Dr.WEB®

Антивирус
для файловых серверов UNIX Samba

Руководство администратора

Защити созданное

© 2013 "Доктор Веб". Все права защищены.

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

ТОРГОВЫЕ ЗНАКИ
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk и логотип Dr.WEB являются зарегистрированными товарными знаками «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.
Linux® – зарегистрированный товарный знак Линуса Торвальдса на территории Соединенных Штатов Америки и других стран.
UNIX® – зарегистрированный товарный знак The Open Group.

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

Антивирус Dr.Web® для файловых серверов UNIX
Версия 6.0.2
Руководство администратора
18.01.2013

Доктор Веб, 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

Введение

В настоящей документации представлено описание следующих программных комплексов:

- **Антивирус Dr.Web® для файловых серверов UNIX** для **Linux**;
- **Антивирус Dr.Web® для файловых серверов UNIX** для **FreeBSD**;
- **Антивирус Dr.Web® для файловых серверов UNIX** для **Solaris** x86.

Поскольку между этими программными комплексами для разных UNIX-систем немного принципиальных различий, в дальнейшем в документации речь будет идти, в основном, об общем случае **Антивируса Dr.Web для файловых серверов UNIX** (далее – **Dr.Web для файловых серверов UNIX**), а отличиям будут посвящены отдельные главы.

Руководство адресовано лицу, отвечающему за антивирусную безопасность и настройку сетей, называемому в данном руководстве "Администратором".

Цель защиты файловых серверов в UNIX-системах заключается в поиске и обезвреживании вирусов и прочих вредоносных программ. Большинство вирусов не специфичны для UNIX-систем, но через локальные сети распространяются обычные Windows-вирусы, в том числе и макровирусы для Word, Excel и других приложений.

Проверка осуществляется в момент выполнения сервером запроса рабочей станции на файловую операцию (т.е. при записи файлов на сервер или при открытии файлов на сервере).

Программный комплекс **Dr.Web для файловых серверов UNIX** состоит из следующих компонентов:

- **Консольный сканер Dr.Web Scanner** служит для обнаружения и лечения вирусов на локальной машине, в том числе и в каталогах общего доступа;

- **Резидентный компонент** **Dr.Web Daemon** используется в качестве подключаемого внешнего антивирусного фильтра;
- **Резидентный компонент** **Dr.Web Monitor** используется для запуска и перезапуска прочих модулей **Dr.Web** в нужном порядке;
- **Резидентный компонент** **Dr.Web Agent** используется для управления конфигурацией модулей **Dr.Web**, сбора статистической информации и интеграции с **Dr.Web Enterprise Security Suite**;
- **Антивирусное ядро** **Dr.Web Engine** и набор постоянно обновляемых вирусных баз данных;
- **Компонент** **Dr.Web Updater**, выполненный в виде perl-скрипта, используется для автоматического обновления вирусных баз данных;
- **Компонент** **Dr.Web Samba VFS SpIDer** используется как монитор файловых операций для файлового сервера **Samba**. Он реализован как подключаемый модуль для интерфейса VFS (Virtual File System) в **Samba**. Одновременно он является клиентом **Dr.Web Daemon**;
- **Веб-интерфейс управления** **Консоль Dr.Web для файловых серверов UNIX** – модуль, интегрирующийся в системный компонент **Webmin** и используемый для управления и настройки **Dr.Web для файловых серверов UNIX** через веб-интерфейс с любого браузера.

Структура компонентов **Dr.Web для файловых серверов UNIX** изображена на рисунке ниже:

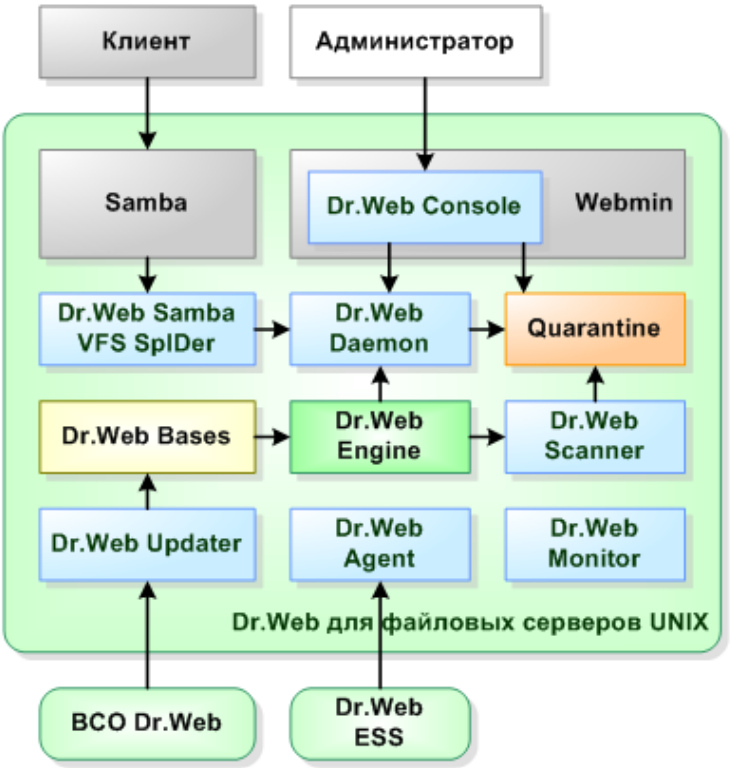


Рис. 1. Структура компонентов Dr.Web для файловых серверов UNIX

В настоящем руководстве будет рассмотрен процесс настройки и использования программного комплекса **Dr.Web для файловых серверов UNIX**, а именно:

- Общая характеристика продукта.
- Установка программного комплекса **Dr.Web для файловых серверов UNIX**.

- Запуск программного комплекса **Dr.Web для файловых серверов UNIX**.
- Использование модуля обновления **Dr.Web Updater**.
- Использование модуля **Dr.Web Agent**.
- Использование консольного сканера **Dr.Web Scanner**.
- Использование антивирусного модуля **Dr.Web Daemon**.
- Использование модуля **Dr.Web Monitor**.
- Использование модуля **Dr.Web Samba VFS SpIDer**.
- Работа с веб-интерфейсом **Консоль Dr.Web для файловых серверов UNIX**.

В заключении руководства приведена информация для контактов со службой технической поддержки.

Необходимо отметить, что продукты **"Доктор Веб"** находятся в постоянном развитии. Обновления баз данных известных вирусов выходят ежедневно (как правило, несколько раз в день). Периодически появляются новые версии отдельных компонентов. Изменения в продуктах касаются как совершенствования приемов диагностики и борьбы с вирусами, так и средств интеграции с другими приложениями UNIX-систем. Кроме того, постоянно расширяется круг приложений, способных работать совместно с продуктами **"Доктор Веб"**. Поэтому не исключено, что некоторые детали настройки и использования текущей версии будут отличаться от описанных в настоящем руководстве.

Используемые 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 **Доктор Веб** 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.
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.

Также для указания каталогов, в которые устанавливаются компоненты программного комплекса, используются условные обозначения `%bin_dir`, `%etc_dir` и `%var_dir`. В зависимости от ОС эти обозначения указывают на следующие каталоги:

для Linux и Solaris:

```
%bin_dir = /opt/drweb/
%etc_dir = /etc/drweb/
%var_dir = /var/drweb/
```

для FreeBSD:

```
%bin_dir = /usr/local/drweb/
%etc_dir = /usr/local/etc/drweb/
%var_dir = /var/drweb/
```

В документе используются следующие термины и сокращения:

Сокращение	Расшифровка
ASCII	American Standard Code for Information Interchange — американская стандартная кодировочная таблица для печатных символов и некоторых специальных кодов
CIDR	Classless Inter-Domain Routing — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации
DEB	Расширение имён файлов «бинарных» пакетов для распространения и установки программного обеспечения в ОС проекта **Debian** и других, использующих систему управления пакетами **dpkg**
DNS	Domain Name System — компьютерная распределённая система для получения информации о доменах
HTML	HyperText Markup Language — язык разметки гипертекста, стандартный язык разметки Web-документов

Сокращение	Расшифровка
IP	Internet Protocol — маршрутизируемый межсетевой протокол сетевого уровня семейства TCP/IP
IPv4	Протокол IP, версия 4
IPv6	Протокол IP, версия 6
IPC	Inter-Process Communication — набор способов обмена данными между множеством потоков в одном или более процессах, запущенных на одном или более компьютерах, связанных между собой сетью
MD5	Message Digest 5 — 128-битный алгоритм хеширования, предназначенный для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности
PID	Process IDentifier — уникальный идентификатор, присваиваемый ОС экземпляру процесса при его запуске
POSIX	Portable Operating System Interface for Unix — набор стандартов, определяющих интерфейсы взаимодействия между операционной системой и прикладной программой, созданный для обеспечения совместимости различных UNIX-подобных операционных систем и переносимости прикладных программ на уровне исходного кода
RFC	Request for Comments — документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети
RPM	Формат пакетов распространения программного обеспечения и название менеджера управления ими
SSL	Secure Socket Layers — так же как и TLS – криптографический протокол, обеспечивающие защищённую передачу данных между узлами в сети Интернет
TCP	Transmission Control Protocol — один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP

Сокращение	Расшифровка
TLS	Transport Layer Security — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет. Использует асимметричную криптографию для обмена ключами, симметричное шифрование для конфиденциальности и коды аутентичности для сохранения целостности сообщений
URL	Uniform Resource Locator — единообразный локатор (определитель местонахождения) ресурса. Стандартизированный способ записи адреса ресурса в сети Интернет
UUID	Unique User IDdentifier — уникальный идентификатор пользователя
XML	eXtensible Markup Language — расширяемый язык разметки, текстовый формат, предназначенный для хранения структурированных данных, обмена информацией между программами, а также для создания на его основе более специализированных языков разметки
ОС	Операционная система — комплекс управляющих и обрабатывающих программ, предназначенных для управления устройствами, вычислительными процессами, эффективного распределения вычислительных ресурсов между вычислительными процессами и организации надёжных вычислений

В разделе описания работы компонента **Консоль Dr.Web для файловых серверов UNIX** используются следующие термины и сокращения:

Сокращение	Расшифровка
CGI	Common Gateway Interface — стандарт интерфейса, используемого для связи внешней программы с веб-сервером
JSON	JavaScript Object Notation — текстовый формат обмена данными, основанный на JavaScript

Системные требования

Компоненты программного комплекса **Dr.Web для файловых серверов UNIX** совместимы:

- с дистрибутивами **Linux**, удовлетворяющим требованиям, приведенным в разделе Совместимость с дистрибутивами Linux;
- с **FreeBSD** версии 6.x и выше для платформы Intel x86 и amd64;
- с **Solaris** версии 10 для платформы Intel x86 и amd64.

Используемая платформа должна обеспечивать полную поддержку системы команд процессора архитектуры x86 в 32-битном и 64-битном режимах. На 64-битных системах обязательно должна быть включена поддержка выполнения 32-битных приложений.

Пример:

Для поддержки 32-битных приложений в системах на основе **Debian**/**Ubuntu Linux** понадобится установить библиотеку `ia32-libs`, а для систем на основе **ALT Linux** – библиотеку `i586-glibc-core`.

Для успешной и стабильной работы **Dr.Web для файловых серверов UNIX** требуются:

- Установленный и запущенный **Dr.Web Daemon** и Антивирусное ядро **Dr.Web Engine** версии не ниже 6.0.2.
- Установленный и настроенный сервер файловой службы **Samba** версии не ниже 3.0.END
- Модуль обновления **Dr.Web Updater** требует установленный **Perl** 5.8.0 и выше.

С точки зрения аппаратного обеспечения требования программного комплекса **Dr.Web для файловых серверов UNIX** совпадают с требованиями консольного (текстового) режима операционной системы, для которой он предназначен. Для установки требуется около 150 Мбайт дискового

пространства. Для установки веб-интерфейса дополнительно требуется 50 Мбайт дискового пространства.

Для работы графического инсталлятора **Dr.Web для файловых серверов UNIX** требуется **X Window System.** Для работы установочного скрипта в графическом режиме необходимо, чтобы в системе был установлен эмулятор терминала **xterm** или **xvt**.

Также в системе должны быть установлены следующие пакеты и утилиты:

- **base64**
- **unzip**
- **crond**

Для корректной работы **Dr.Web для файловых серверов UNIX** в операционной системе **FreeBSD** старше восьмой версии необходимо наличие библиотеки **compat7x**.

В зависимости от задач, решаемых программным комплексом **Dr.Web для файловых серверов UNIX**, и рабочей нагрузки, к аппаратному обеспечению компьютера могут предъявляться дополнительные требования.

Пожалуйста, обратите внимание, что компонент **Dr.Web Samba VFS SpIDer**, входящий в состав **Dr.Web для файловых серверов UNIX**, по умолчанию собран для **Samba** без поддержки опции CLUSTER_SUPPORT. В случае если используемая вами **Samba** работает с опцией CLUSTER_SUPPORT, при сканировании файлов могут возникать ошибки.

Если вы используете **Samba** с опцией CLUSTER_SUPPORT, то вы можете после установки **Dr.Web для файловых серверов UNIX** выполнить процедуру установки **Dr.Web Samba VFS SpIDer** из исходных кодов (подробнее см. ниже, в разделе **Установка и удаление Dr.Web для файловых серверов UNIX**), вручную сконфигурировав их на соответствие используемой **Samba**, включая поддержку опции CLUSTER_SUPPORT.

Чтобы проверить, используете ли вы **Samba** с опцией `CLUSTER_SUPPORT`, выполните команду:

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

Совместимость с дистрибутивами Linux

Программный комплекс **Dr.Web для файловых серверов UNIX** поддерживает дистрибутивы **Linux x86** и **x86-64**.

Требования к версии **ядра** ОС и библиотеке **glibc** зависят от типа установочного пакета:

- Универсальный пакет для UNIX-систем (**Linux x86**):
  - версия **ядра** 2.4.x, версия **glibc** 2.2 (не рекомендуется) и выше,
  - либо версия **ядра** 2.6.x, версия **glibc** 2.3 и выше;
- Универсальный пакет для UNIX-систем (**Linux x86-64**):
  - версия **ядра** 2.6.x, рекомендована версия **glibc** 2.3 и выше;
- Пакеты RPM (**rpm-apt**, **urpmi**, **yum**, **zypper**):
  - версия **ядра** 2.6.18 и выше, версия **glibc** 2.5 и выше;
- Пакеты DEB (**apt**):
  - версия **ядра** 2.6.26 и выше, версия **glibc** 2.7 и выше;

Работоспособность комплекса протестирована на следующих дистрибутивах:

Дистрибутив Linux	Версии	
	32-бит	64-бит
ALT Linux	4.0 – 5.0 СПТ 6.0	5.0 СПТ 6.0

Дистрибутив Linux	Версии	
	32-бит	64-бит
Arch Linux	–	все
ASPLinux	12.0 – 14.0	–
Debian	3.1 – 6.0	4.0 – 6.0
Fedora	–	14.0
Gentoo	все	
Mandriva Linux	старше 2009, CS4	2010.x
Mandrake	10.x	10.x
openSUSE	10.3 – 11.0	10.3 – 11.0
PCLinux	2010	2010
RedHat Enterprise Linux (RHEL)	4.0 – 6.0	5.0 – 6.0
Suse Linux Enterprise Server	9.0 – 11.0	10.0 – 11.0
Ubuntu	7.04 – 11.04	7.04 – 11.04

Совместимость с ОС МСВС

Дистрибутив совместим со следующими версиями операционной системы **МСВС**:

- **МСВС** 3.0 80001-12 (изм. 0, 1, 2, 3);
- **МСВС** 3.0 80001-14 (изм. 0, 1, 2);
- **МСВС** 3.0 80001-08;
- **МСВС** 3.0 80001-16;
- **МСВС** 3.0 ФСТЭК.

Прочие дистрибутивы **Linux**, которые соответствуют приведенным выше требованиям, тоже поддерживаются, но не были протестированы. При возникновении проблем с совместимостью с вашим дистрибутивом, обратитесь в техническую поддержку: http://support.drweb.com/request/.

Расположение файлов пакета

По умолчанию **Dr.Web для файловых серверов UNIX** устанавливается в каталоги `%bin_dir`, `%etc_dir` и `%var_dir`. В этих каталогах создается структура подкаталогов, не зависящая от ОС:

`%bin_dir/` – Исполняемые модули программного комплекса и модуль обновления компонентов **Dr.Web Updater** (perl-скрипт `update.pl`).

`%bin_dir/doc/` – Документация по продукту. Вся документация представлена в виде текстовых файлов и присутствует в двух вариантах — англоязычном и русскоязычном (в кодировках `KOI8-R` и `UTF-8`).

`%bin_dir/doc/samba/` – Документация для модуля **Dr.Web Samba VFS SpIDer**, сценарий для автоматического создания и обновления символических ссылок `update-links.sh` и образец сценария.

`%bin_dir/lib/` – Антивирусное ядро **Dr.Web Engine** в виде подгружаемой библиотеки (`drweb32.dll`). Здесь же могут располагаться различные служебные библиотеки, необходимые для работы компонентов программного комплекса, например:

- `ru_scanner.dwl` – файл языковых ресурсов модуля **Dr.Web Scanner**.

`%bin_dir/web/` – Модуль веб-интерфейса **Dr.Web для файловых серверов UNIX** для подключения к **Webmin**.

`%etc_dir/` – Конфигурационные файлы программного комплекса:

- `drweb32.ini`;
- `agent.conf`;
- `monitor.conf`;
- `smb_spider.conf`;
- `drwebd.enable`;

- drweb-monitor.enable.

Последние два файла (enable-файлы) нужны для настройки работы демонов*.

%etc_dir/agent/ – Дополнительные конфигурационные файлы модуля **Dr.Web Agent**.

%etc_dir/monitor/ – Дополнительные конфигурационные файлы модуля **Dr.Web Monitor**.

%var_dir/bases/ – Базы данных известных вирусов (файлы *.vdb).

%var_dir/infected/ – Каталог **Карантина** для перемещения в него зараженных файлов, если такая реакция на обнаружение зараженных или подозрительных файлов задана в настройках компонентов программного комплекса.

*) Расположение enable-файлов зависит от способа установки **Dr.Web для файловых серверов UNIX**:

- Установка при помощи **универсального пакета для UNIX**:

  Файлы располагаются в каталоге %etc_dir и называются
  drwebd.enable,
  drweb-monitor.enable.

- Установка из **нативных DEB-пакетов**:

  Файлы располагаются в каталоге /etc/defaults и называются
  drwebd,
  drweb-monitor.

- Установка из **нативных RPM-пакетов**:

  Файлы располагаются в каталоге /etc/sysconfig и называются
  drwebd.enable,
  drweb-monitor.enable.

Конфигурационные файлы

Общий формат конфигурационных файлов

Настройка большинства компонентов программного комплекса **Dr.Web для файловых серверов UNIX** производится с помощью конфигурационных файлов. Конфигурационные файлы являются текстовыми файлами, что позволяет редактировать их любым текстовым редактором).

Общий формат файла конфигурации:

```
--- начало файла ---

[Имя секции 1]
Параметр1 = значение1, ..., значениеK
...
ПараметрN = значение1, ..., значениеK

[Имя секции X]
Параметр1 = значение1, ..., значениеK
...

--- конец файла ---
```

Файлы конфигурации формируются по следующему принципу:

- 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.
- Содержимое файла разбивается на последовательность именованных секций. Возможные имена секций жестко заданы и не могут быть произвольными. Имя секции задается в квадратных скобках.
- Каждая секция содержит группу параметров конфигурации, объединенных по смыслу.
- В одной строке файла задается значение только одного

параметра.

- 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 в файле регистронезависимы.
- Порядок следования секций в файле и параметров внутри секций не имеет значения.
- Значения параметров в конфигурационном файле могут быть заключены в кавычки (и должны быть заключены в кавычки в том случае, если содержат пробелы).
- Некоторые параметры могут иметь несколько значений, в этом случае значения параметра разделяются запятой, или значение параметра задается несколько раз в разных строках конфигурационного файла. При перечислении значений параметра через запятую пробелы между значением и запятой, если встречаются, игнорируются. Если пробел является частью значения, всё значение необходимо заключить в кавычки.

Возможность присвоения параметру несколько значений в данном документе 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.

Пример 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 конфигурационного файла:

```
Parameter = Value2
Parameter = Value1
Parameter = "Value 3"
```

Обратите внимание, что порядок следования значений параметра в списке несущественен.

Если какой-либо параметр не задан (отсутствует) в конфигурационном файле, это не означает, что у данного параметра нет значения. В таких случаях значение параметра считается заданным по умолчанию. Лишь некоторые параметры являются необязательными или не имеют значений по умолчанию, о чем, как правило, упоминается отдельно.

Правила описания параметров, принятые в данном документе

В данном руководстве каждый параметр описывается следующим образом:

ИмяПараметра = {Тип параметра | Возможные значения}	Описание параметра. {Может ли иметь несколько значений}. {Особые замечания} {Важные замечания}
	Значение по умолчанию: **ИмяПараметра** = {значение | отсутствует}

Описание параметров и секций конфигурационных файлов дано в порядке их следования в файле конфигурации, создаваемом при установке программного комплекса **Dr.Web для файловых серверов UNIX**.

Поле Тип параметра может принимать следующие значения:

- **числовое значение (numerical value)** — значение параметра является целым неотрицательным числом.
- **время (time)** — значение параметра задается в единицах измерения времени. Значение состоит из целого числа, после которого может идти буква, определяющая вид единиц измерения времени (s – секунды, m – минуты, h – часы, регистр букв не учитывается). Если в значении параметра буквы нет, то считается, что время задано в секундах.

  Примеры: 30s,15m
- **размер (size)** — значение параметра задается в единицах измерения объема памяти (дисковой или оперативной). Значение состоит из целого числа, после которого может идти буква, определяющая вид единиц измерения объема памяти (b – байты, k – килобайты, m – мегабайты, g – гигабайты, регистр букв не учитывается). Если в значении параметра буквы нет, то считается, что размер задан в байтах.

  Примеры: 20b,15k
- **права (permissons)** — значение параметра задаётся трехзначным числом, обозначающим права доступа к файлам в формате, принятом в UNIX-системах. Каждое право является комбинацией (суммой) трех базовых прав:
  - Право чтения (r) обозначается числом 4;
  - Право записи (w) обозначается числом 2;
  - Право исполнения (x) обозначается числом 1.

  При этом первая цифра числа задает права для владельца файла, вторая – для группы владельцев файла, а третья – для всех остальных, не являющихся ни владельцами, ни членами соответствующей группы.

  Примеры: 755,644
- **логический (Yes/No)** — Логический тип, значения

которого представляются строками "Yes" и "No".

- **путь к файлу/каталогу** (path to file/directory) — строка, задающая расположение файла или каталога в файловой системе. Помните, что в ОС семейства Linux/UNIX имена файлов и каталогов регистрозависимы. Если указано, что значением параметра может быть **маска**, то в качестве значений параметра можно использовать файловые маски, содержащие следующие специальные символы:
  - ? – замещает любой один символ;
  - * – замещает любую (в том числе пустую) последовательность символов.

  Пример: "?.e*" – маска, под которую подпадают файлы, имя которых состоит из любого одного символа, а расширение любой длины, и начинается с буквы 'e' (x.exe, g.e, f.enable и т.п.).

- **действие (action)** — строка, содержащая наименование действий, совершаемых над объектами, вызвавшими какую-либо реакцию компонентов программного комплекса **Dr.Web для файловых серверов UNIX**. В некоторых случаях для параметра можно задать одно основное действие и до трех дополнительных. Тип параметра в этом случае называется **список действий (actions list)**. Основное действие в этом случае всегда должно быть первым в списке. Для разных параметров набор допустимых действий может различаться, и в этом случае он указывается отдельно для каждого параметра. Общий перечень действий, которые могут использоваться, см. ниже.

- **адрес (address)** — строка, содержащая адрес сокета компонента **Dr.Web для файловых серверов UNIX** или внешнего модуля или программы.
  Имеет формат `ТИП: АДРЕС`. Допустимы следующие типы:
  - `inet` — используются TCP-сокеты, `АДРЕС` имеет формат `ПОРТ@ИМЯ_УЗЛА`. `ИМЯ_УЗЛА` может быть как прямым IP-адресом, так и доменным именем узла.

    Пример:

    ```
    Address = inet: 3003@localhost
    ```

  - `local` — используются локальные UNIX сокеты, в этом случае адрес является путем к файлу сокета.

    Пример:

    ```
    Address = local: %var_dir/.daemon
    ```

  - `pid` — реальный адрес процесса должен быть прочитан из его PID файла. Такой тип адреса доступен лишь в некоторых случаях и при возможности его использования в значении параметра это указывается явно.
- **текст (text value), строка (string)** — значение параметра задается в виде текстовой строки, текст в строке может быть заключен в кавычки (если в строке есть пробелы, кавычки обязательны).
- **уровень подробности (log level)** — строка, указывающая уровень подробности вывода информации в некоторый журнал или в службу **syslog**.
- **возможные значения (value)** — параметр имеет тип, не описанный в предыдущих пунктах данного списка. В этом случае перечисляется список разрешенных для него значений.

Поведение модулей при некорректно заданных файлах конфигурации

- Если значение какого-либо параметра задано некорректно, **Dr.Web для файловых серверов UNIX** выводит сообщение об ошибке и завершает свою работу.

- Если при загрузке какого-либо конфигурационного файла в нем обнаруживаются неизвестные параметры, работа программы продолжается в нормальном режиме, но в файл журнала (лог) выводится соответствующее предупреждение.

Ведение журналов (логов)

Все компоненты программного комплекса **Dr.Web для файловых серверов UNIX** ведут журналы (логи) своей работы. Для каждого компонента имеется возможность указать способ ведения журнала (самостоятельная запись событий в файл или использование системной службы журналирования **syslog**).

