта команда предложит удалить **все** установленные пакеты **Dr.Web** (не только те, которые входят в состав продукта **Dr.Web для файловых серверов UNIX**). Поэтому ее следует использовать с осторожностью, если у вас установлено несколько продуктов **Dr.Web**.

  2. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 10.1.0).

     

     Имя репозитория, хранящего пакеты версии 10.1.0, см. в разделе Установка из репозитория. Для уточнения способа смены репозиториев обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

  3. Установите новую версию продукта из репозитория, выполнив команду

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

  Дополнительно см. удаление и установку пакетов продукта при помощи репозитория (разделы, соответствующие используемой вами ОС и менеджеру пакетов).

- **В случае использования пакетов DEB (apt-get):**

  1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 10.1.0).
  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 имеющийся у вас лицензионный ключевой файл будет автоматически установлен в надлежащее место для использования новой версией продукта.

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

В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки компании **«Доктор Веб»**.

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 программами установки в графическом режиме и режиме командной строки (при начале установки будет запущена одна из них, в зависимости от возможностей окружения).
2. Выполнив установку продукта в виде набора нативных пакетов (для этого потребуется подключиться к соответствующему репозиторию пакетов компании **«Доктор Веб»**).

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

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.**

Установка универсального пакета

Программный комплекс **Dr.Web для файловых серверов UNIX** распространяется в виде инсталляционного файла с именем **drweb-file-servers_<версия>~<ОС>_<платформа>.run**, где **<версия>** – это строка, включающая в себя версию и дату выпуска продукта, **<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-file-servers_10.1.0.1-1409012000~linux_x86.run
```

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

Чтобы установить компоненты программного комплекса **Dr.Web 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.ru/.
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` (см. в разделе Выборочная установка компонентов).

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

- программа установки для графического режима;
- программа установки для режима командной строки.

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

5. Следуйте инструкциям программы установки.

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

```
# setenforce 0
```

После этого перезапустите программу установки.

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

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

После завершения установки, в графической оболочке рабочего стола, в меню **Приложения,** появится группа **Dr.Web,** содержащая пункт **Удалить компоненты Dr.Web**, предназначенный для запуска программы его удаления.

В случае необходимости вы можете воспользоваться возможностью выборочной установки компонентов продукта (например, для устранения ошибок, возникших в процессе эксплуатации **Dr.Web для файловых серверов UNIX**).

Установка в графическом режиме

После запуска программы установки, работающей в графическом режиме, на экране появится окно мастера установки. На странице приветствия перечисляются пакеты программного продукта, которые находятся в дистрибутиве и могут быть установлены при помощи данной программы установки.

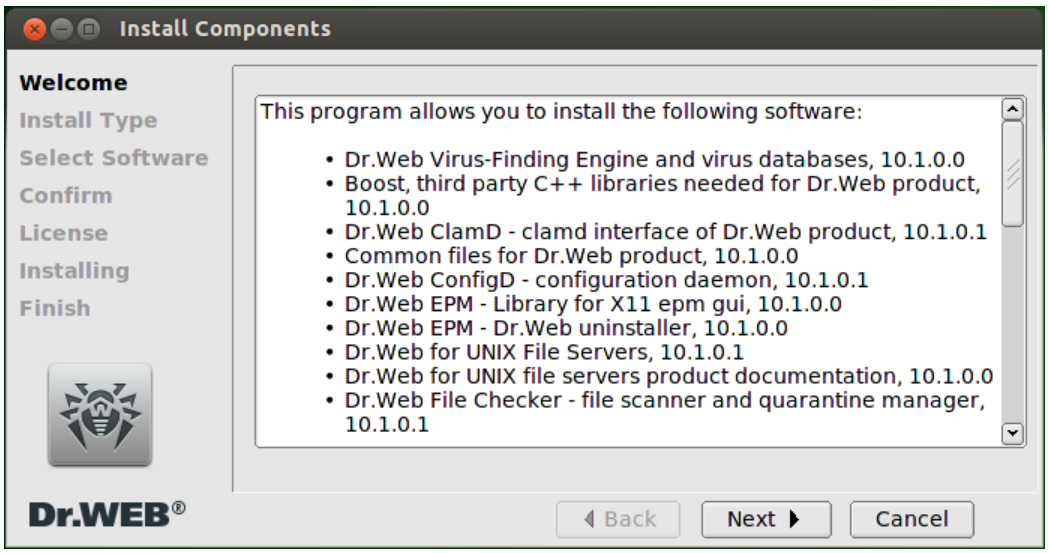

Рисунок 3. Страница приветствия мастера установки

Для начала установки **Dr.Web для файловых серверов UNIX** нажмите кнопку **Next**. Для отказа от установки и завершения работы программы установки нажмите кнопку **Cancel**.

1. На первом шаге необходимо выбрать тип установки, установив соответствующий переключатель. В случае выбора пункта **Dr.Web for UNIX File Servers** для установки автоматически будут отмечены все пакеты, входящие в состав решения **Dr.Web для файловых серверов UNIX**. В случае выбора пункта **Custom Configuration** на следующем экране (шаг 2) вам будет предоставлена возможность выбрать требуемый вам набор пакетов вручную, иначе программа установки перейдет сразу к шагу 3.

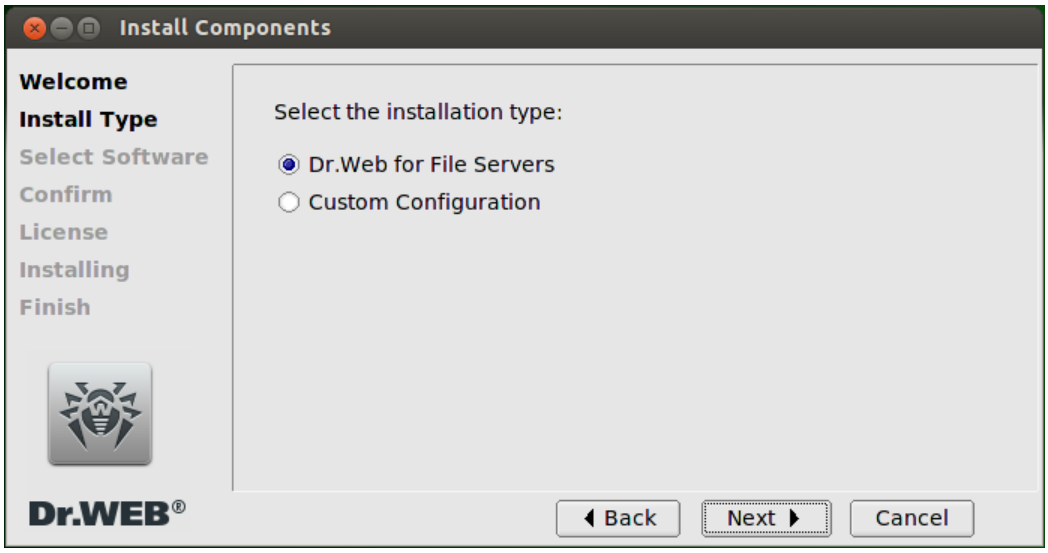

Рисунок 4. Определение типа установки

После определения типа установки нажмите **Next**. Для отказа от установки и завершения работы программы установки нажмите кнопку **Cancel**.

2. Если на первом шаге был выбран тип установки **Custom Configuration**, то на следующем экране вам будет предложено отметить в списке флажками пакеты, которые требуется установить. Нажатие кнопки **Select all** позволяет отметить все имеющиеся пакеты, а нажатие кнопки **Select none** – снять отметку со всех пакетов. Обратите внимание, что при отметке некоторого пакета к установке, автоматически отмечаются к установке все пакеты, от которых он зависит. Аналогично, при снятии отметки с некоторого пакета, автоматически снимаются

отметки со всех пакетов, которые зависят от него.

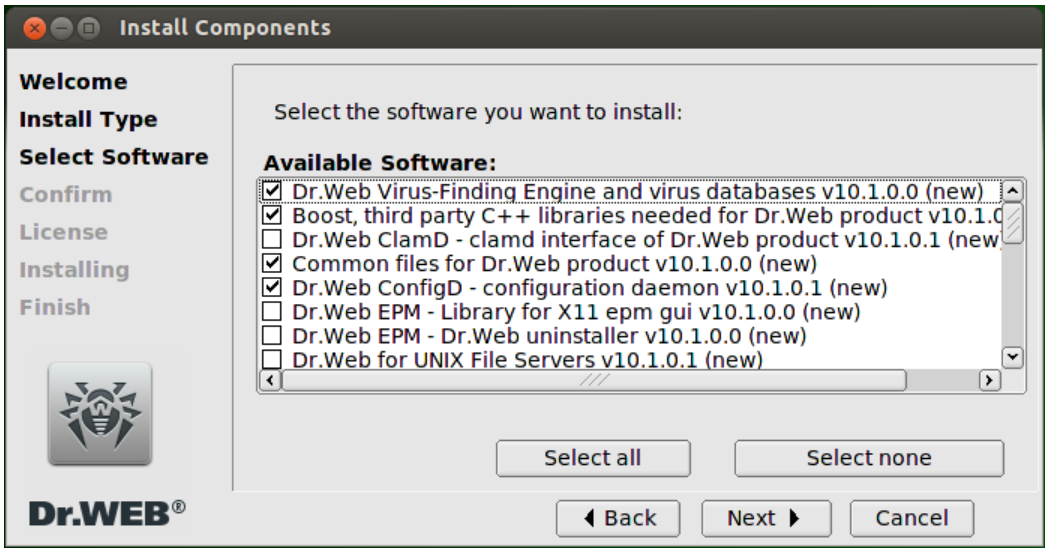

Рисунок 5. Выбор пакетов продукта, подлежащих установке

После выбора набора пакетов, подлежащих установке, нажмите кнопку **Next**. Для отказа от установки и завершения работы программы установки нажмите кнопку **Cancel**.

3. На следующей странице мастера установки вам будет выведен список пакетов продукта, которые будут установлены на ваш компьютер.

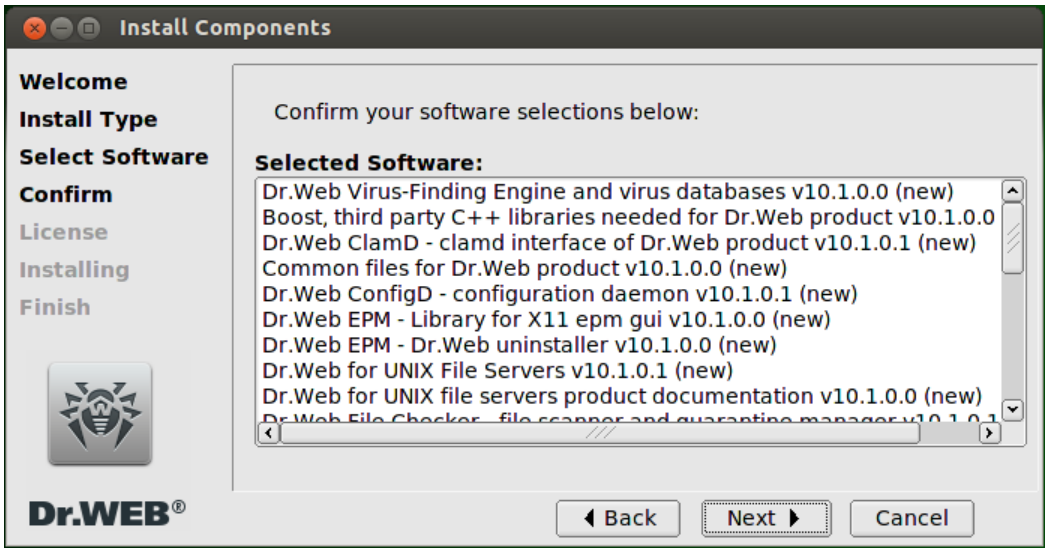

Рисунок 6. Подтверждение перечня пакетов, подлежащих установке

Для подтверждения выбора нажмите кнопку **Next**. Для отказа от установки и завершения работы программы установки нажмите кнопку **Cancel**. Для изменения перечня устанавливаемых пакетов нажмите кнопку **Back**. Обратите внимание, что нажатие кнопки **Back** на данном шаге откроет страницу мастера установки, позволяющую изменить список пакетов, подлежащих установке (шаг 2), вне зависимости от того, какой тип установки был выбран на шаге 1.

3. На следующем шаге вам необходимо ознакомиться с текстом Лицензионного соглашения **Dr.Web** и информацией об авторских правах на устанавливаемые компоненты **Dr.Web для файловых серверов UNIX** (включая авторские права на использованные сторонние компоненты). Для просмотра текста Лицензионного соглашения и информации об авторских

правах выберите соответствующую вкладку. Использование выпадающего списка **Select language** позволяет выбрать язык, на котором будет выведен текст Лицензионного соглашения **Dr.Web**.

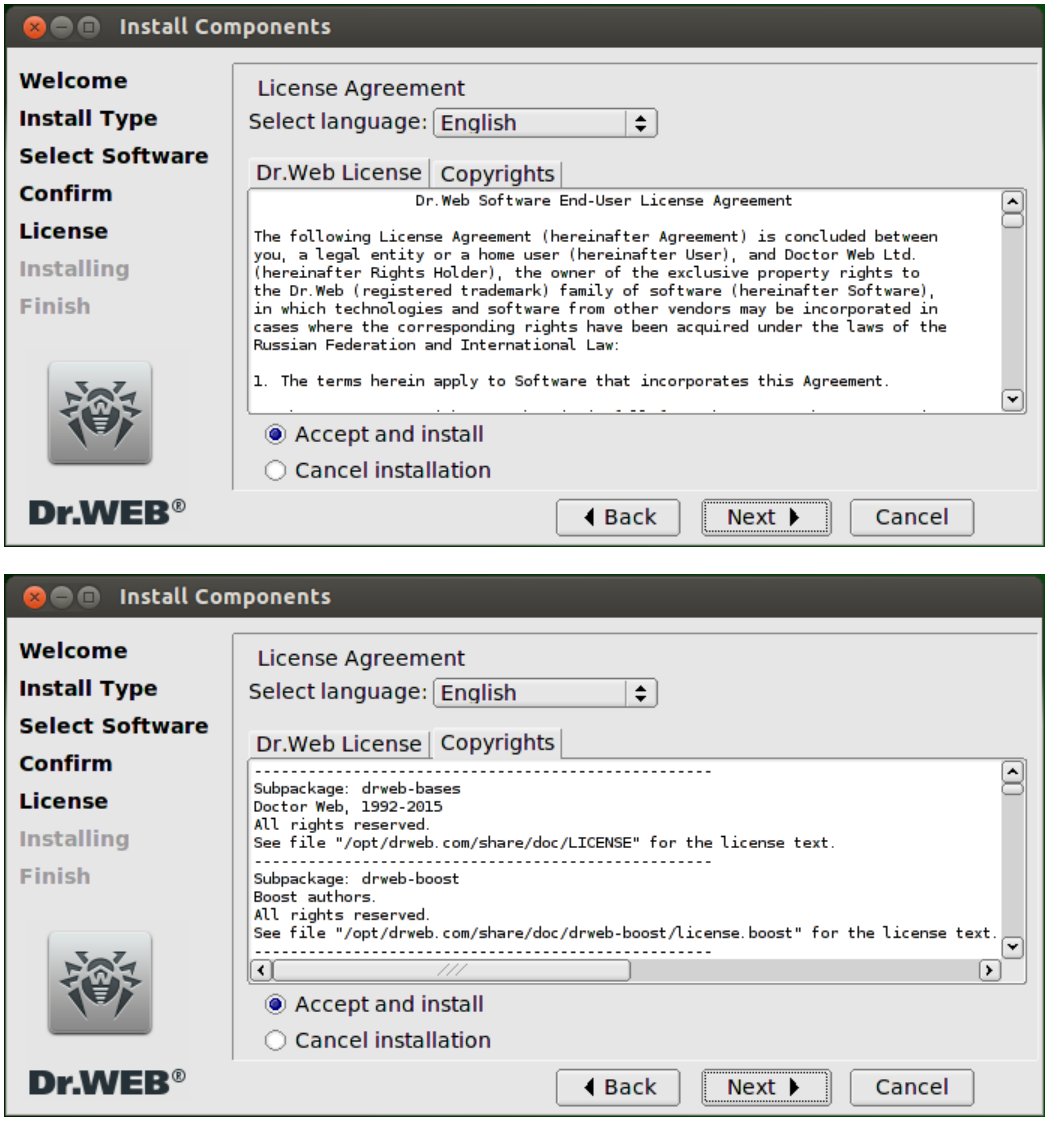

Рисунок 7. Ознакомление с Лицензионным соглашением и информацией об авторских правах

Для начала установки пакетов продукта на ваш компьютер вам необходимо принять условия Лицензионного соглашения (для этого необходимо отметить переключатель **Accept and install**) и нажать кнопку **Next**. Обратите внимание, что если вы выберете переключатель **Cancel installation**, то нажатие кнопки **Next** приведет к завершению работы программы установки, поскольку условия Лицензионного соглашения не были приняты. Также для отказа от установки и завершения работы программы установки вы можете нажать кнопку **Cancel**.

4. После принятия условий Лицензионного соглашения начнется процесс распаковки пакетов и копирования файлов на ваш компьютер.

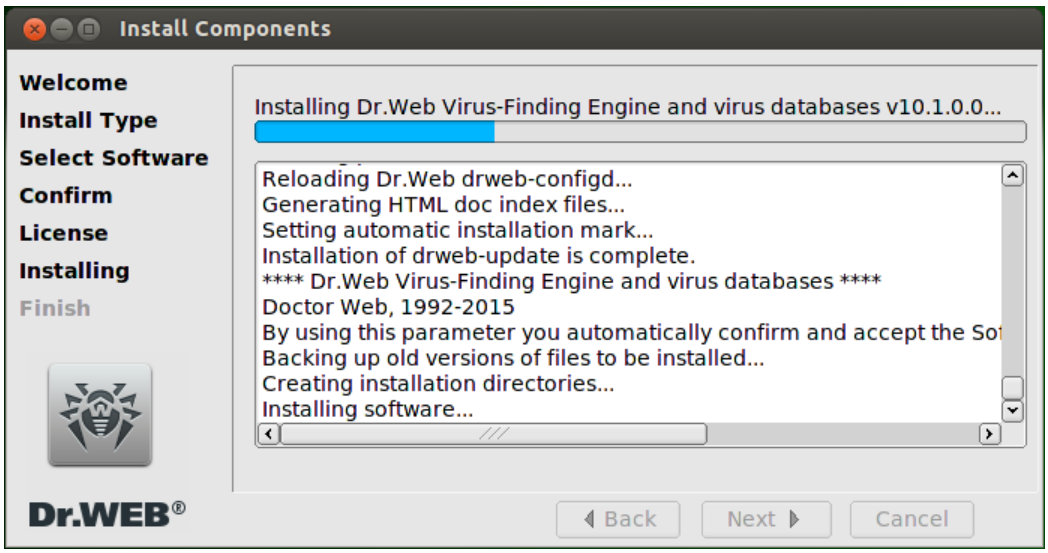

Рисунок 8. Процесс установки пакетов продукта

5. После успешного окончания процесса копирования файлов программы и внесения необходимых изменений в системные файлы, под журналом установки появится флажок **Run interactive postinstall script**. Установите этот флажок, чтобы на следующем шаге мастера запустить интерактивный скрипт настройки продукта. Вы можете пропустить этот шаг и настроить продукт позднее. Далее нажмите кнопку **Next**. Если флажок **Run interactive postinstall script** был установлен, запустится интерактивный скрипт настройки продукта (см. ниже), по завершении которого откроется финальная страница мастера. Если флажок оставить не установленным, то произойдет переход сразу к финальной странице мастера установки.

В системах с отсутствующим эмулятором терминала **xterm** интерактивный скрипт настройки не может быть запущен автоматически. В этом случае вам следует запустить его вручную после окончания установки (файл скрипта **`drweb_smbspider_configure.sh`** располагается в каталоге `<opt_dir>/share/drweb-smbspider-modules/`).

6. На последнем шаге появится финальная страница мастера, содержащая информацию о результатах установки **Dr.Web для файловых серверов UNIX**.

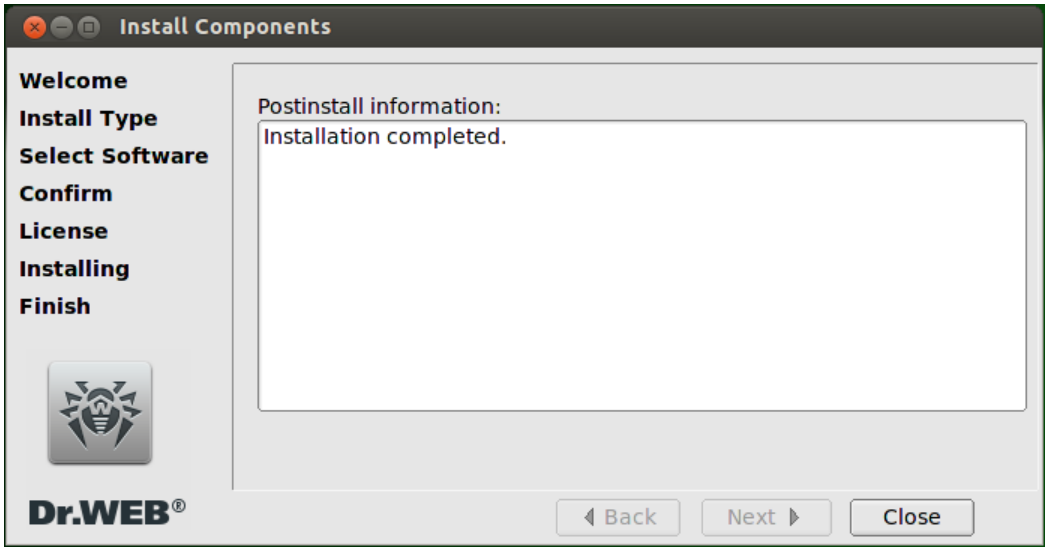

Рисунок 9. Страница окончания установки

Чтобы закрыть окно мастера установки, необходимо нажать кнопку **Close.** Если установка была прервана из-за ошибки, финальная страница мастера будет содержать соответствующее сообщение. В этом случае также следует закрыть мастер установки, нажав кнопку **Close.** После этого устраните проблемы, вызвавшие ошибку установки, и повторите установку заново.

7. После завершения работы программы установки на экране появится информационное сообщение, содержащее инструкции по способам управления работой продукта (текст сообщения дублируется в эмуляторе терминала, если он открыт).

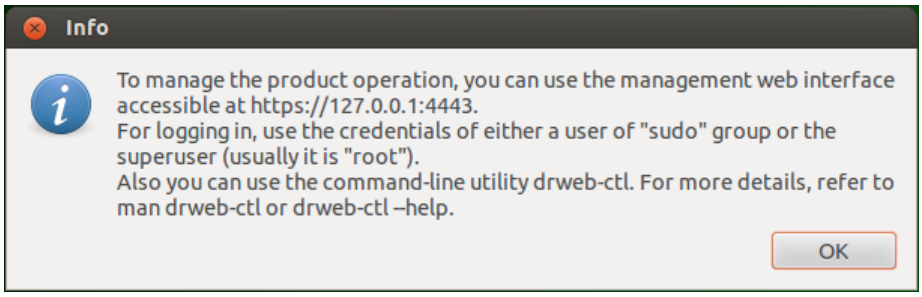

Рисунок 10. Информационное сообщение

Интерактивный скрипт настройки

Интерактивный скрипт настройки позволяет 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**.

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.

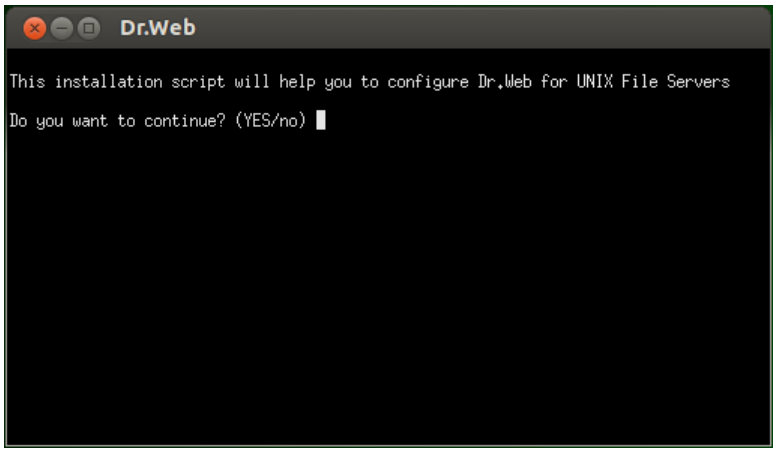

Рисунок 11. Запуск интерактивного скрипта настройки

Если в данный момент на компьютере (в стандартном для продукта каталоге) не имеется ключевого файла, скрипт предложит указать путь к ключевому файлу. Если ключевой файл уже имеется, этот шаг будет автоматически пропущен.

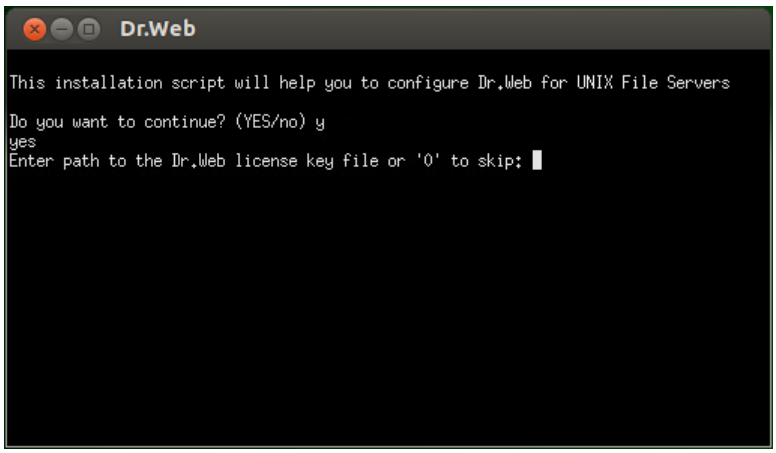

Рисунок 12. Указание пути к ключевому файлу

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.

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.

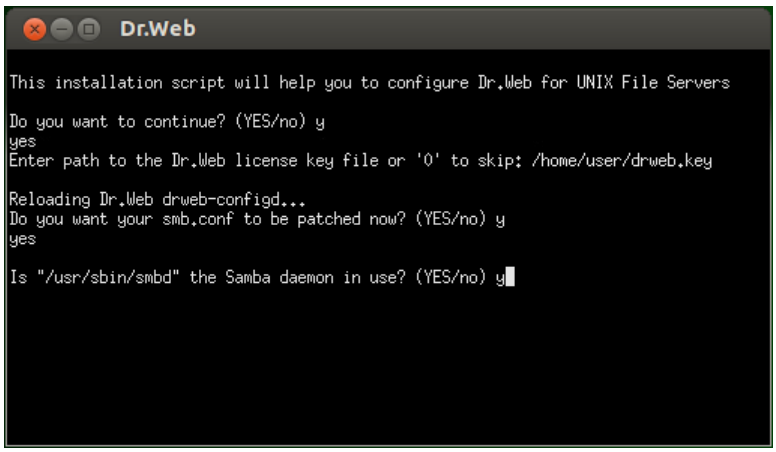

Рисунок 13. Определение используемого сервера Samba и его файла конфигурации

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 символа **A** или **All** добавляет под наблюдение все доступные разделяемые каталоги, а ввод символа **N** или **None** – удаляет все разделяемые каталоги из-под наблюдения.

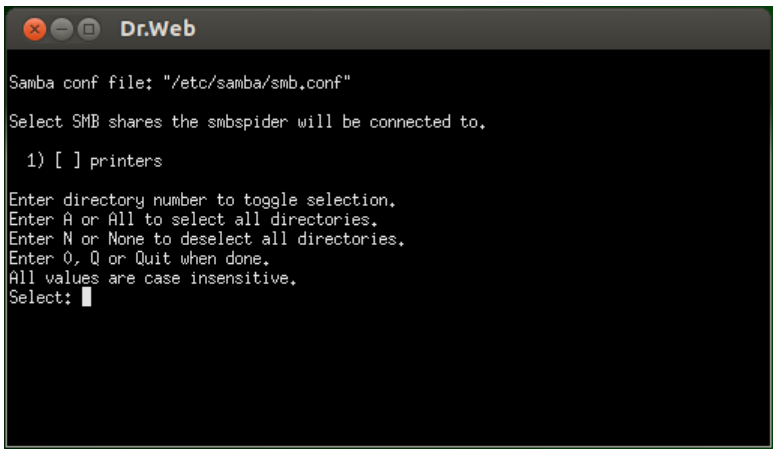

Рисунок 14. Выбор разделяемых каталогов, подлежащих наблюдению

Для завершения выбора и записи внесенных изменений в конфигурационный файл следует ввести **0**, **Q** или **Quit**.

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**.

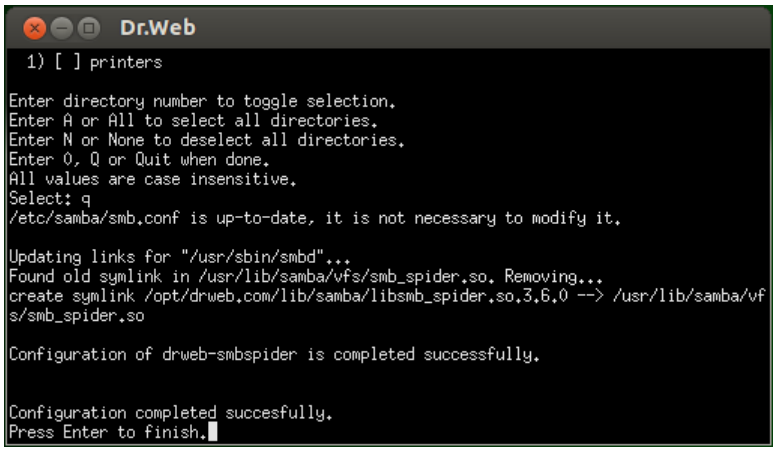

Рисунок 15. Завершение работы скрипта

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

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 wish to continue?». Чтобы отказаться от установки, введите **`No`** или **`N`**. В этом случае работа программы установки будет завершена.

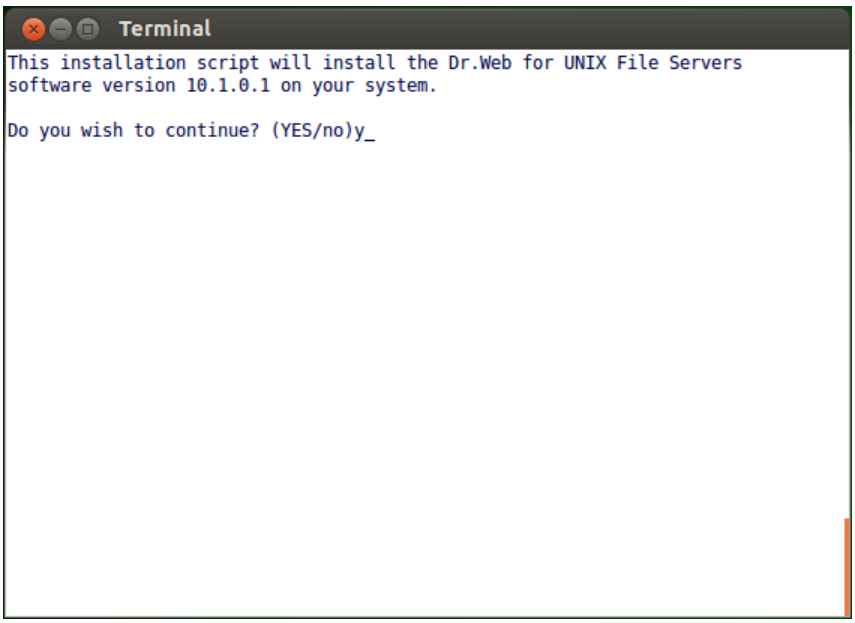

Рисунок 16. Приглашение к установке

2. Далее необходимо выбрать тип установки: продукт **Dr.Web для файловых серверов UNIX** целиком, или требуемый вам набор пакетов **Dr.Web** (пункт меню **Custom Configuration**).

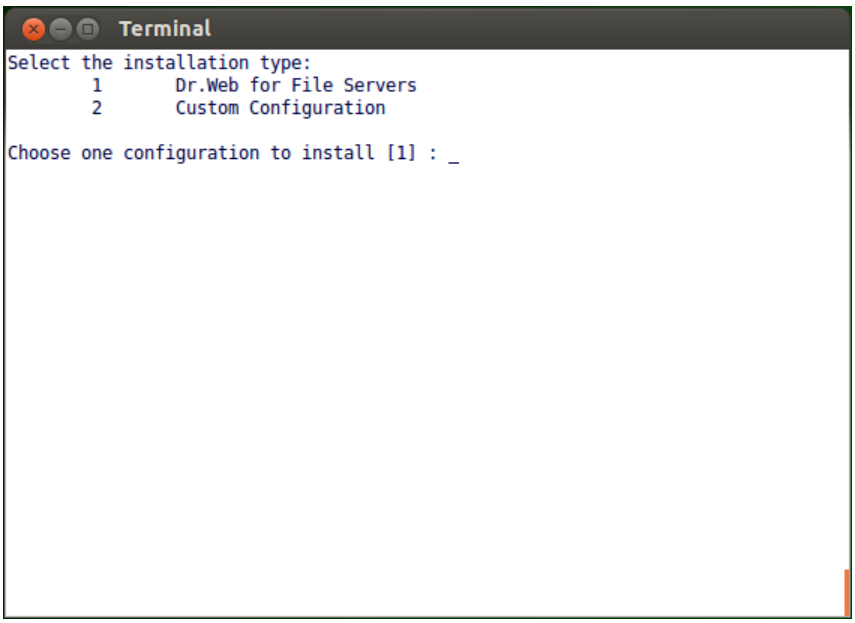

Рисунок 17. Выбор варианта установки

Для выбора соответствующего варианта установки необходимо ввести номер интересующего пункта меню и нажать ENTER.

3. Если на предыдущем шаге был выбран вариант установки **Custom Configuration**, то на следующем экране вам будет предложен для выбора список пакетов, входящих в дистрибутив. В противном случае программа установки перейдет сразу к демонстрации Лицензионного соглашения (пункт 4).

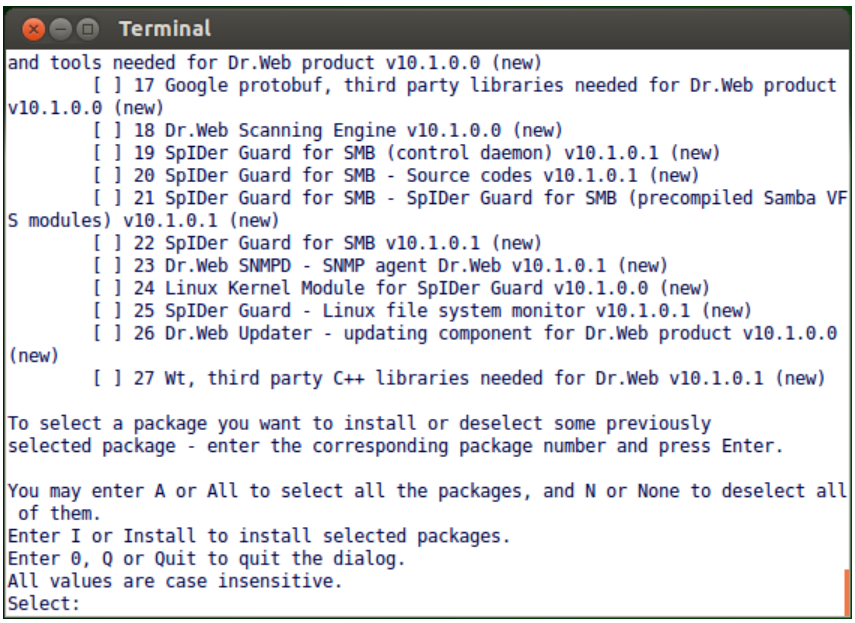

Рисунок 18. Выбор пакетов для установки

Для выбора пакета, который требуется установить, введите его номер в списке. Чтобы отметить все имеющиеся пакеты, введите **A** или **All**, а чтобы снять отметку со всех пакетов, введите **N** или **None**. Обратите внимание, что при отметке некоторого пакета к установке, автоматически отмечаются к установке все пакеты, от которых он зависит. Аналогично, при снятии отметки с некоторого пакета, автоматически снимаются отметки со всех пакетов, которые зависят от него. Чтобы перейти к началу установки отмеченных пакетов, введите **I** или **Install**. Чтобы завершить программу установки, введите **0**, **Q** или **Quit**.

4. 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.

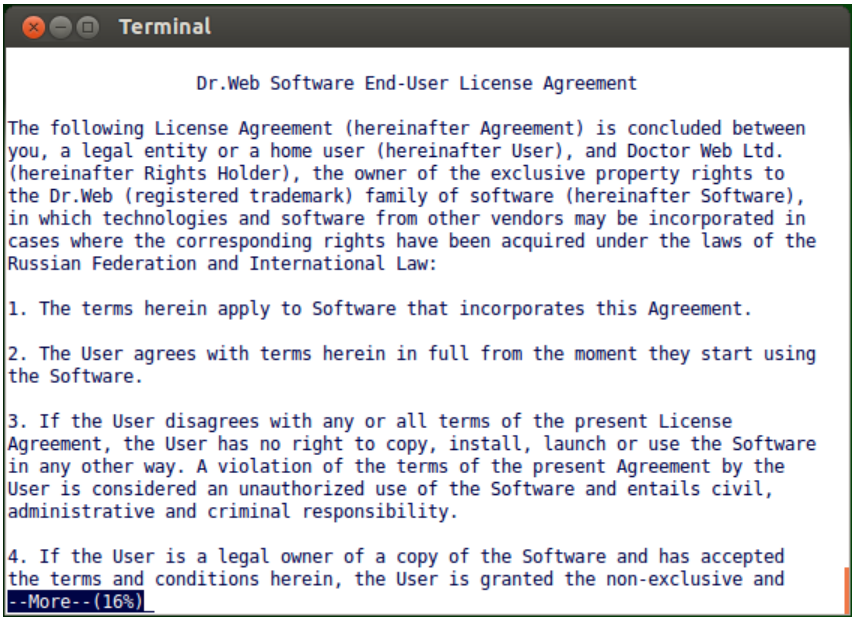

Рисунок 19. Просмотр Лицензионного соглашения

5. 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 **Dr.Web** работа программы установки будет завершена

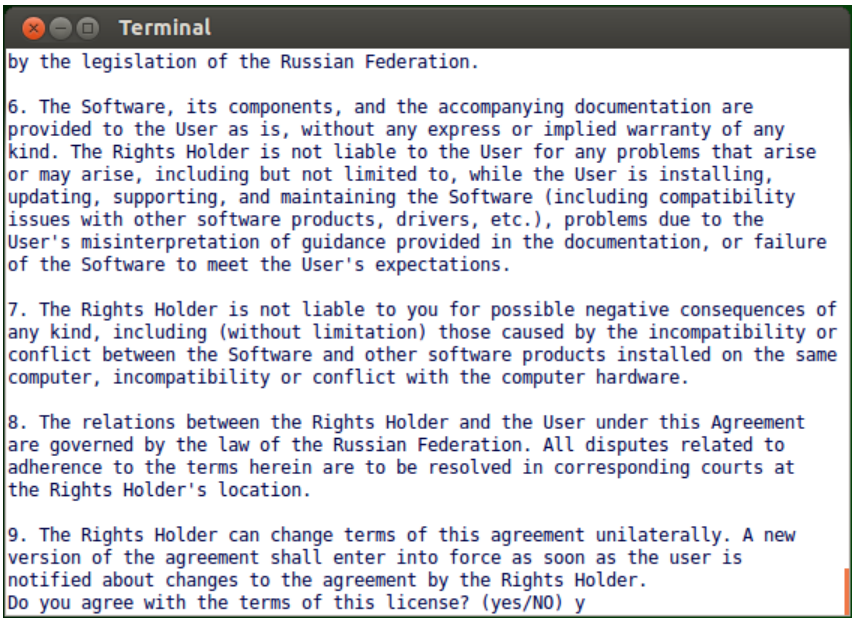

Рисунок 20. Принятие условий Лицензионного соглашения

6. 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.

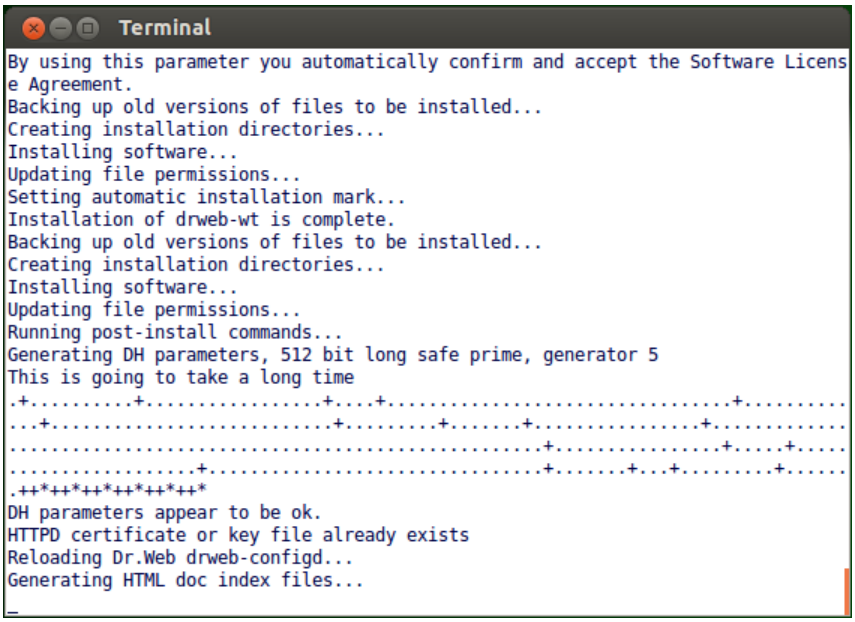

Рисунок 21. Процесс установки

7. В случае успешного окончания процесса установки, будет автоматически запущен интерактивный скрипт настройки. По окончании его работы на экране появится информационное сообщение, содержащее инструкции по способам управления работой продукта.

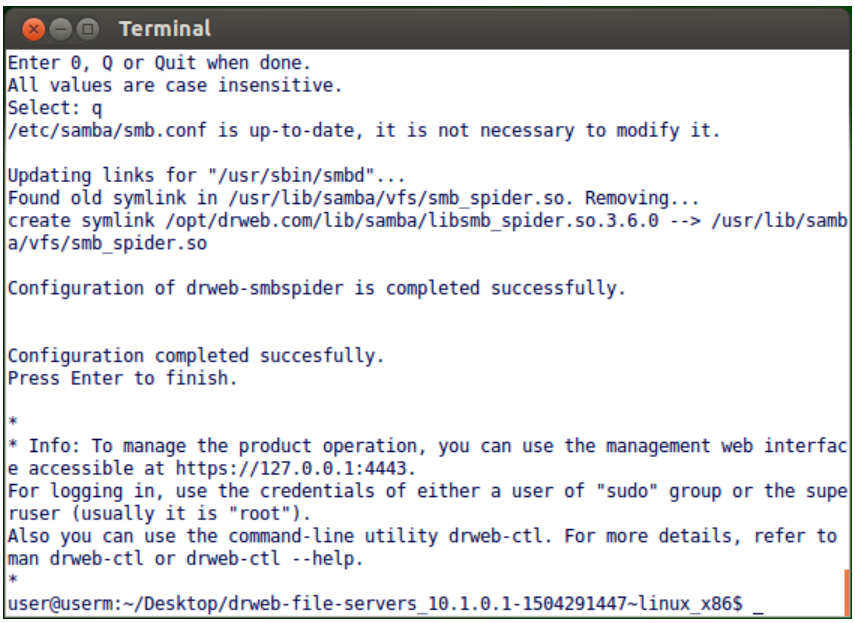

Рисунок 22. Сообщение об окончании установки

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.

Выборочная установка компонентов

Распаковка инсталляционного файла

Если требуется осуществить выборочную установку некоторых компонентов продукта, следует распаковать инсталляционный файл **<имя_файла>.run**, не запуская сам процесс установки продукта. Для этого следует воспользоваться параметром командной строки `--noexec`:

```
$ ./<имя_файла>.run --noexec
```

В результате в текущем каталоге появится вложенный каталог `<имя_файла>`.

Кроме того, вы можете воспользоваться следующими параметрами командной строки при запуске run-файла:

`--keep` – каталог `<имя_файла>`, содержащий установочные файлы продукта, будет распакован в текущий каталог (а не в `/tmp`), и не будет автоматически удален по окончании установки.

`--target <путь_к_каталогу>` – каталог `<имя_файла>`, содержащий установочные файлы продукта, будет распакован в указанный каталог. Обратите внимание, что он автоматически удалится по окончании установки, если также не указать параметр `--noexec` или `--keep`.

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

```
$ ./<имя_файла>.run --help
```

Выборочная установка

Каталог установки содержит пакеты всех компонентов, из которых состоит программный продукт **Dr.Web для файловых серверов UNIX**, а также вспомогательные файлы. Пакет каждого

компонента **<component_name>** снабжен двумя файлами <component_name>.install и <component_name>.remove. По сути эти файлы являются командными скриптами, первый из которых используется для установки пакета, содержащего компонент, а второй – для его удаления. Имена всех пакетов, содержащих компоненты программного комплекса **Dr.Web для файловых серверов UNIX**, начинаются с префикса «drweb».

В общем случае в архиве содержатся следующие пакеты:

Пакет	Содержимое
drweb-bases	Файлы антивирусного ядра **Dr.Web Virus-Finding Engine** и вирусных баз **Dr.Web**
drweb-boost	Библиотеки **Boost**
drweb-clamd	Файлы компонента **Dr.Web ClamD**
drweb-common	Основной конфигурационный файл drweb.ini, основные библиотеки, документация и структура каталогов продукта. В процессе установки данного компонента также будут созданы пользователь drweb и группа drweb
drweb-configd	Файлы компонентов **Dr.Web ConfigD** и **Dr.Web Ctl**
drweb-epm10.1.0-libs	Библиотеки поддержки программ установки
drweb-epm10.1.0-uninst	Библиотеки поддержки программ удаления
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
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**
drweb-spider-kmod	Файлы компонента **SpIDer Guard** (файлы модуля ядра для режима LKM)
drweb-update	Файлы компонента **Dr.Web Updater**
drweb-wt	Библиотеки **Wt** (используется веб-интерфейсом управления)

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

Чтобы выполнить установку компонента, достаточно запустить в консоли (или в эмуляторе консоли – терминале для графического режима) соответствующий install-файл.

Для запуска скриптов установки любого из компонентов необходимы права суперпользователя (пользователя `root`). Для получения прав суперпользователя воспользуйтесь командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

При установке любого компонента продукта поддерживается работа с зависимостями, т.е. если для установки компонента должны быть предварительно установлены другие компоненты, то проверяется их наличие в системе, и в случае отсутствия они также будут установлены автоматически.

Если требуется запустить программу установки программного комплекса целиком, следует запустить из распакованного каталога скрипт автоматической установки, выполнив команду:

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

Установка из репозитория

Нативные пакеты продукта **Dr.Web для файловых серверов UNIX** находятся в официальном репозитории **Dr.Web** http://repo.drweb.com/drweb/. 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)

Репозиторий для этих ОС защищен с помощью механизма цифровой подписи. Для корректной работы нужно импортировать ключ цифровой подписи командой

```
wget -O - http://repo.drweb.com/drweb/drweb.key | apt-key add -
```

или

```
curl http://repo.drweb.com/drweb/drweb.key | apt-key add -
```

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

```
deb http://repo.drweb.com/drweb/debian 10.1.0 non-free
```

Кроме того, вы можете выполнить автоматическое получение ключа и подключение к репозиторию версии 10.1.0, скачав и установив специальный DEB-пакет. Ссылка на скачивание пакета: http://repo.drweb.com/drweb-repo10.deb.

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.

Red Hat Enterprise Linux, Fedora, CentOS (yum)

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

Для 32-разрядной версии:

```
[drweb]
name=DrWeb - 10.1.0
baseurl=http://repo.drweb.com/drweb/el5/10.1.0/i386/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