Уровень подробности ведения журнала работы компонента может быть как очень высоким (например, если задано значение **Debug** для отладочных целей), так и отсутствовать вовсе (например, если задано значение **Quiet**, когда файл журнала не ведется).

Для задания уровня подробности используется параметр с именем **LogLevel**. Также некоторые модули могут иметь дополнительные параметры, регулирующие уровни подробности вывода некоторых сообщений в журнал (например, вывод сообщений подситемы IPC, там, где она используется, регулируется параметром **IPCLevel**).

Если в настройках модуля отсутствуют параметр конфигурации **LogLevel**, то это означает, для него регулирование уровня подробности в журнал невозможно. По умолчанию в этом случае используется уровень журналирования, примерно равный `Debug`.

Используемые уровни подробности ведения журнала

Значения параметров, отвечающих за уровень подробности ведения журнала работы компонентов в общем случае могут задаваться из следующего набора (упорядочен от менее к более подробным):

- **Quiet** – Уровень "Тишина". Запись событий в журнал не ведется.
- **Error** – Уровень "Ошибки". Фиксируются записи только об критических ошибках.
- **Alert** – Уровень "Тревога". Фиксируются записи об ошибках и важных предупреждениях.
- **Warning** – Уровень "Предупреждения". Фиксируются записи об ошибках, важных и обычных предупреждениях.
- **Info** – Уровень "Информационный". Ведется запись сообщений об ошибках, предупреждениях и информационных сообщений.
- **Notice** – Уровень "Уведомительный". То же, что и "Информационный", но добавляются записи уведомлений.
- **Debug** – Уровень "Отладочный", То же, что и "Уведомительный", но добавляются записи отладочной информации.
- **Verbose** – Уровень "Подробный", ведется запись в журнал всех возможных сообщений (режим не рекомендуется из-за большого объема информации, выводимой в журнал, что тормозит как работу приложения, так и службу журналирования **syslog** операционной системы, если она используется).

Для каждого модуля **Dr.Web для файловых серверов UNIX** набор допустимых уровней подробности может различаться, о чем указано в описании соответствующих параметров

Использование службы журналирования syslog

При использовании для ведения службы журналирования **syslog** кроме указания уровня подробности ведения журнала

указывается также метка-источник сообщений, которая может быть использована службой **syslog** для внутренней маршрутизации сообщений по разным фаилам журналов. Эти правила маршрутизации настраиваются в собственном файле конфигурации демона службы **syslog** (обычно `/etc/syslogd. conf`).

Метка, присваиваемая сообщениям для службы **syslog**, указывается в конфигурационных файлах в параметре **`SyslogFacility`**.

Допускается использование следующих меток:

- `Daemon` – От имени резидентного системного сервиса (демона);
- `Local0, ..., Local7` – От имени локального пользовательского приложения (зарезервировано 8 номеров 0-7);
- `Kern` – От имени ядра системы;
- `User` – От имени пользовательского процесса;
- `Mail` – От имени почтовой системы.

Пожалуйста, обратите внимание, что при использовании **syslog** в файле конфигурации может дополнительно присутствовать параметр подробности ведения журнала, используемый для системы **syslog**. Этот параметр имеет название **`SyslogPriority`** и может принимать те же значения, что и основной параметр уровня подробности **(`LogLevel`)**. В случае если вывод в **syslog** не используется, этот параметр, также как и **`SyslogFacility`**, игнорируется. В противном случае для вывода в **syslog** выбирается наименее подробный из двух указанных уровней.

Пример:

Пусть у некоторого модуля **`LogLevel`** = `Debug`, а **`SyslogPriority`** = `Error`. Тогда, если в качестве журнала для записей событий этого модуля выбрана служба **syslog**, фактически будет вестись запись на уровне подробности **`Error`** (будут фиксироваться только сообщения

об ошибках, а отладочная информация **syslog** будет игнорироваться).

Действия с зараженными и подозрительными объектами

В настройках **Dr.Web для файловых серверов UNIX** задаются действия, которые модули, входящие в его состав, должны совершать с объектами, которые по результатам проверки признаны вредоносными, опасными или подозрительными.

Для разных параметров набор допустимых действий может различаться, поэтому для каждого параметра всегда указывается перечень действий, которые могут быть в нем использованы.

При настройке параметров предусмотрено использование следующих действий:

Доступные действия для **Dr.Web Scanner**:

- `Move` — переместить файл в каталог **Карантина**;
- `Delete` — удалить зараженный файл;
- `Rename` — переименовать файл;
- `Ignore` — пропустить файл;
- `Report` — только вывести информацию в отчет.
- `Cure` — попытаться вылечить зараженный объект.

Доступные действия для **Dr.Web Samba VFS SpIDer**:

- `Pass` — разрешить доступ к файлу;
- `Rename` — переименовать файл и запретить к нему доступ;
- `Discard` — удалить файл;
- `Quarantine` — переместить файл каталог **Карантина** и запретить к нему доступ;
- `Reject` — запретить доступ к файлу.

Имена действий для указания в параметрах не чувствительны к регистру (например, значения `Report` и `report` обозначают одно и то же действие).

Установка и удаление Dr.Web для файловых серверов UNIX

Ниже описывается процедура установки, обновления и удаления программного комплекса **Dr.Web для файловых серверов UNIX** из универсального пакета для UNIX-систем. Для осуществления этих операций необходимы права администратора (`root`).

Если ранее в системе продукт был установлен из пакетов других типов (например, rpm- или deb-пакетов), то желательно убедиться, что все эти пакеты удалены.

Универсальный пакет для UNIX-систем поставляется в формате EPM для использования с менеджером пакетов EPM (ESP Package Manager). Отдельные сценарии для установки и удаления компонентов, а также стандартные графические инсталляторы и деинсталляторы, входящие в состав пакетов такого типа, относятся исключительно к самому EPM-пакету, а не к упакованному в него программному комплексу в целом, и не к отдельным его модулям.

Соответственно, установка, обновление и удаление **Dr.Web для файловых серверов UNIX** могут быть осуществлены с помощью:

- графических инсталлятора и деинсталлятора;
- консольных инсталляторов и деинсталляторов.

При установке поддерживается работа с зависимостями, т.е. если для установки какого-либо из компонентов программного комплекса должен быть предварительно установлен другой компонент (например, для установки компонента **drweb-daemon** предварительно должны быть установлены компоненты **drweb-common** и **drweb-bases**), то он будет установлен автоматически.

Пожалуйста, обратите внимание, что компонент **Dr.Web Samba VFS SpIDer**, входящий в состав **Dr.Web для файловых серверов UNIX**, по умолчанию собран для **Samba** без поддержки опции `CLUSTER_SUPPORT`. В случае если используемая вами **Samba** работает с опцией `CLUSTER_SUPPORT`, при сканировании файлов могут возникать ошибки.

Если вы используете **Samba** с опцией `CLUSTER_SUPPORT`, то вы можете после установки **Dr.Web для файловых серверов UNIX** выполнить процедуру установки **Dr.Web Samba VFS SpIDer** из исходных кодов, вручную сконфигурировав их на соответствие используемой **Samba**, включая поддержку опции `CLUSTER_SUPPORT`.

Чтобы проверить, используете ли вы **Samba** с опцией `CLUSTER_SUPPORT`, выполните команду:

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

Необходимо отметить, что если вы устанавливаете программный комплекс **Dr.Web для файловых серверов UNIX** на компьютер, куда ранее из аналогичного универсального EPM-пакета был установлен какой-либо другой продукт **Доктор Веб**, то при каждом использовании графического деинсталлятора вам будет предложено удалить абсолютно все модули **Доктор Веб**, включая установленные ранее в составе других продуктов.

Крайне внимательно подходите к удалению компонентов, чтобы по ошибке не удалить те из них, которые вы планируете использовать в дальнейшем.

Установка универсального пакета для UNIX систем

Дистрибутив программного комплекса **Dr.Web для файловых серверов UNIX** распространяется в виде самораспаковывающегося архива

`drweb-file-servers_[номер версии]~[название ОС].run`.

В общем случае в архиве содержатся следующие пакеты:

- `drweb-common`: пакет содержит основной конфигурационный файл `drweb32.ini`, библиотеки, документацию и структуру каталогов. В процессе установки данного компонента будут созданы пользователь `drweb` и группа `drweb`;
- `drweb-bases`: пакет содержит Антивирусное ядро **Dr.Web Engine** и вирусные базы. Для установки требует пакет `drweb-common`;
- `drweb-libs`: пакет содержит библиотеки, общие для всех компонентов продукта;
- `drweb-epm6.0.2-libs`: пакет содержит библиотеки для графических инсталлятора и деинсталлятора. Для установки требует пакет `drweb-libs`;
- `drweb-epm6.0.2-uninst`: пакет содержит файлы графического деинсталлятора. Для установки требует пакет `drweb-epm6.0.2-libs`;
- `drweb-boost147`: пакет содержит библиотеки, использующиеся **Dr.Web Agent** и **Dr.Web Monitor** совместно. Для установки требует пакет `drweb-libs`;
- `drweb-updater`: пакет содержит модуль обновления Антивирусного ядра **Dr.Web Engine** и вирусных баз **Dr.Web Updater**. Для установки требует пакеты `drweb-common` и `drweb-libs`;
- `drweb-agent`: пакет содержит исполняемые файлы **Dr.Web Agent** и документацию к нему. Для установки требует пакеты `drweb-boost147` и `drweb-common`;
- `drweb-agent-es`: пакет содержит файлы для работы

Dr.Web Agent в режиме центральной защиты. Для установки требует пакеты `drweb-agent`, `drweb-updater` и `drweb-scanner`;

- `drweb-monitor`: пакет содержит исполняемые файлы **Dr.Web Monitor** и документацию к нему. Для установки требует пакеты `drweb-boost147`, `drweb-agent` и `drweb-common`;
- `drweb-daemon`: пакет содержит исполняемые файлы **Dr.Web Daemon** и документацию к нему. Для установки требует пакеты `drweb-bases` и `drweb-libs`;
- `drweb-scanner`: пакет содержит исполняемые файлы консольного сканера **Dr.Web Scanner** и документацию к нему. Для установки требует пакеты `drweb-bases` и `drweb-libs`;
- `drweb-samba-web`: пакет содержит веб-интерфейс **Dr.Web консоль для файловых серверов UNIX**;
- `drweb-file-servers-doc`: пакет содержит документацию к **Dr.Web для файловых серверов UNIX**;
- `drweb-smbspider`: пакет содержит скомпилированные библиотеки для различных версий серверов **Samba**. Для установки требует пакет `drweb-libs`;
- `drweb-smbspider-src`: пакет содержит исходные коды, чтобы пользователь сам смог собрать необходимые библиотеки с учетом особенностей архитектуры своей системы и/или для своей версии **Samba**.

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.

Для автоматической установки компонентов программного комплекса **Dr.Web для файловых серверов UNIX** разрешите исполнение архива, например, командой:

```
# chmod +x drweb-file-servers_[номер версии]~
[название ОС].run
```

и затем запустите его на исполнение командой:

```
# ./drweb-file-servers_[номер версии]~[название ОС].run
```

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

При этом будет создан каталог `drweb-file-servers_[номер версии]~[название ОС]` с набором файлов внутри, и автоматически запустится графический инсталлятор. Если запуск был осуществлен не с правами администратора, то инсталлятор сам попытается получить нужные права.

Если запустить графический инсталлятор не удалось, то автоматически запустится интерактивный консольный инсталлятор.

Если необходимо только распаковать архив, не запуская при этом графический инсталлятор, следует воспользоваться параметром командной строки `--noexec`:

```
# ./drweb-file-servers_[номер версии]~[название ОС].run --noexec
```

Для продолжения установки с помощью графического инсталлятора запустите его командой:

```
# drweb-file-servers_[номер версии]~[название ОС]/install.sh
```

Для установки с использованием консольного инсталлятора потребуется выполнить команду:

```
# drweb-file-servers_[номер версии]~[название ОС]/setup.sh
```

При установке любым из описанных ниже способов происходит следующее:

- в каталог `%etc_dir/software/conf/` записываются оригиналы дистрибутивных конфигурационных файлов с названиями в формате `[имя_конфигурационного_файла].N`;
- конфигурационные файлы устанавливаются в соответствующие каталоги системы;
- устанавливаются остальные файлы, причем если файл с таким именем уже имеется (например, остался после неаккуратного удаления пакетов других типов), то на его место записывается новый файл, а копия старого сохраняется как `[имя_файла].O`. Если в каталоге уже имеется файл с таким именем (`[имя_файла].O`), то он будет удален, а новый файл будет записан на его место;
- Если в соответствующем окне графического инсталлятора установлен флаг **Run interactive postinstall script**, то после установки компонентов будет запущен инсталляционный скрипт для настройки базовой функциональности **Dr.Web для файловых серверов UNIX**.
- запускается скрипт `update-links.sh`, который проверяет, какая версия **Samba** установлена в системе, и в каталоге `/usr/lib/samba/vfs/` создает символическую ссылку на библиотеку в каталоге `%bin_dir/lib/`, нужную для этой конкретной версии **Samba**. Если в один и тот же каталог были установлены две разных версии **Samba**, то символическая ссылка будет создана только для одной из них. Если разные версии **Samba** установлены в разные каталоги, то для каждой из них будет создана соответствующая символическая ссылка. При этом в отчет будут выведены следующие строки для каждой установленной версии **Samba**:

Пример для ОС Linux:

```
Update links for /usr/sbin/smbd
create symlink /opt/drweb/lib/libsmb_spider.
so.3.X.X --> /usr/lib/samba/vfs/smb_spider.so
Please, update your config /etc/samba/smb.conf
```

Пользовательский интерфейс графического инсталлятора

1. При запуске графического инсталлятора командой:

   ```
   # drweb-file-servers_[номер версии]~[название ОС]/install.sh
   ```

   открывается окно программы установки.

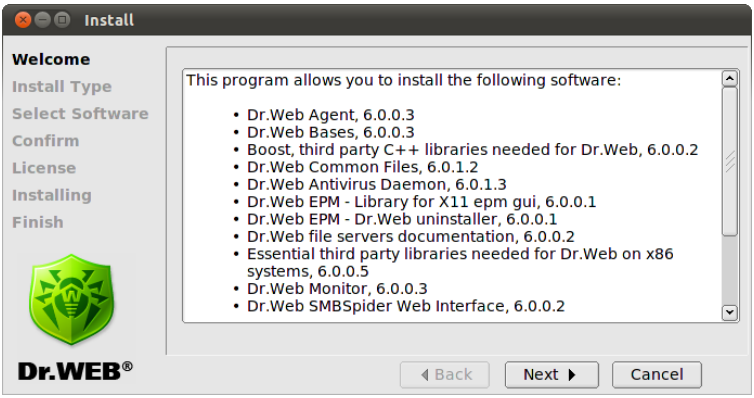


Рис. 2. Окно начала установки программы

Навигация осуществляется с помощью кнопок **Back** и **Next**. Установку можно прервать в любой момент, нажав кнопку **Cancel**.

2. В следующем окне **Install Type** вы можете выбрать тип установки: базовый **Dr.Web for File Servers** со всеми

компонентами по умолчанию или пользовательский.

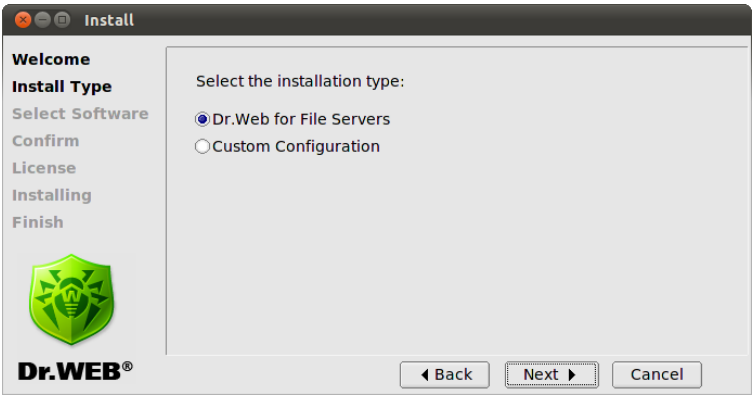


Рис. 3. Тип установки

Если вы выбрали пункт **Custom Configuration**, то следующим откроется окно **Select Software**, в котором вы сможете указать необходимые вам компоненты.

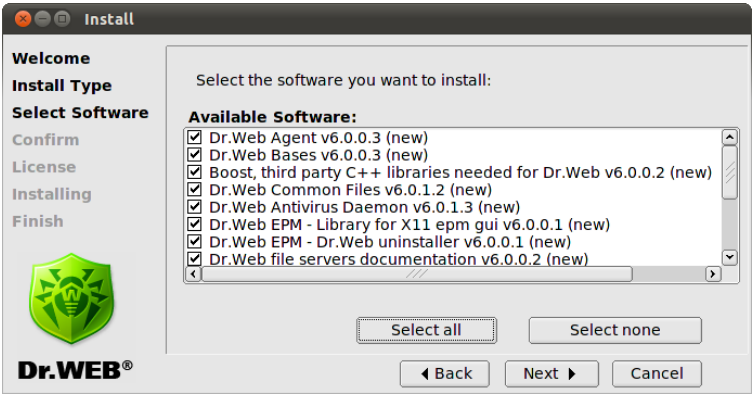


Рис. 4. Окно выбора компонентов для установки

Если для установки выбранного вами компонента должен быть предварительно установлен другой компонент, то соответствующая зависимость будет отмечена автоматически. Таким образом, если вы установите флаг напротив **Dr.Web Antivirus Daemon**, то флаги автоматически появятся напротив пунктов **Dr.Web Bases** и **Dr.Web Common Files**.

Нажатие на кнопку **Select all** выберет все компоненты, нажатие на кнопку **Select none** снимет все установленные флажки.

3. В окне **Confirm** вы увидите все выбранные вами компоненты и сможете принять окончательное решение.

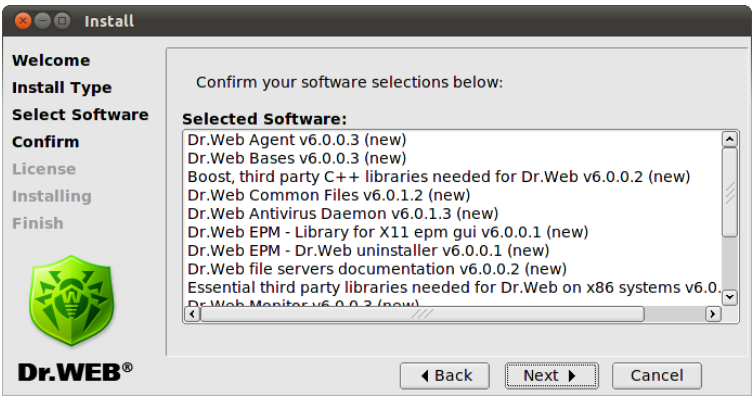


Рис. 5. Окно подтверждения установки компонентов

4. Ознакомьтесь с текстом **Лицензионного Договора** и подтвердите свое согласие с ним, чтобы продолжить установку. С помощью меню **Select language** вы можете выбрать язык (русский или английский), на котором будет изложен текст **Лицензионного Договора**.

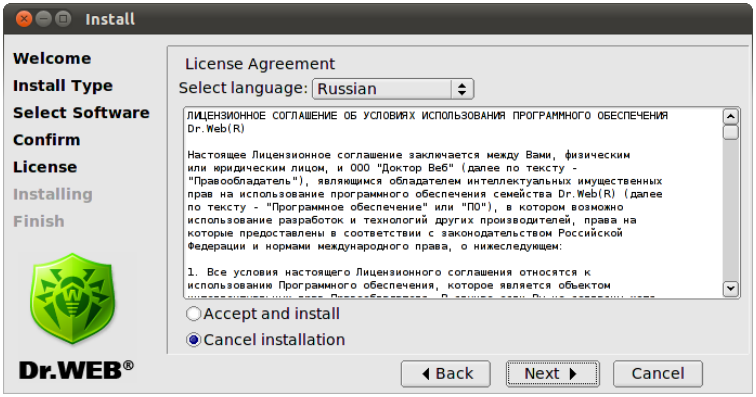


Рис. 6. Окно ознакомления с лицензионным соглашением

5. В следующем окне **Installing** выводится отчет о процессе установки в режиме реального времени.

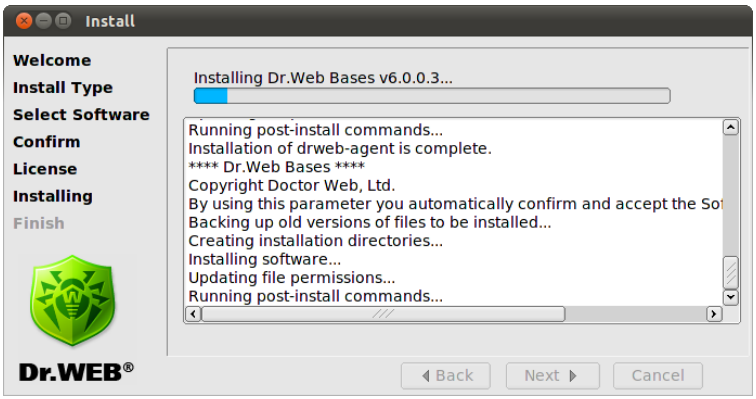


Рис. 7. Окно установки компонентов программы

Одновременно данный отчет копируется в файл `install.log`, расположенный в каталоге `drweb-file-servers_[номер версии]~[название ОС]`. Если установлен флаг **Run interactive postinstall script**, то после установки компонентов будет запущен

инсталляционный скрипт для настройки базовой функциональности **Dr.Web для файловых серверов UNIX**.

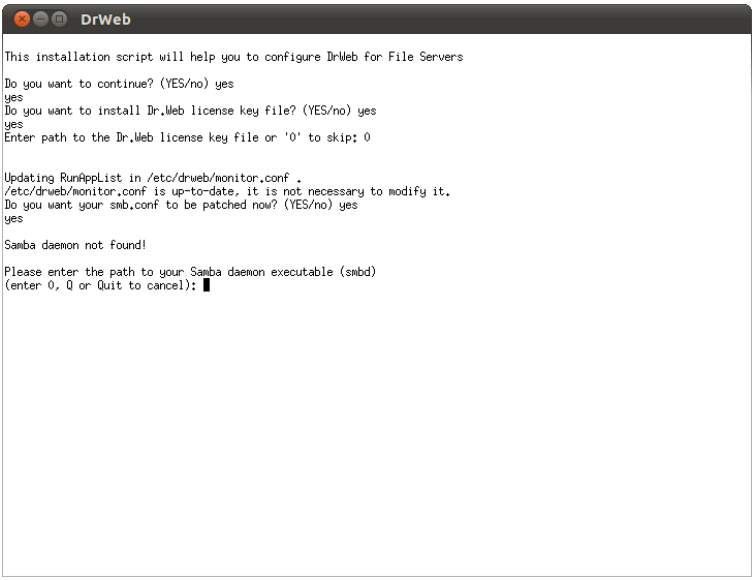


Рис. 8. Интерактивный установочный скрипт

Скрипт предложит указать путь к лицензионному ключевому файлу, установить порядок работы подключаемых модулей, выбрать из списка сетевые диски для защиты их с помощью **Dr.Web для файловых серверов UNIX** и автоматически подключить необходимые для работы сервисы (**Dr.Web Daemon**, **Dr.Web Agent**, **Dr.Web Monitor**).

6. В последнем окне **Finish** содержится напоминание о необходимости дальнейшей настройки системы перед тем, как она сможет полноценно работать. Нажав на кнопку **Close**, вы закроете окно программы установки компонентов.

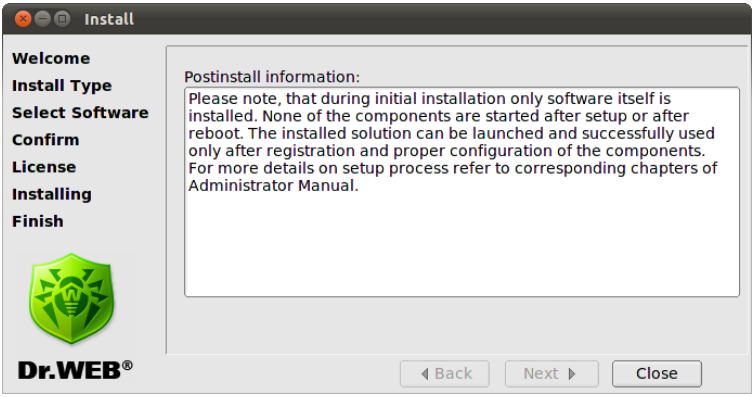


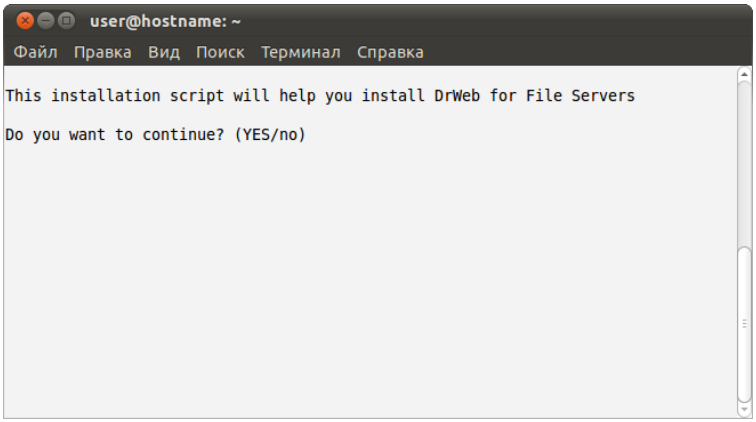
Рис. 9. Окно завершения установки программы

Использование консольного инсталлятора

Консольный инсталлятор запускается автоматически в том случае, если не удалось запустить графический инсталлятор. Если консольный инсталлятор не был запущен автоматически (как правило, это происходит при невозможности повысить права), то можно попробовать запустить его с привилегиями пользователя `root`, выполнив команду:

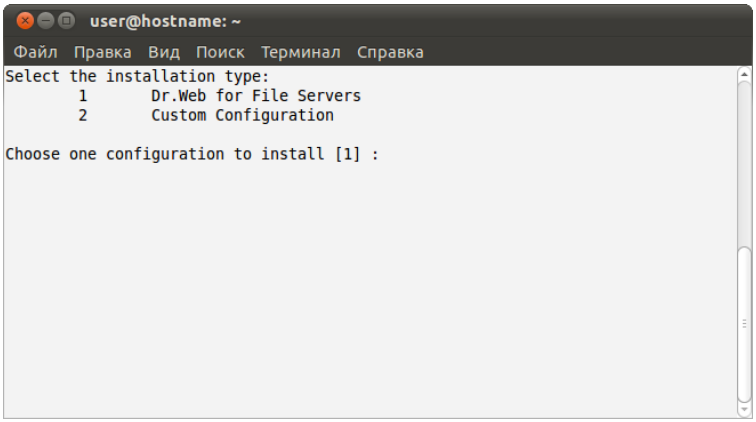
```
# drweb-file-servers_[номер версии]~[название ОС]/setup.sh
```

Откроется диалоговое окно консольного инсталлятора.

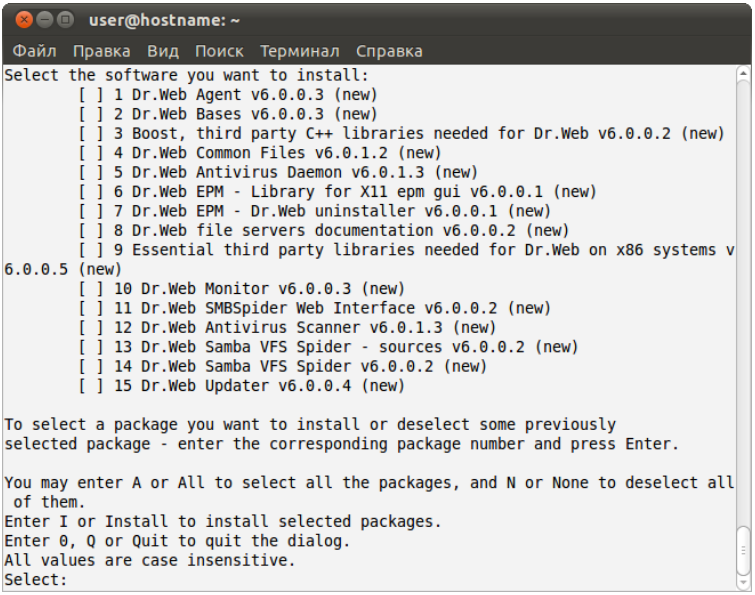


Если вы хотите установить **Dr.Web для файловых серверов UNIX**, укажите **Y** или **Yes** в строке ввода (значения регистронезависимы) и нажмите клавишу ENTER. В противном случае введите **N** или **No**.

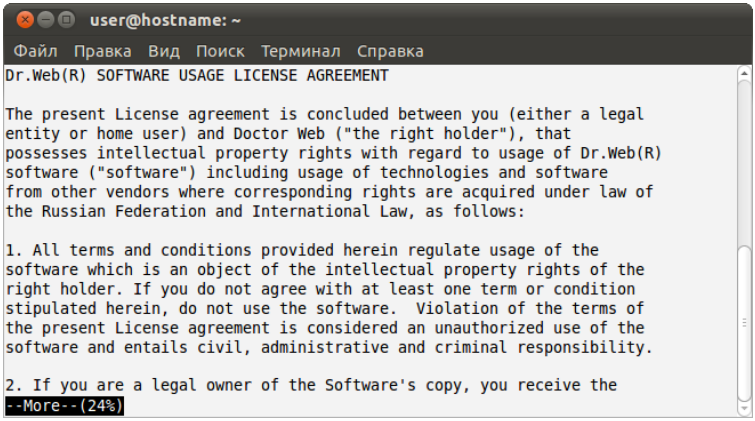
Затем вам будет предложено выбрать тип установки. Укажите номер соответствующего пункта в меню и нажмите ENTER.



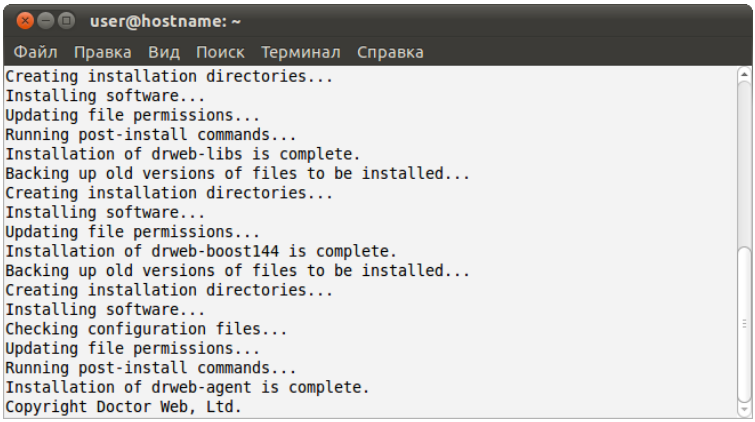
Если вы выбрали пункт **Custom Configuration**, то на следующем этапе вам будет предложено указать необходимые компоненты для установки. Укажите номер соответствующего компонента в меню и нажмите ENTER.



На следующем этапе вам будет предложено ознакомиться с текстом **Лицензионного Договора**. Для пролистывания текста договора нажимайте клавишу ПРОБЕЛ.



Для продолжения установки вы должны будете принять **Лицензионный Договор**, указав **Y** или **Yes** в строке ввода и нажав ENTER. В противном случае установка будет прекращена. После того, как вы примете **Лицензионный Договор**, будет запущен процесс установки. Отчет о результатах прохождения каждого из этапов процесса будет выводиться на консоль в режиме реального времени.



После установки компонентов будет запущен инсталляционный скрипт для настройки базовой функциональности **Dr.Web для файловых серверов UNIX**. Скрипт предложит указать путь к

лицензионному ключевому файлу и автоматически подключить необходимые для работы сервисы (**Dr.Web Daemon**, **Dr.Web Agent**, **Dr.Web Monitor**). Дополнительно Вам будет предложено указать сетевые диски для защиты их с помощью **Dr.Web для файловых серверов UNIX**.

Удаление универсального пакета для UNIX систем

Для удаления с помощью графического деинсталлятора, запустите его командой:

```
# %bin_dir/remove.sh
```

Если запуск был осуществлен не с правами администратора, то деинсталлятор сам попытается получить нужные права.

Если запустить графический деинсталлятор не удалось, то автоматически запустится интерактивный консольный деинсталлятор.

После деинсталляции продукта можно удалить средствами ОС пользователя `drweb` и группу `drweb`.

При удалении любым из вышеописанных способов происходит следующее:

- из каталога `%etc_dir/software/conf/` удаляются все дистрибутивные конфигурационные файлы;
- если рабочие конфигурационные файлы не были изменены пользователем, то они тоже удаляются. Если пользователь вносил в них изменения, они остаются в неприкосновенности;
- удаляются остальные файлы, причем если при установке была создана копия какого-либо старого файла в виде `[имя_файла].O`, то этот файл восстанавливается в прежнем виде;
- лицензионные ключевые файлы и файлы отчетов различных компонентов программного комплекса в

соответствующих каталогах сохраняются.

- запускается скрипт `update-links.sh` с параметром `--remove`, который удаляет символическую ссылку `/usr/lib/samba/vfs/smb_spider.so`.

При наличии нескольких символических ссылок для разных версий Samba, будут удалены все ссылки. При этом в отчет будут выведены строки:

```
Remove link /usr/lib/samba/vfs/smb_spider.so
Please, update your config /etc/samba/smb.conf
```

Обратите внимание, что после удаления **Dr.Web для файловых серверов UNIX** необходимо в конфигурационном файле `smb.conf` из соответствующих секций для каждого из защищаемых разделяемых ресурсов удалить строку:

```
vfs objects = smb_spider
```

Пользовательский интерфейс графического деинсталлятора

1. При запуске графического деинсталлятора командой:

```
# %bin_dir/remove.sh
```

открывается окно программы удаления компонентов.

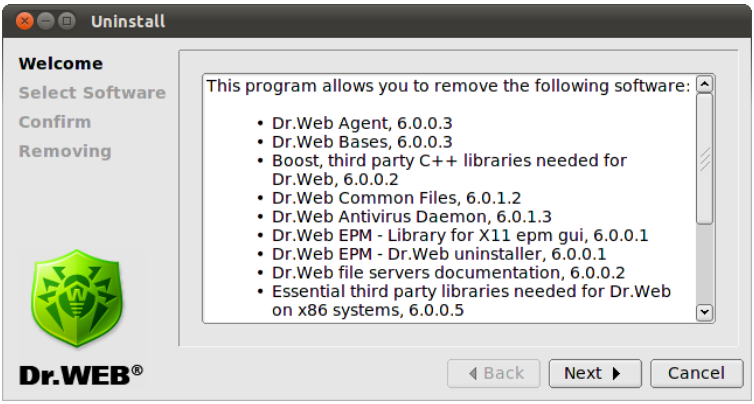


Рис. 10. Окно начала удаления программы

Навигация осуществляется с помощью кнопок **Back** и **Next**. Выйти из программы можно в любой момент, нажав кнопку **Cancel**.

2. В следующем окне **Select Software** вы можете выбрать компоненты, которые хотите удалить. Флаги для соответствующих зависимостей будут проставлены автоматически.

   В случае, если ранее на этом компьютере из EPM-пакета был установлен какой-либо другой продукт **Dr.Web**, то в список компонентов для удаления войдут и его модули тоже. Поэтому необходимо быть крайне внимательным при выборе, чтобы случайно не удалить те компоненты, которые планируется использовать в дальнейшем.

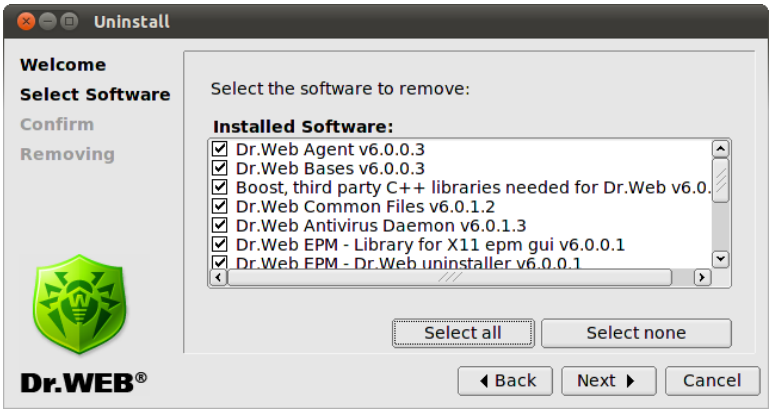


Рис. 11. Окно выбора компонентов для удаления

Нажав на кнопку **Select all**, вы сможете отметить сразу все компоненты. Нажатие на кнопку **Select none** удалит все проставленные флаги.

3. В следующем окне **Confirm** вы увидите все выбранные вами компоненты и сможете принять окончательное решение об их удалении.

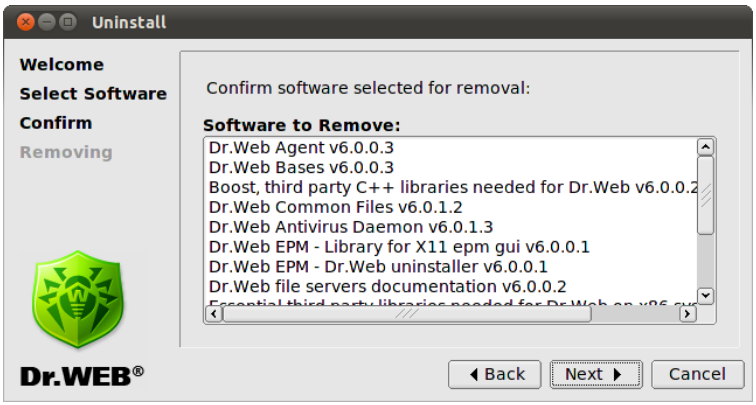


Рис. 12. Окно подтверждения удаления компонентов

4. В последнем окне **Removing** выводится отчет о процессе удаления компонентов программного комплекса в режиме реального времени.

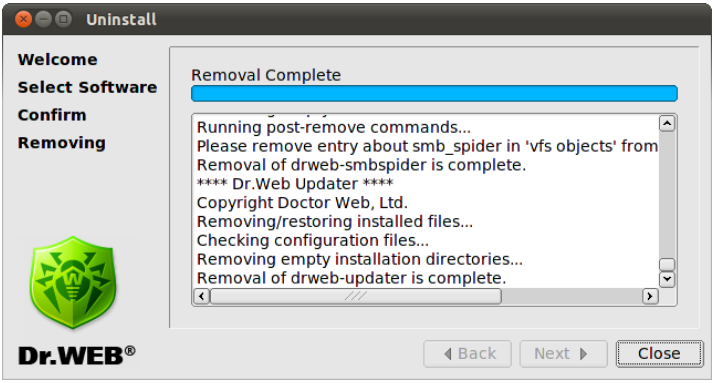


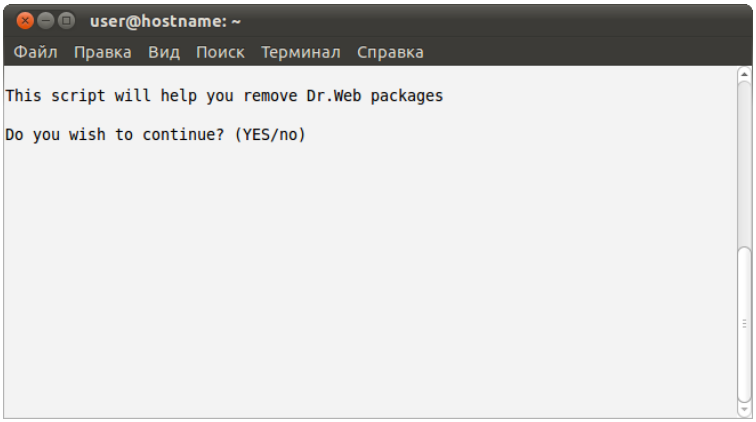
Рис. 13. Окно удаления компонентов программы

5. Нажав на кнопку **Close**, вы закроете окно программы удаления компонентов.

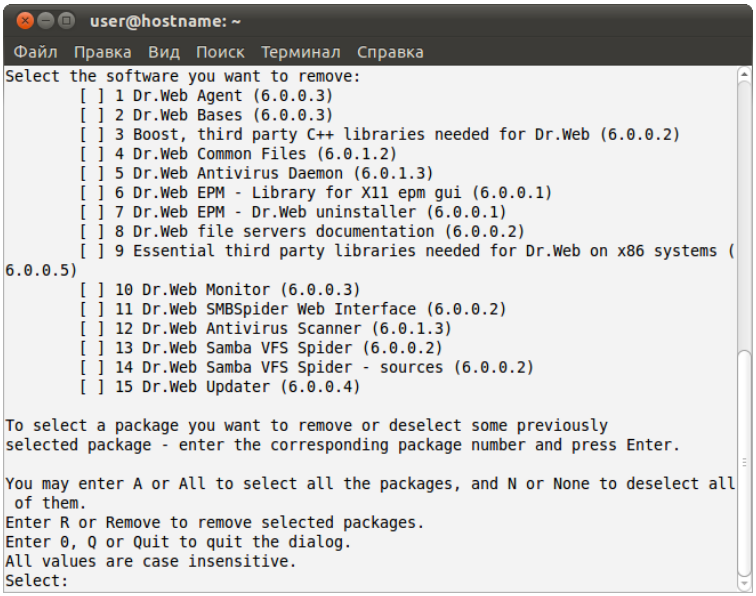
Использование консольного деинсталлятора

Консольный деинсталлятор запускается автоматически в том случае, если не удалось запустить графический деинсталлятор.

Откроется диалоговое окно консольного деинсталлятора.

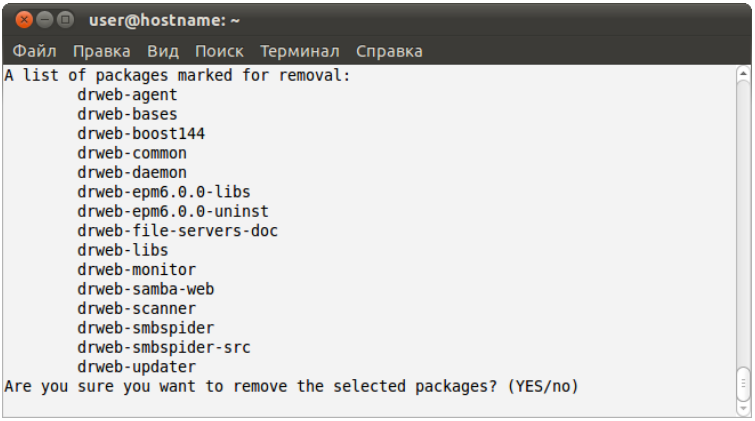


Вам будет предложено выбрать из списка компонентов те, которые вы желаете удалить (следуйте инструкциям на экране).



Для запуска процедуры удаления компонентов вы должны

будете подтвердить сделанный выбор, указав **Y** или **Yes** в строке ввода (значения регистронезависимы) и нажав клавишу ENTER.



Отчет о результатах прохождения каждого из этапов процесса удаления компонентов выводится на консоль в режиме реального времени.

Обновление универсального пакета для UNIX систем

Обновление сочетает в себе процессы установки и удаления. Для обновления программного комплекса **Dr.Web для файловых серверов UNIX** необходимо получить свежую версию продукта, удалить предыдущую версию и установить новую.

При обновлении измененные пользователем конфигурационные файлы, лицензионные ключевые файлы и файлы отчетов различных компонентов программного комплекса сохраняются в соответствующих каталогах.

Установка из нативных пакетов

Вы можете установить **Dr.Web для файловых серверов UNIX** из нативных пакетов для распространенных дистрибутивов **Linux** или операционных систем **Solaris** и **FreeBSD**.

Пакеты находятся в официальном репозитории **Dr.Web** http://officeshield.drweb.com/drweb/. После подключения репозитория к менеджеру пакетов вашей системы, вы можете устанавливать пакеты как любую другую программу из репозитория. Необходимые зависимости будут разрешены автоматически.

После установки пакетов через репозиторий пост-инсталляционный скрипт для автоматической установки лицензионного ключевого файла не будет запущен. Ключевой файл необходимо вручную скопировать в каталог `%bin_dir`.

После обновления через репозиторий все сервисы **Dr.Web** необходимо перезапустить, чтобы обновления вступили в силу.

Ниже приведены инструкции для подключения репозитория **Dr.Web** к поддерживаемым менеджерам пакетов и установки **Dr.Web для файловых серверов UNIX** с помощью консоли.

Все нижеприведенные команды для подключения репозиториев, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами администратора (root), для чего следует воспользоваться командами **sudo** или **su**.

Debian, Ubuntu (apt)

1. Установка:

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

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

или

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

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

```
deb http://officeshield.drweb.com/drweb/debian stable non-free
```

Для установки **Dr.Web для файловых серверов UNIX** выполните команды:

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

2. Удаление:

Для удаления **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 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**.

Установка и удаление пакетов также могут осуществляться с помощью графического менеджера (например, **Synaptic** или **aptitude**).

ALT Linux, PCLinuxOS (apt-rpm)

1. Установка:

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

Для 32-разрядной версии:

```
rpm http://officeshield.drweb.com/drweb/altlinux stable/i386 drweb
```

Для 64-разрядной версии:

```
rpm http://officeshield.drweb.com/drweb/altlinux stable/x86_64 drweb
```

Для установки **Dr.Web для файловых серверов UNIX** выполните команды:

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

2. Удаление:

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

Установка и удаление пакетов также могут осуществляться с помощью графического менеджера (например, **Synaptic** или **aptitude**).

Mandriva (urpmi)

1. Установка:

Загрузите ключ цифровой подписи репозитория с адреса: http://officeshield.drweb.com/drweb/drweb.key и сохраните на диск. Импортируйте ключ с помощью команды

```
rpm --import <путь к ключу репозитория>
```

Откройте файл

http://officeshield.drweb.com/drweb/drweb-i386.urpmi-media

или

http://officeshield.drweb.com/drweb/drweb-x86_64.urpmi-media

и вам будет предложено подключить репозиторий.

Вы также можете подключить репозиторий через командную строку с помощью команды:

```
urpmi.addmedia drweb http://officeshield.drweb.com/drweb/mandriva/stable/i386/
```

или

```
urpmi.addmedia drweb http://officeshield.drweb.com/drweb/mandriva/stable/x86_64/
```

Для установки **Dr.Web для файловых серверов UNIX** выполните команды:

```
urpmi.update drweb
urpmi drweb-file-servers
```

2. Удаление:

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

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

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

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

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

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

Установка и удаление пакетов также могут осуществляться с помощью графического менеджера (например, **rpmdrake**).

Red Hat Enterprise Linux, Fedora, CentOS (yum)

1. Установка:

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

Для 32-разрядной версии:

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

Для 64-разрядной версии:

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

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

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

2. Удаление:

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

```
yum remove drweb-file-servers
```

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**:

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**.

Установка и удаление пакетов также может осуществляться с помощью графического менеджера (например, **PackageKit** или **Yumex**).

SUSE Linux (Zypper)

1. Установка:

Чтобы подключить репозиторий, запустите следующую команду:

```
zypper ar -t YUM http://officeshield.drweb.com/drweb/el5/stable/i386/ drweb
```

или

```
zypper ar -t YUM http://officeshield.drweb.com/drweb/el5/stable/x86_64/ drweb
```

Для установки **Dr.Web для файловых серверов UNIX** выполните команды:

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

2. Удаление:

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

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

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

```
zypper remove drweb*
```

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

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

Установка и удаление пакетов также может осуществляться с помощью графического менеджера (например, **YaST**).

FreeBSD

Установка:

Загрузите архив drweb-file-servers_current-current~freebsd_all.tar.gz с http://officeshield.drweb.com/drweb/freebsd/ports/, распакуйте в отдельный каталог и выполните команду make install для сборки и установки **Dr.Web для файловых серверов UNIX**. При установке **Dr.Web для файловых серверов UNIX** в **FreeBSD** версии 6.1

требуется указать путь к каталогу `/usr/ports/Mk` с помощью параметра командной строки `-I` . В этом каталоге располагается дерево портов.

Пример:

```
tar -xzvf drweb-file-servers-meta_current-current~freebsd_all.tar.gz
make install -I /usr/ports/Mk/
```

Solaris

Установка:

Нативные пакеты для **Solaris** могут быть загружены с публичного FTP-сервера:

ftp://ftp.drweb.com/pub/drweb/unix/release/Solaris/packages

и установлены с помощью утилиты **pkgadd**.

Установка Dr.Web Samba VFS SpIDer из исходных кодов

В случае использования других версий **Samba** либо **Samba** для 64-битных **Linux**-платформ существует возможность собрать **Dr.Web Samba SpIDer** из исходных кодов, входящих в состав пакета `drweb-smbspider-src`. Для этого вам также понадобятся исходные коды вашей **Samba**, которые можно загрузить с сайта **Samba.org** (http://us1.samba.org/samba/ftp/old-versions/).

Для сборки **Dr.Web Samba SpIDer** из исходных кодов необходимо:

- Установить пакет с исходными кодами `drweb-smbspider-src` командой:

```
# drweb-file-servers_[version number]~[название ОС]/drweb-smbspider-src.install.
```

После этого в каталоге `/usr/src/` появится tarball-архив `drweb-smbspider-[version number].src.tar.gz`.

Параметр командной строки `now` позволяет установить компонент, избежав дополнительных манипуляций по подтверждению действий на каждом из этапов установки. При этом следует учесть, что используя этот параметр, вы автоматически соглашаетесь с **Лицензионным Договором** и принимаете его. (Тексты **Лицензионного Договора** на английском и русском языках входят в комплект поставки: файлы `LICENSE` и `LICENSE.ru` соответственно).

- Перейти в каталог `/usr/src/` и распаковать архив командой:

```
# tar -xzvf drweb-smbspider-[version number].src.tar.gz
```

- Перейти в появившийся каталог `drweb-smbspider-[version number].src` и выполнить команду:

```
# ./configure --with-samba-source=<каталог_с_исходными_кодами_Samba>
```

Для успешного выполнения этой команды в системе должны быть установлены макропроцессор `m4`, набор компиляторов `GCC` и утилита `make`.

- Завершить сборку **Dr.Web Samba SpIDer** и установить его командами:

```
# make
# make install
```

Запуск Dr.Web для файловых серверов UNIX

В данном разделе описана процедура запуска **Dr.Web для файловых серверов UNIX** в операционных системах **Linux**, **Solaris** и **FreeBSD**.

ОС Linux и Solaris

Для запуска комплекса необходимо:

1. Зарегистрировать продукт.
2. Скопировать или переместить полученный после регистрации лицензионный ключевой файл с расширением `.key` в каталог с исполняемыми файлами программного комплекса **Dr.Web для файловых серверов UNIX** (по умолчанию `%bin_dir` для UNIX систем). Имя ключевого файла может варьироваться в зависимости от комплекта поставки (подробнее см. в главе Регистрация продукта):
   - Если **Dr.Web для файловых серверов UNIX** был приобретен как самостоятельный продукт, ключевой файл продукта имеет название `drweb32.key`. В таком случае вы можете скопировать данный файл в каталог `%bin_dir`, не изменяя его имени;
   - В случае приобретения **Dr.Web для файловых серверов UNIX** в составе программного комплекса **Dr.Web Enterprise Security Suite**, архив содержит 2 файла: ключевой файл для сервера централизованной защиты **Dr.Web Enterprise Server** (`enterprise.key`) и ключевой файл продукта (`agent.key`). Переименуйте `agent.key` как `drweb32.key` и скопируйте его в каталог `%bin_dir`.