Для 64-разрядной версии:

```
[drweb]
name=DrWeb - 10.1.0
baseurl=http://repo.drweb.com/drweb/el5/10.1.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

Кроме того, вы можете выполнить автоматическое подключение к репозиторию версии 10.1.0, скачав и установив специальный RPM-пакет. Ссылка на скачивание пакета: http://repo.drweb.com/drweb-repo10.rpm.

Для установки **Dr.Web для файловых серверов UNIX** из репозитория выполните команду:

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

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

Настройка политик безопасности для 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 модули **Dr.Web для файловых серверов UNIX.**

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

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

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

Если **SELinux** работает в режиме Enforced, следует временно (на период установки продукта) перевести ее в режим Permissive. Для этого выполните команду **setenforce 0**, которая временно (до первой перезагрузки системы) переведет **SELinux** в режим Permissive.

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

После успешной установки продукта из установочного файла, но до его запуска и активации верните режим Enforced, для чего выполните команду **setenforce 1**.

2. Проблемы функционирования продукта

В некоторых случаях при работающем **SELinux** отдельные 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 вспомогательные модули не могут быть запущены, является появление сообщений об ошибках 119 и 120 в системном журнале **syslog** (обычно расположен в каталоге /var/log/).

Ошибки 119 и 120 также могут сигнализировать о том, что вы пытаетесь запустить **Dr.Web 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.

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

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

Создание политик безопасности SELinux:

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

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

      Обратите внимание, что этот способ можно использовать только в том случае, когда в системном журнале аудита уже зарегистрированы инциденты нарушения политик безопасности **SELinux** модулями **Антивируса.** 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**).

Обратите внимание, что для ОС **Fedora** версии 20 дополнительно обязательно требуется установить пакет `checkpolicy`, иначе вызов утилиты **audit2allow** завершится ошибкой.

Пример использования audit2allow:

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

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

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

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

В большинстве случаев вам не потребуется вносить изменения в файл политики, созданный утилитой **audit2allow**. Поэтому рекомендуется сразу переходить к пункту 4 для установки полученного модуля политики `drweb-se.pp`. Обратите внимание, что по умолчанию утилита **audit2allow** в качестве результата своей работы выводит на экран готовый вызов команды **semodule**. Скопировав его в командную строку и выполнив, вы выполните пункт 4. Перейдите к пункту 2, только если вы хотите внести изменения в политики, автоматически сформированные для компонентов **Dr.Web для файловых серверов UNIX**.

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

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

Пример создания политик при помощи **policygentool**:

- Для модуля **drweb-se**:

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

- Для модуля **drweb-filecheck**:

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

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

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

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

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

Пример использования:

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

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

   Пример:

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

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

   Пример:

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

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

Расположение файлов продукта

Файлы программного комплекса **Dr.Web для файловых серверов UNIX** после установки 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)
`scripts/`	Файлы вспомогательных скриптов
`<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. во Введении.

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

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 как через меню приложений окружения графического рабочего стола, так и при помощи командной строки.

Удаление продукта через меню приложений

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

Удаление продукта из командной строки

Запуск программы удаления осуществляется скриптом **`remove.sh`**, расположенным в каталоге `<opt_dir>/bin`. Таким образом, чтобы запустить удаление продукта, в ОС **Linux**, например, необходимо выполнить следующую команду:

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

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

Чтобы непосредственно запустить программу удаления для режима командной строки, используйте следующую команду (в ОС **Linux**):

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

Процедура удаления **Dr.Web для файловых серверов UNIX** рассмотрена в соответствующих разделах:

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

Удаление в графическом режиме

После запуска программы удаления для графического режима, на экране появится окно мастера удаления. На странице приветствия перечисляется перечень пакетов продукта, которые могут быть удалены при помощи программы удаления.

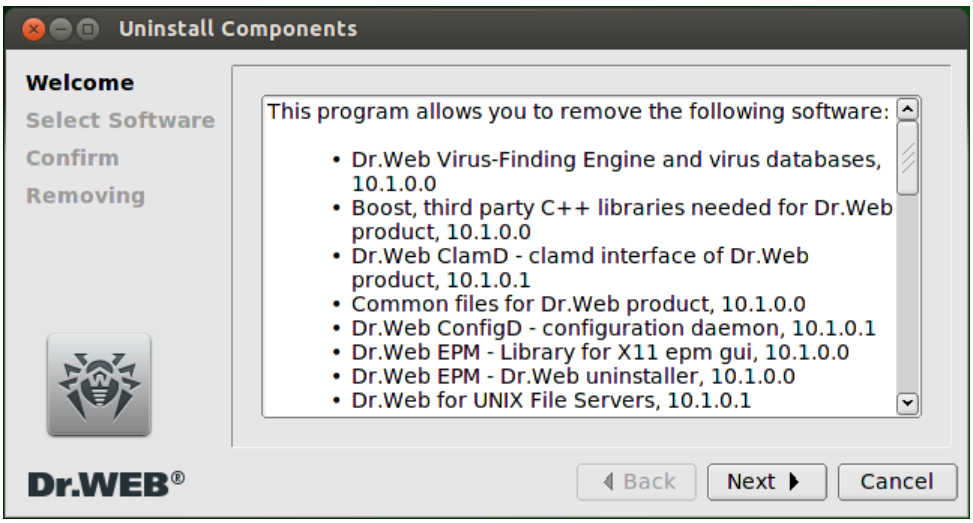

Рисунок 23. Страница приветствия мастера удаления

Для выбора пакетов **Dr.Web**, подлежащих удалению, необходимо нажать кнопку **Next**. Чтобы прекратить работу мастера удаления и отказаться от удаления продукта, нажмите кнопку **Cancel**.

1. На первом шаге вам будет предложено выбрать пакеты продукта, которые следует удалить. Доступно два режима выбора пакетов: простой и расширенный. В *простом* режиме перечисляются целиком продукты **Dr.Web**, которые установлены на вашем компьютере и могут быть удалены. Выбор в списке продукта автоматически отметит для удаления все пакеты этого продукта, которые могут быть удалены, если они не используются другими продуктами **Dr.Web**, установленными на этом компьютере. В *расширенном* режиме перечисляются все пакеты **Dr.Web**, установленные на этом компьютере, и вы можете отметить для удаления только необходимые. Нажатие кнопки **Select all** позволяет выбрать для удаления все элементы списка (установленные продукты или пакеты, в зависимости от режима), а нажатие кнопки **Select none** – снять выбор со всех элементов списка.

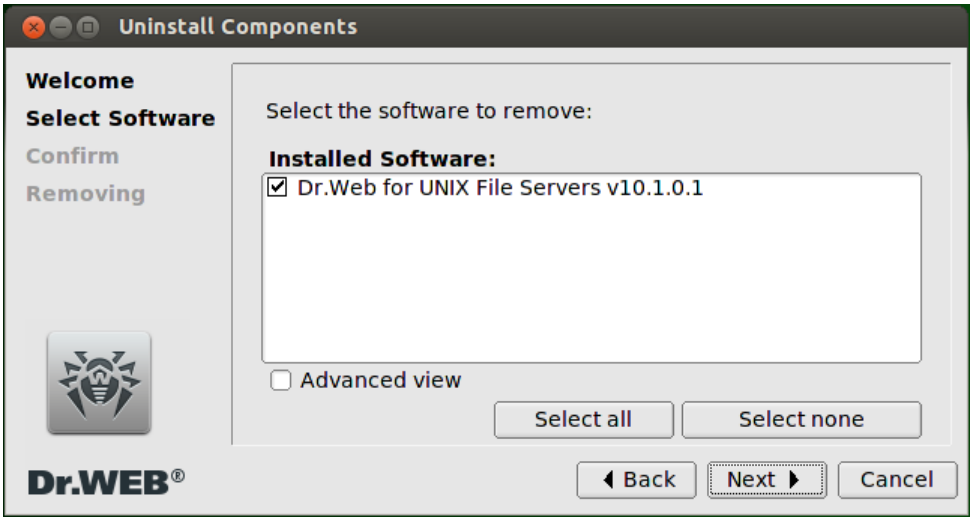

Рисунок 24. Выбор продуктов для удаления в простом режиме

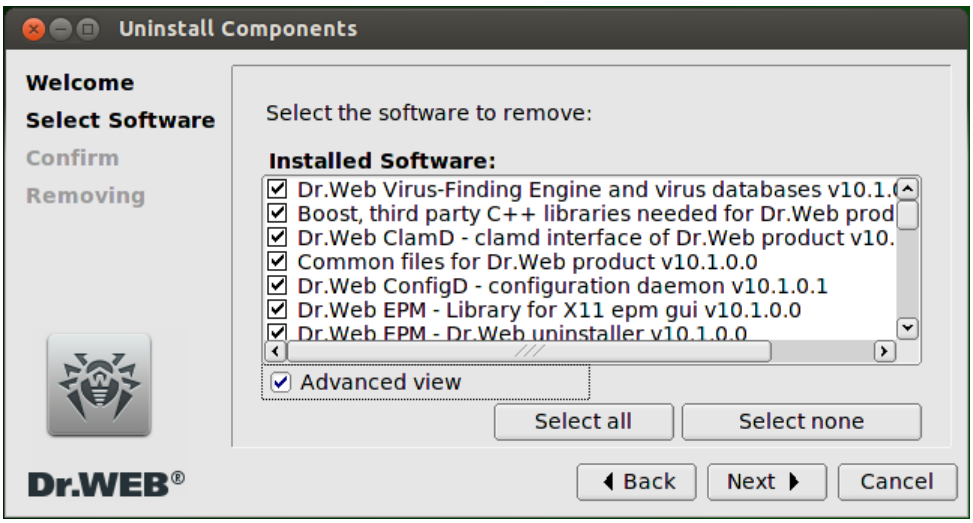

Рисунок 25. Выбор пакетов для удаления в расширенном режиме

Переход в расширенный режим выбора осуществляется установкой флажка **Advanced view**, а возврат в простой режим выбора – сбросом этого флажка. Обратите внимание, что при отметке некоторого пакета к удалению, автоматически отмечаются к удалению все пакеты, которые зависят от него. Аналогично, при снятии отметки с некоторого пакета, автоматически снимаются отметки со всех пакетов, от которых он зависит. После выбора перечня удаляемых продуктов или пакетов, нажмите кнопку **Next** для перехода к подтверждению удаления. Чтобы прекратить работу мастера удаления и отказаться от удаления продукта, нажмите кнопку **Cancel**.

Будьте осторожны при выборе пакетов в расширенном режиме: удалив некоторый пакет, вы можете нарушить работоспособность всех продуктов **Dr.Web**, установленных на вашем компьютере и использующих файлы из данного пакета.

В случае ошибочного удаления пакета, вы можете воспользоваться программой установки в режиме **Custom configuration**, и установить ошибочно удаленный пакет повторно.

2. На следующем шаге мастера удаления вам будет выведен список пакетов **Dr.Web**, которые будут удалены.

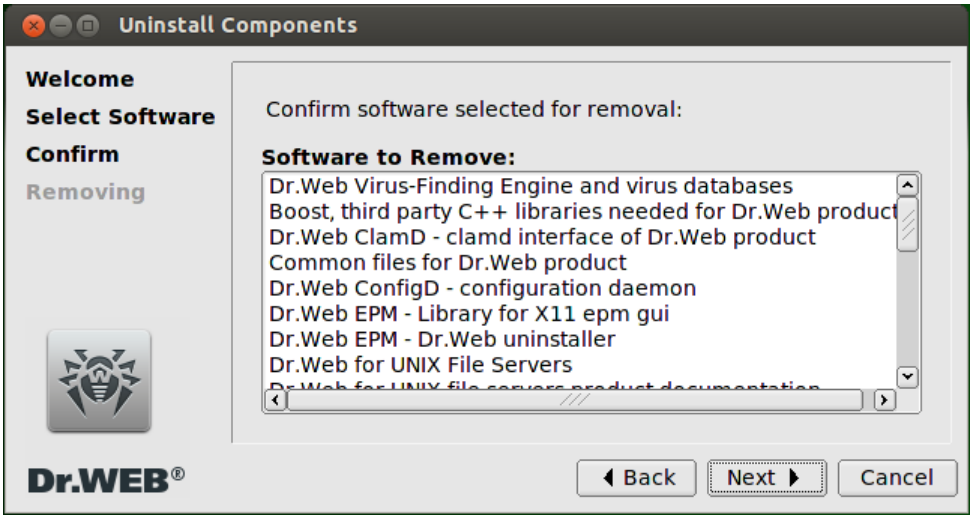

Рисунок 26. Подтверждение удаления

Для подтверждения удаления нажмите кнопку **Next**. Для изменения перечня удаляемых пакетов нажмите кнопку **Back**. Для отказа от удаления и завершения работы программы

удаления нажмите кнопку **Cancel**.

3. После подтверждения начнется процесс удаления файлов **Dr.Web** с вашего компьютера.

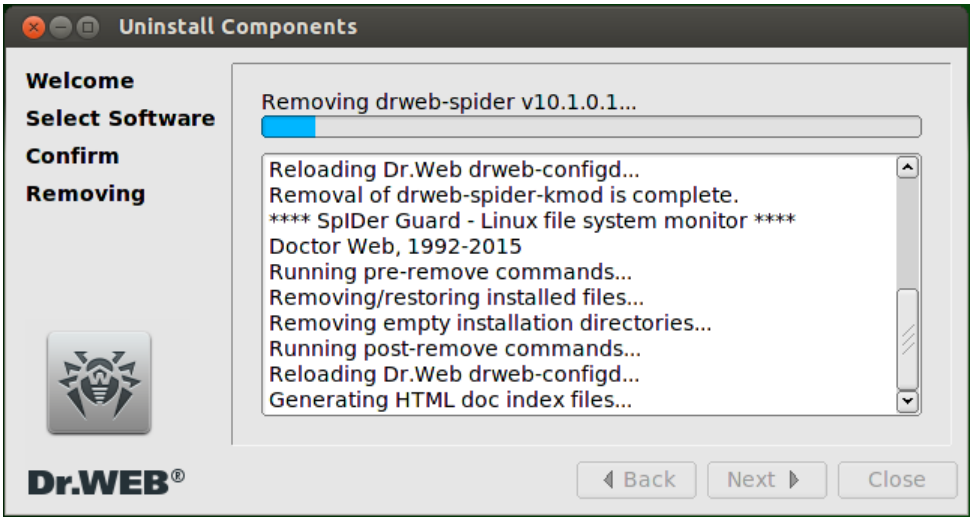

Рисунок 27. Процесс удаления

Для закрытия окна мастера удаления после окончания удаления файлов необходимо нажать кнопку **Close**.

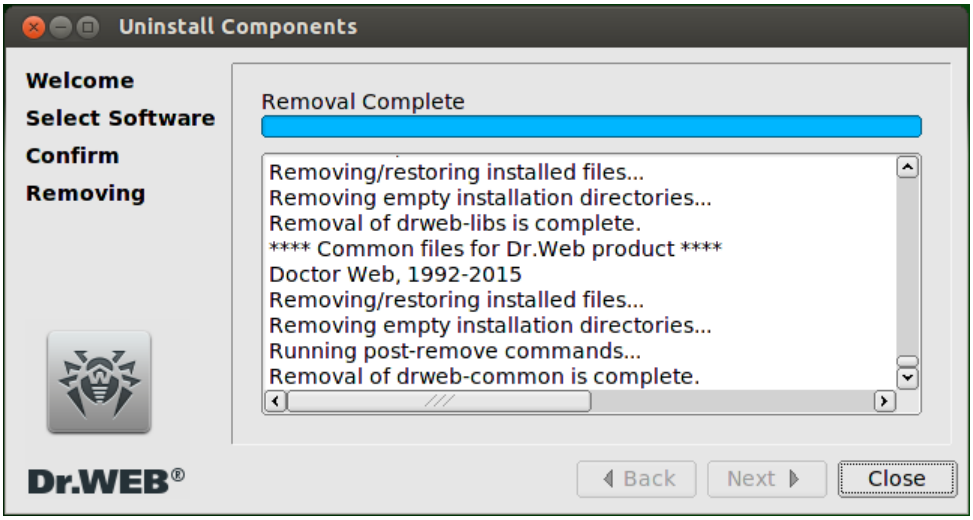

Рисунок 28. Завершение удаления

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 wish to continue?». Чтобы отказаться от удаления продукта, введите `No` или `N`. В этом случае работа программы удаления будет завершена.

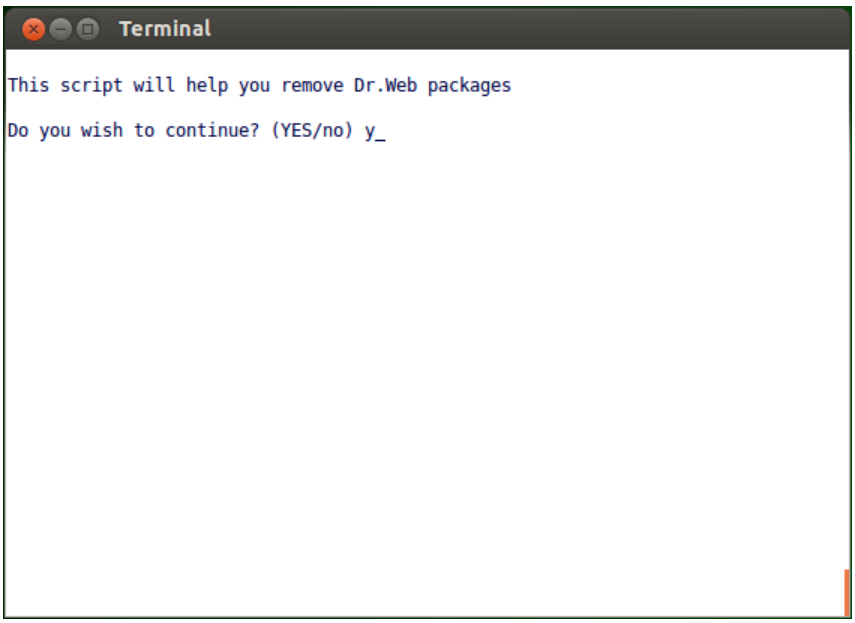

Рисунок 29. Приглашение к удалению

2. Далее на экран будет выведен перечень установленных компонентов **Dr.Web**.

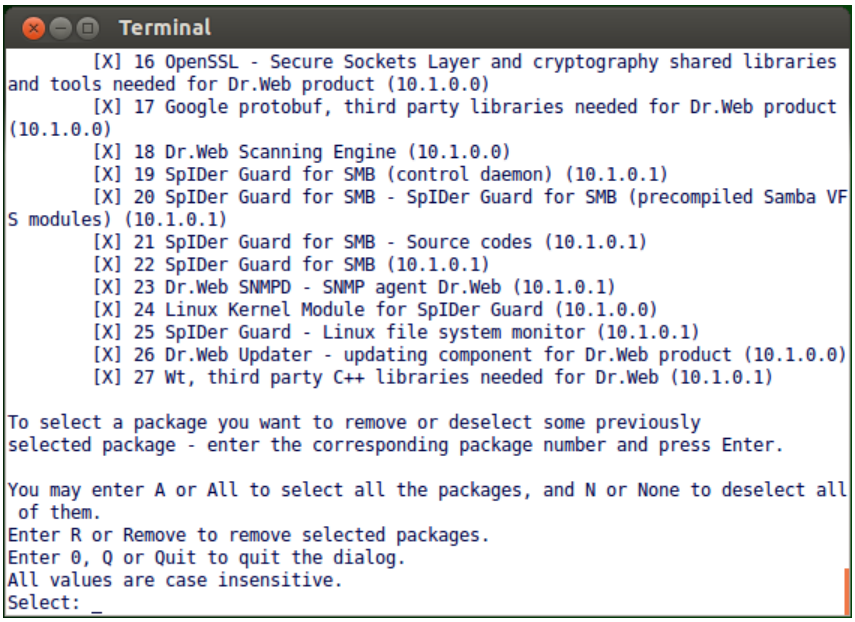

Рисунок 30. Просмотр перечня имеющихся компонентов и выбор компонентов для удаления

3. Для продолжения удаления следует отметить компоненты, подлежащие удалению. Для отметки конкретного пакета необходимо ввести его номер. Обратите внимание, что в случае если от пакета, отмеченного к удалению, зависят какие-то другие пакеты, они также будут отмечены автоматически.
   - Чтобы отметить сразу все имеющиеся компоненты, введите вместо номера слово **All** или **A**.
   - Чтобы сбросить выделение пакетов, введите вместо номера слово **None** или **N**.
   - Чтобы отказаться от удаления, введите вместо номера **0**, **Q** или **Quit**. Это приведет к завершению работы программы удаления.

   После отметки всех подлежащих удалению компонентов, для начала процесса удаления,

введите слово **Remove** или **R**.

5. На следующем экране необходимо просмотреть список пакетов, отмеченных для удаления, и подтвердить удаление, введя **Yes** или **Y**. Чтобы отказаться от удаления, следует ввести **No** или **N**. Это приведет к завершению работы программы удаления.

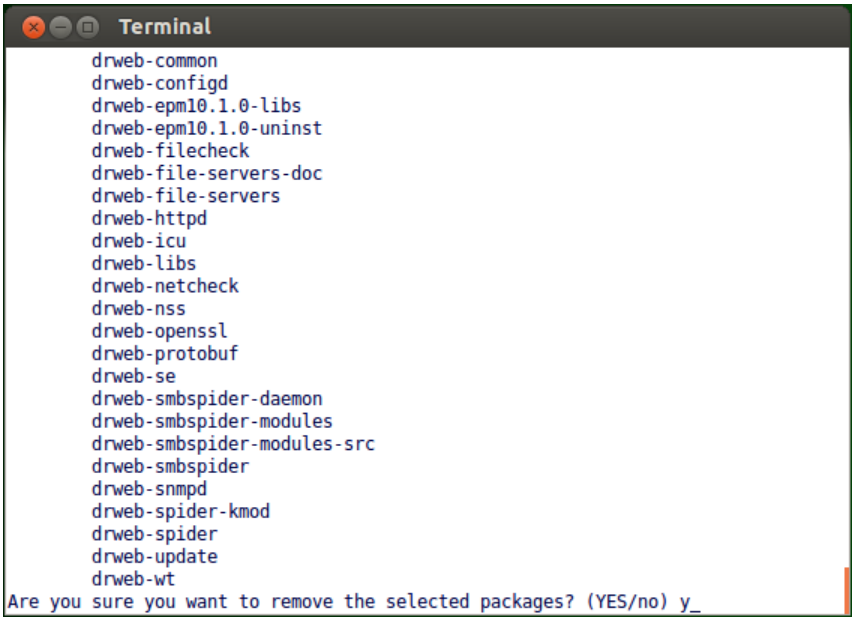

Рисунок 31. Подтверждение удаления отмеченных компонентов

6. После запуска удаления отмеченных ранее пакетов на экран будут выдаваться записи, фиксируемые в журнал удаления и отражающие ход процесса удаления.

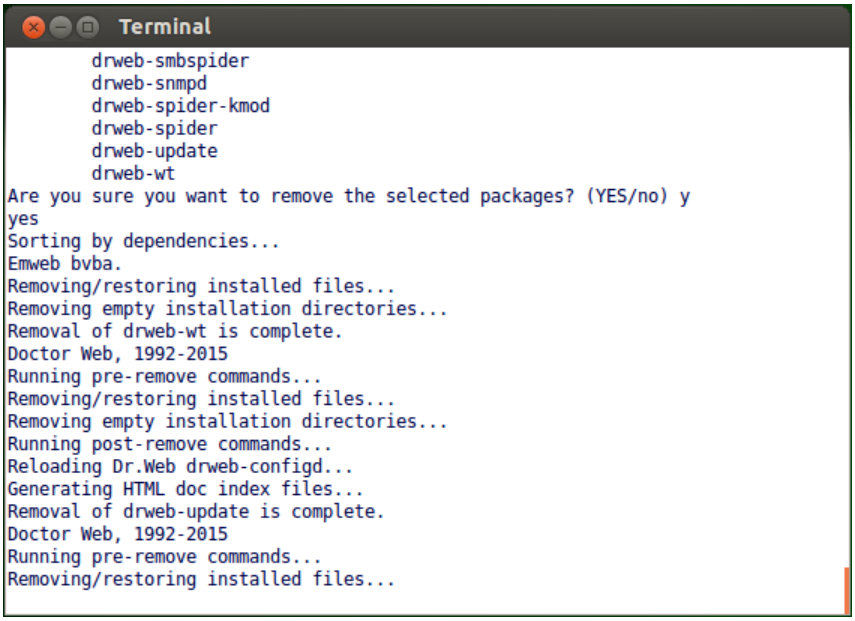

Рисунок 32. Протокол удаления

7. По окончанию процесса программа удаления выведет на экран соответствующее сообщение и завершит свою работу.

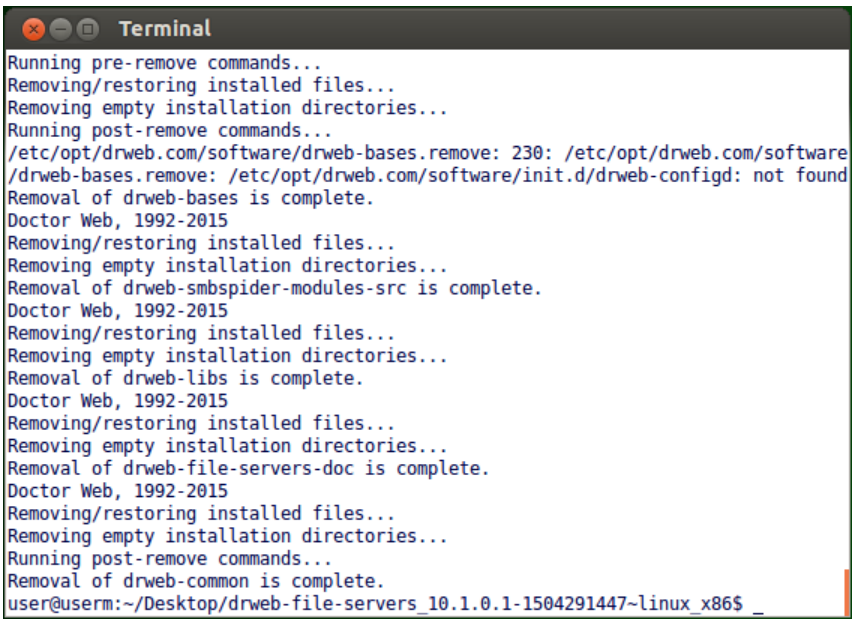

Рисунок 33. Сообщение об окончании удаления

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**).

Red Hat Enterprise Linux, Fedora, CentOS (yum)

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

```
yum remove drweb*
```

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

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**).

Начало работы

1. Для начала работы с установленным **Dr.Web для файловых серверов UNIX** выполните его активацию, получив и установив ключевой файл.
2. Интегрируйте **Dr.Web для файловых серверов UNIX** с требуемыми файловыми службами (см. инструкцию для **Samba**, см. инструкцию для **NSS**).
3. Проверьте состав запущенных компонентов и при необходимости включите дополнительные компоненты, которые по умолчанию отключены, если они необходимы для защиты вашего сервера (например, монитор **SpIDer Guard**, компонент **Dr.Web ClamD** или SNMP-агент **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/`).

Интеграция с файловым сервером Samba

Монитор **SpIDer Guard для SMB**, входящий в состав **Dr.Web для файловых серверов UNIX**, использует для интеграции с **Samba** специальный модуль **VFS SMB**. Совместно со **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 Приложении Ж настоящего Руководства.

Для интеграции **Dr.Web для файловых серверов UNIX** 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**.

   Об условных обозначениях путей `<opt_dir>`, `<etc_dir>` и `<var_dir>` см. во Введении.

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:

   ```
   [<share_name>]
   comment = <any_comment>
   path = </каталог/который/нужно/защитить/>
   vfs objects = smb_spider
   writeable = yes
   browseable = yes
   guest ok = yes
   public = yes
   ```

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

   После этого данный каталог 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.**

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 `[<share_name>]` необходимо добавить строку:

   ```
   smb_spider:socket = <path_to_socket>
   ```

   где `<path_to_socket>` должен быть абсолютным путем к UNIX-сокету, относительно корня, заданного для сервера **Samba** через **chroot**.

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 = <share_name>
   ```

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

   Чтобы добавить новую секцию параметров с тегом `<share_name>` при помощи утилиты управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl**, достаточно использовать команду **drweb-ctl** `cfset SmbSpider.Share.<share_name>.<параметр> <значение>`.

   Пример:

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

   Данная команда добавит в файл конфигурации секцию **[SMBSpider.Share.BuhFiles]**. 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]**.

После внесения изменений в настройки следует перезапустить как сервер **Samba**, так и **SpIDer Guard для SMB**. Для перезапуска **SpIDer Guard для SMB** рекомендуется выполнить перезапуск всего программного комплекса **Dr.Web для файловых серверов UNIX**, выполнив перезапуск демона управления конфигурацией **Dr.Web ConfigD**.

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**).

Скрипты поддержки интеграции

Для удобства настройки интеграции **Dr.Web для файловых серверов UNIX** с файловым сервером **Samba** в составе продукта поставляются специальные скрипты настройки. Они расположены в каталоге `<opt_dir>/share/drweb-smbspider-modules`:

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

Скрипт update-links.sh автоматически запускается сразу при установке продукта **Dr.Web для файловых серверов UNIX**. При необходимости вы можете запускать его в дальнейшем также вручную. Скрипт 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 скрипт 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`** следует указать путь к каталогу файловой системы, в который смонтированы тома файловой системы NSS (по умолчанию используется путь `/media/nss`).
- в параметре **`ProtectedVolumes`** следует перечислить имена томов файловой системы NSS, находящихся в точке монтирования **`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.

После внесения изменений в настройки следует перезапустить **SpIDer Guard для NSS**. Для перезапуска **SpIDer Guard для NSS** рекомендуется выполнить перезапуск всего программного комплекса **Dr.Web для файловых серверов UNIX**, выполнив перезапуск демона управления конфигурацией **Dr.Web ConfigD**.

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 перезапустить программный комплекс Dr.Web для файловых серверов UNIX

Используйте 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**.

Скрипт управления демоном управления конфигурацией **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.
`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

Для подключения продукта **Dr.Web для файловых серверов UNIX** к серверу централизованной защиты необходимо получить от администратора антивирусной сети адрес сервера централизованной защиты и файл его публичного ключа, а также, возможно, дополнительные параметры, такие, как идентификатор хоста и пароль, или идентификаторы основной и тарифной группы.

Далее следует воспользоваться 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 публичного ключа сервера, или опцию `--WithoutKey`, если вы хотите разрешить агенту

централизованной защиты подключиться к серверу без проверки подлинности. Кроме того, можно использовать опцию `--WrongKey`, чтобы разрешить агенту централизованной защиты подключаться к серверу, если публичный ключ из файла не совпадает с открытым ключом, имеющимся на сервере.

Дополнительно вы можете указать идентификатор хоста 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 <server_address> --Key /path/to/server_public_key_file
```

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 необходимо воспользоваться командой `esdisconnect` утилиты 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 http://products.drweb.com/register/.
2. Получите на указанный при регистрации адрес электронной почты (или скачайте 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:

```
[<share_name>]
comment = <any_comment>
path = </каталог/который/нужно/защитить/>
vfs objects = smb_spider
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

где `<share_name>` – любое имя разделяемого ресурса, а `<any_comment>` – 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

- Если вы установили продукт в виде нативных пакетов для вашей ОС из репозитория, воспользуйтесь процедурой обновления, предусмотренной для вашего менеджера пакетов (например, выполнив последовательно команды **`apt-get`** `update` и **`apt-get`** `upgrade` для менеджера пакетов **apt** с правами суперпользователя `root`). Дополнительную информацию вы можете получить из справочных руководств вашей ОС.
- Если вы установили продукт из универсального пакета (файл `.run`), то загрузите обновленную версию дистрибутива и выполните процедуру установки. В процессе установки все компоненты, имеющие обновления, будут заменены на обновленные версии из дистрибутива. Настроенная конфигурация продукта при этом останется неизменной.

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. Предельное время остановки монитора – 40 сек. 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. Компонент обеспечивает схему сбора сообщений ото всех запущенных под его управлением компонентов в единый журнал. Всё, что любой из компонентов аварийно выводит в поток ошибок **`stderr`**, собирается демоном управления конфигурацией и помещается в общий журнал программного комплекса с отметкой о том, какой компонент осуществил это 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 сканирующее ядро **Dr.Web Scanning Engine** и компонент проверки файлов **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 компонента, то компонент завершает работу с кодом 0, в этом случае **Dr.Web ConfigD** перезапустит 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 [options]
```

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

Краткий вариант	Расширенный вариант	Аргументы
`-h`	`--help`	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля		
`-v`	`--version`	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		
`-c`	`--config`	`<путь к файлу>`
Описание: Использование указанного конфигурационного файла		
`-d`	`--daemonize`	
Описание: Запустить компонент в режиме демона, т.е. без доступа к терминалу		
`-p`	`--pid-file`	`<путь к файлу>`
Описание: Использование указанного PID-файла		

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 `/etc/init.d`.

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 модулей продукта **Dr.Web для файловых серверов UNIX** по умолчанию. Используется, если в конфигурации какого-либо из модулей не указан свой уровень подробности ведения журнала.
	Значение по умолчанию: **`DefaultLogLevel`** = `Notice`

LogLevel = {уровень подробности}	Уровень подробности ведения журнала демона управления конфигурацией **Dr.Web ConfigD.** Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала демона управления конфигурацией, а также метод ведения журнала для тех модулей, у которых не указан свой 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 Значение по умолчанию: **Log** = Syslog:Daemon
PublicSocketPath = {путь к файлу}	Путь к публичному коммуникационному сокету для взаимодействия компонентов **Dr.Web для файловых серверов UNIX.** Значение по умолчанию: **PublicSocketPath** = /var/run/.com.drweb.public
AdminSocketPath = {путь к файлу}	Путь к административному коммуникационному сокету для взаимодействия компонентов **Dr.Web для файловых серверов UNIX.** Значение по умолчанию: **AdminSocketPath** = /var/run/.com.drweb.admin
CoreEnginePath = {путь к файлу}	Путь к динамической библиотеке антивирусного ядра **Dr.Web Virus-Finding Engine**. Значение по умолчанию: **CoreEnginePath** = <var_dir>/lib/drweb32.dll Для **Linux**: **CoreEnginePath** = /var/opt/drweb.com/lib/drweb32.dll Для **FreeBSD**: **CoreEnginePath** = /var/drweb.com/lib/drweb32.dll Для **Solaris**: **CoreEnginePath** = /var/opt/drweb.com/lib/drweb32.dll
VirusBaseDir = {путь к каталогу}	Путь к каталогу, в котором хранятся файлы вирусных баз. Значение по умолчанию: **VirusBaseDir** = <var_dir>/bases Для **Linux**: **VirusBaseDir** = /var/opt/drweb.com/bases Для **FreeBSD**: **VirusBaseDir** = /var/drweb.com/bases Для **Solaris**: **VirusBaseDir** = /var/opt/drweb.com/bases
KeyPath = {путь к файлу}	Путь к ключевому файлу. Значение по умолчанию: **KeyPath** = <etc_dir>/drweb32.key Для **Linux**:

	KeyPath = /etc/opt/drweb.com/drweb32.key Для **FreeBSD**: **KeyPath** = /usr/local/etc/drweb.com/drweb32.key Для **Solaris**: **KeyPath** = /etc/opt/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: **CacheDir** = <var_dir>/cache Для **Linux**: **CacheDir** = /var/opt/drweb.com/cache Для **FreeBSD**: **CacheDir** = /var/drweb.com/cache Для **Solaris**: **CacheDir** = /var/opt/drweb.com/cache
TempDir = {путь к каталогу}	Путь к каталогу для хранения временных файлов. Значение по умолчанию: **TempDir** = /tmp
RunDir = {путь к каталогу}	Путь к каталогу, в котором будут храниться PID-файлы и файлы коммуникационных сокетов. Значение по умолчанию: **RunDir** = /var/run
VarLibDir = {путь к каталогу}	Путь к каталогу библиотек. Значение по умолчанию: **VarLibDir** = <var_dir>/lib Для **Linux**: **VarLibDir** = /var/opt/drweb.com/lib Для **FreeBSD**: **VarLibDir** = /var/drweb.com/lib Для **Solaris**: **VarLibDir** = /var/opt/drweb.com/lib
VersionDir = {путь к каталогу}	Параметр не используется. Значение по умолчанию: **VersionDir** =
DwsDir = {путь к каталогу}	Параметр не используется. Значение по умолчанию: **DwsDir** = <var_dir>/dws Для **Linux**: **DwsDir** = /var/opt/drweb.com/dws Для **FreeBSD**: **DwsDir** = /var/drweb.com/dws Для **Solaris**: **DwsDir** = /var/opt/drweb.com/dws
HtmlTemplatesDir =	Параметр не используется.

	Значение по умолчанию: **HtmlTemplatesDir** = <var_dir>/html Для **Linux**: **HtmlTemplatesDir** = /var/opt/drweb.com/html Для **FreeBSD**: **HtmlTemplatesDir** = /var/drweb.com/html Для **Solaris**: **HtmlTemplatesDir** = /var/opt/drweb.com/html
MailTemplatesDir = {путь к каталогу}	Параметр не используется. Значение по умолчанию: **MailTemplatesDir** = <var_dir>/mail Для **Linux**: **HtmlTemplatesDir** = /var/opt/drweb.com/mail Для **FreeBSD**: **MailTemplatesDir** = /var/drweb.com/mail Для **Solaris**: **MailTemplatesDir** = /var/opt/drweb.com/mail
AdminGroup = {имя группы | GID}	Группа пользователей, обладающих административными правами в рамках **Dr.Web для файловых серверов UNIX**. Данные пользователи наряду с root могут повышать полномочия компонентов **Dr.Web для файловых серверов UNIX** до полномочий суперпользователя. Значение по умолчанию: **AdminGroup** =
TrustedGroup = {имя группы | GID}	Параметр не используется. Значение по умолчанию: **TrustedGroup** =
DebugIpc = {логический}	Включать или нет в журнал на отладочном уровне (**LogLevel** = DEBUG) подробные сообщения IPC (взаимодействие демона управления конфигурацией **Dr.Web ConfigD** с другими компонентами). Значение по умолчанию: **DebugIpc** = No

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.

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.

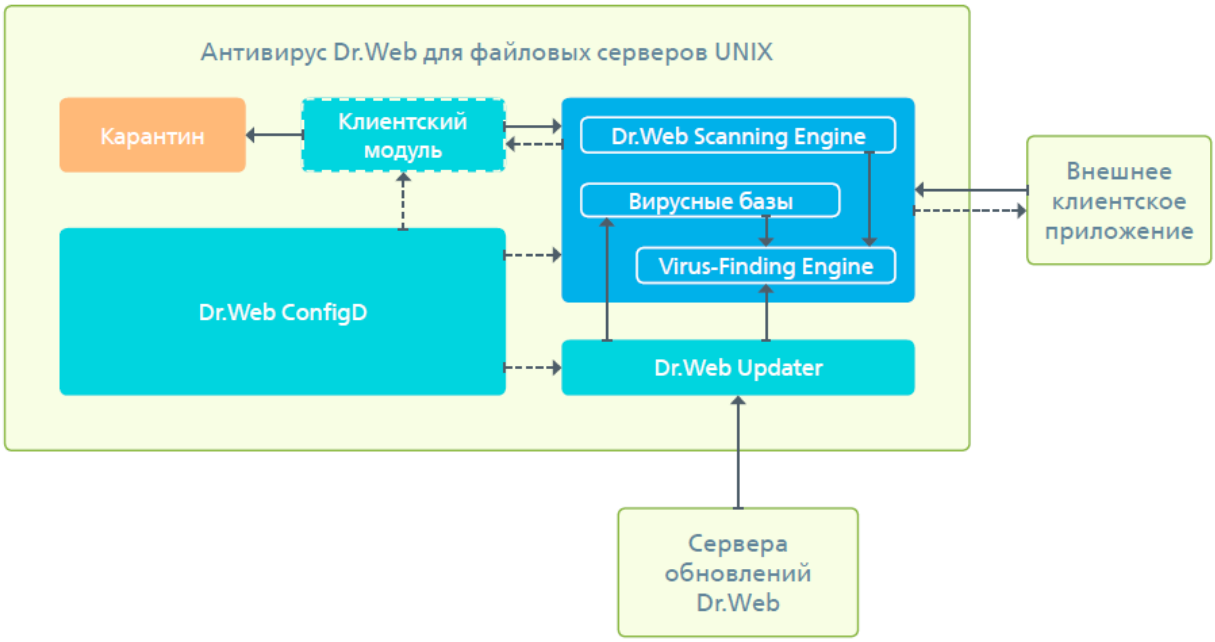

Рисунок 34. Схема работы компонента

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 модулем обновлений **Dr.Web Updater**, входящим в состав продукта, но не являющимся частью сканирующего ядра. Модуль обновления 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), взаимодействующий с сервером

централизованной защиты, и получающий обновления с 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.

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 упакованных 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 консоли операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-se [options]
```

Dr.Web Scanning Engine допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
`-h`	`--help`	

Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.

-v	--version	

Описание: Вывод на экран консоли информации о версии модуля и завершение работы

Дополнительные опции (совпадают с параметрами из конфигурационного файла и замещают их при необходимости):

	--Socket	<адрес>

Описание: Адрес сокета, используемого **Dr.Web Scanning Engine.** Может задаваться как путь к файлу (UNIX-сокет), или в виде пары <IP-адрес:порт>, причем если нужно использовать сетевой интерфейс по умолчанию, вместо IP-адреса можно использовать символ '*'.

Примеры:

```
--Socket /var/opt/drweb.com/ipc/.se
--Socket 127.0.0.1:1000
--Socket *:1000
```

	--EnginePath	<путь к файлу>

Описание: Путь к файлу библиотеки антивирусного ядра **Dr.Web Virus-Finding Engine.**

	--VirusBaseDir	<путь к каталогу>

Описание: Путь к каталогу, содержащему файлы вирусных баз.

	--TempDir	<путь к каталогу>

Описание: Путь к каталогу временных файлов.

	--Key	<путь к файлу>

Описание: Путь к лицензионному ключевому файлу.

	--MaxForks	<число>

Описание: Максимальное разрешенное число дочерних процессов, которые может породить в процессе проверки **Dr.Web Scanning Engine.**

	--WatchdogInterval	<интервал времени>

Описание: Периодичность, с которой **Dr.Web Scanning Engine** проверяет работоспособность дочерних процессов, занимающихся проверкой содержимого файлов, для остановки зависших при проверке.

	--ShellTrace	

Описание: Включить отслеживание оболочки (вывод в журнал расширенной информации о проверке файлов **Dr.Web Virus-Finding Engine**).

	--LogLevel	<уровень подробности>

Описание: Уровень подробности ведения журнала ядром **Dr.Web Scanning Engine** в процессе работы. 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`	`<место назначения>`

Описание: Способ ведения журнала сообщений модуля. 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 -c /etc/opt/drweb.com/drweb.ini --MaxForks=5
```

Данная команда запустит копию сканирующего ядра **Dr.Web Scanning Engine,** заставив его использовать конфигурационный файл `/etc/opt/drweb.com/drweb.ini`, с предписанием порождать не более 5 сканирующих дочерних процессов.

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**) запросы на проверку объектов файловой системы на наличие угроз.) сервис по проверке файлов на наличие угроз. При этом, если в конфигурации **Dr.Web для файловых серверов UNIX** задан параметр **`SeFixedSocketPath`** (в секции `[ScanEngine]`), то одна копия сканирующего ядра всегда будет автоматически запущена демоном управления конфигурацией **Dr.Web ConfigD.** Экземпляры сканирующего ядра, запускаемые непосредственно из командной строки, будут работать в автономном режиме, без подключения к демону управления конфигурацией, даже если он запущен.

Для проверки файлов по требованию следует воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **`drweb-ctl`**).

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 сканирующего ядра **Dr.Web Scanning Engine.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root] Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала сканирующего ядра **Dr.Web Scanning Engine.** Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web Scanning Engine.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-se Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-se Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-se Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-se
FixedSocketPath = {путь к файлу}	Определяет путь к файлу 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: **FixedSocketPath** =
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: **MaxForks** = Автоматически определяется при старте, как удвоенное число доступных процессорных ядер, или 4, если полученное число меньше 4.
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: **WatchdogInterval** = 1.5s
IdleTimeLimit = {интервал времени}	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Минимальное значение – 10s. Если параметр **FixedSocketPath** задан, то настройка

	игнорируется (компонент не завершает свою работу по истечению максимального времени простоя).
	Значение по умолчанию: **IdleTimeLimit** = 1h

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 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.

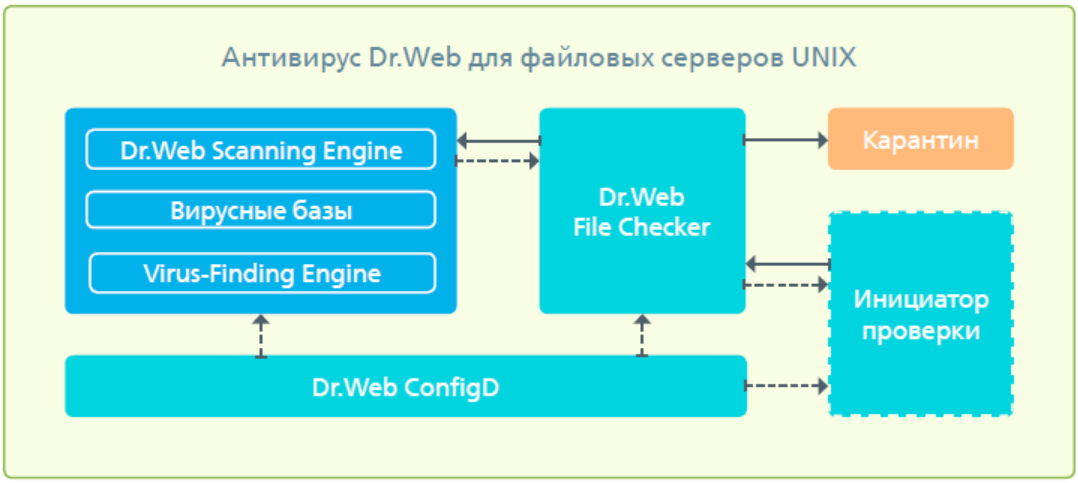

Рисунок 35. Схема работы компонента

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 компонент проверки файлов **Dr.Web File Checker** применяет к нему нейтрализующее действие (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 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 проверки файлов **Dr.Web File Checker** из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-filecheck [options]
```

Dr.Web File Checker допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
-v	--version	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

Пример:

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

Данная команда выведет на экран краткую справку компонента проверки файлов **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 проверки файлов по требованию следует воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **drweb-ctl**).

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 проверки файлов **Dr.Web File Checker.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root]. Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала компонента проверки файлов **Dr.Web File Checker.** Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web File Checker.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-filecheck Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-filecheck Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-filecheck Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-filecheck
DebugClientIpc = {логический}	Включать или нет в журнал на отладочном уровне (**LogLevel** = DEBUG) подробные сообщения IPC. Значение по умолчанию: **DebugClientIpc** = no
DebugScan = {логический}	Включать или нет в журнал на отладочном уровне (**LogLevel** = DEBUG) подробные сообщения, поступающие в процессе проверки файлов. Значение по умолчанию: **DebugScan** = no
DebugFlowScan = {логический}	Включать или нет в журнал на отладочном уровне (**LogLevel** = DEBUG) подробные сообщения о проверке файлов методом «flow». (Обычно метод «flow» используется монитором **SpIDer Guard**). Значение по умолчанию: **DebugFlowScan** = No
DebugProxyScan = {логический}	Включать или нет в журнал на отладочном уровне (**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: **DebugProxyScan** = No
DebugCache = {логический}	Включать или нет в журнал на отладочном уровне (**LogLevel** = DEBUG) подробные сообщения о состоянии кэша проверенных файлов.

	Значение по умолчанию: **DebugCache** = No
MaxCacheSize = {размер}	Максимальный разрешенный размер кэша для хранения информации о проверенных файлах. Если указано 0 – кэширование отключено. Значение по умолчанию: **MaxCacheSize** = 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). Если указано 0 – интервал задержки отсутствует, файл будет проверяться при любом запросе. Значение по умолчанию: **RescanInterval** = 1s
IdleTimeLimit = {интервал времени}	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Минимальное значение – 10s. Значение по умолчанию: **IdleTimeLimit** = 30s

SpIDer Guard

Монитор файловой системы **Linux SpIDer Guard** предназначен для мониторинга файловой активности на томах файловой системы операционных систем **GNU/Linux.** Модуль 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 задание компоненту проверки файлов **Dr.Web File Checker** на инициацию проверки 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.

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

Принципы работы

Монитор файловой системы **SpIDer Guard** может работать как в пользовательском пространстве (*user mode*), так и в режиме модуля ядра **Linux** (*LKM – Linux kernel module*). В настройках рекомендуется использовать автоматический режим (*auto*), который позволит модулю при старте определить и использовать наилучший режим работы, поскольку не все версии ядра **Linux** поддерживают механизм **`fanotify`**, использующийся при работе монитора в *user mode*. В случае если модуль не может использовать указанный режим интеграции, он завершается сразу после старта. Если указан автоматический режим, то модуль сначала попытается использовать пользовательский режим, а затем – режим LKM. В случае если не получится использовать ни один из этих режимов, модуль завершит работу.

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.

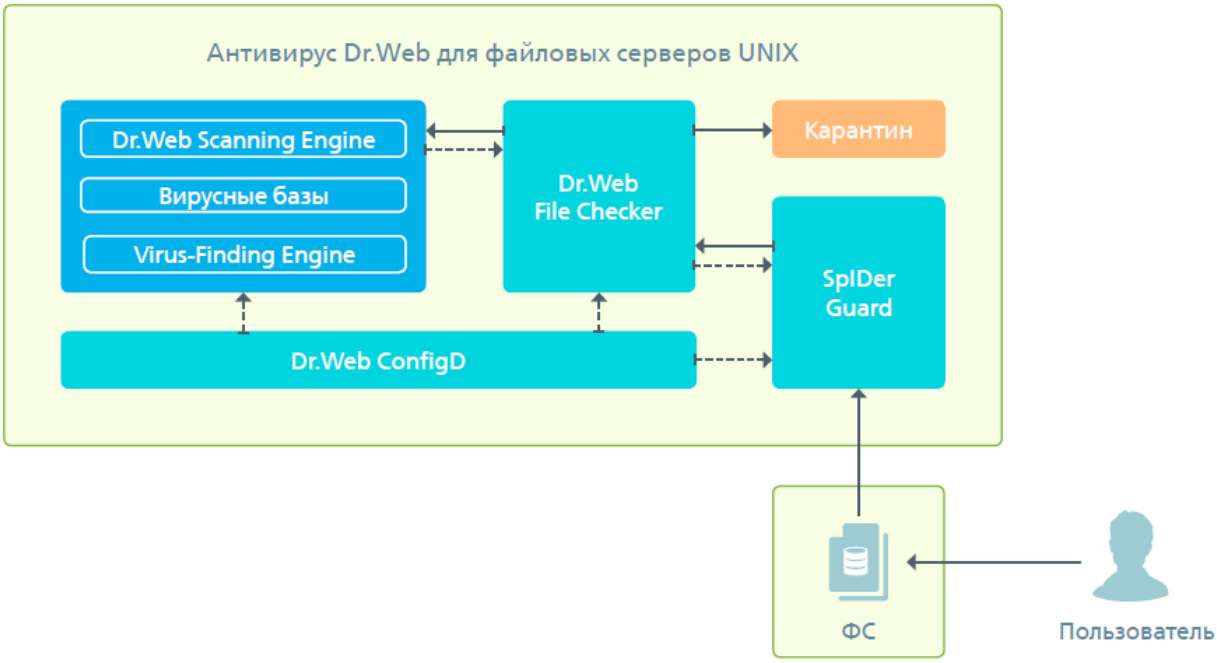

Рисунок 36. Схема работы компонента

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 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 монитора файловой системы **SpIDer Guard** из командной строки операционной системы используется следующая команда:

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

SpIDer Guard допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
-v	--version	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

Пример:

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

Данная команда выведет на экран краткую справку монитора файловой системы **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 запуска или останова работы компонента можно также воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **drweb-ctl**).

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 монитора файловой системы **SpIDer Guard.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root] Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала монитора файловой системы **SpIDer Guard.** Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **SpIDer Guard.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-spider Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-spider
Start = {логический}	Определяет необходимость автозапуска компонента **SpIDer Guard** при старте программного комплекса **Dr.Web для файловых серверов UNIX.** Значение по умолчанию: **Start** = Yes

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. 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. Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Значение по умолчанию: **ExcludedPath** = "/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**. 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. 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, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Значение по умолчанию: **IncludedPath** = /
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, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Значение по умолчанию: **ExcludedProc** =
Mode = {LKM|FANOTIFY|AUTO}	Определяет режим работы монитора файловой системы **SpIDer Guard.** Возможные значения: • LKM – Работа в режиме модуля ядра операционной системы (LKM для **Linux**) • FANOTIFY – Работа в пользовательском режиме.

	• AUTO – Автоматическое определение оптимального режима работы. Обратите внимание, что изменение значения этого параметра следует производить с крайней осторожностью, поскольку не все ядра ОС семейства **GNU/Linux** корректно работают с модулем **SpIDer Guard** в различных режимах. Настоятельно рекомендуется оставлять этот параметр в значении AUTO, чтобы при запуске был выбран оптимальный режим интеграции с диспетчером файловой системы. При этом модуль сначала пытается использовать режим FANOTIFY, потом, в случае неудачи – LKM. Если не удалось использовать ни один из режимов, работа модуля завершается. Значение по умолчанию: **Mode** = AUTO
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: **OnKnownVirus** = 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: **OnIncurable** = 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: **OnSuspicious** = 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: **OnAdware** = 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: **`OnDialers`** = `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: **`OnJokes`** = `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: **`OnRiskware`** = `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: **`OnHacktools`** = `Report`
`ScanTimeout` = `{интервал времени}`	Устанавливает тайм-аут на проверку одного файла по запросу **SpIDer Guard**. Значение 0 указывает, что время проверки не ограничено. Значение по умолчанию: **`ScanTimeout`** = `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: **`HeuristicAnalysis`** = `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**. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **PackerMaxLevel** = 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**. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **ArchiveMaxLevel** = 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**. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **MailMaxLevel** = 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**. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **ContainerMaxLevel** = 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 сжатия должна быть не менее 2. Значение по умолчанию: **MaxCompressionRatio** = 500

SpIDer Guard для SMB

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**.

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**).

Монитор **SpIDer Guard для SMB** использует для интеграции с **Samba** специальный модуль **VFS SMB**. Совместно со **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 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 Приложении Ж настоящего Руководства.

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.

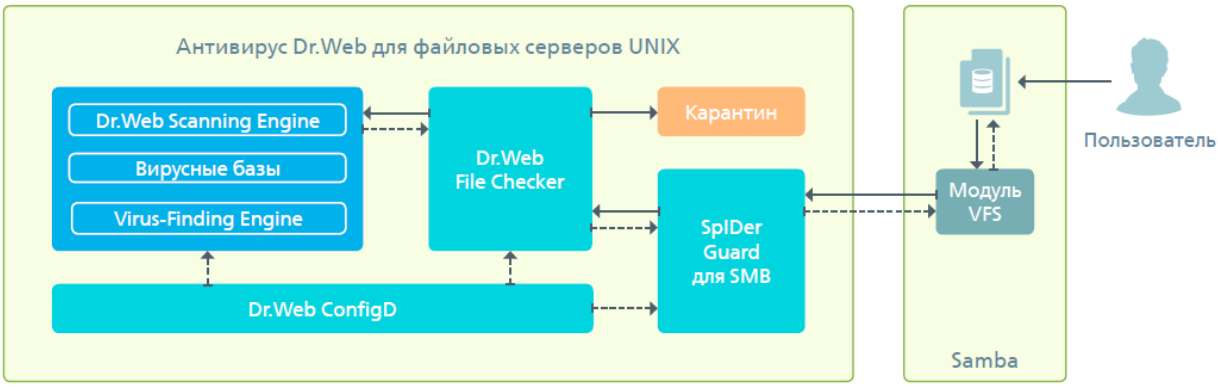

Рисунок 37. Схема работы компонента

Когда в файле, проверенном по запросу от монитора, обнаруживается неизлечимая угроза, или если для данного типа угрозы в настройках было указано действие `'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» или «Переместить в карантин». 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.