   Если вы хотите использовать ключевой файл, расположенный в каком-либо другом каталоге, либо

имеющий другое имя (например, `agent.key`), то путь к нему должен быть задан в настройках конфигурационного файла `drweb32.ini` значением параметра **`Key`**. При работе в режиме `Standalone` альтернативный путь к ключу должен быть также задан в настройках конфигурационного файла **Dr.Web Agent** `agent.conf` в значении параметра **`LicenseFile`**.

3. Настроить программный комплекс, внеся все необходимые изменения в конфигурационные файлы. Для настройки компонентов обратитесь к соответствующим разделам документации.
4. Вручную исправить `enable`-файл `drwebd`, присвоив переменной `ENABLE` значение `1`. Это позволит запустить **Dr.Web Daemon**. Если запускать **Dr.Web Daemon** не нужно (используется **Dr.Web Daemon**, запущенный на другом компьютере в локальной сети), то для переменной `ENABLE` нужно оставить присвоенное по умолчанию значение `0`.
5. Вручную исправить `enable`-файл **Dr.Web Monitor**, присвоив переменной `ENABLE` значение `1`. Это позволит запустить **Dr.Web Monitor**.

Расположение `enable`-файлов может меняться в зависимости от способа установки **Dr.Web для файловых серверов UNIX**:

- Установка при помощи **универсального пакета для UNIX**:

  Файлы располагаются в каталоге `%etc_dir` и называются
  `drwebd.enable`,
  `drweb-monitor.enable`.

- Установка из **нативных DEB-пакетов**:

  Файлы располагаются в каталоге `%etc_dir/defaults` и называются
  `drwebd`,
  `drweb-monitor`.

- Установка из **нативных RPM-пакетов**:

  Файлы располагаются в каталоге `%etc_dir/sysconfig` и называются
  `drwebd.enable`,
  `drweb-monitor.enable`.

6. Запустить инициализационные скрипты для **Dr.Web Daemon** и **Dr.Web Monitor** либо из консоли, либо воспользовавшись встроенными программными средствами вашей операционной системы. После этого **Dr.Web Monitor** сам автоматически запустит остальные компоненты программного комплекса.

   В случае установки из нативных пакетов в Solaris:

   В процессе установки **Dr.Web для файловых серверов UNIX** система управления сервисами SMF производит попытку запуска компонента **Dr.Web Monitor**. В случае если **Dr.Web Monitor** не может обнаружить лицензионный ключевой файл (например при первой установке комплекса **Dr.Web для файловых серверов UNIX**), он завершает свою работу и переводится SMF в состояние maintenance.

Чтобы запустить **Dr.Web Monitor**, необходимо сбросить состояние maintenance:

- Введите команду

```
# svcs -p <FMRI>
```

  где FMRI - уникальный идентификатор управляемого ресурса, в данном случае - компонента **Dr.Web Monitor**.

- Принудительно завершите процессы из списка, выводящегося при исполнии команды `svcs -p`.

```
# pkill -9 <PID>
```

  где PID - номер процесса, представленного в списке выше.

- Перезапустите **Dr.Web Monitor** командой

```
# svcadm clear <FMRI>
```

При установке **Dr.Web для файловых серверов UNIX** из нативных пакетов в **Solaris**, запуск комплекса производится с помощью системы управления сервисами SMF:

```
# svcadm enable <drweb-monitor>
# svcadm enable <drweb-daemon>
```

Для остановки сервиса введите:

```
# svcadm disable <название сервиса>
```

Модуль **drwebd** может быть запущен в двух режимах:

1. Стандартный запуск посредством скрипта `init`
2. С помощью **Dr.Web Monitor**

При работе во втором режиме необходимо установить значение параметра `ENABLE` в `enable`-файле равным нулю.

ОС FreeBSD

Для запуска комплекса необходимо:

1. Зарегистрировать продукт.
2. Скопировать или переместить полученный после регистрации лицензионный ключевой файл с расширением `.key` в каталог с исполняемыми файлами программного комплекса **Dr.Web для файловых серверов UNIX** (по умолчанию `%bin_dir` для UNIX-систем). Имя ключевого файла может варьироваться в зависимости от комплекта поставки (подробнее см. в главе Регистрация продукта):
   - Если **Dr.Web для файловых серверов UNIX** был приобретен как самостоятельный продукт, ключевой файл продукта имеет название `drweb32.key`. В таком случае вы можете скопировать данный файл в каталог `%bin_dir`, не изменяя его имени;
   - В случае приобретения **Dr.Web для файловых серверов UNIX** в составе программного комплекса **Dr.Web Enterprise Security Suite**, архив содержит 2 файла: ключевой файл для сервера централизованной защиты **Dr.Web Enterprise Server** (`enterprise.key`) и ключевой файл продукта (`agent.key`). Переименуйте `agent.key` как `drweb32.key` и скопируйте его в каталог `%bin_dir`.

   Если вы хотите использовать ключевой файл, расположенный в каком-либо другом каталоге, либо имеющий другое имя (например, `agent.key`), то путь к нему должен быть задан в настройках конфигурационного файла `drweb32.ini` значением параметра **`Key`**. При работе в режиме `Standalone` альтернативный путь к ключу должен быть также задан в настройках конфигурационного файла **Dr.Web Agent** `agent.conf` в значении параметра **`LicenseFile`**.

3. Настроить программный комплекс, внеся все необходимые изменения в конфигурационные файлы. Для настройки компонентов обратитесь к соответствующим разделам документации.
4. Вручную исправить файл `/etc/rc.conf`, добавив в него следующие строки:
   - `drweb_monitor_enable="YES"` – для получения возможности запуска **Dr.Web Monitor**.
   - `drwebd_enable="YES"` – для получения возможности запуска **Dr.Web Daemon**. Если запускать **Dr.Web Daemon** не нужно (используется **Dr.Web Daemon**, запущенный на другом компьютере в локальной сети), то указанную строку можно просто не добавлять в `rc.conf`.
5. Запустить инициализационные скрипты для **Dr.Web Daemon** и **Dr.Web Monitor** либо из консоли, либо воспользовавшись встроенными программными средствами вашей операционной системы. После этого **Dr.Web Monitor** сам автоматически запустит остальные компоненты программного комплекса.

Каждый из компонентов можно запускать и отдельно, но при этом модуль **Dr.Web Agent** должен быть запущен самым первым, так как через него остальные компоненты получают свои настройки.

Операционные системы с SELinux

Чтобы при работающем **SELinux** компоненты **Dr.Web Scanner** и **Dr.Web Daemon** могли успешно функционировать, необходимо скомпилировать политики для работы с соответствующими модулями **drweb-scanner** и **drweb-daemon** или установить значение переменной allow_execheap равным `1`.

Пожалуйста, обратите внимание, что во время компиляции модули политик используют шаблоны, большинство из которых разные в зависимости от дистрибутива **Linux**, его версии, набора политик **SELinux** и пользовательских настроек.

Соответственно, для получения более подробной информации о компиляции модулей политик вы можете обратиться к документации вашего дистрибутива **Linux**.

Чтобы создать необходимые политики:

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

Утилита **policygentool**, входящая в состав пакета **selinux-policy** в **RedHat Enterprise Linux** и **CentOS Linux**, может работать некорректно. В таком случае воспользуйтесь **audit2allow**.

Пример:

Для **Сканера**:

```
# policygentool drweb-scanner /opt/drweb/drweb.real
```

Для **Демона**:

```
# policygentool drweb-daemon /opt/drweb/drwebd.real
```

Вам будет предложено указать несколько общих характеристик домена, после чего для каждого модуля будут созданы три файла: `[module_name].te`, `[module_name].fc` и `[module_name].if`

   - С помощью утилиты **audit2allow**. 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.

В общем случае при использовании в системе демона `audit`, файл журнала располагается в `/var/log/audit/audit.log`. В противном случае, сообщения о запрете операции записываются в файл журнала `/var/log/messages`.

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

Пример:

```
# audit2allow -M -i /var/log/audit/audit.
log drweb
```

В данном примере **`audit2allow`** производит поиск сообщений об отказе в доступе в файле `audit.log`.

Пример:

```
# audit2allow -a -M drweb
```

В данном примере **`audit2allow`** ищет сообщения об отказе в доступе в файлах журналов автоматически.

В обоих случаях в результате работы утилиты создаются два файла: исходный файл политики `drweb.te` и готовый к установке модуль политики `drweb.pp`. Если вы хотите внести изменения в разграничения для работы компонентов **Dr.Web для файловых серверов UNIX**, отредактируйте файл `drweb.te` соответствующим образом и перейдите к пункту 2. Если вносить изменения в

файл политики не требуется, перейдите к пункту 4 для установки модуля политики `drweb.pp`.

2. Используя утилиту **`checkmodule`** создайте бинарное представление (.mod файл) исходного файла локальной политики. Обратите внимание, что для успешной работы этой команды в системе должен быть установлен пакет `checkpolicy`.

   Пример:

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

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

   Пример:

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

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

   Пример:

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

Также для разрешения работы компонентов **Dr.Web Scanner** и **Dr.Web Daemon** возможно, но не рекомендуется, установить значение переменной окружения `allow_execheap` равной 1. Переменная окружения `allow_execheap` позволяет или запрещает исполнение данных в *куче (memory heap)* для всех приложений, запущенных в *неограниченном (unconfined)* домене.

Чтобы установить значение переменной `allow_execheap`, выполните в командной строке:

```
# setsebool -P allow_execheap=1
```

Регистрация продукта

Права на использование программного комплекса **Dr.Web для файловых серверов UNIX** регулируются при помощи специального файла, называемого ключевым файлом. В ключевом файле содержится, в частности, следующая информация:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование продукта;
- другие ограничения (например, по числу защищаемых рабочих станций).

Ключевой файл имеет расширение `key` и при работе комплекса по умолчанию должен находиться в одном каталоге с исполняемыми файлами продукта.

Ключевой файл защищен от редактирования при помощи механизма электронной подписи. Редактирование файла делает его недействительным. Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Коммерческие пользователи, приобретающие **Dr.Web для файловых серверов UNIX** у авторизованных поставщиков продукта, получают лицензионный ключевой файл. Параметры этого ключевого файла, регулирующие права пользователя, установлены в соответствии с лицензионным договором. В такой файл также заносится информация о пользователе и продавце продукта.

Для целей ознакомления с программным комплексом **Dr.Web для файловых серверов UNIX** может быть получен демонстрационный ключевой файл. Такие ключевые файлы обеспечивают полную функциональность основных компонентов комплекса, но имеют ограниченный срок действия и не предполагают оказания поддержки пользователю.

Ключевые файлы поставляются пользователю:

- в виде ключевого файла для рабочей станции `drweb32.key` или в виде ZIP-архива, содержащего этот файл, в случае приобретения **Dr.Web для файловых серверов UNIX** в качестве отдельного продукта.
- в виде zip-архива, содержащего ключевой файл для сервера **Dr.Web Enterprise Server** (`enterprise.key`) и ключевой файл для рабочей станции (`agent.key`) в случае приобретения **Dr.Web для файловых серверов UNIX** в составе программного комплекса **Dr.Web Enterprise Security Suite**.

Ключевой файл может быть получен пользователем:

- по электронной почте в виде ZIP-архива, содержащего файл с расширением `key` (обычно после регистрации на веб-сайте, см. ниже). Необходимо извлечь файл при помощи архиватора данного формата и скопировать/переместить его в каталог с исполняемыми файлами программного комплекса **Dr.Web для файловых серверов UNIX** (по умолчанию `%bin_dir` для UNIX систем);
- в составе дистрибутива продукта;
- на отдельном носителе в виде файла с расширением `key`. В этом случае его необходимо скопировать в вышеуказанный каталог.

Лицензионный ключевой файл высылается пользователям по электронной почте, как правило, после регистрации на специальном веб-сайте (адрес сайта регистрации указан в регистрационной карточке, прилагаемой к продукту). Для получения лицензионного ключевого файла необходимо зайти на указанный сайт, заполнить форму со сведениями о покупателе и ввести в соответствующее поле регистрационный серийный номер (находится на регистрационной карточке). Это процедура активации лицензии, в результате которой для данного серийного номера создается лицензионный ключевой файл. Затем этот файл высылается на указанный при регистрации адрес электронной почты.

Рекомендуется сохранять лицензионный ключевой файл до

истечения срока его действия и использовать его при переустановке или восстановлении программы. В случае утраты лицензионного ключевого файла можно использовать ту же процедуру, что и при активации лицензии: повторно ввести регистрационный серийный номер и адрес электронной почты — и робот вышлет соответствующий указанному серийному номеру ключевой файл.

Регистрация с одним и тем же регистрационным серийным номером допускается не более 25 раз. При необходимости восстановить утерянный лицензионный ключевой файл после 25 регистраций следует разместить запрос на восстановление ключевого файла по адресу в Интернете http://support.drweb.com/request/, указать данные, введенные при регистрации, адрес электронной почты и подробно описать ситуацию. Запрос будет рассмотрен специалистами службы технической поддержки. В случае положительного решения ключевой файл будет либо выдан через автоматизированную систему поддержки пользователей, либо выслан по электронной почте.

Путь к ключу для соответствующего компонента должен быть задан в настройках конфигурационного файла `drweb32.ini` значением параметра **`Key`**.

Пример:

```
Key = %bin_dir/drweb32.key
```

Если ключевой файл, указанный в параметре **`Key`**, не удается прочитать (неверный путь, нет прав), истек срок действия, файл заблокирован или недействителен, то соответствующий компонент завершит свою работу.

Если до истечения срока действия ключевого файла осталось менее двух недель, **Dr.Web Scanner** предупредит об этом при запуске. **Dr.Web Daemon** в такой ситуации может извещать пользователя по электронной почте. Сообщения отправляются для каждого установленного ключевого файла при каждом запуске, перезапуске или перезагрузке **Dr.Web Daemon**, если до истечения срока действия лицензионного ключевого файла осталось менее двух недель. Чтобы воспользоваться этой возможностью, следует настроить параметр **`MailCommand`** в

секции `[Daemon]` файла `drweb32.ini`.

Если требуется расположить ключевой файл в каталоге, отличном от стандартного, то следует также указать его новое расположение в параметре **`LicenseFile`** секции `[StandaloneMode]` конфигурационного файла компонента **Dr.Web Agent** (см. раздел Секция [StandaloneMode]).

Модуль обновления Dr.Web Updater

Для автоматизации получения и установки обновлений вирусных баз **"Доктор Веб"** используется модуль обновления **Dr.Web Updater**. Модуль обновления представляет собой написанный на **Perl** скрипт **update.pl** и находится в каталоге, содержащем исполняемые файлы программного комплекса **Dr.Web для файловых серверов UNIX**.

Модуль обновления **Dr.Web Updater** требует наличия установленного **Perl** 5.8.0 и выше.

Настройки модуля обновления **Dr.Web Updater** хранятся в в секции `[Updater]` главного конфигурационного файла (`drweb32.ini` по умолчанию), который находится в каталоге `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске скрипта обновления.

Для запуска скрипта обновления используйте команду:

```
$ %bin_dir/update.pl [параметры]
```

Перечень параметров, которые можно использовать, см. в разделе Параметры командной строки.

Обновление антивируса и вирусных баз

Компоненты программного комплекса **Dr.Web для файловых серверов UNIX** нуждаются в регулярном обновлении баз данных вирусов.

Вирусные базы **Dr.Web для файловых серверов UNIX** состоят из нескольких файлов с расширением `vdb`. На серверах **Всемирной Системы Обновлений Dr.Web** (**ВСО Dr.Web**) эти

файлы могут храниться также в lzma-архивах. При появлении новых вирусов выпускаются небольшие, размером в один или несколько килобайт, файлы (дополнения), которые содержат фрагменты баз, описывающие эти вирусы.

Дополнения являются едиными для всех поддерживаемых платформ и делятся на два вида:

- ежедневные "горячие" обновления (`drwtoday.vdb`);
- еженедельные регулярные обновления (`drwXXXYY.vdb`), где `XXX` – номер версии антивируса, а `YY` – порядковый номер обновления, начиная с номера `00` (например, файл первого регулярного обновления для версии 6.0.1 именуется `drw60100.vdb`).

"Горячие" обновления выпускаются ежедневно или несколько раз в день для оперативной реакции на новые вирусные угрозы. Особенность установки "горячих" дополнений связана с тем, что в промежутке между выходом регулярных (нумерованных) дополнений файл `drwtoday.vdb` пополняется новыми записями, т.е. его необходимо устанавливать вместо имевшегося ранее. В момент выхода очередного регулярного дополнения все записи из этого файла переписываются в регулярное дополнение, а сам он очищается (выпускается файл `drwtoday.vdb`, не содержащий ни одной записи базы данных).

Следовательно, при обновлении баз вручную необходимо устанавливать все отсутствующие у пользователя регулярные дополнения, после чего переписывать файл "горячего" дополнения вместо имевшегося ранее.

Чтобы подключить дополнение к основным вирусным базам, соответствующий файл должен быть помещен в каталог программного комплекса **Dr.Web для файловых серверов UNIX** (по умолчанию в `%var_dir/bases/`) или иной каталог, определенный в конфигурационном файле.

Сигнатуры, позволяющие обнаруживать и предотвращать распространение вирусоподобных вредоносных программ (рекламных, программ дозвона, программ взлома и т.п.),

поставляются в виде двух отдельных вирусных баз с аналогичной структурой – drwrisky.vdb и drwnasty.vdb. К этим базам также поставляются регулярные обновления dwrXXYYY.vdb и dwnXXYYY.vdb, а также "горячие" обновления dwrtoday.vdb и dwntoday.vdb.

Периодически (в частности, в связи с появлением радикально новых вирусных и антивирусных технологий) выпускаются новые версии пакета с обновленными алгоритмами, заложенными в Антивирусное ядро **Dr.Web Engine**. Одновременно с этим сводятся воедино все ранее выпущенные дополнения баз, и новая версия пакета комплектуется новейшими вирусными базами, содержащими описания всех известных на момент ее выхода вирусов. Как правило, при переходе на новую версию пакета сохраняется преемственность формата баз, т.е. новые вирусные базы могут быть подключены к старому Антивирусному ядру. Однако при этом не гарантируется обнаружение или излечение новых вирусов, для борьбы с которыми потребовались обновленные алгоритмы Антивирусного ядра.

При регулярном получении дополнений вирусные базы пакета приобретает следующую структуру:

- drwebase.vdb – основная база, получаемая вместе с новой версией пакета;
- drwXXXYY.vdb – еженедельные регулярные дополнения вирусных баз;
- drwtoday.vdb – "горячие" дополнения;
- drwnasty.vdb – основная база вредоносных программ, получаемая вместе с новой версией пакета;
- dwnXXXYY.vdb – еженедельные регулярные дополнения базы вредоносных программ;
- dwntoday.vdb – "горячие" дополнения базы вредоносных программ;
- drwrisky.vdb – основная база потенциально опасных программ, получаемая вместе с новой версией пакета;
- dwrXXXYY.vdb – еженедельные регулярные

дополнения базы потенциально опасных программ;

- `dwrtoday.vdb` – "горячие" дополнения базы потенциально опасных программ.

Вирусные базы могут быть автоматически обновлены, используя модуль обновления компонентов **Dr.Web Updater** (`%bin_dir/update.pl`).

После установки **Dr.Web для файловых серверов UNIX** автоматически создаётся файл расписания **cron** (`/etc/cron.d/drweb-update`) для запуска **Dr.Web Updater** каждые 30 минут. Это обеспечивает регулярное обновление и наилучшую защиту.

Настройка cron

Для Linux: при установке компонентов программного комплекса в каталоге `/etc/cron.d/` будет создан пользовательский файл расписания для настройки взаимодействия **cron** с **Dr.Web Updater**.

В создаваемом задании для **crond** используется наиболее распространённый синтаксис vixie cron. Если в вашей системе используется другой демон **cron**, например **dcron**, необходимо вручную создать задание для автоматического запуска модуля обновления **Dr.Web Updater**.

Для FreeBSD и Solaris: необходимо вручную настроить **cron** для работы с **Dr.Web Updater**.

Например, при работе с **FreeBSD** можно добавить в `crontab` пользователя `drweb` следующую строку:

```
*/30 * * * * /usr/local/drweb/update.pl
```

При работе с **Solaris** можно использовать следующий набор команд:

```
# crontab -e drweb
# 0,30 * * * * /opt/drweb/update.pl
```

Обратите внимание, что по умолчанию демон **cron** будет запускать модуль **Dr.Web Updater** с периодичностью раз в 30 минут (в 0 и 30 минут каждого часа). Это может вызывать повышенную нагрузку на сервера **BCO Dr.Web** и приводить к задержке обновления. Чтобы избежать подобной ситуации, рекомендуется изменить моменты запуска, заданные по умолчанию, на произвольные.

Параметры командной строки

Параметр `--help` используется для вывода краткой справки о ключах программы.

Для использования другого конфигурационного файла, полный путь к нему необходимо указать параметром командной строки `--ini`. Если имя конфигурационного файла не задано, используется `%etc_dir/drweb32.ini`.

Пример:

```
$ /opt/drweb/update.pl --ini=/path/to/conf_file
```

Параметр командной строки `--what` позволяет временно переопределить значение параметра **`Section`** при запуске модуля обновления. Значение параметра будет действовать до следующего запуска скрипта. Возможные значения: `scanner` или `daemon`.

Пример:

```
$ /opt/drweb/update.pl --what=Scanner
```

Чтобы просмотреть список всех компонентов продукта, доступных для обновления, нужно указать параметр `--components`.

Пример:

```
$ /opt/drweb/update.pl --components
```

В качестве параметра командной строки также может быть указан `--not-need-reload`. Возможны три варианта его использования:

- Если данный параметр не задан, то по завершении работы скрипта обновления **update.pl** будут перезагружаться все демоны (**Dr.Web Daemon** для программного комплекса **Dr.Web для файловых серверов UNIX**), для которых в процессе обновления был изменен/удален/добавлен хотя бы один компонент;
- Если указать параметр `--not-need-reload`, не задав значения, то по завершении работы модуля обновления **update.pl** ни один из демонов перезагружаться не будет;
- Если при задании параметра `--not-need-reload` в качестве его значения были указаны названия демонов (через запятую, без пробелов, регистр не важен), то соответствующие демоны перезагружаться не будут, а все остальные — будут при наличии обновлений.

Пример:

```
$ /opt/drweb/update.pl --not-need-reload=drwebd
```

Блокирование обновлений для компонентов

Вы можете заблокировать обновления для определенных компонентов **Dr.Web для файловых серверов UNIX**.

Чтобы получить список доступных компонентов, запустите **Dr.Web Updater** с параметром командной строки `--components`.

Пример:

```
# ./update.pl --components

Available Components:
    agent
    drweb          (frozen)
    icapd          (frozen)
    vaderetro_lib
```

Если обновления для компонента заблокированы, такой компонент будет отмечен как замороженный (frozen). Замороженные компоненты не будут обновляться при запуске **Dr.Web Updater**.

Блокирование обновлений

Чтобы заблокировать обновления для определенных компонентов, запустите **Dr.Web Updater** с параметром командной строки `--freeze=<components>`, где `<components>` – список имен компонентов, разделенных запятыми.

Пример:

```
# ./update.pl --freeze=drweb
Updates for component 'drweb' are frozen.
Run command './updater --unfreeze=drweb' to start
updates again.
```

Разблокирование обновлений

Чтобы вновь разрешить обновления для замороженных компонентов, запустите **Dr.Web Updater** с параметром командной строки `--unfreeze=<components>`, где `<components>` – список имен компонентов, разделенных запятыми.

Пример:

```
# ./update.pl --unfreeze=drweb
Updates for component 'drweb' are no longer frozen.
```

Обратите внимание, что размораживание компонента само по себе не приведет к его обновлению.

Восстановление компонентов

При обновлении компонентов **Dr.Web для файловых серверов UNIX**, **Dr.Web Updater** сохраняет в рабочем каталоге их резервные копии. Это позволяет вернуть компонент к предыдущему состоянию в случае каких-либо проблем с обновлением.

Чтобы восстановить компонент к предыдущему состоянию, следует запустить **Dr.Web Updater** с параметром командной строки `--restore=<components>`, где `<components>` - это список имен компонентов, разделенных запятыми.

Пример:

```
# ./update.pl --restore=drweb

Restoring backup for component 'drweb'...
Updates for component 'drweb' are frozen.
Run command './updater --unfreeze=drweb' to start
updates again.

Backup for component 'drweb' has been restored!
Dr.Web (R) restore details:

Following files has been restored:
      /var/drweb/bases/drwtoday.vdb
      /var/drweb/bases/dwntoday.vdb
      /var/drweb/bases/dwrtoday.vdb
      /var/drweb/bases/timestamp
      /var/drweb/updates/timestamp
```

При восстановлении компонент будет автоматически заморожен. Чтобы возобновить обновления для восстановленного компонента, его необходимо разморозить.

Настройки

Настройки модуля обновления компонентов **Dr.Web Updater** хранятся в секции `[Updater]` конфигурационного файла программы (по умолчанию `drweb32.ini`), который размещается в каталоге `%etc_dir`.

Устройство конфигурационного файла и краткое описание правил задания параметров конфигурации приведены в разделе Конфигурационные файлы.