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 проверки 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 файловых хранилищ **Samba 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 монитора файловых хранилищ **Samba SpIDer Guard для SMB** из командной строки операционной системы используется следующая команда:

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

SpIDer Guard для SMB допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
`-h`	`--help`	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
`-v`	`--version`	

Описание: Вывод на экран консоли информации о версии модуля и завершение работы

Пример:

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

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

Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки консоли операционной системы в автономном режиме. Он запускается автоматически, при старте операционной системы, демоном управления конфигурацией **Dr.Web ConfigD.** Для запуска или останова работы компонента можно также воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **drweb-ctl**).

Параметры конфигурации

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

В секции представлены следующие параметры:

LogLevel = {уровень подробности}	Уровень подробности ведения журнала монитора каталогов SMB **SpIDer Guard для SMB.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root] Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала монитора каталогов SMB **SpIDer Guard для SMB.** Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **SpIDer Guard для SMB.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-smbspider-daemon Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-smbspider-daemon Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-smbspider-daemon Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-smbspider-daemon
Start = {логический}	Определяет необходимость автозапуска компонента **SpIDer Guard для SMB** при старте программного комплекса Значение по умолчанию: **Start** = Yes
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: **SambaChrootDir** =
[*] **ExcludedPath** = {путь к файлу или каталогу}	Определяет путь к объекту в разделяемом каталоге, 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 `[ ]`, `[! ]`, `[^ ]`). Если указан каталог, то будет пропущено всё содержимое этого каталога. Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Значение по умолчанию: **ExcludedPath** =
[*] **IncludedPath** = {путь к файлу или каталогу}	Определяет путь к объекту в разделяемом каталоге, 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 `[ ]`, `[! ]`, `[^ ]`). Если указан каталог, то будут проверены все содержащиеся в этом каталоге файлы и подкаталоги. Обратите внимание, что этот параметр имеет приоритет над параметром **ExcludedPath** в этой же секции, т.е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен. Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Значение по умолчанию: **IncludedPath** =
[*] **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: **AlertFiles** = `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: **`OnKnownVirus`** = `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: **`OnIncurable`** = `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: **`OnSuspicious`** = `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: **`OnAdware`** = `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: **`OnDialers`** = `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: **`OnJokes`** = `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: **OnRiskware** = 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: **OnHacktools** = Pass
[*] **BlockOnError** = {логический}	Определяет, следует ли **SpIDer Guard для SMB** блокировать файл для доступа, если в процессе его проверки произошла ошибка. Возможные значения: • `Yes` – Блокировать доступ к файлу. • `No` – Не блокировать. Значение по умолчанию: **BlockOnError** = Yes
[*] **ScanTimeout** = {интервал времени}	Устанавливает тайм-аут на проверку одного файла по запросу от **SpIDer Guard для SMB**. Значение 0 указывает, что время проверки не ограничено. Значение по умолчанию: **ScanTimeout** = 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: **HeuristicAnalysis** = 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**. Значение 0 указывает, что вложенные объекты не проверяются.

	Значение по умолчанию: **PackerMaxLevel** = 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**. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **ArchiveMaxLevel** = 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**. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **MailMaxLevel** = 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**. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **ContainerMaxLevel** = 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 сжатия должна быть не менее 2. Значение по умолчанию: **MaxCompressionRatio** = 500
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 **ChrootPath**. Значение по умолчанию: **SmbSocketPath** = 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: **ActionDelay** = 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: **MaxCacheSize** = 10mb

Настройка индивидуальных параметров проверки

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 = <someTag>
```

где `<someTag>` – это уникальный тег, присвоенный модулю **VFS SMB** SMB-сервером **Samba** для некоторого разделяемого каталога.

Если для некоторого модуля **VFS SMB** определен уникальный тег `<someTag>`, 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.<someTag>]**.

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.<someTag>]**, 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.<someTag>]** удалить некоторый параметр, то для этой секции (и соответствующего каталога с тегом **<someTag>**) 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 `<someTag>` 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.<someTag>.<параметр> <значение>`.

Пример:

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

Данная команда добавит в файл конфигурации секцию **[SMBSpider.Share.BuhFiles]**. Эта 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]**.

SpIDer Guard для NSS

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.

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.

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.

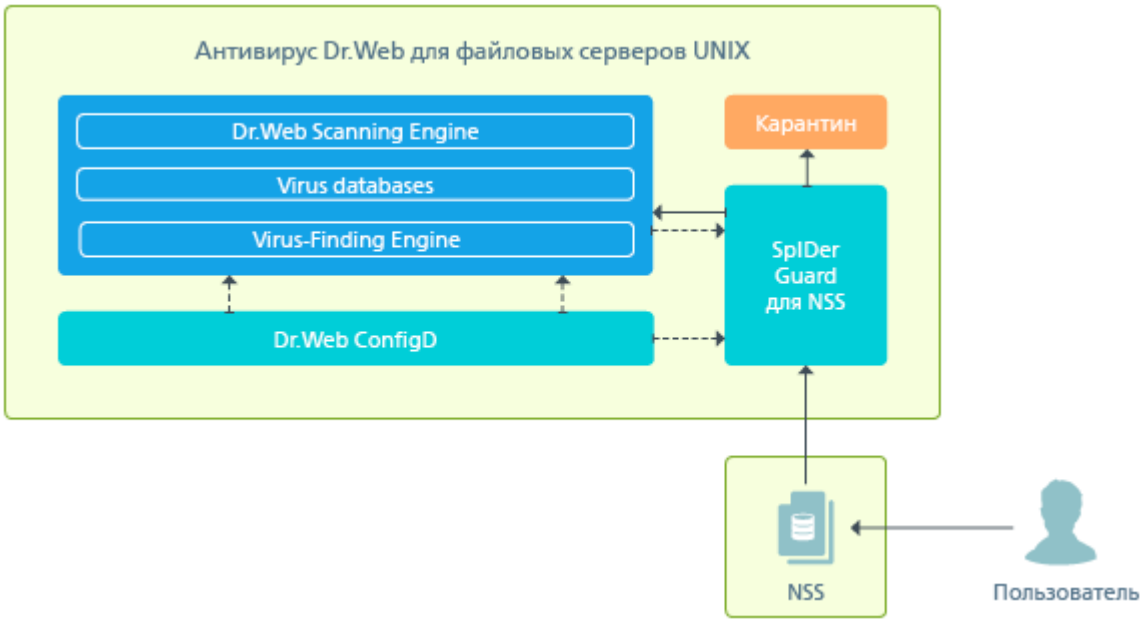

Рисунок 38. Схема работы компонента

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.

При необходимости имеется возможность запретить монитору **SpIDer Guard для NSS** осуществлять мониторинг файловой активности для некоторых файлов или каталогов. Это бывает необходимо, например, в случае 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.

Аргументы командной строки

Для запуска монитора томов NSS **SpIDer Guard для NSS** из командной строки операционной системы используется следующая команда:

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

SpIDer Guard для NSS допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
`-h`	`--help`	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
`-v`	`--version`	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

Пример:

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

Данная команда выведет на экран краткую справку монитора томов NSS **SpIDer Guard для NSS**.

Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки консоли операционной системы в автономном режиме. Он запускается автоматически, при старте операционной системы, демоном управления конфигурацией **Dr.Web ConfigD.** Для запуска или останова работы компонента можно также воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **drweb-ctl**).

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 монитора томов NSS **SpIDer Guard для NSS.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции `[Root]` Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала монитора томов NSS **SpIDer Guard для NSS.** Значение по умолчанию: **Log** = Auto
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: **LogProtocol** = No
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **SpIDer Guard для NSS.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-nss Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-nss
Start = {логический}	Определяет необходимость автозапуска компонента **SpIDer Guard для NSS** при старте программного комплекса **Dr.Web для файловых серверов UNIX.** Значение по умолчанию: **Start** = Yes
NssVolumesMountDir = {путь к каталогу}	Указывает путь к каталогу файловой системы, в который смонтированы тома файловой системы NSS. Значение по умолчанию: **NssVolumesMountDir** = /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 **NssVolumesMountDir**. Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).

	Значение по умолчанию: **ProtectedVolumes** =
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. Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пути в списке указываются относительными – относительно пути, указанного в **NssVolumesMountDir**. Значение по умолчанию: **ExcludedPath** =
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. Обратите внимание, что этот параметр имеет приоритет над параметром **ExcludedPath** в этой же секции, т.е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен. Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пути в списке указываются относительными – относительно пути, указанного в **NssVolumesMountDir**. Значение по умолчанию: **IncludedPath** =
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: **OnKnownVirus** = 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: **OnIncurable** = 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: **OnSuspicious** = 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: **OnAdware** = 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: **OnDialers** = 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: **OnJokes** = 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: **OnRiskware** = 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: **OnHacktools** = 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: **OnError** = Report
ScanTimeout = {интервал времени}	Устанавливает тайм-аут на проверку одного файла по запросу от монитора томов NSS. Значение 0 указывает, что время проверки не ограничено. Значение по умолчанию: **ScanTimeout** = 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: **HeuristicAnalysis** = 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. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **PackerMaxLevel** = 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. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **ArchiveMaxLevel** = 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.

	Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **MailMaxLevel** = 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. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: **ContainerMaxLevel** = 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 сжатия должна быть не менее 2. Значение по умолчанию: **MaxCompressionRatio** = 500

Если в настройках 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.

Dr.Web Updater

Компонент обновления **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 компонент **Dr.Web ES Agent**, а **Dr.Web Updater** для загрузки обновлений не используется.

Принципы работы

Компонент предназначен для подключения к серверам обновлений компании **«Доктор Веб»** для проверки наличия обновлений вирусных баз и антивирусного ядра **Dr.Web Virus-Finding Engine**. Списки серверов, которые доступны для получения 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. 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.

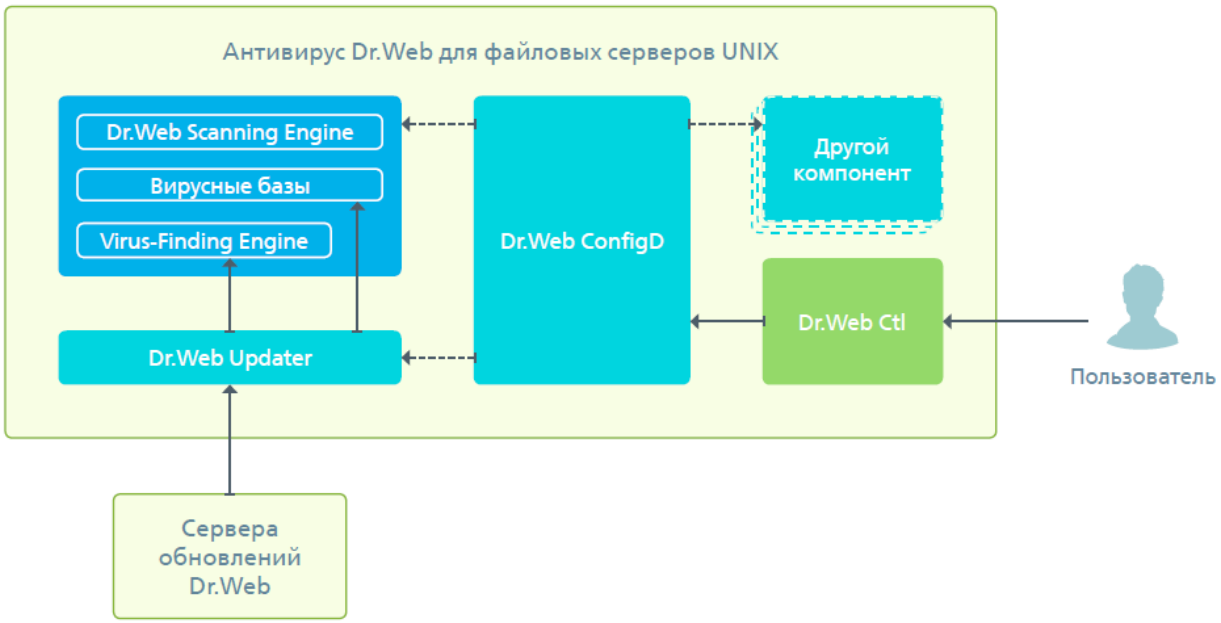

Рисунок 39. Схема работы компонента

При наличии на сервере 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.**

Аргументы командной строки

Для запуска компонента обновления **Dr.Web Updater** из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-update [options]
```

Dr.Web Updater допускает использование следующих параметров:

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

Пример:

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

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

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 обновления вирусных баз и антивирусного ядра с серверов обновлений компании **«Доктор Веб»** по запросу можно

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

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 модуля обновлений **Dr.Web Updater.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root]. Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала компонента обновления **Dr.Web Updater.** Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web Updater.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-update Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-update Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-update Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-update
UpdateInterval = {интервал времени}	Частота проверки наличия обновлений для вирусных баз и антивирусного ядра. Период времени, который должен пройти от предыдущего успешного обновления (автоматического или инициированного пользователем) до следующей попытки выполнить обновление. Значение по умолчанию: **UpdateInterval** = 30m
RetryInterval = {интервал времени}	Частота повторных попыток обновления в случае если очередное обновление завершилось неудачей. Параметр может значение от 1m до 30m. Значение по умолчанию: **RetryInterval** = 3m
MaxRetries = {целое число}	Количество повторных попыток выполнить обновление (предпринимаемых через промежутки времени **RetryInterval**), если предыдущая попытка обновления окончилась неудачей. Если значение параметра – 0, повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени **UpdateInterval**).

	Значение по умолчанию: **MaxRetries** = 3
Proxy = {строка подключения}	Хранит параметры подключения к прокси-серверу, который используется компонентом обновления **Dr.Web Updater** для подключения к серверам обновлений компании **«Доктор Веб»** (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 хоста, на котором работает прокси (IP-адрес или имя домена). • <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 хосте proxyhost.company.org на порт 123: **Proxy** = proxyhost.company.org:123 • Подключение к прокси на хосте 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 хосте 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: **Proxy** =

ExcludedFiles = {имя файла}	Определяет имя файла, который не будет обновляться компонентом обновления **Dr.Web Updater.** Может иметь список значений, указанных через запятую. Допускается повторение параметра в секции. Если указывается более одного файла и используется список, разделенный запятой, то имена файлов следует указывать в кавычках: **ExcludedFiles** = "file1", "file2" Рекомендуется использовать множественное указание параметра в формате "по одному значению на строку", в этом случае кавычки можно опустить: **ExcludedFiles** = file1 **ExcludedFiles** = file2 Значение по умолчанию: **ExcludedFiles** = drweb32.lst
NetworkTimeout = {интервал времени}	Тайм-аут на сетевые операции компонента обновления при выполнении обновлений. 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: **NetworkTimeout** = 60s
BaseDrlPath = {путь к файлу}	Определяет путь к используемому подписанному файлу списка серверов обновлений, используемых компонентом обновления Значение по умолчанию: **BaseDrlPath** = <var_dir>/bases/update.drl Для **Linux**: **BaseDrlPath** = /var/opt/drweb.com/bases/update.drl Для **FreeBSD**: **BaseDrlPath** = /var/drweb.com/bases/update.drl Для **Solaris**: **BaseDrlPath** = /var/opt/drweb.com/bases/update.drl
BaseCustomDrlPath = {путь к файлу}	Определяет путь к используемому подписанному файлу дополнительного списка серверов обновлений, используемых компонентом обновления Значение по умолчанию: **BaseCustomDrlPath** = <var_dir>/drl/custom.drl Для **Linux**: **BaseCustomDrlPath** = /var/opt/drweb.com/drl/custom.drl Для **FreeBSD**: **BaseCustomDrlPath** = /var/drweb.com/drl/custom.drl Для **Solaris**:

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

RunAsUser = {UID | имя пользователя}	Параметр указывает компоненту обновления, от имени какого пользователя ему следует запускаться при выполнении обновлений. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр, оно указывается с префиксом `name:`, например: **RunAsUser** = name:123456 В случае если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.
	Значение по умолчанию: **RunAsUser** = drweb

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,** компонент **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 и не управляет заданиями на проверку объектов файловой системы.

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.

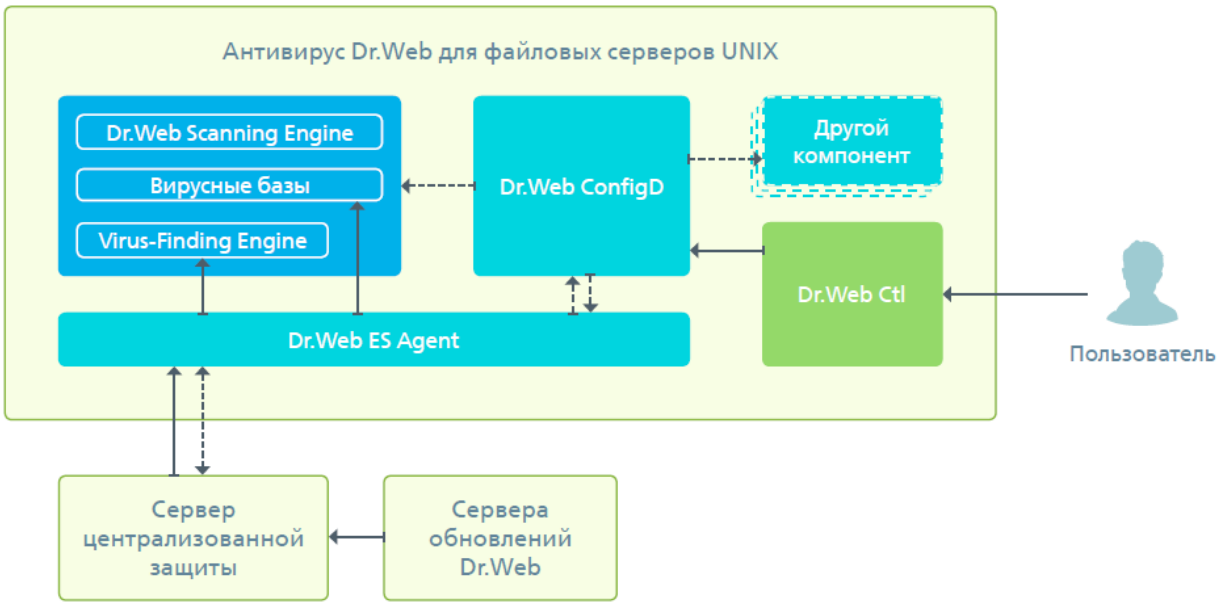

Рисунок 40. Схема работы компонента

Для подключения **Dr.Web ES Agent** к серверу централизованной защиты требуется иметь пароль и идентификатор хоста, а также файл публичного ключа шифрования, используемого сервером для подтверждения его подлинности. Вместо идентификатора хоста 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 хост файлового сервера как «новичок». В этом случае, после подтверждения заявки на подключение хоста администратором, сервер централизованной защиты автоматически сгенерирует для хоста файлового сервера новые идентификатор и пароль, которые отправит агенту для использования при последующих подключениях.

Не рекомендуется, но имеется возможность разрешить агенту **Dr.Web ES Agent** подключаться к серверу централизованной защиты без использования публичного ключа сервера, или используя неправильный публичный ключ. Подробнее см. в описании команды **esconnect** утилиты **Dr.Web Ctl**.

Аргументы командной строки

Для запуска агента централизованной защиты **Dr.Web ES Agent** из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-esagent [options]
```

Dr.Web ES Agent допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
`-h`	`--help`	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
`-v`	`--version`	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

Пример:

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

Данная команда выведет на экран краткую справку агента централизованной защиты **Dr.Web ES Agent.**

Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически, по мере необходимости, демоном управления конфигурацией **Dr.Web ConfigD.** Для подключения **Dr.Web для файловых серверов UNIX** к серверу централизованной защиты можно воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **drweb-ctl**) .

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 **Dr.Web ES Agent.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции `[Root]` Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала **Dr.Web ES Agent.** Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web ES Agent.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-esagent Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-esagent Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-esagent Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-esagent

DebugIpc = {логический}	Включать или нет в журнал на отладочном уровне (**LogLevel** = DEBUG) подробные сообщения IPC (взаимодействие **Dr.Web ES Agent** и демона управления конфигурацией **Dr.Web ConfigD**). Значение по умолчанию: **DebugIpc** = 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 модуль **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: **MobileMode** = 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: **Discovery** = On

Dr.Web HTTPD

Сервер веб-интерфейса управления **Dr.Web HTTPD** предоставляет веб-интерфейс, предназначенный для управления работой **Dr.Web для файловых серверов UNIX** без использования внешних веб-серверов (таких, например, как **httpd Apache)** и утилит удаленного администрирования наподобие **Webmin.**

Для обеспечения безопасности, при взаимодействии с клиентами используется защищенный протокол HTTPS (HTTP over SSL). Вследствие этого необходимо наличие в системе установленного `OpenSSL` (по умолчанию компонент использует версию `OpenSSL`, поставляемую в составе продукта **Dr.Web для файловых серверов UNIX**).

Принципы работы

Dr.Web HTTPD играет роль упрощенного веб-сервера. Не требует дополнительной установки полноценных веб-серверов (таких, как **Apache**), а также управляющего сервиса **Webmin.** Кроме того, он может работать с ними на одном хосте, не препятствуя функционированию уже настроенных веб-сервисов.

Сервер веб-интерфейса управления обслуживает запросы, поступающие по протоколу HTTPS на указанный в настройках сетевой интерфейс, что позволяет использовать его независимо от работы стандартного веб-сервера (если он используется на этом хосте). Схема работы компонента показана на рисунке ниже.

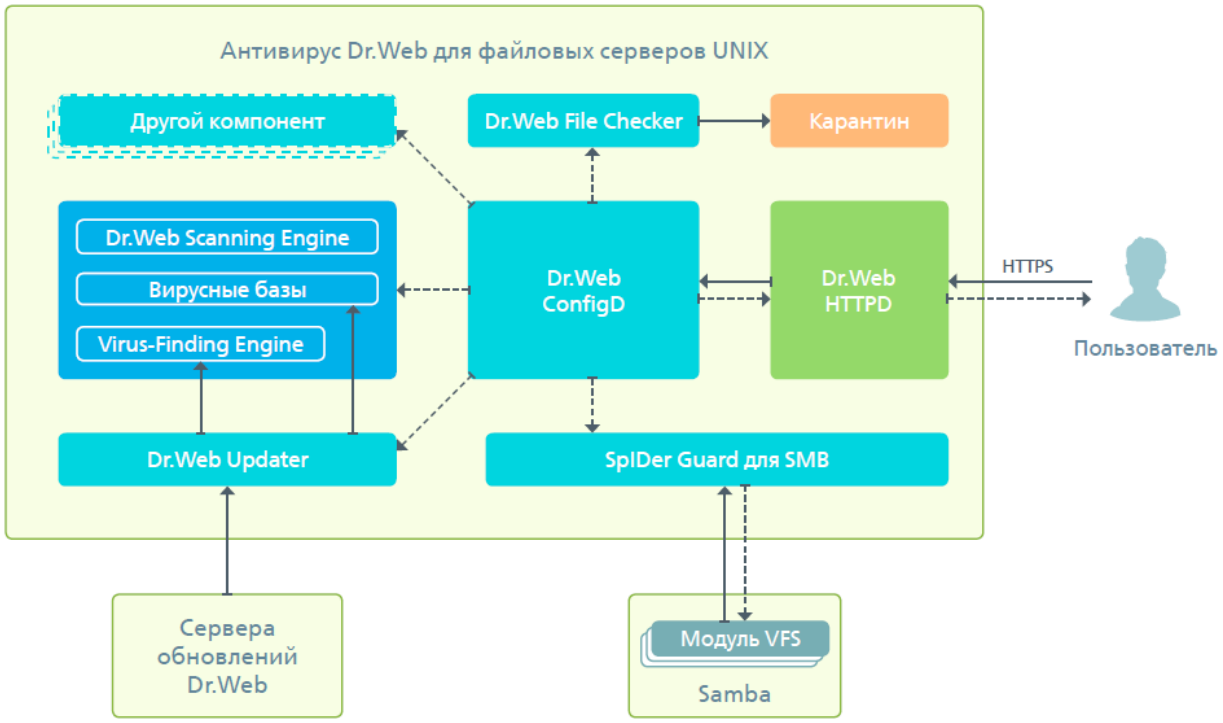

Рисунок 41. Схема работы компонента

Компонент **Dr.Web HTTPD** формирует управляющие команды к демону управления конфигурацией **Dr.Web для файловых серверов UNIX**, компоненту проверки файлов **Dr.Web File Checker** и монитору **SpIDer Guard для NSS**, на основании команд, полученных от пользователя через веб-интерфейс.

Управление компонентами продукта через веб-интерфейс, предоставляемый **Dr.Web HTTPD**, описано в соответствующем разделе.

Аргументы командной строки

Для запуска сервера веб-интерфейса управления **Dr.Web HTTPD** из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-httpd [options]
```

Dr.Web HTTPD допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
-v	--version	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

Пример:

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

Данная команда выведет на экран краткую справку сервера веб-интерфейса управления **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, то для управления работой компонентов **Dr.Web для файловых серверов UNIX** достаточно выполнить HTTPS-подключение к адресу, прослушиваемому компонентом, при помощи любого стандартного браузера.

Кроме того, для управления работой компонента можно воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **drweb-ctl**).