Секция [Updater]

UpdatePluginsOnly = {логический}	Значение `Yes` предписывает модулю не производить обновление **Dr.Web Daemon** и **Dr.Web Scanner**, а

	ограничиться только обновлением плагинов. Значение по умолчанию: **UpdatePluginsOnly** = No
Section = {Daemon | Scanner}	Указывает, из какой секции конфигурационного файла **Dr.Web Updater** берёт настройки, такие как путь к ключевому файлу, путь к вирусным базам и т.п. Возможные значения параметра: Scanner или Daemon. Значение параметра возможно временно переопределить при запуске модуля обновления с помощью параметра командной строки --what. Измененное таким образом значение параметра будет действовать до следующего запуска скрипта. Значение по умолчанию: **Section** = Daemon
ProgramPath = {путь к файлу}	Путь к исполняемому файлу компонента, который будет обновляться. Требуется модулю обновления для получения информации о версии компонента. Значение по умолчанию: **ProgramPath** = %bin_dir/drwebd
SignedReader = {путь к файлу}	Путь к файлу программы чтения подписанных файлов. Значение по умолчанию: **SignedReader** = %bin_dir/read_signed

LzmaDecoderPath = {путь к каталогу}	Путь к каталогу, в котором располагается утилита lzma, используемая для распаковывания lzma-архивов. Значение по умолчанию: **LzmaDecoderPath** = %bin_dir/
LockFile = {путь к файлу}	Путь к файлу, предназначенному для предотвращения совместного использования некоторых файлов на время их обработки модулем обновления. Значение по умолчанию: **LockFile** = %var_dir/run/update.lock
CronSummary = {логический}	Значение Yes предписывает модулю обновления выдавать отчет сессии обновления на стандартный вывод (stdout). Данный режим используется для посылки уведомлений администратору по электронной почте при запуске модуля обновления демоном **cron**. Значение по умолчанию: **CronSummary** = Yes
DrlFile = {путь к файлу}	Путь к специальному файлу, содержащему список серверов обновления **ВСО Dr.Web**. Модуль обновления выбирает сервера обновления из этого списка случайным образом. Подробнее об алгоритме выбора сервера для обновления см. в разделе Процедура обновления Данный файл подписан компанией **Доктор Веб**, не подлежит редактированию пользователем и

	обновляется автоматически. Значение по умолчанию: **DrlFile** = %var_dir/bases/update.drl
CustomDrlFile = {путь к файлу}	Путь к файлу, содержащему альтернативный список серверов обновления **BCO Dr.Web**. Модуль обновления выбирает сервера обновления из этого списка случайным образом. Подробнее об алгоритме выбора сервера для обновления см. в разделе Процедура обновления Данный файл подписан компанией **Доктор Веб**, не подлежит редактированию пользователем и обновляется автоматически. Значение по умолчанию: **CustomDrlFile** = %var_dir/bases/custom.drl
FallbackToDrl = {логический}	Разрешение использовать файл **DrlFile** в том случае, если не удалось подключиться ни к одному из серверов, заданных в файле **CustomDrlFile**. В случае если значение параметра No, файл **DrlFile** не используется. В случае если файл **CustomDrlFile** не существует, обращение к файлу **DrlFile** производится вне зависимости от значения параметра **FallbackToDrl**. Подробнее об алгоритме выбора сервера для обновления см. в разделе Процедура обновления Значение по умолчанию: **FallbackToDrl** = Yes

DrlDir = {путь к каталогу}	Путь к каталогу, содержащему подписанные **Доктор Веб** drl-файлы со списками серверов обновления **BCO Dr.Web** для каждого из плагинов. Значение по умолчанию: **DrlDir** = %var_dir/drl/
Timeout = {числовое значение}	Максимальное время ожидания для загрузки обновлений с **BCO Dr.Web** в секундах. Значение по умолчанию: **Timeout** = 90
Tries = {числовое значение}	Количество попыток установки соединения модулем обновления **Dr.Web Updater** с серверами **BCO Dr.Web** Значение по умолчанию: **Tries** = 3
ProxyServer = {IP-адрес | имя хоста}	Имя или IP-адрес используемого прокси-сервера. Значение по умолчанию: **ProxyServer** =
ProxyLogin = {текст}	Имя пользователя прокси-сервера. Значение по умолчанию: **ProxyLogin** =
ProxyPassword = {текст}	Пароль пользователя прокси-сервера. Значение по умолчанию: **ProxyPassword** =
LogFileName = {syslog | путь к файлу}	Имя файла журнала или syslog, если журнал будет вестись средствами системного сервиса **syslog**

	Значение по умолчанию: **LogFileName** = syslog
SyslogFacility = {метка syslog}	Метка записи при использовании системного сервиса **syslog** Значение по умолчанию: **SyslogFacility** = Daemon
LogLevel = {уровень подробности}	Уровень подробности ведения журнала. Допускается использование следующих уровней: • Quiet • Error • Warning • Info • Debug • Verbose Значение по умолчанию: **LogLevel** = Info
AgentConfPath = {путь к файлу}	Путь к конфигурационному файлу **Dr.Web Agent**. Значение по умолчанию: **AgentConfPath** = %var_dir/agent.conf
ExpiredTimeLimit = {числовое значение}	Количество дней до истечения срока действия лицензии, в течение которых **Dr.Web Updater** будет пытаться обновить лицензионный ключевой файл. Значение по умолчанию: **ExpiredTimeLimit** = 14
ESLockfile = {путь к файлу}	Путь к блокирующему файлу. Если данный файл существует, то **Dr.**

	Web Updater перестает использовать расписания **cron** для обновления. Значение по умолчанию: **ESLockfile** = %var_dir/run/es_updater.lock

Процедура обновления

Обновление происходит следующим образом:

1. Модуль обновления **Dr.Web Updater** читает конфигурационный файл (по умолчанию – drweb32.ini).
2. Из конфигурационного файла используются параметры, находящиеся в секции [Updater] (описание параметров см. выше), а также параметры **EnginePath**, **VirusBase**, **UpdatePath** и **PidFile**.
3. **Dr.Web Updater** выбирает сервер **BCO Dr.Web** для получения обновлений. Выбор сервера обновления происходит следующим образом:
   - Производится чтение файлов со списками серверов, указанных в параметрах **DrlFile** и **CustomDrlFile** конфигурационного файла;
   - Если оба файла отсутствуют, то обновление не происходит;
   - Если существует только один из файлов (указанный в **DrlFile** или **CustomDrlFile**), то используется существующий, вне зависимости от значения, указанного в параметре **FallbackToDrl**;
   - Если существуют оба файла, то в первую очередь проверяются сервера из файла, указанного в **CustomDrlFile**;
   - Если не получилось подключиться ни к одному из серверов, заданных в файле, указанном в **CustomDrlFile**, и значение параметра **FallbackToDrl**=Yes, то проверяются сервера из

файла, указанного в **DrlFile**. В противном случае обновление не происходит.

4. Производятся попытки подключения к случайно выбираемым серверам из списка, содержащегося в файле, до тех пор, пока попытка подключения к серверу не окажется успешной (при подключении **Dr.Web Updater** ожидает ответа от выбранного сервера ответа в течение периода времени, указанного в параметре **Timeout**).
5. Модуль запрашивает с сервера **BCO Dr.Web**, к которому удалось подключиться, список обновлений, а затем lzma-архивы соответствующих баз. В случае отсутствия последних базы скачиваются в виде `vdb`-файлов. Для распаковывания lzma-архивов используется утилита **lzma**, путь к которой (точнее, к каталогу, в котором она располагается) задается значением параметра **LzmaDecoderPath**.
6. Обновления раскладываются по каталогам, как описано в разделе Обновление антивируса и вирусных баз.

Dr.Web Agent

Компонент **Dr.Web Agent** представлен модулем **drweb-agent**. Это постоянно загруженный модуль, который управляет настройками модулей программного комплекса **Dr.Web для файловых серверов UNIX**, определяет политику работы комплекса в зависимости от установленной лицензии и собирает статистику вирусных инцидентов. Эта статистика, в зависимости от режима работы **Dr.Web Agent**, отсылается с заданной периодичностью либо на публичный сервер статистики компании **Доктор Веб**, либо на сервер централизованной защиты, под управлением которого работает **Dr.Web Agent**.

В ходе работы **Dr.Web Agent** может взаимодействовать с другими модулями программного комплекса, обмениваясь с ними различными управляющими сигналами.

Поскольку все компоненты **Dr.Web для файловых серверов UNIX** (кроме **Dr.Web Monitor**) получают свои конфигурационные данные через модуль **drweb-agent**, он должен запускаться перед другими компонентами, непосредственно после **Dr.Web Monitor**.

Пожалуйста, обратите внимание, что если в конфигурационном файле компонента указано несколько параметров с одним именем, то **Dr.Web Agent** их объединяет через запятую. При задании значений параметров в конфигурационных файлах можно использовать обратный слэш "\". В этом случае **Dr.Web Agent** объединит в одну строку все строки, разделённые с помощью обратного слэша. Обратите внимание, что использование пробела после символа слэша не допускается.

Режимы работы

При необходимости продукты компании **"Доктор Веб"** могут быть подключены к корпоративной или частной **Антивирусной**

сети, управляемой комплексом **Dr.Web Enterprise Security Suite** (далее **Dr.Web ESS**). Работа в таком режиме центральной защиты не требует установки дополнительного программного обеспечения или удаления **Dr.Web для файловых серверов UNIX**.

Для обеспечения этой возможности, **Dr.Web Agent** может работать в одном из двух режимов:

- Одиночном (**standalone mode**) режиме, когда защищаемый компьютер не включен в **Антивирусную сеть** и управляется локально. В этом режиме конфигурационные и ключевые файлы находятся на локальных дисках, а **Dr.Web Agent** полностью управляется с защищаемого компьютера. Статистика вирусных инцидентов отсылается на сервер статистики компании **"Доктор Веб"**.
- Режиме центральной защиты (**enterprise mode**), когда защитой компьютера управляет сервер центральной 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. В этом режиме используется лицензионный ключевой файл с центрального сервера защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется. Статистика вирусных инцидентов отсылается на управляющий сервер централизованной защиты.

Чтобы использовать режим центральной защиты

1. Свяжитесь с системным администратором вашей сети, чтобы получить файл с открытым ключом и параметры соединения с центральным сервером защиты.
2. В конфигурационном файле **Dr.Web Agent** (по умолчанию `%etc_dir/agent.conf`) установите значения следующих параметров в секции `[EnterpriseMode]`:
   - Укажите путь к файлу с открытым ключом, полученному от администратора сети, в параметре **`PublicKeyFile`** (обычно `%var_dir/drwcsd.pub`). Этот файл содержит открытый ключ, используемый для зашифрованного соединения с сервером **Dr.**

Web ESS (далее – **Dr.Web Enterprise Server**). Если вы – администратор сети, то вы можете найти этот файл в соответствующем каталоге на **Dr.Web Enterprise Server**.

- Укажите IP-адрес или имя узла **Dr.Web Enterprise Server** в параметре **ServerHost**.
- Укажите номер порта для связи с **Dr.Web Enterprise Server** параметре **ServerPort**.

3. Чтобы включить режим центральной защиты, установите `Yes` в качестве значения параметра **UseEnterpriseMode**.

   В режиме центральной защиты некоторые функции и настройки **Dr.Web для файловых серверов UNIX** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл с центрального сервера защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется.

Для работы **Dr.Web Agent** в режиме центральной защиты должен быть установлен пакет `drweb-agent-es`.

Чтобы **Dr.Web для файловых серверов UNIX** полностью поддерживал режим центральной защиты, **Dr.Web Monitor** также должен работать в режиме центральной защиты. Для подробностей обратитесь к разделу Режимы работы **Dr.Web Monitor**.

Чтобы использовать одиночный (standalone) режим

1. Убедитесь, что все параметры в секции `[StandaloneMode]` конфигурационного файла **Dr.Web Agent** (по умолчанию, `%etc_dir/agent.conf`) установлены корректно.
2. Установите `No` в качестве значения параметра **UseEnterpriseMode** секции `[EnterpriseMode]` конфигурационного файла **Dr.Web Agent**.

При включении этого режима все настройки **Dr.Web для файловых серверов UNIX** будут разблокированы и вы вновь получите доступ ко всем функциям и настройкам **Dr.Web для файловых серверов UNIX**.

Для работы в одиночном режиме **Dr.Web для файловых серверов UNIX** необходим действующий лицензионный ключ. Ключевые файлы, полученные с сервера центральной защиты, не могут быть использованы в этом режиме.

Совместное использование Dr.Web для файловых серверов UNIX и Антивируса Dr.Web для Linux в режиме центральной защиты

Ввиду особенностей реализации, одновременное использование в режиме централизованной защиты **Dr.Web для файловых серверов UNIX** и **Антивируса Dr.Web для Linux**, установленных на одном компьютере, невозможно. Для включения режима централизованной защиты **Dr.Web для файловых серверов UNIX** необходимо перевести **Антивирус Dr.Web для Linux** в режим автономной работы, после чего удалить или переместить в другой каталог файлы `%etc_dir/agent/drweb-cc.amc` и `%etc_dir/agent/drweb-spider.amc`.

Рекомендуется сохранить эти файлы в качестве резервной копии в каталоге, отличном от `%etc_dir/agent`, если в дальнейшем вы планируете перевести перевести **Антивирус Dr.Web для Linux** в режим централизованной защиты. В таком случае, отключите режим централизованной защиты **Dr.Web для файловых серверов UNIX**, копируйте резервные копии файлов `drweb-cc.amc` и `drweb-spider.amc` в каталог `%etc_dir/agent/` и следуйте инструкциям, представленным в руководстве пользователя **Антивируса Dr.Web для Linux**.

Параметры командной строки

Для запуска **Dr.Web Agent** используется следующая команда:

```
drweb-agent [параметры]
```

Dr.Web Agent допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля		
-v	--version	
Описание: Вывод на экран информации о текущей версии **Dr.Web Agent** и завершение работы модуля		
-u	--update-all	
Описание: Запуск процесса обновления для всех компонентов **Dr.Web для файловых серверов UNIX**		
-f	--update-failed	
Описание: Запуск процесса обновления для тех компонентов **Dr.Web для файловых серверов UNIX**, которые не удалось обновить в штатном режиме		
-C	--check-only	
Описание: Проверка корректности конфигурации модуля **Dr.Web Agent**. Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра **Dr.Web Agent**		
-c	--conf	<путь к файлу>
Описание: Использование при запуске указанного конфигурационного файла		

Краткий вариант	Расширенный вариант	Аргументы
-d	--droppwd	
Описание: Сбросить регистрационную информацию (имя пользователя и пароль), используемую **Dr.Web Agent** для доступа к **Dr.Web Enterprise Server**. При следующей попытке соединения с **Dr.Web Enterprise Server** будет запущен процесс регистрации новой станции		
-p	--newpwd	
Описание: Смена имени пользователя и пароля на используемом сервере центральной защиты **Dr.Web Enterprise Server**		
-s	--socket	<путь к файлу>
Описание: Использование компонентом для коммуникации с управляемыми модулями сокета, указанного в аргументе		
-P	--pid-file	<путь к файлу>
Описание: Использование в качестве PID-файла **Dr.Web Agent** файла, указанного в аргументе		
-e	--export-config	<имя приложения>
Описание: Экспорт конфигурации приложения, имя которого указано в аргументе, на **Dr.Web Enterprise Server**. В качестве аргумента следует использовать имя приложения, указанное в заголовке секции Application "<имя приложения>" соответствующего amc-файла (см. раздел Взаимодействие с компонентами программного комплекса). Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра **Dr.Web Agent**. Также он не может быть использован для экспорта конфигурации **Антивируса Dr.Web для Linux**		

Конфигурационный файл

Настройки компонента **Dr.Web Agent** задаются отдельным конфигурационным файлом %etc_dir/agent.conf.

Общие принципы устройства конфигурационных файлов компонентов **Dr.Web для файловых серверов UNIX** и краткое описание правил задания параметров конфигурации приведены в разделе Конфигурационные файлы.

Секция [Logging]

В секции `[Logging]` собраны параметры, управляющие ведением журналов работы компонента **Dr.Web Agent** программного комплекса **Dr.Web для файловых серверов UNIX:**

Секция [Logging]

Level = {уровень подробности}	Уровень подробности сохранения в журнал работы компонента общих событий. Допускается использование следующих уровней: • Quiet • Error • Alert • Info • Debug Значение по умолчанию: **Level** = Info
IPCLevel = {уровень подробности}	Уровень подробности сохранения в журнал работы компонента событий подсистемы IPC. Допускается использование следующих уровней: • Quiet • Error • Alert • Info • Debug

	Значение по умолчанию: **IPCLevel** = Error
SyslogFacility = {метка syslog}	Метка записи при использовании системного сервиса **syslog** Значение по умолчанию: **SyslogFacility** = Daemon
FileName = {syslog | путь к файлу}	Имя файла журнала или syslog, если нужно использовать системный сервис **syslog** Значение по умолчанию: **FileName** = syslog

Секция [Agent]

В секции [Agent] собраны основные настройки компонента **Dr.Web Agent**:

Секция [Agent]

MetaConfigDir = {путь к каталогу}	Расположение файлов мета-конфигурации **Dr.Web Agent**. В файлах мета-конфигурации описываются особенности взаимодействия **Dr.Web Agent** с другими модулями программного комплекса. Содержание файлов мета-конфигурации задается разработчиками **"Доктор Веб"** и не требует редактирования. Значение по умолчанию: **MetaConfigDir** = %etc_dir/agent/
UseMonitor = {логический}	Значение Yes данного параметра, указывает **Dr.Web Agent**, что в составе программного комплекса используется

	Dr.Web Monitor. Значение по умолчанию: **UseMonitor** = Yes
MonitorAddress = {адрес}	Сокет, через который **Dr.Web Agent** взаимодействует с **Dr.Web Monitor** (значение параметра должно совпадать со значением параметра **Address** конфигурационного файла **Dr.Web Monitor**). Значение по умолчанию: **MonitorAddress** = local:%var_dir/ipc/.monitor
MonitorResponseTime = {числовое значение}	Максимальное время отклика **Dr.Web Monitor** в секундах. Если в течение этого времени от **Dr.Web Monitor** не поступает реакции, то предполагается, что он не запущен, и **Dr.Web Agent** больше не предпринимает попыток взаимодействия с **Dr.Web Monitor**. Значение по умолчанию: **MonitorResponseTime** = 5
PidFile = {путь к файлу}	Путь к файлу, в который записывается PID исполняемого модуля drweb-agent при запуске. Значение по умолчанию: **PidFile** = %var_dir/run/drweb-agent.pid

Секция [Server]

В этой секции располагаются параметры, управляющие взаимодействием **Dr.Web Agent** с другими модулями программного комплекса **Dr.Web для файловых серверов UNIX:**

Секция [Server]

Address = {адрес}	Сокет, через который **Dr.Web Agent** взаимодействует с другими модулями программного комплекса. Допускается несколько сокетов, перечисленных через запятую. Значение по умолчанию: **Address** = local:%var_dir/ipc/.agent, inet:4040@127.0.0.1
Threads = {числовое значение}	Количество одновременных потоков drweb-agent. Параметр управляет максимальным количеством одновременных подключений к модулям, передающим **Dr.Web Agent** вирусную статистику. Этот параметр не может быть изменен при перезапуске по сигналу SIGHUP. Если указано значение 0, количество одновременных потоков не ограничивается (не рекомендуется). Значение по умолчанию: **Threads** = 2
Timeout = {числовое значение}	Максимальное время (в секундах) установления соединения между **Dr.Web Agent** и другими компонентами программного комплекса. Если указано значение 0, время установления соединения не

	ограничивается. Значение по умолчанию: **Timeout** = 15

Секция [EnterpriseMode]

В этой секции расположены параметры, управляющие работой **Dr.Web Agent** в режиме **Enterprise:**

Секция [EnterpriseMode]

UseEnterpriseMode = {логический}	При значении Yes данного параметра **Dr.Web Agent** работает в режиме **Enterprise**, при значении No – в режиме **Standalone**. Значение по умолчанию: **UseEnterpriseMode** = No
ComputerName = {текст}	Название этого компьютера в **Антивирусной сети**. Значение по умолчанию: **ComputerName** =
VirusbaseDir = {путь к каталогу}	Путь к каталогу вирусных баз. Значение по умолчанию: **VirusbaseDir** = %var_dir/bases
PublicKeyFile = {путь к файлу}	Путь к файлу открытого ключа для доступа к **Dr.Web Enterprise Server**. Значение по умолчанию: **PublicKeyFile** = %bin_dir/drwcsd.pub
ServerHost = {IP-адрес}	IP-адрес **Dr.Web Enterprise Server**. Значение по умолчанию: **ServerHost** = 127.0.0.1

ServerPort = {числовое значение}	Номер порта доступа к **Dr.Web Enterprise Server**. Значение по умолчанию: **ServerPort** = 2193
CryptTraffic = {Yes | Possible | No}	Шифрование трафика, передаваемого между **Dr.Web Enterprise Server** и **Dr.Web Agent**: • Yes – обязательно шифровать • Possible – если возможно • No – не шифровать Значение по умолчанию: **CryptTraffic** = possible
CompressTraffic = {Yes | Possible | No}	Сжатие трафика, передаваемого между **Dr.Web Enterprise Server** и **Dr.Web Agent**: • Yes – обязательно шифровать • Possible – если возможно • No – не шифровать Значение по умолчанию: **CompressTraffic** = possible
CacheDir = {путь к каталогу}	Путь к каталогу, в котором хранятся служебные файлы: конфигурационные файлы компонентов и файлы, содержащие информацию о правах каждого из приложений, на случай, если **Dr.Web Enterprise Server** по какой-либо причине окажется недоступен, файлы с регистрационной информацией на **Dr.Web Enterprise Server** и т.п. Значение по умолчанию: **CacheDir** = %var_dir/agent

Секция [StandaloneMode]

Настройки **Dr.Web Agent** для одиночного режима работы.

Секция [StandaloneMode]

StatisticsServer = {текст}	URL сервера вирусной статистики. Если URL сервера не указан, то статистика не будет отправляться. Значение по умолчанию: **StatisticsServer** = stat.drweb.com:80/update
StatisticsUpdatePeriod = {числовое значение}	Период обновления статистической информации в минутах. Не может быть меньше 5. Значение по умолчанию: **StatisticsUpdatePeriod** = 10
StatisticsProxy = {IP-адрес | имя хоста}	IP-адрес или имя хоста прокси-сервера для вирусной статистики. Обратите внимание, что если значение параметра не задано, используется значение переменной окружения http_proxy. **Пример**: **StatisticsProxy** = localhost:3128 Значение по умолчанию: **StatisticsProxy** =
StatisticsProxyAuth = {текст}	Строка аутентификации (<имя пользователя>:<пароль>) для доступа к прокси-серверу.

	Пример: **StatisticsProxyAuth** = test:testpwd Значение по умолчанию: **StatisticsProxyAuth** =
UUID = {текст}	Личный идентификатор пользователя на сервере статистики http://stat.drweb.com/. Данный параметр является обязательным для передачи статистики — соответственно, если вы желаете подключить эту возможность, вы должны указать в его значении персональный UUID (в качестве которого обычно используется md5-сумма лицензионного ключевого файла). Значение по умолчанию: **UUID** =
LicenseFile = {список путей к файлам}	Расположение ключевых файлов программного комплекса **Dr.Web для файловых серверов UNIX** (лицензионных или демонстрационных). Пути в списке разделяются запятой Значение по умолчанию: **LicenseFile** = %bin_dir/drweb32.key

Секция [Update]

В этой секции собраны параметры, относящиеся к процессу обновления компонентов программного комплекса **Dr.Web для файловых серверов UNIX** через **Dr.Web Enterprise Server** (подробнее см. в Руководстве администратора антивирусной сети **Dr.Web ESS**):

Секция [Update]

CacheDir = {путь к каталогу}	Каталог, в котором **Dr.Web Agent** временно сохраняет загруженные файлы обновлений. Значение по умолчанию: **CacheDir** = %var_dir/updates/cache
Timeout = {числовое значение}	Максимальное время обработки **Dr.Web Agent** полученных обновлений в секундах. Если указано значение 0, время обработки не ограничивается. Значение по умолчанию: **Timeout** = 120
RootDir = {путь к каталогу}	Путь к корневому каталогу. Значение по умолчанию: **RootDir** = /

Запуск

Обратите внимание, что в процессе работы установочного скрипта при выборе соответствующей возможности в диалоге все сервисы, включая **Dr.Web Agent**, будут запущены автоматически.

В процессе запуска **Dr.Web Agent** при установках по умолчанию осуществляются следующие действия:

- производится поиск и загрузка конфигурационного файла; если файл не найден, то загрузка прекращается;
- если в файле конфигурации заданы параметры секции `[EnterpriseMode]` (и программный комплекс **Dr.Web для файловых серверов UNIX** работает в составе **Антивирусной сети**), **Dr.Web Agent** запускается в режиме **Enterprise**. В противном случае, если в файле настроек заданы параметры секции `[Standalone]`, **Dr.Web Agent** запускается в одиночном режиме. Если параметры секции `[Standalone]` также не заданы, то загрузка **Dr.Web Agent** прекращается;
- создается сокет для взаимодействия с другими модулями программного комплекса. В случае TCP-соединения подключений может быть несколько (загрузка продолжается, если удалось создать хотя бы одно из них). Если используется UNIX-сокет, то он может быть создан только тогда, когда каталог, содержащий его, доступен на запись и чтение пользователю, с чьими правами работает модуль **drweb-agent**. Если ни один сокет не может быть создан, загрузка **Dr.Web Agent** прекращается.

Дальнейший процесс загрузки **Dr.Web Agent** зависит от того, в каком режиме он работает.

Если **Dr.Web Agent** работает в режиме **Enterprise**:

- производится соединение с **Dr.Web Enterprise Server**, используемым в **Антивирусной сети**. Если при первом подключении сервер недоступен, либо **Dr.Web Agent** не удалось авторизоваться, **Dr.Web Agent** завершает свою работу. Если ранее **Dr.Web Agent** уже работал с данным сервером, но в данный момент он недоступен (например, в случае проблем с соединением), **Dr.Web Agent** использует резервные копии конфигурационных файлов, полученных от сервера во время предыдущего подключения. Данные файлы зашифрованы и не предназначены для правки пользователем. Попытка изменить их вручную приведёт к их неработоспособности;

- если соединение успешно установлено, происходит получение лицензионных ключей и настроек компонентов программного комплекса с сервера централизованной защиты. После завершения этой операции **Dr.Web Agent** готов к работе.

Если **Dr.Web Agent** работает в режиме **Standalone**:

- загружаются файлы мета-конфигурации компонентов программного комплекса. В файлах мета-конфигурации описываются особенности взаимодействия **Dr.Web Agent** с компонентами. Расположение файлов мета-конфигурации берется из параметра **MetaConfigDir** секции настроек `[Agent]` файла конфигурации **Dr.Web Agent**. После завершения этой операции **Dr.Web Agent** готов к работе.

Взаимодействие с компонентами программного комплекса

Взаимодействие с компонентами программного комплекса осуществляется с помощью `amc`-файлов. В этих файлах описывается конфигурация компонентов и параметры, значения которых **Dr.Web Agent** выдает компонентам.

Описание каждого компонента содержится в секции `Application "имя_компонента"`. В конце секции обязательно должно быть поставлено `EndApplication`. В описании компонента должны присутствовать следующие параметры:

- **id**: идентификатор компонента на используемом **Dr.Web Enterprise Server**;
- **ConfFile**: путь к конфигурационному файлу компонента;
- **Components**: описание компонентов. В конце описания ставится **EndComponents**. Для каждого из компонентов указываются: его название и через пробел — список секций конфигурационного файла и параметров в них, которые требуются компоненту для нормальной работы.

Секции и параметры перечисляются через запятую.
Для описания параметров необходимо указывать полный путь к ним (например, `/Quarantine/DBISettings`), а для описания секций достаточно указания имени секции (например, `General`).
Символ обратного слэша "\" используется для экранирования переводов строки.
Если компоненту нужны все настройки из конфигурационного файла, достаточно указать вместо перечня секций и/или параметров путь "`/*`".

Пример amc-файла Dr.Web Samba VFS SpIDer для Linux:

```
Application "Dr.Web (R) SMB_SPIDER"
    ID          110
    ConfFile     "/etc/drweb/smb_spider.conf"
    Components
        smb_spider      DaemonCommunication,
Scanning, Actions, Logging
    EndComponents
EndApplication
```

Интеграция с Dr.Web Enterprise Security Suite

Возможны следующие ситуации, в которых требуется интегрировать программный комплекс **Dr.Web для файловых серверов UNIX** с **Антивирусной сетью** под управлением **Dr.Web ESS**:

- первоначальная установка и настройка **Dr.Web для файловых серверов UNIX** в уже работающей **Антивирусной сети** под управлением **Dr.Web ESS**;
- встраивание работающего UNIX-сервера с установленным и настроенным программным комплексом **Dr.Web для файловых серверов UNIX** в **Антивирусную сеть** под

управлением **Dr.Web ESS**.

Для того, чтобы **Dr.Web для файловых серверов UNIX** мог работать в составе **Антивирусной сети** под управлением **Dr.Web ESS**, необходимо настроить компоненты **Dr.Web Agent** и **Dr.Web Monitor** для работы в режиме **Enterprise** и зарегистрировать комплекс на сервере централизованной защиты **Dr.Web Enterprise Server**.

В соответствии с политикой подключения новых станций (подробнее см. Руководство администратора Антивирусной сети **Dr.Web ESS**), подключить **Dr.Web для файловых серверов UNIX** к **Dr.Web Enterprise Server** можно двумя способами:

- создав учетную запись на сервере автоматически;
- создав учетную запись на сервере вручную.

Настройка компонентов для работы в режиме Enterprise

После установки для запуска в режиме **Enterprise** необходимо вручную внести изменения в локальные конфигурационные файлы **Dr.Web Agent** и **Dr.Web Monitor**.

Для Dr.Web Agent

В секции `[EnterpriseMode]` конфигурационного файла **Dr.Web Agent** `%etc_dir/agent.conf` установите следующие значения параметров:

- **`UseEnterpriseMode`** = `Yes`;
- **`PublicKeyFile`** = `%var_dir/drwcsd.pub` (открытый ключ шифрования для доступа к **Dr.Web Enterprise Server**. Администратор должен самостоятельно взять данный файл из соответствующего каталога **Dr.Web Enterprise Server** и разместить его по указанному пути);
- **`ServerHost`** = IP-адрес или имя хоста **Dr.Web Enterprise Server**;
- **`ServerPort`** = порт **Dr.Web Enterprise Server** (`2193`

по умолчанию).

Для Dr.Web Monitor

В секции `[Monitor]` конфигурационного файла **Dr.Web Monitor** `%etc_dir/monitor.conf` установите следующие значения параметров:

- **`UseEnterpriseMode`** = `Yes`.

Автоматическое создание учетной записи

При автоматическом создании учетной записи:

- при первом запуске в режиме **Enterprise** **Dr.Web Agent** запрашивает регистрационные данные (идентификатор станции и пароль) у **Dr.Web Enterprise Server**;
- если на **Dr.Web Enterprise Server** установлен режим "**Ручное подтверждение доступа**" (режим по умолчанию, см. Руководство администратора Антивирусной сети **Dr.Web ESS**), то администратору в течение одной минуты с момента запроса необходимо подтвердить регистрацию новой станции через веб-интерфейс **Центра управления Dr.Web**;
- после первого подключения **Dr.Web Agent** записывает хэш идентификатора станции и пароля пользователя в файл с названием `pwd`. Данный файл создаётся в каталоге, заданном значением параметра **`CacheDir`** секции `[EnterpriseMode]` (по умолчанию `%var_dir/agent/`);
- в дальнейшем данные из этого файла используются для подключения программного комплекса **Dr.Web для файловых серверов UNIX** к **Dr.Web Enterprise Server**;
- удаление файла с паролем приведет к повторному запросу регистрационных данных у **Dr.Web Enterprise Server** при следующем запуске **Dr.Web Agent**.

Создание учетной записи на сервере вручную

Для создания учетной записи на сервере вручную:

- Создайте учетную запись на сервере с указанием идентификатора станции и пароля (см. Руководство администратора Антивирусной сети **Dr.Web ESS**);
- Запустите **Dr.Web Agent** с параметром командной строки `--newpwd` (или `-p`) и введите идентификатор и пароль. Хэш идентификатора станции и пароля пользователя записывается в файл с названием `pwd`. Данный файл создаётся в каталоге, путь к которому задается значением параметра **`CacheDir`** секции `[EnterpriseMode]` (по умолчанию `%var_dir/agent/`);
- В дальнейшем данные из этого файла используются для подключения **Dr.Web для файловых серверов UNIX** к **Dr.Web Enterprise Server**;
- Удаление файла с паролем приведет к необходимости повторить процедуру регистрации при следующем запуске **Dr.Web Agent**.

Задание конфигурации компонентов через Центр Управления Dr.Web

Через веб-интерфейс **Центра Управления Dr.Web** можно управлять настройкой конфигурации компонентов **Dr.Web для файловых серверов UNIX** и **Dr.Web Daemon** (антивирусного модуля, входящего в базовый пакет **Dr.Web**).

В поставку **Dr.Web ESS** включены стандартные конфигурационные файлы компонентов **Dr.Web для файловых серверов UNIX** и **Dr.Web Daemon** для основных UNIX-платформ: **Linux**, **FreeBSD** и **Solaris**. Соответственно, при настройке компонентов задание значений параметров происходит в этих файлах через веб-интерфейс **Центра Управления Dr.Web**. Затем каждый раз при запуске какого-либо из компонентов **Dr.Web Agent** запрашивает и получает

конфигурацию от сервера централизованной защиты **Dr.Web Enterprise Server**.

Экспорт существующей конфигурации на сервер

При помощи **Dr.Web Agent**, работающего в режиме **Enterprise**, возможно автоматически экспортировать конфигурацию компонентов на **Dr.Web Enterprise Server**. Для этого необходимо экспортировать конфигурацию параметром командной строки `--export-config` (или `-e`) с указанием названия компонента (`DAEMON`, `SMB_SPIDER`).

Пример:

```
# %bin_dir/drweb-agent --export-config SMB_SPIDER
```

Запуск комплекса

Чтобы запустить комплекс:

- Запустите **Dr.Web Monitor** на локальной станции:

  Для **Linux** и **Solaris**:

  ```
  # /etc/init.d/drweb-monitor start
  ```

  Для **FreeBSD**:

  ```
  # /usr/local/etc/rc.d/00.drweb-monitor.sh start
  ```

Работа с вирусной статистикой

При работе программного комплекса **Dr.Web для файловых серверов UNIX** с подключенным антивирусным модулем может производиться сбор сведений о вирусных событиях.

Собранная информация передается на сервер статистики **"Доктор Веб"** (http://stat.drweb.com/), либо на сервер централизованной защиты **Dr.Web Enterprise Server**, если **Dr.Web Agent** работает в режиме **Enterprise**.

Для соединения **Dr.Web Agent** с сервером статистики **"Доктор Веб"** необходим идентификатор пользователя – `UUID`. По умолчанию в качестве `UUID` используется `md5`-хэш от ключевого файла. Также вы можете получить персональный `UUID`, обратившись в службу поддержки. Такой `UUID` указывается в файле конфигурации **Dr.Web Agent** (параметр **`UUID`** в секции `[StandaloneMode]`).

Статистика собирается только для тех модулей **Dr.Web**, которые получают настройки от **Dr.Web Agent**. Информация о том, как настроить получение настроек от **Dr.Web Agent**, приведена в описании каждого модуля.

По адресу http://stat.drweb.com/ можно ознакомиться как с результатами обработки статистических данных по вашему серверу, так и с обобщенной статистической информацией по всем серверам, обслуживаемым антивирусными продуктами **Dr.Web** для ОС **UNIX** либо программным комплексом **Dr.Web для файловых серверов UNIX** с подключенным антивирусным модулем.

В случае если работа ведется в режиме централизованной защиты, со статистикой можно ознакомиться также и на специальной странице **Центра управления Dr.Web**. Однако и в этом случае вся статистика, собранная сервером централизованной защиты **Dr.Web Enterprise Server**, также передается им на сервер статистики **"Доктор Веб"** в обобщенном виде для всей **Антивирусной сети**.

Результаты обработки содержат сведения о наиболее часто обнаруживаемых вирусах (для обобщенной статистики только в виде процента от общей суммы, а для индивидуальной – и в виде количества обнаруженных вирусов) за определенный период.

Сведения могут представляться как в формате HTML, так и в виде файла с XML-разметкой. Последний вариант особенно удобен, если предполагается публикация полученных данных на веб-сайте, поскольку позволяет предварительно преобразовать данные в соответствии с дизайном сайта и концепцией представления информации на нем.

Для получения обобщенной статистики по всем обслуживаемым серверам откройте в веб-браузере страницу http://stat.drweb.com/. На странице представлен список обнаруженных вирусов на обслуживаемых серверах (в порядке убывания частоты встречаемости) с указанием для каждого из них количества обнаружений в процентной форме. Внешний вид страницы может различаться в зависимости от используемого веб-браузера.

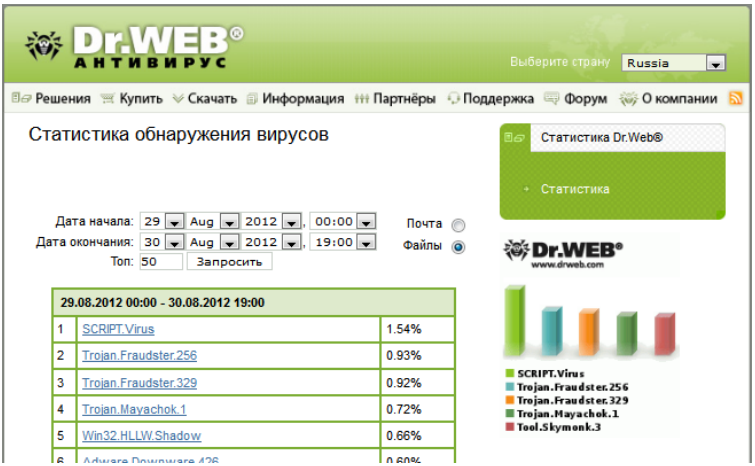


Рис. 14. Вирусная статистика

Вы можете изменить параметры запроса и повторить его:

- Установите переключатель в положение **Почта** или **Файлы** для получения статистики по вирусам, найденным в почтовых сообщениях или файлах.
- В раскрывающихся списках **Дата начала** и **Дата** окончания установите время и дату начала и окончания

периода, за который требуется статистика.

- Введите в поле **Top** количество строк в таблице (будут представлены только наиболее часто встречающиеся вирусы).
- Нажмите на кнопку **Запросить**.

Файл с обобщенной статистикой в формате XML находится по адресу http://info.drweb.com/export/xml/top/.

Пример такого файла приведен ниже:

```
<drwebvirustop period="24" top="5"
  vdbaseurl="http://info.drweb.com/
virus_description/"
  updatedutc="2009-06-09 09:32:02">
 <item>
  <vname>Win32.HLLM.Netsky</vname>
  <dwvlid>62083</dwvlid>
  <place>1</place>
  <percents>34.201062139103</percents>
 </item>
 <item>
  <vname>Win32.HLLM.MyDoom</vname>
  <dwvlid>9353</dwvlid>
  <place>2</place>
  <percents>25.1303270912579</percents>
 </item>
 <item>
  <vname>Win32.HLLM.Beagle</vname>
  <dwvlid>26997</dwvlid>
  <place>3</place>
  <percents>13.4593034783378</percents>
 </item>
 <item>
  <vname>Trojan.Botnetlog.9</vname>
  <dwvlid>438003</dwvlid>
  <place>4</place>
  <percents>7.86446592583328</percents>
 </item>
 <item>
  <vname>Trojan.DownLoad.36339</vname>
  <dwvlid>435637</dwvlid>
  <place>5</place>
  <percents>7.31494163115527</percents>
 </item>
</drwebvirustop>
```

В данном файле используются следующие атрибуты:

- `period` – продолжительность времени сбора статистики (в часах);
- `top` – количество представленных в таблице наиболее часто встречающихся вирусов;
- `updatedutc` – время последнего обновления статистики;
- `vname` – наименование вируса;
- `place` – место в статистике;
- `percents` – процент от общего числа обнаружений.

Пользователь не может задать продолжительность периода сбора статистики и размер выборки.

Для получения персональной статистики откройте страницу http://stat.drweb.com/view/<UUID>, где `<UUID>` – это md5-хэш ключевого файла пользователя. Страница персональной статистики имеет формат, аналогичный формату страницы обобщенной статистики, за исключением того, что для персональной статистики указывается также количество обнаруженных вирусов, а не только процент от общего количества.

Файл с персональной статистикой в формате XML находится по адресу http://stat.drweb.com/xml/<UUID>, где `<UUID>` – это md5-хэш ключевого файла пользователя.

Ниже приводится сокращенный пример такого файла:

```
<drwebvirustop period="24" top="2"
user="<UUID>"
  lastdata="2005-04-12 07:00:00+04">
 <item>
  <caught>69</caught>
  <percents>24.1258741258741</percents>
  <place>1</place>
  <vname>Win32.HLLM.Netsky.35328</vname>
 </item>
 <item>
  <caught>57</caught>
  <percents>19.9300699300699</percents>
  <place>2</place>
  <vname>Win32.HLLM.MyDoom.54464</vname>
 </item>
</drwebvirustop>
```

В данном файле используются следующие атрибуты:

- `period` – продолжительность времени сбора статистики (в часах);
- `top` – количество представленных в таблице наиболее часто встречающихся вирусов;
- `user` – идентификатор пользователя;
- `lastdata` – время последнего получения данных от пользователя;
- `vname` – наименование вируса;
- `place` – место в статистике;
- `caught` – количество обнаружений данного вируса;
- `percents` – процент от общего числа обнаружений.

Как и в случае запроса обобщенной статистики, пользователь не может задать продолжительность периода сбора статистики и размер выборки.

Dr.Web Monitor

Компонент **Dr.Web Monitor** представлен модулем **drweb-monitor** и предназначен для повышения отказоустойчивости всего программного комплекса **Dr.Web для файловых серверов UNIX**. Он осуществляет запуск всех модулей, подгружая при необходимости их дополнительные компоненты. Если запустить какой-либо модуль не удалось, **Dr.Web Monitor** повторяет попытку. Количество попыток и время между ними определяются настройками компонента.

После того, как все модули были загружены, **Dr.Web Monitor** осуществляет постоянный контроль их работы. **Dr.Web Monitor** может обмениваться с этими модулями различными управляющими сигналами. В случае сбоя какого-либо модуля или одного из его компонентов **Dr.Web Monitor** перезапускает его. Максимальное количество попыток перезапуска и время между ними также определяются настройками **Dr.Web Monitor**. При возникновении неполадок в работе какого-либо модуля **Dr.Web Monitor** одним из доступных ему способов оповещает об этом администратора.

Dr.Web Monitor может взаимодействовать с компонентом **Dr.Web Agent**, обмениваясь с ним управляющими сигналами.

Режимы работы

При необходимости продукты компании **"Доктор Веб"** могут быть подключены к корпоративной или частной **Антивирусной сети**, управляемой комплексом **Dr.Web ESS**. Работа в таком режиме центральной защиты не требует установки дополнительного программного обеспечения или удаления **Dr.Web для файловых серверов UNIX**.

Для обеспечения этой возможности, **Dr.Web Monitor** может работать в одном из двух режимов:

- Одиночном (**standalone mode**) режиме, когда защищаемый компьютер не включен в **Антивирусную**

сеть и управляется локально. В этом режиме конфигурационные и ключевые файлы находятся на локальных дисках, **Dr.Web Monitor** полностью управляется с защищаемого компьютера, а все необходимые модули **Dr.Web** запускаются в соответствии с локальными настройками **Dr.Web Monitor**.

- Режиме центральной защиты (**enterprise mode**), когда защитой компьютера управляет сервер центральной защиты **Dr.Web Enterprise Server**. 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. В этом режиме используется лицензионный ключевой файл, получаемый от сервера центральной защиты **Dr.Web Enterprise Server**. Персональный лицензионный ключевой файл на локальном компьютере не используется.

Чтобы использовать режим центральной защиты

1. Свяжитесь с системным администратором вашей сети чтобы получить файл с открытым ключом и параметры соединения с центральным сервером защиты.
2. В конфигурационном файле **Dr.Web Monitor** (по умолчанию `%etc_dir/monitor.conf`) установите `Yes` в качестве значения параметра **`UseEnterpriseMode`**.

   В режиме центральной защиты некоторые функции и настройки **Dr.Web для файловых серверов UNIX** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл с центрального сервера защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется.

Чтобы **Dr.Web для файловых серверов UNIX** полностью поддерживал режим центральной защиты, **Dr.Web Agent** также должен работать в режиме центральной защиты. Для подробностей обратитесь к разделу Режимы работы **Dr.Web Agent**.

Чтобы использовать одиночный (standalone) режим

1. Убедитесь, что все необходимые модули, указанные в параметре **RunAppList** в секции [Monitor] конфигурационного файла **Dr.Web Monitor** (по умолчанию %etc_dir/monitor.conf), установлены и настроены корректно.
2. Установите No в качестве значения параметра **UseEnterpriseMode** секции [Monitor] конфигурационного файла **Dr.Web Monitor**.

   При включении этого режима все настройки **Dr.Web для файловых серверов UNIX** будут разблокированы, и вы вновь получите доступ ко всем функциям и настройкам **Dr.Web для файловых серверов UNIX** .

Для работы в одиночном режиме **Dr.Web для файловых серверов UNIX** необходим действующий лицензионный ключ. Ключевые файлы, полученные от сервера центральной защиты **Dr.Web Enterprise Server**, не могут быть использованы в этом режиме.

Параметры командной строки

Для запуска **Dr.Web Monitor** используется следующая команда:

```
drweb-monitor [параметры]
```

Dr.Web Monitor допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля		
-v	--version	
Описание: Вывод на экран информации о текущей версии **Dr.Web Monitor** и завершение работы модуля		
-u	--update	
Описание: Запуск процесса обновления для всех компонентов **Dr.Web для файловых серверов UNIX**		
-C	--check-only	
Описание: Проверка корректности конфигурации модуля **Dr.Web Monitor**. Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра **Dr.Web Monitor**		
-A	--check-all	<путь к файлу>
Описание: Проверка корректности конфигурации всех компонентов **Dr.Web для файловых серверов UNIX**		
-c	--conf	<путь к файлу>
Описание: Использование при запуске указанного конфигурационного файла		

Краткий вариант	Расширенный вариант	Аргументы
-r	--run	<имя приложения>[, <имя приложения>,...]
Описание: Запуск указанных приложений. В качестве аргументов следует использовать имена приложений, указанных в заголовке секции Application "<имя приложения>" соответствующего mmc-файла (см. раздел Взаимодействие с компонентами программного комплекса). Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра **Dr.Web Monitor**		

Пример использования:

```
drweb-monitor -r AGENT
```

Конфигурационный файл

Настройки компонента **Dr.Web Monitor** задаются отдельным конфигурационным файлом `%etc_dir/monitor.conf`.

Устройство конфигурационного файла и краткое описание правил задания параметров конфигурации приведены в разделе Конфигурационные файлы.

Секция [Logging]

В секции `[Logging]` собраны параметры, управляющие ведением журналов работы компонента **Dr.Web Monitor** программного комплекса **Dr.Web для файловых серверов UNIX:**

Секция [Logging]

Level = {уровень подробности}	Уровень подробности сохранения в журнал работы компонента общих событий. Допускается использование следующих уровней: • Quiet • Error • Alert • Info • Debug Значение по умолчанию: **Level** = Info
IPCLevel = {уровень подробности}	Уровень подробности сохранения в журнал работы компонента событий подсистемы IPC. Допускается использование следующих уровней: • Quiet • Error • Alert • Info • Debug Значение по умолчанию: **IPCLevel** = Error

SyslogFacility = {метка syslog}	Метка записи при использовании системного сервиса **syslog** Значение по умолчанию: **SyslogFacility** = Daemon
FileName = {syslog | путь к файлу}	Имя файла журнала или syslog, если нужно использовать системный сервис **syslog** Значение по умолчанию: **FileName** = syslog

Секция [Monitor]

В секции [Monitor] собраны основные настройки компонента **Dr.Web Monitor:**

Секция [Monitor]

RunForeground = {логический}	Значение Yes запрещает **Dr.Web Monitor** переходить в режим демона, т. е. становиться фоновым процессом без управляющего терминала. Эта возможность может быть использована некоторыми средствами мониторинга (например, **daemontools**). Значение по умолчанию: **RunForeground** = No
User = {текст}	Имя пользователя, с правами которого запускается **Dr.Web Monitor**. Значение по умолчанию: **User** = drweb
Group = {текст}	Имя пользовательской группы, с правами которой запускается **Dr.Web Monitor**.

	Значение по умолчанию: **Group** = drweb
PidFileDir = {путь к каталогу}	Имя каталога, содержащего файл, в который при запуске **Dr.Web Monitor** записывается информация об идентификаторе его процесса (PID). Значение по умолчанию: **PidFileDir** = %var_dir/run/
ChDir = {путь к каталогу}	Смена активного каталога при запуске **Dr.Web Monitor**. Если значение параметра задано, то при запуске **Dr.Web Monitor** делает активным каталог, указанный в значении этого параметра. Если значение параметра не задано, то смены активного каталога не происходит. Значение по умолчанию: **ChDir** = /
MetaConfigDir = {путь к каталогу}	Путь к каталогу с файлами мета-конфигурации. В этих файлах задаются параметры работы **Dr.Web Monitor** с модулями программного комплекса. Содержание файлов мета-конфигурации задается разработчиками программного продукта и не требует редактирования. Значение по умолчанию: **MetaConfigDir** = %etc_dir/monitor/
Address = {адрес}	Сокет, через который **Dr.Web Monitor** взаимодействует с другими модулями антивируса.