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 сервера веб-интерфейса управления **Dr.Web HTTPD.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root]. Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала сервера веб-интерфейса управления **Dr.Web HTTPD.** Значение по умолчанию: **Log** = Auto

ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web HTTPD.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-httpd Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-httpd Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-httpd Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-httpd
Start = {логический}	Определяет необходимость автозапуска компонента **Dr.Web HTTPD** при старте программного комплекса **Dr.Web для файловых серверов UNIX.** Значение по умолчанию: **Start** = Yes
ListenAddress = {адрес}	Определяет сокет (IP-адрес и порт), прослушиваемый **Dr.Web HTTPD** в ожидании подключений от клиентов. Значение по умолчанию: **ListenAddress** = 127.0.0.1:4443
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. Значение по умолчанию: **ServerSslCertificate** = <etc_dir>/certs/serv.crt Для **Linux**: **ServerSslCertificate** = /etc/opt/drweb.com/certs/serv.crt Для **FreeBSD**: **ServerSslCertificate** = /usr/local/etc/drweb.com/certs/serv.crt Для **Solaris**: **ServerSslCertificate** = /etc/opt/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. Значение по умолчанию: **ServerSslKey** = <etc_dir>/certs/serv.key Для **Linux**: **ServerSslKey** = /etc/opt/drweb.com/certs/serv.key Для **FreeBSD**: **ServerSslKey** = /usr/local/etc/drweb.com/certs/serv.key Для **Solaris**:

	ServerSslKey = /etc/opt/drweb.com/certs/serv.key
DhPath = {путь к файлу}	Определяет путь к файлу, содержащему параметры протокола шифрования Диффи-Хеллмана, используемые сервером веб-интерфейса управления для взаимодействия с клиентами по протоколу HTTPS. Данный файл генерируется автоматически при установке компонента. Значение по умолчанию: **DhPath** = <etc_dir>/certs/dh.pem Для **Linux**: **DhPath** = /etc/opt/drweb.com/certs/dh.pem Для **FreeBSD**: **DhPath** = /usr/local/etc/drweb.com/certs/dh.pem Для **Solaris**: **DhPath** = /etc/opt/drweb.com/certs/dh.pem
DocumentRoot = {путь к каталогу}	Определяет путь к каталогу, в котором хранится статическое содержимое сайта, используемое сервером веб-интерфейса управления (корневой каталог, аналогия каталога htdocs для **httpd**). Значение по умолчанию: **DocumentRoot** = <opt_dir>/share/drweb-httpd/www Для **Linux**: **DocumentRoot** = /opt/drweb.com/share/drweb-httpd/www Для **FreeBSD**: **DocumentRoot** = /usr/local/libexec/drweb.com/share/drweb-httpd/www Для **Solaris**: **DocumentRoot** = /opt/drweb.com/share/drweb-httpd/www
AppRoot = {путь к каталогу}	Определяет путь к каталогу, в котором хранятся файлы, используемые в работе сервером веб-интерфейса управления. Значение по умолчанию: **AppRoot** = <opt_dir>/share/drweb-httpd Для **Linux**: **AppRoot** = /opt/drweb.com/share/drweb-httpd Для **FreeBSD**: **AppRoot** = /usr/local/libexec/drweb.com/share/drweb-httpd Для **Solaris**: **AppRoot** = /opt/drweb.com/share/drweb-httpd
AccessLogPath = {путь к файлу}	Определяет путь к файлу, хранящему журнал всех запросов HTTP, поступающих от клиентов к серверу веб-интерфейса управления. Если параметр не задан, журнал HTTP-запросов сервером не ведется. Значение по умолчанию: **AccessLogPath** =

Управление работой продукта через веб-интерфейс

Веб-интерфейс управления **Dr.Web для файловых серверов UNIX** позволяет выполнять следующие действия:

1. Просматривать состояние, запускать и останавливать компоненты **Dr.Web для файловых серверов UNIX** (например, монитор **SpIDer Guard для SMB**);
2. Просматривать состояние обновлений и запускать обновление вручную при необходимости;
3. Просматривать перечень обнаруженных угроз и управлять содержимым карантина (через компонент **Dr.Web File Checker**);
4. Выполнять редактирование настроек компонентов **Dr.Web для файловых серверов UNIX**.

Системные требования веб-интерфейса

Корректная работа веб-интерфейса управления гарантируется в следующих браузерах:

- **Internet Explorer** – версия 8 и выше;
- **Mozilla Firefox** – версия 25 и выше;
- **Google Chrome** – версия 30 и выше.

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 верхней части страниц веб-интерфейса управления расположено главное меню, пункты которого позволяют выполнить следующее:

- Главная – открывает главную страницу, на которой отображается перечень компонентов **Dr.Web для файловых серверов UNIX** и их состояние.
- Угрозы – открывает страницу, отображающую все обнаруженные угрозы. В этом разделе вы можете осуществлять управление 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.
- **Справка** – открывает (в новой вкладке браузера) справку по установленным компонентам продукта.

- **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 мониторинг угроз, и сервисные, обеспечивающие корректную работу продукта в целом.

В таблице перечисляются компоненты, выполняющие мониторинг файловой системы (состав компонентов 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. В случае если в работе компонента произошла ошибка, щелчок мышью по надписи *Ошибка* выводит на экран окно с подробной информацией о произошедшей ошибке. Возможные состояния переключателя:

    – Компонент отключен и не используется;

    – Компонент включен и корректно функционирует;

    – Компонент включен, но не функционирует вследствие произошедшей ошибки.
3. **Средняя нагрузка.** Для каждого компонента указывается среднее число файлов, обработанных им за секунду 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 компонентов, осуществляющих мониторинг, перечисляются сервисные 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.

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 **Загрузить** – продлить или обновить лицензию (вам будет предложено загрузить действующий ключевой файл).

Управление угрозами

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

На этой странице показывается полный перечень угроз, обнаруженных различными компонентами **Dr.Web для файловых серверов UNIX** в процессе работы. В левой 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, изолированные 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):

 – Попытаться вылечить отмеченные файлы.

 – Переместить отмеченные файлы в карантин.

 – Восстановить отмеченные файлы из карантина в исходное место.

 – Удалить отмеченные файлы.

Еще – Применить некоторое дополнительное действие к отмеченным файлам (выбирается из выпадающего списка). Доступны следующие дополнительные действия:

- **Игнорировать** – Игнорировать угрозы, обнаруженные в отмеченных файлах, и удалить их из списка обнаруженных угроз.
- **Сохранить локально** – Сохранить отмеченные файлы на локальный компьютер.

Обратите внимание, что для работами с угрозами, обнаруженными на томах NSS, требуется, чтобы был 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**.

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 жирным шрифтом.

Если компонент имеет кроме основной секции настроек также и дополнительные, специфичные секции настроек (например, такие секции имеются у модуля 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 символ сворачивания/разворачивания дополнительных (подчиненных) секций настроек этого компонента. Если символ сворачивания имеет вид , то дополнительные секции скрыты и не видны. Если символ 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 символу сворачивания/разворачивания сбоку от имени интересующего компонента в меню.

- Дополнительные секции настроек компонента отмечены значком . 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 символу +, располагающемуся в меню справа от имени 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 символу ×, располагающемуся в меню справа от имени (тега) секции. 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**, **Расширенные** 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. Примеры изменения простых значений параметров изображены на рисунке ниже (обратите внимание, что состав и наименование компонентов, отображаемых в боковом меню, зависит от поставки продукта и может отличаться от приведенного примера). Во всех этих случаях измененное значение параметра сразу же фиксируется в конфигурации компонента.

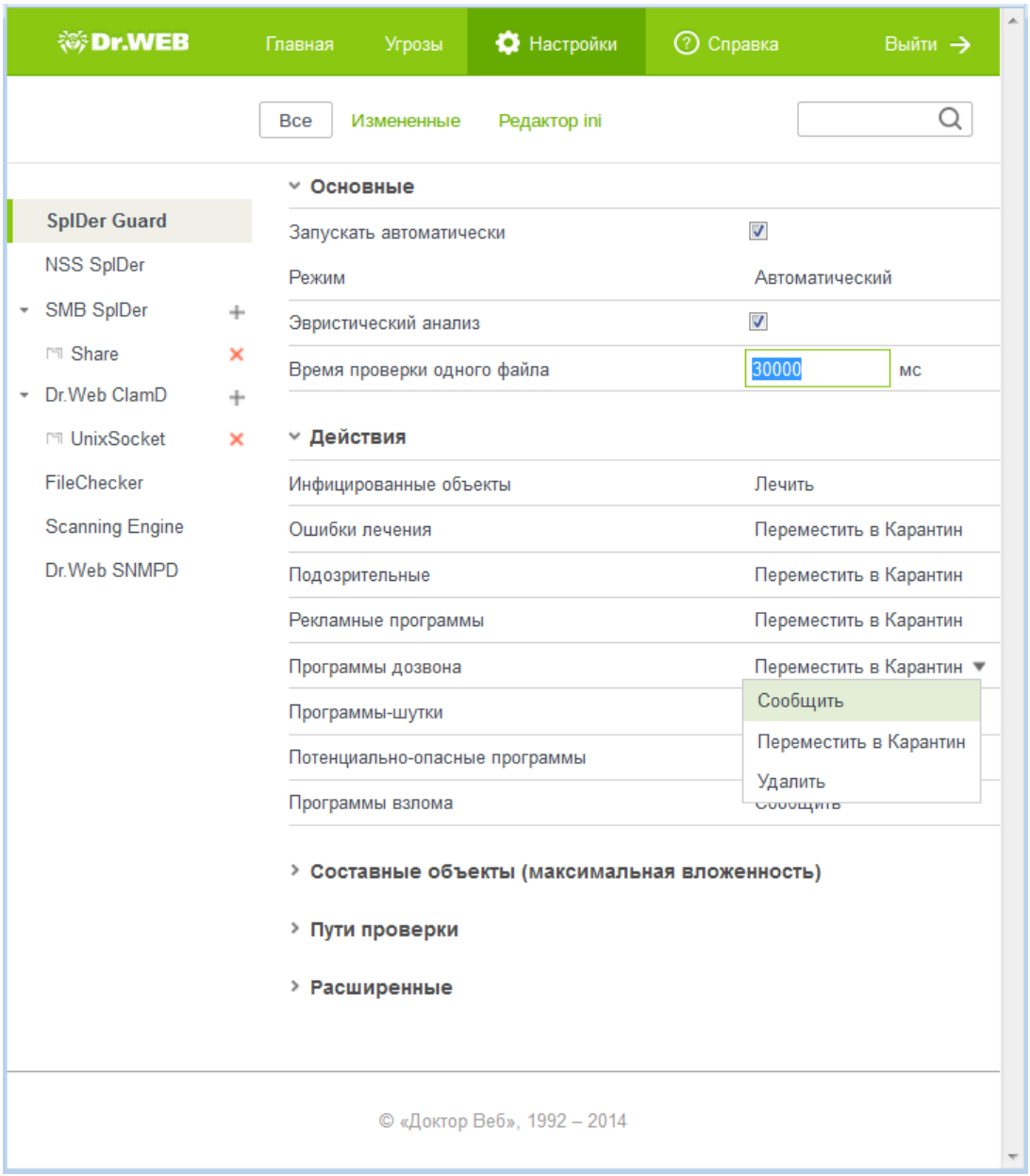

Рисунок 42. Представление настроек компонента в табличной форме

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.

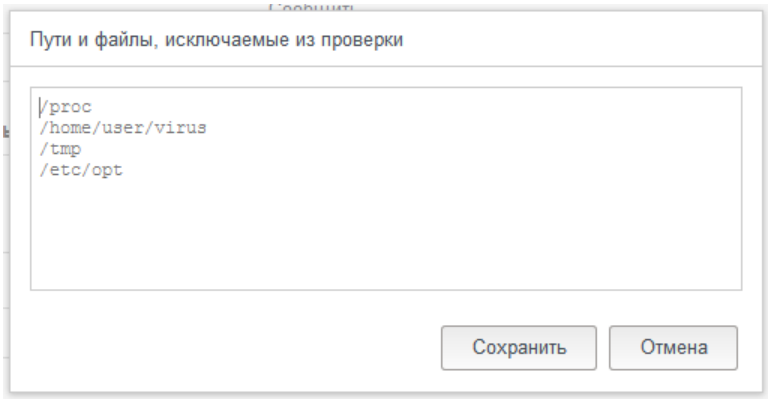

Рисунок 43. Редактирование списка значений

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**.

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.

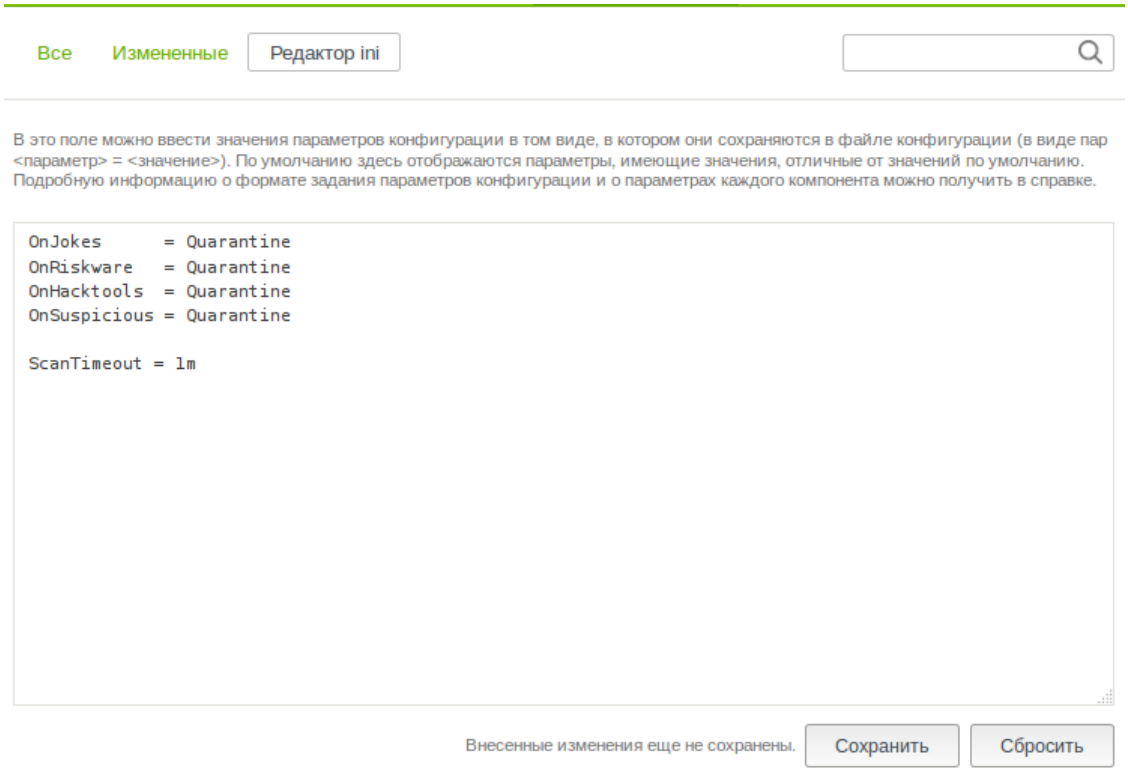

Рисунок 44. Редактор настроек для простого вида

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.

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 Приложении Г.

Дополнительно

- Параметры конфигурации компонента **SpIDer Guard**.
- Параметры конфигурации компонента **SpIDer Guard для NSS**.
- Параметры конфигурации компонента **SpIDer Guard для SMB**.
- 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**.

Dr.Web Ctl

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 обновления вирусных баз.
- 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.

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 -h <команда>`** или **`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 -d <команда>`**

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.

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) и опции --stdin или --stdin0. **Опции:** -a [--Autonomous] – запустить отдельную копию сканирующего ядра **Dr.Web Scanning Engine** и компонента проверки файлов **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). --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'). Обратите внимание, что при использовании обеих этих опций пути в списке не должны содержать шаблонов. Предпочтительное использование опций --stdin и --stdin0 – обработка в команде **scan** списка путей, сформированного внешней утилитой, например, **find** (см. примеры). --Report <BRIEF|DEBUG> – 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 упакованных 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 сообщений (pst, tbb и т.п.). Значение 0 указывает, что вложенные объекты будут пропущены.

Команда	Описание
	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*. Значение по умолчанию: On --OnKnownVirus <действие> – действие, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: REPORT, CURE, QUARANTINE, DELETE. Значение по умолчанию: REPORT --OnIncurable <действие> – действие, которое следует выполнить в случае если лечение (CURE) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: REPORT, QUARANTINE, DELETE. Значение по умолчанию: REPORT --OnSuspicious <действие> – действие, которое следует выполнить в случае если Эвристический анализ обнаружит подозрительный объект. Возможные действия: REPORT, QUARANTINE, DELETE. Значение по умолчанию: REPORT --OnAdware <действие> – действие, которое следует выполнить в случае если обнаружена рекламная программа. Возможные действия: REPORT, QUARANTINE, DELETE. 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
bootscan	**Назначение:**

Команда	Описание
`<устройство> | ALL`	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. Если вместо файла устройства указано `ALL`, будут проверены все загрузочные записи на всех доступных дисковых устройствах. Обязательный аргумент. **Опции:** `-a [--Autonomous]` – запустить отдельную копию сканирующего ядра **Dr.Web Scanning Engine** и компонента проверки файлов **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). `--Report <BRIEF|DEBUG>` – 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*. 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 не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него. **Аргументы:** Нет. **Опции:** `-a [--Autonomous]` – запустить отдельную копию сканирующего ядра **Dr.Web Scanning Engine** и компонента проверки файлов **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).

Команда	Описание
	`--Report <BRIEF|DEBUG>` – 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*. Значение по умолчанию: `On` `--PackerMaxLevel <число>` – установить максимальный уровень вложенности объектов при проверке упакованных объектов. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8` `--OnKnownVirus <действие>` – действие, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnIncurable <действие>` – действие, которое следует выполнить в случае если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnSuspicious <действие>` – действие, которое следует выполнить в случае если Эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnAdware <действие>` – действие, которое следует выполнить в случае если обнаружена рекламная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnDialers <действие>` – действие, которое следует выполнить в случае если обнаружена программа дозвона. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--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`

Команда	Описание
	`--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 распределённой проверки файлов **Dr.Web Network Checker**. Если настроенные соединения с другими хостами, на которых имеется **Антивирус Dr.Web**, 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 <BRIEF|DEBUG>` – 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*. Значение по умолчанию: `On` `--PackerMaxLevel <число>` – установить максимальный уровень вложенности объектов при проверке упакованных 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 сообщений (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`.

Команда	Описание
	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**). 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*. Значение по умолчанию: On --PackerMaxLevel <число> – установить максимальный уровень вложенности объектов при проверке упакованных 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 сообщений (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`
`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**). 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 <BRIEF|DEBUG>` – установить тип отчета о проверке. Возможные значения: • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. Значение по умолчанию: `BRIEF`

Команда	Описание
	`--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*. Значение по умолчанию: `On` `--PackerMaxLevel <число>` – установить максимальный уровень вложенности объектов при проверке упакованных 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 сообщений (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`
`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). Для проверки файлов и каталогов рекомендуется использовать команду **`scan`**. **Аргументы:** `<путь>` – путь к файлу или каталогу, который нужно проверить. **Опции:** `--ScanEngine <path>` – 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 <BRIEF|DEBUG>` – 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.

Команда	Описание
	Значение 0 указывает, что время проверки не ограничено. Значение по умолчанию: 0 --PackerMaxLevel <число> – установить максимальный уровень вложенности объектов при проверке упакованных 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 сообщений (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*. 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.
cloudscan <путь>	**Назначение:** Инициировать проверку указанного файла или каталога с обращением к облачному сервису **Dr.Web Cloud** за информацией о вредоносности данного файла. Не реализована в данной версии продукта. Для проверки файлов и каталогов используйте команду **scan**. **Аргументы:** <путь> – путь к файлу или каталогу, который нужно проверить. **Опции:** --Report <BRIEF|DEBUG> – установить тип отчета о проверке. Возможные значения: • BRIEF – краткий отчет. • DEBUG – подробный отчет. Значение по умолчанию: BRIEF

Команда	Описание
	`--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 упакованных 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 сообщений (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*. 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.

3.2. Команды управления обновлением и работой в режиме централизованной защиты

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

Команда	Описание
update	**Назначение:** Инициировать процесс обновления компонентом обновления вирусных баз и антивирусного ядра с серверов обновлений компании **«Доктор Веб»**, или прервать уже запущенный процесс обновления. Команда не имеет эффекта, если **Dr.Web для файловых серверов UNIX** работает под управлением сервера централизованной защиты. **Аргументы:** Нет.

Команда	Описание
	Опции: `--Stop` – прервать уже идущий процесс обновления.
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 Антивируса. **Аргументы**: • `<сервер>` – IP-адрес или имя хоста 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). `--WithoutKey` – разрешать подключаться к серверу без использования публичного ключа сервера. `--WrongKey` – разрешать подключаться к серверу, даже если указан некорректный публичный ключ сервера. Опции `--Key` и `--WithoutKey` являются взаимоисключающими. При этом в команде обязательно должна быть указана любая из них. Обратите внимание, что для выполнения этой команды требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя.
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** находится в одиночном режиме. **Аргументы**: Нет.

Команда	Описание
	Опции: Нет. Обратите внимание, что для выполнения этой команды требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя.

3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
cfset <секция>.<параметр> <значение>	**Назначение**: Изменить активное значение указанного параметра текущей конфигурации. Обратите внимание, что знак равенства не используется. **Аргументы**: • <секция> – имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент. • <параметр> – имя изменяемого параметра. Обязательный аргумент. • <значение> – значение, которое следует присвоить изменяемому параметру. Обязательный аргумент. Для задания значения параметров всегда используется формат <секция>.<параметр> <значение> Описание конфигурационного файла доступно в Приложении Г данного руководства, а также в документации **man** drweb.ini(5). **Опции:** -a [--Add] – не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). -e [--Erase] – не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). -r [--Reset] – сбросить параметр в значение по умолчанию. <значение> в этом случае в команде не указывается, а если указано – игнорируется. Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе – список значений) заменяется на указанное значение. Для опции -r предусмотрен также особый синтаксис вызова команды **cfset**: **cfset** <секция>.* -r В этом случае все параметры указанной секции сбрасываются в значения по умолчанию. 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>, достаточно использовать команду

Команда	Описание
	cfset ClamD.Endpoint.<point>.<параметр> <значение>, например: **cfset** ClamD.Endpoint.point1.ClamdSocket 127.0.0.1:1234 **cfset** SmbSpider.Share.<tag>.<параметр> <значение>, например: **cfset** SmbSpider.Share.BuhFiles.OnAdware Quarantine Обратите внимание, что для выполнения команды **cfset** требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя.
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. --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).

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. **Аргументы**: Нет. **Опции**: -f [--Follow] – выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (**^C** прерывает ожидание). --Cure <список угроз> – выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую).

Команда	Описание
	`--Quarantine <список угроз>` – выполнить перемещение в карантин перечисленных угроз (идентификаторы угроз перечисляются через запятую) `--Delete <список угроз>` – выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Ignore <список угроз>` – игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить данную команду ко всем обнаруженным угрозам, вместо `<список угроз>` следует указать `all`. Например, команда **`drweb-ctl`** `threats --Quarantine all` перемещает в карантин все обнаруженные объекты с угрозами.
`quarantine` `[<действие> <объект>]`	**Назначение:** Применить действие к указанному объекту, находящемуся в карантине. Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине, с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в карантин. **Аргументы:** Нет. **Опции:** `--Delete <объект>` – удалить указанный объект из карантина. Обратите внимание, что удаление из карантина – необратимая операция. `--Cure <объект>` – попытаться вылечить указанный объект в карантине. Обратите внимание, что, даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина следует воспользоваться командой восстановления `--Restore`. `--Restore <объект>` – восстановить указанный объект из карантина в исходное место. Обратите внимание, что для выполнения этой команды может потребоваться, чтобы **`drweb-ctl`** была запущена от имени суперпользователя. Восстановить файл из карантина можно, даже если он инфицирован. 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.
`nss_threats`	**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. **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (**`^C`** прерывает ожидание).

Команда	Описание
	`--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). `--Ignore <список угроз>` – игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить данную команду ко всем обнаруженным угрозам, вместо `<список угроз>` следует указать `all`. Например, команда **`drweb-ctl`** `nss_threats --Quarantine all` перемещает в карантин NSS все обнаруженные объекты с угрозами. Обратите внимание, что для выполнения этой команды требуется, чтобы был запущен **SpIDer Guard для NSS**.
`nss_quarantine`	**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. **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. 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. `--TargetDir <путь>` – восстановить объект, указанный в опции `--Restore`, не в исходное место, а в указанный каталог. Эта опция применяется только в дополнение к опции `--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`** `nss_quarantine --Restore all`

Команда	Описание
	восстанавливает из карантина NSS все имеющиеся в нем объекты. Обратите внимание, что для выполнения этой команды требуется, чтобы был запущен **SpIDer Guard для NSS**.

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 модулях **Dr.Web для файловых серверов UNIX.** **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об изменении состояния модулей и выводить их на экран сразу, как только они будут поступать (**`^C`** прерывает ожидание).
`baseinfo`	**Назначение:** Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз. **Аргументы:** Нет. **Опции:** Нет.
`license`	**Назначение:** Вывести на экран информацию об активной лицензии. **Аргументы:** Нет. **Опции:** Нет.
`stat`	**Назначение:** Вывести на экран статистику работы компонентов, обрабатывающих файлы (**`^C`** или **`q`** прерывает отображение статистики) или агента сетевого сканирования **Dr.Web Network Checker**. В статистике отображается: • имя компонента, инициировавшего проверку файлов; • PID компонента,

Команда	Описание
	• 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 сетевого сканирования 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 сетевого сканирования 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 сетевого сканирования.