	Значение по умолчанию: **Address** = local:%var_dir/ipc/.monitor
Timeout = {числовое значение}	Максимальное время установления соединения между **Dr.Web Monitor** и другими компонентами программного комплекса в секундах. Значение по умолчанию: **Timeout** = 5
TmpFileFmt = {текст}	Шаблон имени временных файлов **Dr.Web Monitor**. Формат шаблона: путь_к_файлу.XXXXXX, где X - произвольный символ (буква или цифра) в именах создаваемых временных файлов. Значение по умолчанию: **TmpFileFmt** = %var_dir/msgs/tmp/monitor.XXXXXX
RunAppList = {текст}	Список модулей, запускаемых **Dr.Web Monitor**. Названия модулей отделяются друг от друга запятыми. Обратите внимание, что при удалении какого-либо модуля из системы его название не удаляется из списка RunAppList автоматически и должно быть удалено вручную. В противном случае **Dr.Web Monitor** не сможет запуститься сам и запустить остальные компоненты. Значение по умолчанию: **RunAppList** = AGENT
UseEnterpriseMode = {логический}	При значении Yes данного параметра список модулей, запускаемых **Dr.Web**

	Monitor, берется не из параметра **RunAppList**, а от модуля **Dr.Web Agent**. Значение по умолчанию: **UseEnterpriseMode** = No
RecoveryTimeList = {список числовых значений}	Временные промежутки между попытками перезапуска "зависших" приложений в секундах. Для параметра можно задать несколько значений, перечислив их через запятую. Первая попытка перезагрузки приложения производится через время, указанное первым значением параметра, вторая – через время, указанное вторым и т.д. Значение по умолчанию: **RecoveryTimeList** = 0,30,60
InjectCmd = {текст}	Команда для отсылки отчетов. Обратите внимание, что для отправки сообщений на адрес, отличный от root@localhost, надо в команде указать действительный адрес. Значение по умолчанию: **InjectCmd** = "/usr/sbin/sendmail -t"
AgentAddress = {адрес}	Сокет, через который **Dr.Web Monitor** взаимодействует с **Dr.Web Agent** (значение параметра должно совпадать со значением параметра **Address** конфигурационного файла **Dr.Web Agent**). Значение по умолчанию: **AgentAddress** = local:%var_dir/ipc/.agent

AgentResponseTime = {числовое значение}	Максимальное время отклика модуля **Dr.Web Agent** в секундах Если в течение этого времени от модуля не поступает ответа, то **Dr.Web Monitor** перезапускает его. Если указано значение 0, время отклика не ограничивается. Значение по умолчанию: **AgentResponseTime** = 5

Запуск

В процессе запуска **Dr.Web Monitor** (при установках по умолчанию) осуществляются следующие действия:

- производится поиск и загрузка конфигурационного файла; если файл не найден, то загрузка прекращается;
- **Dr.Web Monitor** переходит в режим демона, поэтому сообщения о дальнейших проблемах не могут быть выведены на терминал и выводятся только в файл журнала;
- создается сокет для взаимодействия с другими модулями программного комплекса **Dr.Web для файловых серверов UNIX**. В случае использования TCP-соединений, подключений может быть несколько (загрузка продолжится, если удалось создать хотя бы одно из них). Если используется UNIX-сокет, то он может быть создан только тогда, когда содержащий его каталог доступен на запись и чтение пользователю, с чьими привилегиями работает модуль **drweb-monitor**. Если ни один сокет не может быть создан, загрузка прекращается;
- создается PID-файл, в котором хранится информация об идентификаторе процесса **Dr.Web Monitor**. Если создать PID-файл не удалось, то загрузка прекращается;
- модуль **drweb-monitor** запускает остальные модули программного комплекса **Dr.Web для файловых серверов UNIX**. Если какой-либо из модулей не загружается, **Dr.Web Monitor** пытается запустить его

повторно. Если все попытки **Dr.Web Monitor** загрузить модуль окончились неудачей, **Dr.Web Monitor** выгружает все уже загруженные модули и завершает свою работу. Обо всех проблемах с запуском модулей программного комплекса **Dr.Web Monitor** сообщает одним из доступных ему способов (записью в файл журнала, сообщением электронной почты, запуском произвольной программы). Способы оповещения, используемые для разных модулей, задаются в файле мета-конфигурации **Dr.Web Monitor**.

Для успешного запуска **Dr.Web Monitor** в автоматическом режиме:

- либо в `enable`-файле **Dr.Web Monitor** переменной `ENABLE` должно быть присвоено значение `1` (для **Linux** и **Solaris**);
- либо строка `drweb_monitor_enable="YES"` должна быть добавлена в файл `/etc/rc.conf` (для **FreeBSD**).

В процессе работы установочного скрипта при выборе соответствующей возможности в диалоге все сервисы, включая **Dr.Web Monitor**, будут запущены автоматически.

Расположение `enable`-файлов зависит от способа установки **Dr.Web для файловых серверов UNIX**:

- Установка при помощи **универсального пакета для UNIX**:

  Файлы располагаются в каталоге `%etc_dir` и называются
  `drwebd.enable`,
  `drweb-monitor.enable`.

- Установка из **нативных DEB-пакетов**:

  Файлы располагаются в каталоге `/etc/defaults` и называются
  `drwebd`,
  `drweb-monitor`.

- Установка из **нативных RPM-пакетов**:

  Файлы располагаются в каталоге `/etc/sysconfig` и называются
  `drwebd.enable`,
  `drweb-monitor.enable`.

Взаимодействие с компонентами программного комплекса

Взаимодействие с компонентами программного комплекса осуществляется с помощью `mmc`-файлов. В этих файлах описывается состав компонентов, расположение бинарных файлов, порядок их запуска и параметры запуска.

Описание каждого компонента содержится в секции `Application "имя_компонента"`. В конце секции обязательно должно быть поставлено `EndApplication`.

В описании компонента должны присутствовать следующие параметры:

- **`FullName`**: полное имя приложения;
- **`Path`**: путь к бинарным файлам;
- **`Depends`**: имена компонентов, которые должны запускаться до запуска описываемого компонента. Например, компонент `AGENT` должен запускаться до компонента `DAEMON`, поэтому в `mmc`-файле для **Dr.Web Daemon** параметр **`Depends`** имеет значение `"AGENT"`. Если подобные зависимости отсутствуют, то параметр может быть пропущен;
- **`Components`**: список бинарных файлов компонентов, запускаемых при старте приложения. Компоненты запускаются в том порядке, в котором перечислены. Для каждого из компонентов через пробел указываются:
  - Аргументы командной строки (могут быть заключены в кавычки);
  - Максимальное время, отводимое на запуск компонента;
  - Максимальное время для остановки;
  - Тип оповещения и права для запуска.

  Тип оповещения указывает, куда высылать сообщения о сбоях компонента. Он может принимать значения `MAIL`

(осуществляется отсылка оповещений по почте) и LOG (информация о сбоях только записывается в лог).

Права для запуска указывают группу и пользователя, с чьими правами будет запускаться компонент.

Пример mmc-файла Dr.Web Daemon для Linux:

```
Application "DAEMON"
    FullName    "Dr.Web (R) Daemon"
    Path        "/opt/drweb/"
    Depends     "AGENT"
    Components
          # name     args     MaxStartTime
 MaxStopTime     NotifyType  User:Group
          drwebd   "-a=local:/var/drweb/ipc/.
agent --foreground=yes"   30  10  MAIL  drweb:
drweb
    EndComponents
EndApplication
```

Консольный сканер Dr.Web Scanner

Консольный сканер **Dr.Web Scanner** служит для обнаружения и лечения вирусов на локальной машине. Консольный сканер представлен исполняемым модулем **drweb**.

Dr.Web Scanner проверяет указанные при запуске файлы и загрузочные записи указанных дисков. Для антивирусной проверки и лечения **Dr.Web Scanner** использует Антивирусное ядро **Dr.Web Engine** и вирусные базы, но не использует резидентный модуль **Dr.Web Daemon** (работа производится независимо от него).

Запуск

Запуск **Dr.Web Scanner** осуществляется командой:

```
$ %bin_dir/drweb
```

В том случае, если каталог `%bin_dir` внесен в переменную окружения командной оболочки `PATH`, запуск осуществляется из произвольного каталога. Следует учесть, что последний вариант не рекомендуется из соображений безопасности, равно как и создание символической ссылки на исполняемый файл **drweb** в каком-либо из каталогов типа `/bin/`, `/usr/bin/` и т.д.

Dr.Web Scanner может быть запущен как с правами администратора, так и с правами обычного пользователя. Разумеется, в последнем случае проверка будет выполняться только в тех каталогах, к которым пользователь имеет доступ на чтение, а лечение зараженных файлов будет производиться только в каталогах, в которых он имеет право на запись (обычно это домашний каталог пользователя, `$HOME`). Существуют и другие ограничения при запуске **Dr.Web Scanner** в пользовательском режиме, например, на перемещение и переименование зараженных файлов.

После запуска **Dr.Web Scanner** на экран выводится заставка с названием программы и ее целевой платформы, номером версии и датой ее выпуска, контактными координатами.

Далее выводится сообщение о регистрационных данных пользователя и загрузке вирусных баз **"Доктор Веб"**, включая их обновления, если они были установлены:

```
Dr.Web (R) Сканер для Linux v6.0.1 (19 февраля 2010)
Copyright (c) Игорь Данилов, 1992-2010
"Доктор Веб", Москва, Российская Федерация.
Техподдержка: http://support.drweb.com/
Отдел продаж: http://buy.drweb.com/
Версия оболочки: 6.0.1.10060 <API:2.2>
Антивирусное ядро: 6.0.1.9170 <API:2.2>
Загрузка /var/drweb/bases/drwtoday.vdb - Ok,
вирусных записей: 1533
Загрузка /var/drweb/bases/drw60012.vdb - Ok,
вирусных записей: 3511
-------------------------------------------
Загрузка /var/drweb/bases/drw60000.vdb - Ok,
вирусных записей: 1194
Загрузка /var/drweb/bases/dwn60001.vdb - Ok,
вирусных записей: 840
Загрузка /var/drweb/bases/drwebase.vdb - Ok,
вирусных записей: 78674
Загрузка /var/drweb/bases/drwrisky.vdb - Ok,
вирусных записей: 1271
Загрузка /var/drweb/bases/drwnasty.vdb - Ok,
вирусных записей: 4867
Вирусных записей: 538681
Ключевой файл: /opt/drweb/drweb32.key
Номер лицензионного ключа: XXXXXXXXXX
Дата активации лицензионного ключа: XXXX-XX-XX
Дата истечения действия лицензионного ключа: XXXX-
XX-XX
```

После этого возвращается приглашение командной оболочки.

При запуске **Dr.Web Scanner** с параметрами по умолчанию не осуществляется лечение зараженных файлов. Не предусмотрены также действия в отношении неизлечимых

файлов и подозрительных файлов. Все эти действия требуют указания дополнительных параметров командной строки - параметров действия.

Наборы параметров действия могут различаться в каждом конкретном случае, однако обычно представляются целесообразными следующие:

- **cu** – лечение зараженных файлов и системных областей, без удаления, перемещения или переименования зараженных файлов;
- **icd** – удаление неизлечимых файлов;
- **spr** – переименование подозрительных файлов.
- **spm** – перемещение подозрительных файлов;

Запуск **Dr.Web Scanner** с параметром лечения **cu** означает, что программа предпримет попытку восстановить состояние зараженного объекта. Это возможно только тогда, когда обнаружен известный вирус, причем необходимые инструкции по излечению имеются в вирусных базах, однако и в этих случаях попытка излечения может не быть успешной, например, если зараженный файл уже серьезно поврежден.

Если при проверке архивов в их составе были обнаружены зараженные файлы, лечение последних, как и удаление, перемещение или переименование, не производится. Для уничтожения вирусов в таких объектах архивы должны быть вручную распакованы соответствующими программными средствами, желательно, в отдельный каталог, который и будет указан как аргумент при повторном запуске **Dr.Web Scanner**.

При запуске с параметром удаления **icd** программа уничтожит зараженный файл на диске. Этот параметр целесообразен для неизлечимых (необратимо поврежденных вирусом) файлов.

Параметр переименования **spr** вызывает замену расширения имени файла на некое установленное (по умолчанию «*.#??», т.е. первый символ расширения заменяется символом «#»). Этот параметр целесообразно применять для файлов других ОС (например, DOS/Windows), выявленных при эвристическом анализе как подозрительные. Переименование сделает невозможным случайный запуск исполняемых модулей в этих

системах, загрузку документов **Word** или **Excel** без дальнейшей проверки и таким образом предотвратит заражение возможным вирусом и дальнейшее его распространение.

Параметр перемещения **spm** переместит зараженный (или подозрительный) файл в предназначенный для этого каталог **Карантина** (по умолчанию `%var_dir/infected/`). Пока он имеет чисто теоретическое значение: для файлов других ОС перемещение не имеет смысла, т.к они не могут нанести вреда UNIX-системе, перемещение же подозрительных файлов самой UNIX-системы может вызвать ошибки в работе системы, вплоть до полного ее отказа.

В результате форма запуска **Dr.Web Scanner** для повседневного использования представляется следующей:

```
$ drweb <путь> -cu -icd -spm -ar -ha -fl- -ml -sd
```

Такая команда может быть сохранена в виде текстового файла, который затем с помощью команды:

```
# chmod a+x [имя файла]
```

может быть оформлен как сценарий командной оболочки или серия сценариев для различных ситуаций.

Параметры командной строки

Общий формат запуска программы следующий:

```
$ %bin_dir/drweb <путь> [параметры командной строки]
```

где `<путь>` – путь или пути к проверяемым каталогам или маска проверяемых файлов. Если путь задан с префиксом: `disk://<путь к файлу устройства>` (файлы устройств размещаются в каталоге `/dev`), то будет проверен загрузочный сектор соответствующего устройства и при необходимости произведено его лечение. Путь может быть предварен необязательным ключом `path`.

Запущенный без параметров, только с указанием пути в качестве аргумента, консольный сканер **Dr.Web Scanner** осуществляет проверку указанного каталога, используя набор параметров по умолчанию (см. ниже). В следующем примере проверяется домашний каталог пользователя:

```
$ %bin_dir/drweb ~
```

По окончании проверки, в случае обнаружения зараженных или подозрительных файлов, **Dr.Web Scanner** выводит информацию обо всех таких файлах в следующем виде:

```
/path/file инфицирован [вирусом] ИМЯ_ВИРУСА
```

После вывода информации о зараженных и подозрительных файлах, если таковые были обнаружены, **Dr.Web Scanner** выдает отчет примерно следующего вида:

```
Отчет для "/opt/drweb/tmp":
Проверено   : 34/32   Исцелено   : 0
Инфицировано : 5/5    Удалено    : 0
Модификаций  : 0/0    Переименовано: 0
Подозрительных: 0/0    Перемещено  : 0
Время проверки: 00:00:02  Скорость   : 5233 KB/s
```

Числа, разделенные символом "/", означают: первое - общее количество файлов, второе - количество файлов в архивах.

Для того, чтобы пользователь имел возможность проверить работоспособность антивируса, в состав дистрибутива продукта входит специальный тестовый файл `readme.eicar.rus`. С помощью текстового редактора из него легко изготовить программу `eicar.com` (см. указания внутри самого файла), которая ведет себя подобно вирусу, вызывая сообщение вида:

```
 %bin_dir/doc/eicar.com инфицирован Eicar Test File
(Not a Virus!)
```

Этот файл не является вирусом и используется исключительно для тестирования. С этой целью все современные антивирусные программы включают информацию о нем в свои

вирусные базы.

Dr.Web Scanner может быть настроен с помощью многочисленных параметров командной строки. Полный список параметров командной строки для консольного сканера **Dr.Web Scanner** можно получить, запустив программу **drweb** с параметрами `-?`, `-h` или `--help`.

Основные параметры консольного сканера **Dr.Web Scanner** можно сгруппировать следующим образом:

- Параметры области проверки;
- Параметры диагностики;
- Параметры действий;
- Параметры интерфейса.

Параметры области проверки

Эти параметры указывают, где следует проводить проверку на вирусы:

Параметр	Описание
-path [=] { путь}	Задает пути для сканирования. В одном параметре может быть задано несколько путей. Символ '=' можно опустить, в этом случае путь для сканирования отделяется от ключа пробелом. Можно несколько раз указать ключ `path` с разными путями, в этом случае они будт объединены в один список. Кроме того, пути можно задавать, не используя ключ `path`. Если в параметрах запуска путь задан с префиксом: disk: //<путь к файлу устройства>, то будет проверен загрузочный сектор (MBR) соответствующего устройства и при необходимости произведено его лечение. Файл устройства – это специальный файл, расположенный в каталоге файлов устройств `/dev` и имеющий имя вида **sdX**

Параметр	Описание
	или **hdX**, где **X** – латинская буква (a, b, c, ...). Например: **hda**, **sda**. Таким образом, чтобы проверить, например, загрузочную запись диска **sda**, следует указать путь: disk:///dev/sda
-@[+] {файл}	Задает проверку объектов, перечисленных в указанном файле. Символ «+» (плюс) предписывает не удалять файл со списком объектов по окончании проверки. Этот файл может содержать пути к периодически проверяемым каталогам или просто список файлов, подлежащих регулярной проверке.
--	Указывает, что список объектов для сканирования следует считать из стандартного потока ввода stdin.
-sd	Задает рекурсивный поиск и проверку файлов во вложенных папках.
-fl	Указывает следовать символическим ссылкам как для файлов, так и для папок. Ссылки, приводящие к «зацикливанию», игнорируются.
-mask	Игнорировать маски имен файлов.

Параметры диагностики

Эти параметры определяют, какие типы объектов и каким образом должны проверяться на вирусы:

Параметр	Описание
-al	Указывает, что по заданным путям необходимо проверять все файлы вне зависимости от их расширения и внутреннего формата. Этот параметр противоположен по действию параметру **-ex**.
-ex	Указывает, что по заданным путям необходимо проверять только файлы заданного типа

Параметр	Описание
	(разрешения). Разрешения указываются в конфигурационном файле (задается параметром **-ini**) в переменной **FileTypes**. По умолчанию осуществляется проверка файлов со следующими расширениями: EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, MPP, OCX, VS*, DVB, CPY, BMP, RPM, ISO, DEB, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, LHA, LZH, BZ2, MSG, EML, 7Z, CPIO. Этот параметр противоположен по действию параметру **-al**.
-ar[d| m| r][n]	Задает проверку файлов в архивах (ARJ, CAB, GZIP, RAR, TAR, ZIP и др.). Под архивами в данном случае понимаются не только собственно архивы (например, вида *.tar), но и их сжатые формы (например, сжатые TAR–архивы вида *.tar.bz2 и *.tbz). Если параметр указан без дополнительных модификаторов d, m или r, то в случае обнаружения архива с вредоносными или подозрительными файлами, производится только информирование пользователя. Если параметр дополняется модификатором d, m или r, то применяются соответствующие действия для устранения обнаруженной угрозы.
-cn[d| m| r][n]	Задает проверку файлов в контейнерах (HTML, RTF, PowerPoint). Если параметр указан без дополнительных модификаторов d, m или r, то в случае обнаружения контейнера с вредоносными или подозрительными объектами, производится только информирование пользователя. Если параметр дополняется модификатором d, m

Параметр	Описание
	или `r`, то применяются соответствующие действия для устранения обнаруженной угрозы.
-ml[d| m| r][n]	Задает проверку файлов почтовых программ. Если параметр указан без дополнительных модификаторов `d`, `m` или `r`, то в случае обнаружения файла с вредоносными или подозрительными элементами, производится только информирование пользователя. Если параметр дополняется модификатором `d`, `m` или `r`, то применяются соответствующие действия для устранения обнаруженной угрозы.
-upn	Проверка исполняемых файлов, упакованных LZEXE, DIET, PKLITE, EXEPACK без вывода имен утилит упаковки (в противном случае имя утилиты-упаковщика будет выводиться на экран).
-ha	Задает использование эвристического анализа для поиска неизвестных угроз.

Для некоторых параметров доступны также следующие дополнительные модификаторы:

- `d` – использовать удаление объекта для устранения угрозы;
- `m` – использовать перемещение объекта в **Карантин** для устранения угрозы;
- `r` – использовать переименование объекта для устранения угрозы (первый символ расширения заменяется на символ «#»);
- `n` – не указывать в отчете типы архиваторов, контейнеров, почтовых файлов или упаковщиков.

При обнаружении вредоносных элементов в составных объектах (архивах, контейнерах, упакованных или почтовых файлах), указанное действие применяется ко всему составному объекту целиком, а не только к вредоносному элементу.

Параметры действия

Эти параметры определяют, какие действия должны быть выполнены в отношении зараженных (или подозрительных) объектов:

Параметр	Описание
-cu[d| m| r]	Задает действие для инфицированных файлов и загрузочных секторов дисков. Если параметр указан без дополнительных модификаторов, то производится лечение излечимых объектов и удаление неизлечимых файлов (если другое не задано параметром **-ic**). Дополнительные модификаторы позволяют задать иное действие взамен лечения, но оно применяется только для инфицированных файлов. Действие для неизлечимых файлов в таком случае должно быть задано параметром **-ic**.
-ic[d| m| r]	Задает действие для неизлечимых файлов. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-sp[d| m| r]	Задает действие для подозрительных файлов. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-adw[d| m| r| i]	Задает действие для файлов, содержащих рекламные программы. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-dls[d| m| r| i]	Задает действие для файлов, содержащих программы дозвона. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-jok[d| m| r| i]	Задает действие для файлов, содержащих программы-шутки. Если параметр указан без дополнительных

Параметр	Описание
	модификаторов, то производится только информировании об угрозе.
-rsk[d| m| r| i]	Задает действие для файлов, содержащих потенциально опасные программы. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-hck[d| m| r| i]	Задает действие для файлов, содержащих программы, используемые для взлома. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.

Дополнительные модификаторы задают действие, необходимое для устранения угрозы:

- d – удаление файла;
- m – перемещение файла в **Карантин**;
- r – переименование файла (первый символ расширения заменяется на символ «#»);
- i – игнорирование (доступно только для незначительных угроз, например, рекламных программ); при использовании этого модификатора объект пропускается без каких-либо действий и оповещение сообщение об угрозе не выводится.

При обнаружении вредоносных элементов в составных объектах (архивах, контейнерах, упакованных или почтовых файлах), указанное действие применяется ко всему составному объекту целиком, а не только к вредоносному элементу.

Параметры интерфейса

Эти параметры определяют условия вывода результатов работы консольного сканера **Dr.Web Scanner**:

Параметр	Описание
-v, -version, **--version**	Задает вывод информации о версии продукта и версии антивирусного ядра и завершение работы консольного сканера **Dr.Web Scanner**.

Параметр	Описание
-ki	Задает вывод информации о лицензии и ее владельце (только в кодировке UTF8).
-go	Задает пакетный режим работы консольного сканера **Dr.Web Scanner**. Все вопросы, подразумевающие ожидание ответа от пользователя, пропускаются; решения, требующие выбора, принимаются автоматически. Этот режим полезно использовать для автоматической проверки файлов, например, при ежедневной или еженедельной проверке жесткого диска.
-ot	Переключает вывод информации на стандартный вывод (`stdout`).
-oq	Отключает вывод информации на экран.
-ok	Задает вывод полного списка сканируемых объектов, сопровождая безопасные объекты пометкой **Ok**.
-log =[+] {путь к файлу}	Включает протоколирование работы консольного сканера **Dr.Web Scanner** в указанном файле. При отсутствии имени файла отчет записываться на будет. Символ «+» (плюс) предписывает не перезаписывать файл отчета, а добавлять новую информацию.
-ini = {путь к файлу}	Задает использование указанного конфигурационного файла. По умолчанию конфигурационный файл не входит в состав консольного сканера **Dr.Web Scanner**.
-lng = {путь к файлу}	Задает использование указанного альтернативного языкового файла. По умолчанию используется английский язык.

Параметр	Описание
-a = {адрес Агента}	Запустить консольный сканер **Dr.Web Scanner** в режиме централизованной защиты под управлением выбранного **Dr.Web Agent**.
-ni	Отключает использование конфигурационного файла для настройки консольного сканера **Dr.Web Scanner**. Настройка сканирования в данном случае будет осуществляться только с использованием параметров из командной строки.
-ns	Запрещает возможность прерывания проверки, в том числе при получении сигнала остановки процесса (SIGINT).
--only-key	При запуске от **Dr.Web Agent** будет получен только ключевой файл.

Некоторые из параметров отменяют соответствующее им действие, если оканчиваются символом минуса (без пробела). К ним относятся следующие параметры:

-ar -cu -ha -ic -fl -ml -ok -sd -sp

Например, при запуске консольного сканера **Dr.Web Scanner** командой вида:

```
$ drweb <путь> -ha-
```

проверка будет производиться без использования **Эвристического анализатора**, который обычно по умолчанию включен.

Для параметров **-cu**, **-ic** и **-sp** «отрицательная» форма отменяет выполнение любых действий, указанных в их описании. Это означает, что информация о зараженных и подозрительных объектах будет фиксироваться в отчете, но никаких действий под устранению представляемых ими угроз предприниматься не будет.

Для параметров **-al** и **-ex** «отрицательная» форма не предусмотрена, однако задание одного из них отменяет действие другого.

Если не производились действия по перенастройке программы, то по умолчанию (то есть без отдельного указания параметров) **Dr.Web Scanner** запускается с параметрами:

```
-ar -ha -fl- -ml -sd -al -ok
```

Этот набор параметров по умолчанию (включающий проверку архивов и упакованных файлов, файлов почтовых программ, рекурсивный поиск, эвристический анализ и т.д.) достаточно целесообразен для целей диагностики и может использоваться в большинстве типичных случаев. Если какой-либо из параметров по умолчанию не нужен в конкретной ситуации, его можно отключить, указав после него минус, как это было показано выше на примере параметра **-ha** (использование **Эвристического анализатора**).

Следует добавить, что отключение проверки архивированных и упакованных файлов резко снижает уровень антивирусной защиты, т.к. именно в виде архивов (часто самораспаковывающихся) распространяются файловые вирусы в виде почтовых вложений. Документы прикладных программ, потенциально подверженные заражению макровирусами (**Word**, **Excel** и др.), также обычно пересылаются по электронной почте в архивированном и упакованном виде.

При запуске **Dr.Web Scanner** с параметрами по умолчанию не осуществляется лечение зараженных файлов. Не предусмотрены также действия в отношении неизлечимых файлов и подозрительных файлов. Все эти действия требуют указания дополнительных параметров командной строки - параметров действия.

Настройки

Можно использовать **Dr.Web Scanner** с настройками по умолчанию, но значительно удобнее настроить его для соответствия конкретным требованиям и условиям эксплуатации. Настройки **Dr.Web Scanner** хранятся в конфигурационном файле программы (по умолчанию `drweb32.ini`), который размещается в каталоге `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске **Dr.Web Scanner**, например:

```
$ %bin_dir/drweb -ini=%bin_dir/etc/drweb.ini
```

Устройство конфигурационного файла и краткое описание правил задания параметров конфигурации приведены в разделе Конфигурационные файлы.