Примеры использования

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

1) Запустить 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, используется разделение символом перевода строки):

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

3) Выполнить проверку списка путей, разделённых символом NUL:

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

4) Запустить проверку загрузочной записи на диске **sda**:

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

5) Вывести на экран все параметры из секции `[Root]` активной конфигурации:

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

6) Задать значение `'No'` для параметра **Start** из секции `[SMBSpider]` (это приведет к остановке работы монитора разделяемых каталогов **Samba SpIDer Guard для SMB**):

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

Примеры использования утилиты **find** для формирования выборки файлов, подлежащих проверке (команда **drweb-ctl** scan --stdin):

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

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

2) Проверить все файлы всех каталогов, начиная с корневого, кроме файлов, находящихся в каталогах /var/log/messages и /var/log/syslog:

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

3) Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователю root:

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

4) 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
```

5) 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
```

6) 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
```

7) Проверить файлы в корневом каталоге, не заходя во вложенные каталоги:

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

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

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

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

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

10) Проверить во всех каталогах, начиная с корневого, файлы, созданные не позже, чем 03.07.2013:

```
$ find / -type f -newermt 2013-07-03 | drweb-ctl scan --stdin
```

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].

Dr.Web Network Checker

Агент распределенной проверки файлов **Dr.Web Network Checker** предназначен для организации распределенной проверки файлов на наличие угроз. Он представляет собой агент, позволяющий организовать соединение между набором узлов сети с установленным на них продуктом **Dr.Web для файловых серверов UNIX** с целью приема и передачи файлов между узлами сети для их проверки. Компонент организует автоматическое распределение задач на проверку набора файлов (передавая для проверки содержащиеся в них данные по сети) на все доступные узлы сети, с которыми настроено соединение, обеспечивая балансировку их нагрузки, вызванной проверкой отправленных файлов.

В случае если соединения с удаленными узлами не настроены, компонент передает все файлы на проверку локальному сканирующему ядру **Dr.Web Scanning Engine**.

Для защищенного взаимодействия агентов распределенной проверки файлов должно быть настроено безопасное соединение через SSL. Обратите внимание, что для этого необходимо, чтобы в вашей системе был установлен `OpenSSL` (по умолчанию компонент использует версию `OpenSSL`, поставляемую в составе продукта **Dr.Web для файловых серверов UNIX**).

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 серверов UNIX** версии не ниже 10.1) для организации распределенной проверки файлов на наличие 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 файлов **Dr.Web Network Checker**).

На каждом узле сети, включенном в «сканирующий кластер», агент **Dr.Web Network Checker** организует автоматическое распределение задач на проверку набора файлов, передавая данные для проверки по сети на все доступные узлы, с которыми настроено соединение. При этом агент обеспечивает балансировку нагрузки на узлы, вызванной проверкой содержимого файлов, 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.

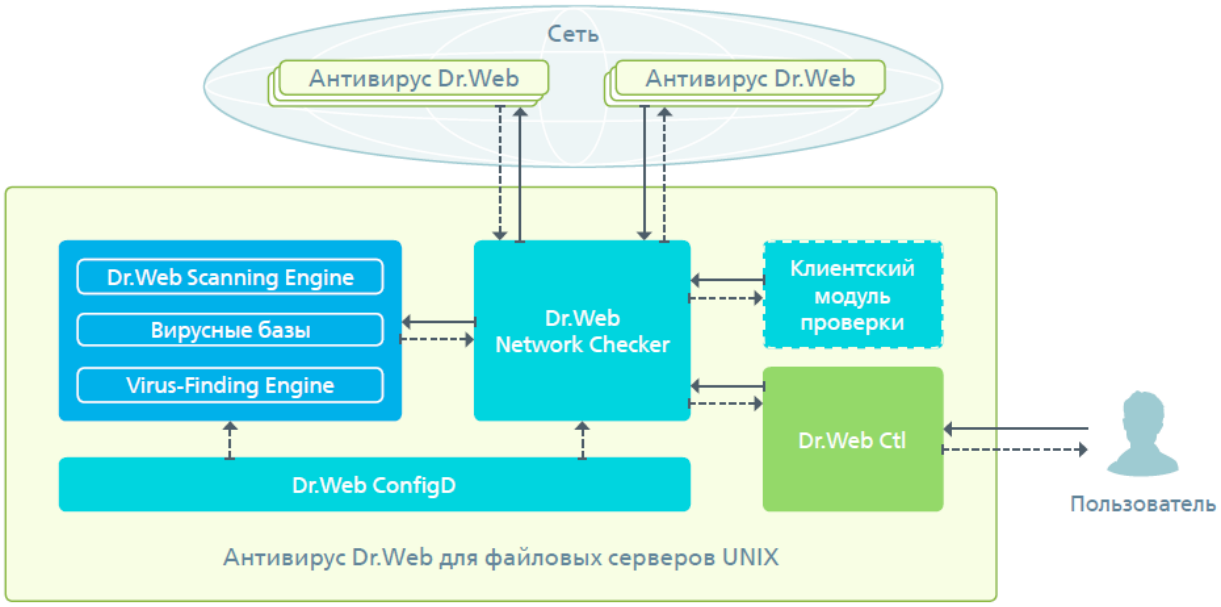

Рисунок 45. Схема работы компонента

При этом любой узел сети, включенный в «сканирующий кластер», может выступать как в роли клиента сканирования, передающего файлы на удаленную проверку, так и в роли сервера сканирования, принимающего с указанных узлов сети файлы для проверки. При необходимости агент распределенной проверки файлов **«Доктор Веб»** можно настроить таким образом, чтобы узел выступал только в качестве сервера сканирования или только в качестве клиента сканирования.

На локальной машине сетевое сканирование может быть инициировано как непосредственно по команде пользователя, заданной через утилиту управления из командной строки, 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.

Аргументы командной строки

Для запуска агента распределенной проверки файлов **Dr.Web Network Checker** из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-netcheck [options]
```

Dr.Web Network Checker допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
`-h`	`--help`	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
`-v`	`--version`	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

Пример:

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

Данная команда выведет на экран краткую справку агента распределенной проверки файлов **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). Для запуска сетевого сканирования (при наличии настроенного соединения с другими узлами сети) можно воспользоваться утилитой управления продуктом **Dr.Web для файловых серверов UNIX** из командной строки **Dr.Web Ctl** (запускается командой **`drweb-ctl`**). Если соединение с другими узлами сети не настроено, вместо сетевого сканирования будет запущено обычное сканирование силами локального сканирующего ядра.

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 агента распределенной проверки файлов **Dr.Web Network Checker.** Если параметр не указан, используется значение параметра **`DefaultLogLevel`** из секции `[Root]` Значение по умолчанию: **`LogLevel`** = `Notice`
`Log` = {тип журнала}	Метод ведения журнала агента распределенной проверки файлов **Dr.Web Network Checker.** Значение по умолчанию: **`Log`** = `Auto`
`ExePath` = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web Network Checker.** Значение по умолчанию: **`ExePath`** = `<opt_dir>/bin/drweb-netcheck` Для **Linux**: **`ExePath`** = `/opt/drweb.com/bin/drweb-netcheck` Для **FreeBSD**:

	ExePath = /usr/local/libexec/drweb.com/bin/drweb-netcheck Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-netcheck
LoadBalanceUseSsl = {логический}	Флаг, определяющий использование для соединения с другими узлами безопасного соединения SSL. Возможные значения: • Yes – Использовать SSL • No – Не использовать SSL Значение по умолчанию: **LoadBalanceUseSsl** = No
LoadBalanceSslCertificate = {путь к файлу}	Определяет путь к файлу серверного сертификата, используемого агентом распределенной проверки файлов для взаимодействия с другими узлами через безопасное соединение SSL. Значение по умолчанию: **LoadBalanceSslCertificate** =
LoadBalanceSslKey = {путь к файлу}	Определяет путь к файлу закрытого ключа, используемого агентом распределенной проверки файлов для взаимодействия с другими узлами через безопасное соединение SSL. Значение по умолчанию: **LoadBalanceSslKey** =
LoadBalanceSslCa = {путь к файлу}	Путь к файлу корневого сертификата центра сертификации, удостоверяющего подлинность сертификатов, используемых агентами внутри «сканирующего кластера» при обмене данными через SSL. Значение по умолчанию: **LoadBalanceSslCa** =
LoadBalanceServerSocket = {адрес}	Определяет сокет (IP-адрес и порт), прослушиваемый агентом распределенной проверки файлов на данном узле для получения файлов на проверку от удаленных узлов (если она может работать как сервер сетевого сканирования). Значение по умолчанию: **LoadBalanceServerSocket** =
LoadBalanceAllowFrom = {IP-адрес}	Определяет IP-адрес удаленного узла сети, от которого агент распределенной проверки файлов на данном узле может принимать файлы на проверку (как сервер сетевого сканирования) . Если параметр пуст, удаленные файлы на проверку не принимаются (узел не работает в режиме сервера). Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Значение по умолчанию: **LoadBalanceAllowFrom** =
LoadBalanceSourceAddress = {IP-адрес}	Определяет IP-адрес сетевого интерфейса, используемого

	агентом распределенной проверки файлов 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: **LoadBalanceSourceAddress** =
LoadBalanceTo = {адрес}	Определяет сокет (IP-адрес и порт) удаленного узла, на который агент распределенной проверки файлов на данном узле может отправлять файлы на удаленную проверку (как клиент сетевого сканирования). Если параметр пуст, локальные файлы не передаются на удаленную проверку (узел не работает в режиме клиента сетевого сканирования). Может иметь список значений. Значения в списке указываются через запятую, заключаются в кавычки. Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Значение по умолчанию: **LoadBalanceTo** =
LoadBalanceStatusInterval = {интервал времени}	Определяет длину интервала времени между рассылками данным узлом информации о своей загруженности для всех клиентов сканирования, перечисленных в параметре **LoadBalanceAllowFrom**. Значение по умолчанию: **LoadBalanceStatusInterval** = 1s
SpoolDir = {путь к каталогу}	Каталог в локальной файловой системе, используемый для хранения файлов, принятых агентом распределенной проверки файлов по сети от клиентов сканирования для проверки. Значение по умолчанию: **SpoolDir** = /tmp/netcheck
LocalScanPreference = {дробное число}	Определяет 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 распределенной проверки файлов для локальной проверки. Значение по умолчанию: **LocalScanPreference** = 1
IdleTimeLimit = {интервал времени}	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Минимальное значение – 10s. Если параметр **LoadBalanceAllowFrom** задан, то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя). Значение по умолчанию: **IdleTimeLimit** = 30s

RunAsUser = {UID | имя пользователя}	Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при обслуживании распределенного сканирования. Можно указать как числовой UID пользователя, так и его имя (логин). Если имя пользователя состоит из цифр, оно указывается с префиксом name:, например: **RunAsUser** = name:123456 В случае если имя пользователя не указано, работа компонента завершается ошибкой сразу после попытки запуска.
	Значение по умолчанию: **RunAsUser** = drweb

Dr.Web ClamD

Dr.Web ClamD – это компонент, эмулирующий для продукта **Dr.Web для файловых серверов UNIX** интерфейс 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 клиентских приложений проверку на наличие угроз как содержимого файлов, расположенных в локальной файловой системе, так и непосредственно потоки данных, передаваемые клиентским приложением через сокет. Кроме того, компонент может проверять содержимое файлов, для которых клиентское приложение передало через сокет отрытый дескриптор. В случае если приложение предоставило путь к файлу, компонент передает задание на проверку указанного файла компоненту проверки файлов **Dr.Web File Checker**, иначе он передает полученные от клиента через сокет данные агенту сетевого сканирования **Dr.Web Network Checker**, как показано на рисунке ниже.

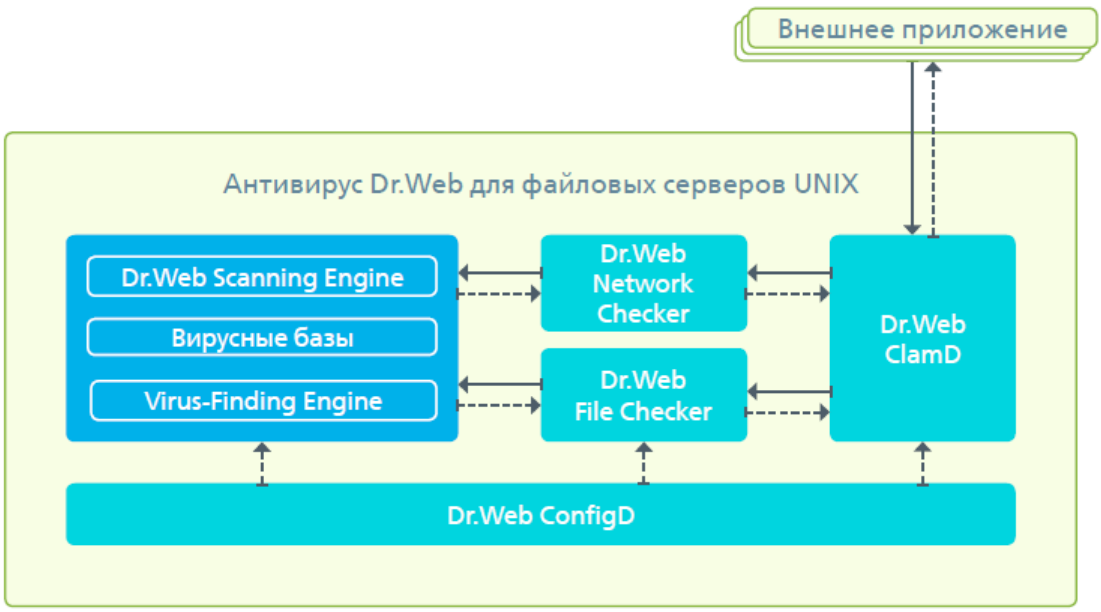

Рисунок 46. Схема работы компонента

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 поступление от внешних приложений запросов на проверку указанных файлов или потоков передаваемых данных. В настройках можно определить набор различных точек подключения клиентских приложений, указав для каждой свои собственные настройки проверки.

Обнаруженные угрозы не нейтрализуются средствами **Dr.Web для файловых серверов UNIX**, клиентскому приложению только возвращается результат проверки. Таким образом, клиентское 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 [options]
```

Dr.Web ClamD допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
-v	--version	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

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).

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 **Dr.Web ClamD.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root]. Значение по умолчанию: **LogLevel** = Notice
Log =	Метод ведения журнала

	Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web ClamD.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-clamd Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-clamd Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-clamd Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-clamd
Start = {логический}	Компонент должен быть запущен демоном управления конфигурацией **Dr.Web ClamD.** Значение по умолчанию: **Start** = No
Endpoint.<tag>.ClamdSocket = {IP-адрес | UNIX-сокет}	Определяет точку подключения с именем <tag> и сокет (адрес IPv4 или адрес сокета UNIX) для клиентов, желающих проверять файлы на наличие угроз. Для одной точки <tag> может быть задано несколько сокетов, для этого параметр нужно повторить несколько раз с одинаковым префиксом **Endpoint.<tag>.** Значение по умолчанию: **Endpoint.<tag>.ClamdSocket** =
[Endpoint.<tag>.]ReadTimeout = {интервал времени}	Определяет тайм-аут на ожидание данных от клиента. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]ReadTimeout** = 5s
[Endpoint.<tag>.]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.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]StreamMaxLength** = 25mb
[Endpoint.<tag>.]ScanTimeout = {интервал времени}	Определяет таймаут на проверку одного файла (или одной порции данных), поступившего от клиента. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]ScanTimeout** = 30s

[Endpoint.<tag>.] HeuristicAnalysis = {On | Off}	Определяет, следует ли использовать эвристический анализ при проверке. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]HeuristicAnalysis** = On
[Endpoint.<tag>.] PackerMaxLevel = {целое число}	Определяет максимальный уровень вложенности для проверки упакованных объектов. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]PackerMaxLevel** = 8
[Endpoint.<tag>.] ArchiveMaxLevel = {целое число}	Определяет максимальный уровень вложенности для проверки архивов. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **Endpoint.<tag>.]ArchiveMaxLevel** = 8
[Endpoint.<tag>.]MailMaxLevel = {целое число}	Определяет максимальный уровень вложенности для проверки почтовых файлов. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]MailMaxLevel** = 8
[Endpoint.<tag>.] ContainerMaxLevel = {целое число}	Определяет максимальный уровень вложенности для проверки объектов, находящихся в контейнерах. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]ContainerMaxLevel** = 8
[Endpoint.<tag>.] MaxCompressionRatio = {целое число}	Определяет максимальное значение коэффициента сжатия для запакованных объектов. Если указан префикс **Endpoint.<tag>**, то параметр определен для точки <tag>, иначе он определен для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: **[Endpoint.<tag>.]MaxCompressionRatio** = 500

Особенность настроек компонента

Параметры, отмеченные необязательным префиксом **[Endpoint.<tag>.]**, могут быть сгруппированы. Каждая такая группа определяет точку подключения (endpoint) с задаваемым уникальным идентификатором **<tag>**, используемую клиентами для подключения к модулю. 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.<tag>**, 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.<tag>**).

Параметр **ClamdSocket** должен обязательно задаваться с префиксом **Endpoint.<tag>**, 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 только через UNIX-сокет, а серверы из группы `servers2` – как через UNIX-сокет, так и 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 = /tmp/srv2.socket
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.servers1.ClamdSocket /tmp/srv1.socket
# drweb-ctl cfset ClamD.Endpoint.servers2.ClamdSocket /tmp/srv2.socket
# drweb-ctl cfset -a 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**.

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.

Продукт	Интеграция
	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).

1. Пример подключения **ProFTPd** к **Dr.Web ClamD**:

   1) Настройка **Dr.Web ClamD**:

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

   2) Настройка **ProFTPd**:

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

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**);
- Перечень обнаруженных угроз.

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 **Dr.Web** разделе MIB (Management Information Base). В разделе MIB, определенном **Dr.Web**, описывается следующая информация:

1. Формат оповещений SNMP trap об обнаружении угроз. Оповещение включает в себя:
   - Имя файла (включая путь), в котором обнаружена угроза
   - Имя инфицированного объекта
   - Тип угрозы
   - Имя угрозы
   - Имя компонента программного комплекса, по чьему запросу была обнаружена угроза.
2. Формат оповещений SNMP trap о неудачной попытке нейтрализации угрозы. Оповещение включает в себя те же поля, что и SNMP trap об обнаружении угрозы, добавляя дополнительное поле, включающее описание произошедшей ошибки.
3. Статистика работы программного комплекса и состояние его компонентов:
   a) Счетчики обнаруженных угроз
      - Известных вирусов
      - Подозрительных объектов
      - Рекламных программ
      - Программ-шуток
      - Программ дозвона
      - Потенциально опасных программ
      - Программ взлома
      - Таблица угроз (имя, сколько раз найдена)

   b) Счетчики ошибок программного комплекса
4. Данные о состоянии компонентов:
   - PID
   - Состояние
   - Время последнего завершения
   - Код последнего завершения.

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.

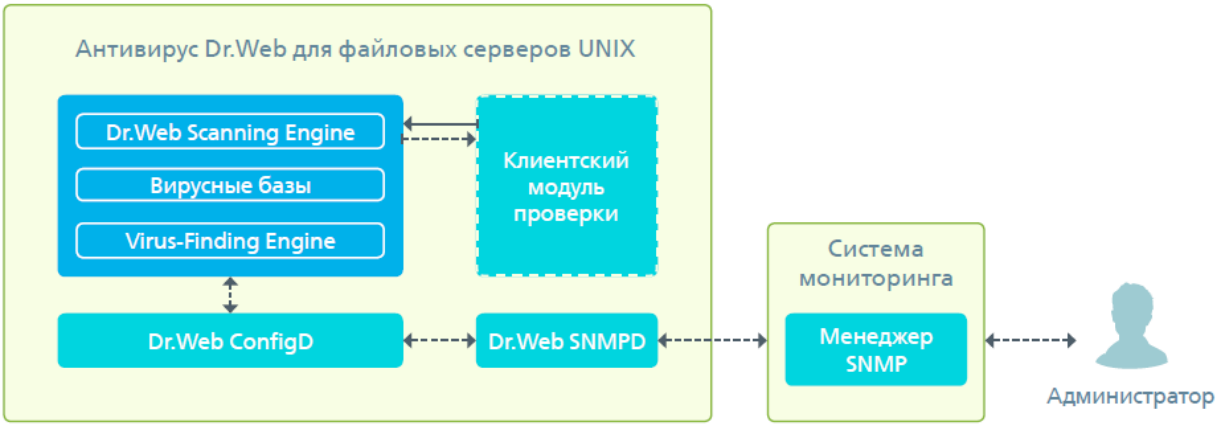

Рисунок 47. Схема работы компонента

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.

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 <ver> -c <community> <host>:<port> <MIB branch>
```

Где:

- `<ver>` – используемая версия SNMP (2c, 3);
- `<community>` – «community string», используемая **Dr.Web SNMPD;**
- `<host>:<port>` – адрес, прослушиваемый **Dr.Web SNMPD;**
- `<MIB branch>` – OID ветки MIB, содержащей описания переменных и trap, используемых **Dr.Web** (`.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 стандартный системный **snmpd**, то для **Dr.Web SNMPD** в параметре **ListenAddress** следует указать другой порт (`50000` в данном примере).

Аргументы командной строки

Для запуска **SNMP-агента Dr.Web** из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-snmpd [options]
```

Dr.Web SNMPD допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран консоли краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
-v	--version	
Описание: Вывод на экран консоли информации о версии модуля и завершение работы		

Пример:

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

Данная команда выведет на экран краткую справку **SNMP-агента Dr.Web.**

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).

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 SNMP-агента **Dr.Web.** Если параметр не указан, используется значение параметра **DefaultLogLevel** из секции [Root] Значение по умолчанию: **LogLevel** = Notice
Log = {тип журнала}	Метод ведения журнала SNMP-агента **Dr.Web.** Значение по умолчанию: **Log** = Auto
ExePath = {путь к файлу}	Путь к исполняемому файлу компонента **Dr.Web SNMPD.** Значение по умолчанию: **ExePath** = <opt_dir>/bin/drweb-snmpd Для **Linux**: **ExePath** = /opt/drweb.com/bin/drweb-snmpd Для **FreeBSD**: **ExePath** = /usr/local/libexec/drweb.com/bin/drweb-snmpd

	Для **Solaris**: **ExePath** = /opt/drweb.com/bin/drweb-snmpd
Start = {логический}	Компонент должен быть запущен демоном управления конфигурацией **Dr.Web ConfigD.** Значение по умолчанию: **Start** = Yes
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: **ListenAddress** = 127.0.0.1:161
SnmpVersion = {V2c | V3}	Используемая версия протокола SNMP (*SNMPv2c* или *SNMPv3*). Значение по умолчанию: **SnmpVersion** = V2c
V3EngineId = {строка}	Строка-идентификатор Engine ID для SNMPv3 (согласно RFC3411) Значение по умолчанию: **V3EngineId** = 800073FA044452574542
TrapReceiver = {список адресов}	Список адресов (IP-адрес и порт), на которые **Dr.Web SNMPD** будет отправлять SNMP trap при обнаружении угроз компонентами **Dr.Web для файловых серверов UNIX**. Адреса указываются через запятую. Значение по умолчанию: **TrapReceiver** =
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 **SnmpVersion** = V2c Значение по умолчанию: **V2cCommunity** = public
V3UserName = {строка}	Имя пользователя для аутентификации менеджеров SNMP (протокол SNMPv3) для доступа к переменным MIB **Dr.Web.** Параметр используется в случае **SnmpVersion** = V3 Значение по умолчанию: **V3UserName** = 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). Параметр используется в случае **SnmpVersion** = V3 При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа \. **Пример:** 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\(123456\) Значение по умолчанию: **V3Auth** = 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). Параметр используется в случае **SnmpVersion** = V3 При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа \. **Пример:** 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\(supersecret\) Значение по умолчанию: **V3Privacy** = 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 доступных для контроля данных 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 модулем поставляются необходимые шаблоны настроек для популярных систем мониторинга:

- Cacti
- Munin
- Nagios
- Zabbix

Шаблоны настроек для систем мониторинга находятся в каталоге `<opt_dir>/share/drweb-snmpd/connectors`.

Интеграция с системой мониторинга Cacti

Система мониторинга **Cacti** для отображения статистики о работе приложений на хостах или сетевом оборудовании использует описания объектов и их счетчиков, импортируемые из шаблонов. Поэтому сначала подготавливаются шаблоны для всех счетчиков, данные которых необходимо контролировать, а затем шаблоны счетчиков привязываются, как объекты, к шаблонам графиков. После этого шаблоны графиков привязываются к шаблонам хостов. Таким образом, шаблон хоста (устройства) получается корневым, он описывает хост, добавляемый в **Cacti** для наблюдения, после этого для него становятся доступными списки счетчиков, с которых будет сниматься статистика и набор преднастроенных графиков.

Для подключения **Dr.Web SNMPD** к системе мониторинга **Cacti** в каталоге `<opt_dir>/share/drweb-snmpd/connectors/cacti` поставляется готовый XML-файл `cacti_host_template_drweb.xml`, содержащий шаблон описания наблюдаемого хоста с установленным антивирусным продуктом **Dr.Web**.

Этот шаблонный файл позволяет выполнить подключение хоста к системе мониторинга, и снимать с него статистику обнаружения на хосте угроз различных типов и статистику проверки файлов. Имеется возможность импорта этого готового шаблона непосредственно в **Cacti**, кроме того, его можно модифицировать и создавать на его основе новые шаблоны.

Подключение хоста к Cacti

В данной инструкции предполагается, что система мониторинга **Cacti** уже корректно развернута на сервере мониторинга, а на наблюдаемом хосте корректно функционирует **Dr.Web SNMPD** (возможно, в режиме прокси совместно с **snmpd**).

1. В веб-интерфейсе **Cacti** выполнить импорт шаблона хоста `cacti_host_template_drweb.xml` (для этого нужно выбрать пункт меню **Console** –> **Import Templates**, указать путь к файлу шаблона, нажать **Import**). Если импорт прошел успешно, то в результатах импорта должен отображаться список импортированных объектов (шаблон хоста **DrWeb Host**).
2. Добавить в список **Devices** веб-интерфейса **Cacti** хост, подлежащий наблюдению (пункт меню **Console** –> **Devices** –> **Add**). В качестве шаблона хоста необходимо выбрать шаблон **DrWeb Host**, импортированный на предыдущем шаге. При добавлении хоста следует присвоить ему некоторый идентификатор (например – **DrWeb-Device**), указать его сетевой адрес (FQDN или IP-адрес) и задать корректные параметры SNMP (версия протокола, порт, read community и т.д., в зависимости от версии протокола). Нажать **Save**. Добавленный хост должен появиться в списке **Devices** веб-интерфейса **Cacti**.

3. Для добавленного устройства создать графики, отражающие работу **Dr.Web** на хосте. Для этого выбрать пункт меню **Console** –> **New Graphs**, выбрать наблюдаемый хост из списка устройств (в примере – **DrWeb-Device**), указать тип графиков – **Graph Template Based**. Далее отметить флажками доступные счетчики из импортированного шаблона, нажать **Create**.
4. Убедиться, что создались источники данных для выбранных на предыдущем шаге графиков. Для этого выбрать пункт меню **Console** –> **Data Sources**. На странице должны присутствовать источники данных из указанного списка:

   ```
   DrWeb-Device - adware counter *
   DrWeb-Device - dialers counter
   DrWeb-Device - hacktools counter
   DrWeb-Device - jokes counter
   DrWeb-Device - known viruses counter
   DrWeb-Device - riskware counter
   DrWeb-Device - suspicios counter
   DrWeb-Device - filecheck scanned bytes
   ```

   *) DrWeb-Device в данном случае – имя устройства, указанного вами на шаге 2.

   Рекомендуется для каждого источника данных убедиться, что для него создан соответствующий RRA-архив **RRD Tool**. Для этого необходимо щелкнуть по источнику и нажать **Turn On Data Source Debug Mode**. Это приведет к показу команды формирования источника данных и показу результата ее выполнения.
5. Выбрав пункт меню **Console** –> **Graph Management**, активировать графики. Имеется возможность просмотреть уже построенные графики. Для этого необходимо щелкнуть по названию интересующего графика. Если график не отображается, то нажав **Turn On Graph Debug Mode**, можно увидеть команду создания графика и ее результат. В списке отметить графики:

   ```
   DrWeb filecheck scan statistic
   DrWeb found malware
   ```

   В поле **Choose an action** выбрать значение **Place on a Tree (Default Tree)**, нажать **Go**.
6. Для просмотра графиков щелкнуть **graphs**. Обратите внимание, что результаты должны появиться примерно через 10 минут после добавления источников данных. При этом графики и источники данных могут не создаться до первого опроса SNMP (примерно 5 минут от добавления устройства).

В случае необходимости можно расширить набор имеющихся источников данных, и графиков, соответственно. Для этого нужно добавить новый источник данных, сформированный на основе системного шаблона *SNMP - Generic OID Template*. В настройках добавленного шаблона необходимо указать OID требуемого счетчика. Далее полученный *Data Template* следует добавить как объект к уже существующим шаблонам графиков.

Система мониторинга **Cacti** в базовой поставке не поддерживает сбор и отображение SNMP trap, а также отправку нотификаций по событиям. Для поддержки работы с SNMP trap и отправку нотификаций следует установить соответствующие подключаемые модули.

Настройка подключаемого модуля сбора SNMP trap на работу с уведомлениями от **Dr.Web SNMPD** аналогична настройке сбора SNMP trap для любого другого источника.

С официальной документацией по настройке системы мониторинга **Cacti** вы можете ознакомиться по ссылке http://docs.cacti.net/manual:088.

Интеграция с системой мониторинга Munin

Система мониторинга **Munin** состоит из централизованного сервера (мастера) **munin**, собирающего статистику от клиентов **munin-node**, располагающихся локально на хостах, подлежащих наблюдению. Каждый клиент мониторинга по запросу от сервера собирает данные о работе наблюдаемого хоста, запуская плагины, 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` поставляется готовый плагин сбора данных **drweb**, используемый **munin-node**. Этот плагин собирает данные для построения двух графиков:

- Количество обнаруженных угроз;
- Статистика проверки файлов.

Плагин поддерживает использование протокола SNMP версий 1, 2c и 3. На основе данного шаблонного плагина можно создать любые плагины, опрашивающие состояние программного комплекса **Dr.Web для файловых серверов UNIX** через **Dr.Web SNMPD**. Фактически этот плагин представляет собой набор плагинов, поскольку с точки зрения **Munin**, один плагин выполняет возвращение данных только для одного графика.

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

Файл	Описание
`plugins/drweb`	Плагин **munin-node** для опроса **Dr.Web SNMPD** через SNMP
`plugin-conf.d/drweb.cfg`	Шаблон настроек конфигурации **munin-node** для подключения к **Dr.Web SNMPD**

Подключение хоста к Munin

В данной инструкции предполагается, что система мониторинга **Munin** уже корректно развернута на сервере мониторинга, а на наблюдаемом установлены и корректно функционируют **Dr.Web SNMPD** (возможно, в режиме прокси совместно с **snmpd**), **munin-node** и **snmpget** (пакет **net-snmp**).

1) Настройка на наблюдаемом хосте

- Скопируйте файл **drweb** в каталог библиотек плагинов **munin-node** `<munin_lib_plugins>`;
- Создайте две символические ссылки в каталоге `<munin_plugins>` плагинов **munin-node**:

```
<munin_plugins>/drweb_malware -> <munin_lib_plugins>/drweb
<munin_plugins>/drweb_scanstat -> <munin_lib_plugins>/drweb
```

- Скопируйте файл `drweb.cfg` в каталог файлов конфигурации **munin-node** `/etc/munin/munin-node`, и отредактируйте в нем параметры для подключения плагинов из **drweb** к **Dr.Web SNMPD**:

```
[drweb_*]
user root
group root
env.SNMP_WALK_COMMAND snmpwalk -c public -v 2c localhost:161
```

- Отредактируйте значения перечисленных параметров, присвоив им актуальные значения (должны соответствовать настройке **Dr.Web SNMPD**). В примере указаны значения,

использующиеся по умолчанию.

- В файле конфигурации `munin-node.conf` укажите регулярное выражение, которому должны соответствовать IP-адреса машин, с которых разрешено подключаться к **munin-node** для получения значений контролируемых параметров, например:

```
allow ^10\.20\.30\.40$
```

  В данном случае регулярное выражение разрешает получение параметров хоста только машине с IP-адресом 10.20.30.40.

- Перезапустите **munin-node** (например, командой **`service`** `munin-node restart`).

Пути `<munin_lib_plugins>` и `<munin_plugins>` зависят от ОС. В ОС **Debian/Ubuntu** это пути `/usr/share/munin/plugins` и `/etc/munin/plugins` соответственно.

2) Настройка на сервере (мастере) **Munin**

В конфигурационный файл мастера **Munin** `munin.conf`, который по умолчанию хранится в `/etc` (в системах **Debian/Ubuntu** – `/etc/munin/munin.conf`), следует добавить запись с адресом и идентификатором наблюдаемого хоста:

```
[<ID>;<hostname>.<domain>]
address <host IP address>
use_node_name yes
```

где `<ID>` – отображаемый идентификатор хоста, `<hostname>` – имя хоста, `<domain>` – имя домена, `<host IP address>` – IP-адрес хоста.

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 хоста с установленным антивирусным продуктом **Dr.Web**
`snmptt.drweb.zabbix.conf`	Настройки приемника SMNP trap **`snmptt`**

Шаблон описания наблюдаемого хоста содержит:

- Набор описаний счетчиков (Items, в терминологии **Zabbix**). По умолчанию шаблон настроен на использование SNMP v2.
- Набор настроенных графиков: количество проверенных файлов и распределение обнаруженных угроз по типам.

Подключение хоста 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 хоста оповещения SNMP trap (в частности, об обнаружении угроз **Dr.Web для файловых серверов UNIX**), 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 хоста из каталога `<opt_dir>/share/drweb-snmpd/connectors/zabbix/zbx_drweb.xml`.
2. Добавьте наблюдаемый хост в список хостов (используйте ссылку **Hosts** –> **Create host**). Укажите параметры хоста и корректные настройки SNMP-интерфейса (должны соответствовать настройкам **`drweb-se`** и **`snmpd`** на хосте):

- Вкладка **Host**:

  Host name: `drweb-host`

  Visible name: `DRWEB_HOST`

  Groups: выбрать `Linux servers`

  Agent interfaces: укажите IP-адрес и порт **Dr.Web SNMPD** (`127.0.0.1` и `10050` по умолчанию).

  Snmp interfaces: Нажмите **add** и укажите IP-адрес и порт, который прослушивается **snmptrapd** на хосте с **Zabbix** (см. ниже, `127.0.0.1` и `161` по умолчанию).

- 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 хоста.

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 хосту, 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 item `drweb-traps` служит для сбора 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 SNMP trap от **Dr.Web SNMPD** см. ниже.
5. В случае необходимости, имеется возможность настроить для добавленного наблюдаемого хоста триггер, изменяющий свое состояние при получении SNMP trap от **Dr.Web SNMPD**. Изменение состояния этого триггера можно использовать как источник событий для формировать соответствующих нотификаций. Триггер для наблюдаемого хоста добавляется стандартным способом, ниже показан пример выражения, указываемого в поле **trigger expression** для описанного триггера:

   ```
   ({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)
   ```

   Данный триггер срабатывает (устанавливается в значение 1), если журнал оповещений SNMP trap от **Dr.Web SNMPD** был обновлен в течение минуты. Если же журнал в течение минуты не обновлялся, то триггер выключается (меняет состояние на 0).

Настройка приема SNMP trap для Zabbix

1. На наблюдаемом хосте в настройках **Dr.Web SNMPD** (`SNMPD.TrapReceiver`) указывается адрес, который прослушивается **snmptrapd** на хосте 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 SNMP trap (в данном случае – **snmptthandler**, компонент **snmptt**):

```
snmpTrapdAddr 10.20.30.40:162
traphandle default /usr/sbin/snmptthandler
```

3. Компонент **snmptthandler** сохраняет принимаемые оповещения SNMP trap в файл на диске в соответствии с указанным форматом, который должен соответствовать регулярному выражению, заданному в шаблоне хоста для **Zabbix** (item drweb-traps). Формат сохраняемого сообщения об SNMP trap поставляется в файле <opt_dir>/share/drweb-snmpd/connectors/zabbix/snmptt.drweb.zabbix.conf. Этот файл 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 оповещениях 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	Скрипт сбора данных от хоста с продуктом **Dr.Web**
plugins/eventhandlers/submit_check_result	Скрипт обработки SMNP trap
snmp/snmptt.drweb.nagios.conf	Настройки приемника SMNP trap **snmptt**

Подключение хоста 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 хоста оповещения SNMP trap (в частности, об обнаружении угроз **Dr.Web для файловых серверов UNIX**), 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 скриптом <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** хосты с продуктом **Dr.Web**, подлежащие наблюдению (на них должен быть запущен **Dr.Web SNMPD**), по умолчанию в данную группу включен только хост **localhost**.
3. Отредактируйте (при необходимости) команду **check_drweb**, в которой указывается обращение к **Dr.Web SNMPD** на хостах **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 заменяется **Nagios** на правильный адрес хоста при вызове команды автоматически). 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 исправте путь к скрипту **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=$LASTSERVICECHECK$||$HOSTNAME$||$SERVIC
EDESC$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
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 SNMP trap для Nagios

1. На наблюдаемом хосте в настройках **Dr.Web SNMPD** (SNMPD.TrapReceiver) указывается адрес, который прослушивается **snmptrapd** на хосте с **Nagios**, например:

```
SNMPD.TrapReceiver = 10.20.30.40:162
```

2. Проверить наличие скрипта <NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result, который будет вызываться при получении SNMP trap. Если этого скрипта нет, то следует скопировать в это место файл submit_check_result из <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. Скопировать файл snmptt.drweb.nagios.conf в каталог /etc/snmp/snmp/. В этом файле необходимо изменить путь к скрипту **submit_check_result**, наример, 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. Добавить 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 тебуемые 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. В случае отсутствия ошибок затем **Nagios** можно перезапустить стандартно (например, командой **service** nagios restart).

Подробнее с официальной документацией по **Nagios** вы можете ознакомиться по ссылке http://www.nagios.org/documentation/.

Приложения

Приложение А. Виды компьютерных угроз

Под термином *«угроза»* в данной классификации следует понимать любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они также могут нанести вред пользователю.

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Большая часть вирусов создается для повреждения или уничтожения данных.

В компании **«Доктор Веб»** вирусы делят по типу файлов, которые они инфицируют:

- **файловые вирусы** инфицируют файлы операционной системы (обычно исполняемые файлы и динамические библиотеки) и активизируются при обращении к инфицированному файлу;
- **макро-вирусы** инфицируют документы, которые используют программы из пакета **Microsoft® Office** (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). Макросы – это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в **Microsoft® Word** макросы могут запускаться при открытии, закрытии или сохранении документа);
- **скрипт-вирусы** пишутся на языках сценариев (скриптов) и в большинстве случаев инфицируют другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях;
- **загрузочные вирусы** инфицируют загрузочные сектора дисков и разделов, а также главные загрузочные сектора жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- **шифрованные вирусы** шифруют свой код при каждом новом инфицировании, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры;
- **полиморфные вирусы** используют помимо шифрования кода специальную процедуру

расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур;

- **стелс-вирусы** (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т.д.) и по инфицируемым ими операционным системам.

Компьютерные черви

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

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

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

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

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

Троянские программы

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

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

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

выделяют в отдельные классы:

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

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

Программы взлома

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

Рекламные программы

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

Программы-шутки

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

Программы дозвона

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

службам.

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-сервера 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 **Вирусной лаборатории компании «Доктор Веб».**

Приложение Б. Устранение компьютерных угроз

Все антивирусные продукты, разработанные компанией **Dr.Web**, применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Методы обнаружения угроз

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. *Сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах **Dr.Web** составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing™

Это уникальная технология **Dr.Web**, которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы 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 упакованных 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, упакованных 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 Dr.Web** обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту **Dr.Web**, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

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;
- **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.

Приложение В. Техническая поддержка

Страница службы технической поддержки компании **«Доктор Веб»** находится по адресу http://support.drweb.com/.

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу http://download.drweb.com/;
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/;
- посетить **Форумы Dr.Web** по адресу http://forum.drweb.com/.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела http://support.drweb.com/.

Найти ближайшее представительство компании **«Доктор Веб»** и всю информацию, необходимую пользователю, вы можете по адресу http://company.drweb.com/contacts/moscow.

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 **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. во Введении.

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.
2. Выполнить в командной строке команду:

   ```
   drweb-ctl cfset <section>.<parameter> <new_value>
   ```

   

   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 Утилита управления из командной строки.

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 модулями **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.
- 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_1**w**N_2**d**N_3**h**N_4**m**N_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 мин, 2 сек, 500 мсек:

1. В файле конфигурации:

```
UpdateInterval = 30m2.5s
```

2. С использованием команды **drweb-ctl** `cfset`:

```
drweb-ctl cfset Root.UpdateInterval 1802.5s
```

3. Задание через параметр командной строки (например, для модуля **drweb-se**):

```
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** (используется только для модуля **drweb-configd**).

    Дополнительная опция `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени.
  - `Auto` – Способ сохранения сообщений в журнал определяется автоматически, в соответствии с настройками демона управления конфигурацией **Dr.Web ConfigD**. Определено для всех компонентов, кроме демона управления конфигурации, используется как значение по умолчанию.
  - `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 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 модуля **drweb-se**):

```
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.
  - `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. Описание известных ошибок

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

Сообщение об ошибке: *Функция не реализована.*

Код ошибки: `x65`

Описание: Некоторый компонент программного комплекса **Dr.Web для файловых серверов UNIX** не может функционировать, поскольку производятся попытки использования его функций, которые еще не реализованы в текущей версии.

Устранение ошибки:

- Выполните сброс настроек программного комплекса в значения по умолчанию, для этого:
  1. Очистите содержимое файла `<etc_dir>/drweb.ini`. Рекомендуется выполнить предварительное сохранение резервной копии файла. Например:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

  2. Выполните команду

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

     для перезапуска программного комплекса **Dr.Web для файловых серверов UNIX**.

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

Сообщение об ошибке: *Недопустимый DRL-файл.*

Код ошибки: `x90`

Описание: Обновление невозможно, так как **Dr.Web Updater** обнаружил нарушение целостности или отсутствие подписанного файла со списком серверов обновлений.

Устранение ошибки:

- Выполните отдельную установку компонентов (пакетов) `drweb-bases` и `drweb-dws`, после чего выполните обновление.
- Если ошибка повторится, удалите продукт **Dr.Web для файловых серверов UNIX** целиком, после чего установите его повторно и выполните обновление.
- 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: **Dr.Web Updater** обнаружил нарушение целостности или отсутствие файла архива, полученного с сервера обновлений.

Устранение ошибки:

- Выполните обновление повторно через некоторое время.

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

Сообщение об ошибке: *Ошибка аутентификации на прокси-сервере.*

Код ошибки: `x93`

Описание: **Dr.Web Updater** не смог подключиться к серверу обновлений, поскольку не прошел аутентификацию на прокси-сервере, используемом для получения обновлений.

Устранение ошибки:

- Проверьте и исправьте параметры используемого прокси-сервера (имя пользователя и пароль, используемые для аутентификации).
- Если ошибка повторится, смените используемый прокси-сервер или откажитесь от использования прокси-сервера.

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

Сообщение об ошибке: *Нет доступных серверов обновлений.*

Код ошибки: `x94`

Описание: **Dr.Web Updater** не смог подключиться ни к одному серверу обновлений.

Устранение ошибки:

- Проверьте наличие и работоспособность сетевого соединения, а также, что ваш компьютер имеет доступ к сети Интернет.
- Если доступ в интернет разрешен только через прокси-сервер, то настройте его использование при получении обновлений.
- Если используется прокси-сервер, то проверьте и исправьте параметры подключения к прокси-серверу.

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

Сообщение об ошибке: *Формат ключевого файла неизвестный или не поддерживается.*

Код ошибки: `x95`

Описание: Получение обновлений невозможно, поскольку нарушена целостность ключевого файла.

Устранение ошибки:

- Установите ключевой файл из резервной копии. Если резервная копия отсутствует, приобретите его повторно, обратившись в техническую поддержку.

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

Сообщение об ошибке: *Срок действия лицензии уже истек.*

Код ошибки: `x96`

Описание: Получение обновлений невозможно, поскольку срок действия лицензии закончился.

Устранение ошибки:

- Приобретите новую лицензию и активируйте продукт.

Если вы уверены, что срок действия лицензии не истек, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Истек тайм-аут сетевой операции.*

Код ошибки: `x97`

Описание: **Dr.Web Updater** не смог получить обновления из-за разрыва соединения.

Устранение ошибки:

- Проверьте наличие и работоспособность сетевого соединения, а также, что ваш компьютер имеет доступ к сети Интернет.
- Если используется прокси-сервер, то проверьте и исправьте параметры подключения к прокси-серверу.
- Если ошибка повторится, смените используемый прокси-сервер или откажитесь от использования прокси-сервера.

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

Сообщение об ошибке: *Недопустимая контрольная сумма.*

Код ошибки: `x98`

Описание: **Dr.Web Updater** получил файл обновления, контрольная сумма которого не совпадает с ожидаемой.

Устранение ошибки:

- Выполните обновление повторно через некоторое время.

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

Сообщение об ошибке: *Недопустимый демонстрационный ключевой файл.*

Код ошибки: `x99`

Описание: Получение обновлений невозможно, поскольку нарушена целостность демонстрационного ключевого файла, или он используется несанкционированно.

Устранение ошибки:

- Приобретите лицензию и активируйте продукт.

Если вы уверены, что демонстрационный ключевой файл действительный, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Ключевой файл заблокирован.*

Код ошибки: `x100`

Описание: Получение обновлений невозможно, поскольку используемый ключевой файл заблокирован компанией **«Доктор Веб»**.

Устранение ошибки:

- Приобретите лицензию и активируйте продукт.

Если вы уверены, что используемый ключевой файл действительный, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Недопустимая конфигурация.*

Код ошибки: `x102`

Описание: Некоторый компонент программного комплекса **Dr.Web для файловых серверов UNIX** не может функционировать из-за неправильных настроек конфигурации.

Устранение ошибки:

Компонент **SpIDer Guard**: задан способ работы модуля, который не поддерживается операционной системой.

- Выполните команду

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

  для перевода **SpIDer Guard** в автоматический режим определения подходящего способа работы.
- 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).

Другие компоненты:

- Выполните сброс настроек программного комплекса в значения по умолчанию, для этого:
  1. Очистите содержимое файла `<etc_dir>/drweb.ini`. Рекомендуется выполнить предварительное сохранение резервной копии файла. Например:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```
  2. Выполните команду

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

     для перезапуска программного комплекса **Dr.Web для файловых серверов UNIX**.

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

Сообщение об ошибке: *Недопустимый исполняемый файл.*

Код ошибки: `x104`

Описание: Исполняемый файл некоторого компонента программного комплекса **Dr.Web для файловых серверов UNIX** отсутствует или испорчен.

Устранение ошибки:

- Выполните отдельную установку пакета, содержащего требуемый компонент:
  - `drweb-spider`, если испорчен исполняемый файл **SpIDer Guard**
  - `drweb-update`, если испорчен исполняемый файл **Dr.Web Updater**
- Если ошибка повторится, или если вы не можете определить, исполняемый файл какого компонента испорчен, 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, сообщив код ошибки.

Сообщение об ошибке: *Недопустимый файл Антивирусного ядра.*

Код ошибки: `x105`

Описание: Программный комплекс **Dr.Web для файловых серверов UNIX** не может функционировать, так как файл динамической библиотеки антивирусного ядра **Dr.Web Virus-Finding Engine** отсутствует или испорчен.

Устранение ошибки:

- Выполните обновление вирусных баз.
- Если ошибка повторится, выполните отдельную установку пакета `drweb-bases`, содержащего антивирусное ядро и вирусные базы.
- Если 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, сообщив код ошибки.

Сообщение об ошибке: *Вирусные базы отсутствуют.*

Код ошибки: `x106`

Описание: Программный комплекс **Dr.Web для файловых серверов UNIX** не может осуществлять антивирусную защиту, так как отсутствуют или испорчены вирусные базы.

Устранение ошибки:

- Выполните обновление вирусных баз.
- Если ошибка повторится, выполните отдельную установку пакета `drweb-bases`, содержащего антивирусное ядро и вирусные базы.
- Если 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, сообщив код ошибки.

Сообщение об ошибке: *Обнаружено несовместимое программное обеспечение.*

Код ошибки: `x109`

Описание: Некоторый компонент программного комплекса **Dr.Web для файловых серверов UNIX** не может функционировать, поскольку обнаружено программное обеспечение, препятствующие его корректной работе.

Устранение ошибки:

- 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 компонент ScanEngine.*

Код ошибки: `x119`

Описание: Невозможно проверять файлы, поскольку отсутствует или не запускается модуль **`drweb-se`**, используемый для проверки наличия вредоносного содержимого.

Устранение ошибки:

- 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 для SELinux).

- Выполните команду

  ```
  # drweb-ctl cfshow ScanEngine.ExePath
  ```

  если выведенная на экран строка отличается от `ScanEngine.ExePath = <opt_dir>/bin/drweb-se`, то выполните команду

  ```
  # drweb-ctl cfset ScanEngine.ExePath <opt_dir>/bin/drweb-se
  ```

- Если предыдущие шаги не помогли, выполните отдельную установку компонента (пакета) `drweb-se`.

- Если 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, сообщив код ошибки.

Сообщение об ошибке: *Недоступен компонент FileCheck.*

Код ошибки: `x120`

Описание: Невозможно осуществлять проверку файлов, поскольку отсутствует компонент **drweb-filecheck**, используемый для проверки файлов.

Устранение ошибки:

- 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.
- Если ваша ОС использует подсистему безопасности **SELinux,** настройте политику безопасности для модуля **drweb-filecheck** (см. раздел Настройка политик безопасности для SELinux).
- Выполните команду

  ```
  # drweb-ctl cfshow FileCheck.ExePath
  ```

  если выведенная на экран строка отличается от `FileCheck.ExePath = <opt_dir>/bin/drweb-filecheck`, то выполните команду

  ```
  # drweb-ctl cfset FileCheck.ExePath <opt_dir>/bin/drweb-filecheck
  ```

- Если предыдущие шаги не помогли, выполните отдельную установку компонента (пакета) `drweb-filecheck`.
- Если 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, сообщив код ошибки.

Сообщение об ошибке: *Недоступен компонент NetCheck.*

Код ошибки: `x123`

Описание: Отсутствует или не может быть запущен вспомогательный модуль **drweb-netcheck**, предназначенный для проверки файлов, загруженных по сети.

Устранение ошибки:

- Выполните команду

  ```
  # drweb-ctl cfshow NetCheck.ExePath
  ```

  если выведенная на экран строка отличается от `NetCheck.ExePath = <opt_dir>/bin/drweb-netcheck`, то выполните команду

  ```
  # drweb-ctl cfset NetCheck.ExePath <opt_dir>/drweb-netcheck
  ```

- Если ошибка повторится, выполните отдельную установку компонента (пакета) `drweb-netcheck`.
- Если 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, сообщив код ошибки.

Ошибки, не имеющие кодов

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:

- Выполните команду

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

  для перезапуска **Dr.Web ConfigD** и **Dr.Web для файловых серверов UNIX** в целом.
- Если эта команда вернет ошибку или не даст никакого эффекта, выполните отдельную установку компонента (пакета) drweb-configd.
- Обратите внимание, что это также может означать, что в системе для аутентификации пользователей не используется **PAM**. Если это так, что установите и настройте его, поскольку без PAM корректная работа продукта невозможна.
- 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, сообщив код ошибки.

Приложение E. Сборка модуля ядра для SpIDer Guard

Если операционная система не предоставляет механизм **fanotify**, используемый **SpIDer Guard** для мониторинга действий с объектами файловой системы, он может использовать специальный загружаемый модуль, работающий в пространстве ядра.

По умолчанию в составе **SpIDer Guard** поставляется скомпилированный модуль ядра для ОС **CentOS** и **Red Hat Enterprise Linux** версий 5.10 и 6.5, поскольку эти ОС не предоставляют **fanotify**. Также совместно со **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 **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 проверочный скрипт **check-kmod-install.sh**, запустив 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. 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 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>`. Обратите внимание, что версия ядра, выдаваемая командой **`uname -r`**, может не совпадать с именем каталога `<версия_ядра>`!

Приложение Ж. 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 упакованы 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-10.1.0.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-10.1.0.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 конфигурацию (**./configure**) и сборку (**make**) сервера. При конфигурации 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 **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.

8. 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**).

Предметный Указатель

Предметный Указатель