Секция [Scanner]

EnginePath = {путь к файлу}	Расположение модуля **drweb32.dll** (Антивирусное ядро **Dr.Web Engine**). Этот параметр также используется модулем обновления **Dr.Web Updater**. Значение по умолчанию: **EnginePath** = %bin_dir/lib/drweb32.dll
VirusBase = {список масок файлов}	Маски для подключаемых вирусных баз. Этот параметр также используется модулем обновления **Dr.Web Updater**. Допустимо перечисление нескольких масок через запятую. По умолчанию вирусные базы хранятся в файлах с расширением `vdb` Значение по умолчанию: **VirusBase** = %var_dir/bases/*.vdb

UpdatePath = {путь к каталогу}	Этот параметр используется модулем обновления **Dr.Web Updater** и должен быть задан обязательно. Значение по умолчанию: **UpdatePath** = %var_dir/updates/
TempPath = {путь к каталогу}	Этот каталог используется Антивирусным ядром **Dr.Web Engine** для создания временных файлов. При нормальной работе каталог практически не используется, он нужен для распаковки некоторых видов архивов, или когда в системе не хватает памяти. Значение по умолчанию: **TempPath** = /tmp/
LngFileName = {путь к файлу}	Расположение файла языковых ресурсов. По умолчанию файлы языковых ресурсов имеют расширение .dwl Значение по умолчанию: **LngFileName** = %bin_dir/lib/ru_scanner.dwl
Key = {путь к ключевому файлу}	Расположение ключевого файла (лицензионного или демонстрационного). По умолчанию ключевой файл имеет расширение .key Значение по умолчанию: **Key** = %bin_dir/drweb32.key
OutputMode = {Terminal | Quiet}	Режим вывода информации при запуске: • Terminal – вывод на консоль, • Quiet – отменяет вывод.

	Значение по умолчанию: **OutputMode** = Terminal
HeuristicAnalysis = {логический}	Включение/отключение использования **Эвристического анализатора**. Эвристический анализ делает возможным обнаружение неизвестных вирусов по априорным соображениям об устройстве вирусного кода. Особенностью этого типа поиска вирусов является вероятностный характер обнаружения заражения, что позволяет говорить не о зараженных, а о подозрительных объектах. При отключении этого режима осуществляется только поиск известных вирусов по вирусным базам **"Доктор Веб"**. Целый класс программ ввиду использования сходного с вирусами кода может вызывать ложные срабатывания **Эвристического анализатора**. Кроме того, данный режим может незначительно увеличить время проверки. Данные обстоятельства могут быть доводами в пользу отключения использования **Эвристического анализатора**. Вместе с тем, включение этого типа анализа увеличивает надежность антивирусной защиты. Все файлы, обнаруженные **Эвристическим анализатором**, лучше всего отправить разработчикам через сайт http://vms.drweb.com/sendvirus/. Отправку подозрительных файлов рекомендуется производить следующим образом: запаковать файл в архив с паролем, пароль сообщить в теле письма, при этом желательно приложить отчет **Dr.Web Scanner**.

	Значение по умолчанию: **HeuristicAnalysis** = Yes
ScanPriority = {числовое значение}	Приоритет работы **Dr.Web Scanner**. Значение параметра должно быть в диапазоне от высшего значения (-20) до низшего (19 для **Linux**, 20 для остальных ОС). Значение по умолчанию: **ScanPriority** = 0
FilesTypes = {список расширений файлов}	Список типов файлов, которые будут проверяться при сканировании по типу, т.е. когда параметр **ScanFiles** (см. ниже) имеет значение ByType. Допускаются символы маски '*' и '?'. Значение по умолчанию: FilesTypes = EXE, COM, SYS, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, VXD, 386, DLL, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, AR?, ZIP, R??, PP?, OBJ, LIB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SHS, SHB, PIF, SO, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, BMP, MPP, OCX, DVB, CPY, MSG, EML
FilesTypesWarnings = {логический}	Выводить ли предупреждение о файлах неизвестных типов. Значение по умолчанию: **FilesTypesWarnings** = Yes
ScanFiles = {All | ByType}	Дополнительное ограничение на файлы, подлежащие проверке. При задании значения ByType

	учитываются расширения файлов, значения которых заданы или по умолчанию, или в параметре (параметрах) **FilesTypes**. В противном случае проверяются все файлы. Внутри почтовых файлов всегда действует режим `All`. Значение `ByType` может быть использовано только в режиме **локального сканирования**. Значение по умолчанию: **ScanFiles** = `All`
ScanSubDirectories = {логический}	Проверка содержимого вложенных подкаталогов. Значение по умолчанию: **ScanSubDirectories** = `Yes`
CheckArchives = {логический}	Проверка файлов, содержащихся в архивах. Поддерживаются архивы форматов `ZIP` (WinZip, InfoZIP и др.), `RAR`, `ARJ`, `TAR`, `GZIP`, `CAB` и др. Значение по умолчанию: **CheckArchives** = `Yes`
CheckEMailFiles = {логический}	Проверка файлов в почтовых (e-mail) форматах. Значение по умолчанию: **CheckEMailFiles** = `Yes`
ExcludePaths = {список путей (масок)}	Маски для тех файлов, которые не должны проверяться. Значение по умолчанию: **ExcludePaths** = `/proc,/sys,/dev`

FollowLinks = {логический}	Следование символическим ссылкам при сканировании. Значение по умолчанию: **FollowLinks** = No
RenameFilesTo = {маска}	Маска для переименования файлов, если сработало действие Rename. Значение по умолчанию: **RenameFilesTo** = #??
MoveFilesTo = {путь к каталогу}	Путь к каталогу **Карантина**. Значение по умолчанию: **MoveFilesTo** = %var_dir/infected/
EnableDeleteArchiveAction = {логический}	Разрешение применения действия Delete для составных объектов (архивов, почтовых ящиков, HTML-страниц), если они содержат зараженные объекты. Важно понимать, что при наличии данного разрешения будет удален весь составной объект, т.е. весь архив или все письмо, а не только зараженное вложение в письмо или элемент архива. Значение по умолчанию: **EnableDeleteArchiveAction** = No
InfectedFiles = {действие}	Задает реакцию на обнаружение файла, зараженного известным вирусом. Допустимые значения параметра: Report, Cure, Delete, Move, Rename, Ignore. Удаление и перемещение, заданное в связи с обнаружением зараженных объектов в архивах, контейнерах и

	почтовых ящиках, применяется к соответствующему архиву, контейнеру или почтовому ящику целиком. Значение по умолчанию: **InfectedFiles** = Report

Далее указаны параметры, аналогичные параметру **InfectedFiles** и задающие реакцию программы на обнаружение тех или иных объектов. Для них предусмотрены те же возможные значения, что и для параметра **InfectedFiles**, кроме значения Cure:

SuspiciousFiles = {действие}	Действие, которое нужно выполнить в случае, если файл заражен неизвестным вирусом или представляет собой потенциальную угрозу. Допустимые значения параметра: Report, Delete, Move, Rename, Ignore. Значение по умолчанию: **SuspiciousFiles** = Report
IncurableFiles = {действие}	Действие, которое нужно выполнить в случае, если зараженный файл не может быть вылечен (параметр имеет смысл, только если **InfectedFiles** = Cure) Допустимые значения параметра: Report, Delete, Move, Rename, Ignore. Значение по умолчанию: **IncurableFiles** = Report
ActionAdware = {действие}	Действие, которое нужно выполнить в случае, если файл содержит программу для показа рекламы (adware). Допустимые значения параметра: Report, Delete, Move, Rename, Ignore.

	Значение по умолчанию: **ActionAdware** = Report
ActionDialers = {действие}	Действие, которое нужно выполнить в случае, если файл содержит программу автоматического дозвона. Допустимые значения параметра: Report, Delete, Move, Rename, Ignore. Значение по умолчанию: **ActionDialers** = Report
ActionJokes = {действие}	Действие, которое нужно выполнить в случае, если файл содержит программу-шутку, которая может пугать или раздражать пользователя. Допустимые значения параметра: Report, Delete, Move, Rename, Ignore. Значение по умолчанию: **ActionJokes** = Report
ActionRiskware = {действие}	Действие, которое нужно выполнить в случае, если файл содержит потенциально опасную программу, которая может быть использована не только ее владельцем, но и злоумышленниками. Допустимые значения параметра: Report, Delete, Move, Rename, Ignore. Значение по умолчанию: **ActionRiskware** = Report
ActionHacktools = {действие}	Действие, которое нужно выполнить в случае, если файл содержит программу, которая используется для взлома

	компьютеров. Допустимые значения параметра: `Report, Delete, Move, Rename, Ignore.` Значение по умолчанию: **`ActionHacktools`** = `Report`
`ActionInfectedMail` = `{действие}`	Действие, которое нужно выполнить в случае, если почтовое сообщение или почтовый ящик содержат зараженный объект. Допустимые значения параметра: `Report, Delete, Move, Rename, Ignore.` Значение по умолчанию: **`ActionInfectedMail`** = `Report`
`ActionInfectedArchive` = `{действие}`	Действие, которое нужно выполнить в случае, если архив (ZIP, TAR, RAR и др.) содержит зараженный файл. Допустимые значения параметра: `Report, Delete, Move, Rename, Ignore.` Значение по умолчанию: **`ActionInfectedArchive`** = `Report`
`ActionInfectedContainer` = `{действие}`	Действие, которое нужно выполнить в случае, если файл контейнер (OLE, HTML, PowerPoint и др.) содержит зараженный объект. Допустимые значения параметра: `Report, Delete, Move, Rename, Ignore.`

	Значение по умолчанию: **ActionInfectedContainer** = Report

Параметры регистрации событий:

LogFileName = {syslog | путь к файлу}	Имя файла журнала или syslog, если нужно использовать системный сервис **syslog**. Значение по умолчанию: **LogFileName** = syslog
SyslogFacility = {метка syslog}	Метка записи при использовании системного сервиса **syslog**. Значение по умолчанию: **SyslogFacility** = Daemon
SyslogPriority = {уровень подробности}	Уровень подробности ведения журнала при использовании системного сервиса **syslog**. Допускается использование следующих уровней: • Error • Alert • Warning • Info • Notice Значение по умолчанию: **SyslogPriority** = Info
LimitLog = {логический}	Ограничение размера файла журнала, если не используется **syslog**. Ограничение размера файла отчета реализуется следующим образом: при запуске **Dr.Web Scanner** проверяет размер файла журнала, и если он превышает значение, заданное в

	параметре **MaxLogSize**, файл журнала стирается и ведение журнала начинается с нуля. Значение по умолчанию: **LimitLog** = No
MaxLogSize = {числовое значение}	Максимальный размер файла журнала в килобайтах, если не используется **syslog** и **LimitLog** = Yes. Если указано значение 0, размер файла журнала проверяться не будет. Значение по умолчанию: **MaxLogSize** = 512
LogScanned = {логический}	Вывод в журнал информации обо всех проверяемых объектах, независимо от того, обнаружены вирусы или нет. Значение по умолчанию: **LogScanned** = Yes
LogPacked = {логический}	Вывод в журнал дополнительной информации о файлах, упакованных утилитами DIET, PKLITE и др. Значение по умолчанию: **LogPacked** = Yes
LogArchived = {логический}	Вывод в журнал дополнительной информации об архиваторах. Значение по умолчанию: **LogArchived** = Yes
LogTime = {логический}	Вывод в журнал времени каждой записи. Параметр игнорируется, если используется **syslog** Значение по умолчанию: **LogTime** = Yes

LogStatistics = {логический}	Запись в журнал суммарной статистики задания для сканирования. Значение по умолчанию: **LogStatistics** = Yes
RecodeNonprintable = {логический}	Перекодировка при выводе в журнал символов, не являющихся отображаемыми для данного терминала (см. следующие два параметра). Значение по умолчанию: **RecodeNonprintable** = Yes
RecodeMode = {Replace | QuotedPrintable}	При **RecodeNonprintable** = Yes задает метод перекодировки неотображаемых символов. При **RecodeMode** = Replace все такие символы заменяются на значение параметра **RecodeChar** (см. ниже). При **RecodeMode** = QuotedPrintable производится перекодировка неотображаемых символов в формат Quoted Printable. Значение по умолчанию: **RecodeMode** = QuotedPrintable
RecodeChar = {"?" | "_" | ...}	При **RecodeMode** = Replace задает символ, на который будут заменены все неотображаемые символы. Значение по умолчанию: **RecodeChar** = "?"

Следующие параметры могут быть использованы для уменьшения времени проверки архивов за счет отказа от проверки некоторых объектов в архиве.

MaxCompressionRatio = {числовое значение}	Максимальный коэффициент сжатия, т. е. отношение длины файла в распакованном виде к длине файла в

	запакованном виде (внутри архива). Если коэффициент превышает данное значение, файл не будет извлечен и, соответственно, не будет проверен. Письмо с таким файлом воспринимается программой как "*почтовая бомба*". Параметр может принимать только натуральные значения. Если указано значение 0, проверка коэффициента сжатия проводиться не будет. Значение по умолчанию: **MaxCompressionRatio** = 5000
CompressionCheckThreshold = {числовое значение}	Минимальный размер файла внутри архива (в килобайтах), начиная с которого будет производиться проверка коэффициента сжатия (если это предписано параметром **MaxCompressionRatio**). Значение по умолчанию: **CompressionCheckThreshold** = 1024
MaxFileSizeToExtract = {числовое значение}	Максимальный размер файла, извлекаемого из архива, в килобайтах. Если размер файла внутри архива превышает это значение, он будет пропущен. Письмо с таким файлом воспринимается программой как "*почтовая бомба*". Значение по умолчанию: **MaxFileSizeToExtract** = 500000
MaxArchiveLevel = {числовое значение}	Максимальный уровень вложенности архивов (когда архив вложен в архив, который тоже вложен в архив и т.д.). При превышении этого уровня архив будет пропущен (не будет проверен). Письмо с таким файлом воспринимается

	программой как "*почтовая бомба*". Если указано значение 0, уровень вложенности проверяемых архивов проверяться не будет. Значение по умолчанию: **MaxArchiveLevel** = 8
MaximumMemoryAllocationSize = {числовое значение}	Максимальный размер памяти в мегабайтах, выделяемой **Dr.Web Scanner** при сканировании одного файла. Если установлено значение 0, размер выделяемой памяти не ограничен. Значение по умолчанию: **MaximumMemoryAllocationSize** = 0
ScannerScanTimeout = {числовое значение}	Максимальное время сканирования одного файла (в секундах). Если установлено значение 0, время сканирования одного файла не ограничено. Значение по умолчанию: **ScannerScanTimeout** = 0
MaxBasesObsolescencePeriod = {числовое значение}	Максимальный период времени (в часах) с момента последнего обновления, в течение которого вирусные базы считаются "свежими". По истечении этого времени в консоли выводится уведомление о том, что базы устарели. Если установлено значение 0, "свежесть" вирусных баз не проверяется. Значение по умолчанию: **MaxBasesObsolescencePeriod** = 24

ControlAgent = {адрес}	Адрес сокета **Dr.Web Agent**.
	Пример:
	`ControlAgent = inet:4040@127.0.0.1,local:/var/drweb/ipc/.agent`
	Dr.Web Scanner получает от **Dr.Web Agent** ключ и конфигурационный файл (если в качестве значения параметра **OnlyKey** задано No).
	Значение по умолчанию:
	`ControlAgent = local:%var_dir/ipc/.agent`

OnlyKey = {логический}	Подключение возможности запросить только ключевой файл от **Dr.Web Agent**, не запрашивая конфигурацию. При этом будет использоваться локальный конфигурационный файл. Если указан адрес сокета **Dr.Web Agent** и значение параметра **OnlyKey** установлено в No, **Dr.Web Agent** будет отправляться статистика работы **Dr.Web Scanner** (после сканирования каждого файла **Dr.Web Scanner** будет отправлять информацию **Dr.Web Agent**). Значение по умолчанию: `OnlyKey = No`

Антивирусный модуль Dr.Web Daemon

Dr.Web Daemon – основной компонент безопасности. Он представляет собой постоянно загруженный (резидентный) антивирусный модуль **drwebd**, который позволяет по запросу от других компонентов комплекса проверять файлы на диске или данные, переданные ему через сокет. Запросы на антивирусную проверку осуществляются по специальному протоколу через UNIX- или TCP-сокеты. **Dr.Web Daemon** использует то же Антивирусное ядро **Dr.Web Engine** и вирусные базы, что и **Dr.Web Scanner**, и способен обнаруживать и лечить все вирусы, известные Антивирусному ядру **Dr. Engine**.

Dr.Web Daemon всегда готов к выполнению своих функций и имеет понятный и доступный протокол для запросов сканирования, что делает его подходящим компонентом для создания антивирусного фильтра для файловых серверов. Программный комплекс **Dr.Web для файловых серверов UNIX** является готовым решением по интеграции **Dr.Web Daemon** с файловыми серверами **Samba** версии 3.0 или выше.

Параметры командной строки

Для запуска **Dr.Web Daemon** используется следующая команда:

```
drwebd [параметры]
```

Dr.Web Daemon допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h, -?	-help, --help	
Описание: Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля		

Краткий вариант	Расширенный вариант	Аргументы
-a		<адрес Агента>
Описание: Запуск **Dr.Web Daemon** в режиме центральной защиты под управлением указанного **Dr.Web Agent**		
-ini		<путь к файлу>
Описание: Использование указанного конфигурационного файла		
	--foreground	<yes| no>
Описание: Задание режима работы **Dr.Web Daemon** при запуске. Если выбрано значение yes, то **Dr.Web Daemon** будет работать как приоритетная задача. При значении no **Dr.Web Daemon** будет работать в фоновом режиме		
	--check-only	<параметры командной строки для проверки>
Описание: Проверка правильности конфигурации **Dr.Web Daemon** при запуске. Если указаны какие-либо параметры командной строки, то правильность задаваемых с их помощью значений также будет проверена		
	--only-key	
Описание: При запуске **Dr.Web Daemon** получит от **Dr.Web Agent** только лицензионный ключевой файл		

Запуск

В процессе загрузки **Dr.Web Daemon** выполняются следующие действия:

1. Поиск и загрузка конфигурационного файла. Если конфигурационный файл не найден, загрузка **Dr.Web Daemon** прекращается. Путь к конфигурационному файлу может быть задан при запуске параметром командной строки -ini: {путь/к/drweb32.ini}, иначе будет

использовано значение `%etc_dir/drweb32.ini`, заданное по умолчанию. При загрузке проверяется допустимость некоторых параметров и, если значение параметра недопустимо, берется значение по умолчанию;

2. Создается файл отчета. Каталог с файлом отчета должен быть доступен на запись пользователю, с правами которого работает **Dr.Web Daemon**. Каталог `/var/log/`, используемый по умолчанию, недоступен пользователям на запись. Поэтому, если задано значение параметра **User**, необходимо также указать путь к альтернативнойму каталогу для хранения отчётов в значении параметра **LogFileName**;
3. Производится загрузка ключевого файла по пути, указанному в конфигурационном файле. Если ключевой файл не найден, загрузка **Dr.Web Daemon** прекращается;
4. Если задан параметр **User**, **Dr.Web Daemon** пытается изменить свои права;
5. Производится загрузка антивирусного ядра **Dr.Web Engine** (файл **drweb32.dll**). Если Антивирусное ядро не найдено (ошибки в конфигурационном файле) или повреждено, загрузка **Dr.Web Daemon** прекращается;
6. Загружаются вирусные базы. Поиск вирусных баз осуществляется по заданным в конфигурационном файле путям, порядок загрузки вирусных баз не регламентирован. Если вирусные базы повреждены или отсутствуют, загрузка **Dr.Web Daemon** продолжается;
7. **Dr.Web Daemon** отключается от терминала, поэтому сообщения о дальнейших проблемах не могут быть выведены на терминал и выводятся только в файл отчета;
8. Создается сокет, в случае использования TCP-сокетов, возможно, не один. Если какой-либо TCP-сокет создать не удалось, загрузка **Dr.Web Daemon** продолжается. В случае использования UNIX-сокета следует убедиться, что каталог, содержащий его, доступен на запись и чтение пользователю, с чьими правами работает **Dr.Web Daemon**. Для пользователей, с правами которых будут работать интеграционные модули, каталог должен быть доступен на выполнение, а сам файл сокета — на запись и чтение. Каталог по умолчанию (`/var/run/`) недоступен

пользователям на запись и выполнение. Поэтому, если задано значение параметра **User**, необходимо также указать путь к альтернативному каталогу для сокетов в значении параметра **Socket**. Если UNIX-сокет создать не удалось, загрузка **Dr.Web Daemon** прекращается;

9. После этого создается PID-файл, в котором хранится информация об идентификаторе процесса **Dr.Web Daemon** и о транспортных адресах, по которым доступен **Dr.Web Daemon**. Каталог с PID-файлом также должен быть доступен на запись пользователю, с правами которого работает **Dr.Web Daemon**. Используемый по умолчанию каталог `/var/run/` недоступен пользователям на запись и выполнение. Поэтому, если задано значение параметра **User**, необходимо также указать путь к альтернативному каталогу для PID-файла в значении параметра **PidFile**. Если создать PID-файл не удалось, загрузка **Dr.Web Daemon** прекращается.

Проверка работоспособности Dr.Web Daemon

Если в ходе загрузки не возникло проблем, **Dr.Web Daemon** готов к работе. Для проверки корректности загрузки **Dr.Web Daemon** можно узнать, созданы ли необходимые для его работы сокеты. Для этого используется команда:

```
$ netstat -a
```

В случае TCP-сокетов:

```
. . .
Active Internet connections (servers and
established)
Proto   Recv-Q   Send-Q   Local Address   Foreign
Address   State
. . .
tcp     0        0        localhost:3000  *:*
       LISTEN
. . .
```

В случае UNIX-сокетов:

```
. . .
Active UNIX domain sockets (servers and established)
Proto   RefCnt   Flags   Type    State      I-Node
Path
. . .
unix    0       [ ACC ]  STREAM  LISTENING  1127
%var_dir/.daemon
. . .
```

Если созданные сокеты не появились в списке, значит, имеются проблемы загрузки.

Для проверки работоспособности **Dr.Web Daemon** можно использовать **Консольный клиент Dr.Web Daemon** (**drwebdc**), запустив его для получения служебной информации о **Dr.Web Daemon**. Если запустить **drwebdc**, он выдаст список всех поддерживаемых параметров.

В случае TCP-сокета:

```
$ drwebdc -nHOSTNAME -pPORTNUM -sv -sb
```

В случае UNIX-сокета:

```
$ drwebdc -uSOCKETFILE -sv -sb
```

На консоли появится информация, подобная следующей:

```
- Version: DrWeb Daemon 6.00
- Loaded bases:
Base /var/drweb/bases/drwtoday.vdb
contains 5 records.
Base /var/drweb/bases/drw60003.vdb
contains 409 records.
Base /var/drweb/bases/drw60002.vdb
contains 543 records.
Base /var/drweb/bases/drwebase.vdb
contains 51982 records.
Base /var/drweb/bases/drw60001.vdb
contains 364 records.
Total 53303 virus-finding records.
```

Если этого не произошло, следует провести расширенную диагностику:

В случае TCP-сокета:

```
$ drwebdc -nHOSTNAME -pPORTNUM -sv -sb -v
```

В случае UNIX-сокета:

```
$ drwebdc -uSOCKETFILE -sv -sb -v
```

Более подробный вывод может прояснить ситуацию:

```
dwlib: fd: connect() failed - Connection refused
dwlib: tcp: connecting to 127.0.0.1:3300 - failed
dwlib: cannot create connection with a DrWeb daemon
ERROR: cannot retrieve daemon version
Error -12
```

Проверить работоспособность **Dr.Web Daemon** можно с помощью программы `eicar.com`, получаемой из входящего в дистрибутив файла `readme.eicar.rus` с помощью любого текстового редактора (см. указания об этом внутри самого файла).

В случае лицензии для файловых серверов:

Для TCP-сокета:

```
$ drwebdc -n<ИМЯ_УЗЛА> -p<НОМЕР_ПОРТА> eicar.com
```

Для UNIX-сокета:

```
$ drwebdc -u<ФАЙЛ_СОКЕТА> eicar.com
```

Результатом команды должно быть сообщение:

```
Results: daemon return code 0x20
(known virus is found)
```

Если его не появилось, проверьте в файле отчета **Dr.Web Daemon** наличие записи о проверке этого файла. Если файл так и не был проверен, проведите расширенную диагностику (см. выше).

Если проверка файла прошла успешно, **Dr.Web Daemon** находится в рабочем состоянии.

Обратите внимание, что **Dr.Web Daemon** не может сканировать файлы размером больше 2 гигабайт. Такие файлы не будут отправляться на сканирование клиентами **Dr.Web Daemon**.

При сканировании архивов больших размеров могут возникать ошибки, связанные с истечением времени ожидания. При возникновении таких ошибок увеличьте значения, указанные в параметрах `FileTimeout` и `SocketTimeout`.

Режимы проверки

Dr.Web Daemon имеет два основных режима проверки:

- проверка фрагмента данных, полученного из сокета (удаленное сканирование);
- проверка файла на диске (локальное сканирование).

При использовании первого режима **Dr.Web Daemon** получает данные для проверки из сокета — фактически, это некоторый фрагмент данных. Данный фрагмент может быть поименованным или нет, что отразится исключительно на форме записи в файле отчета **Dr.Web Daemon**. Пример работы **Dr.Web Daemon** в этом режиме приведен в предыдущем пункте: клиент читает файл и отсылает его **Dr.Web Daemon** для проверки. **Dr.Web Daemon** может проверять любой фрагмент данных, не обязательно файл.

Более эффективен режим, в котором **Dr.Web Daemon** проверяет указанный файл на диске — локальное сканирование. Клиент сообщает **Dr.Web Daemon** лишь путь к файлу, а не передает весь файл. Путь к проверяемому файлу задается относительно **Dr.Web Daemon** (т.к. клиенты могут находиться на других машинах и т.д.). Этот режим обеспечивает большую производительность и упрощает создание рабочих схем с лечением (например, на файловых серверах).

Режим локального сканирования требует более тщательной

настройки прав, т.к. **Dr.Web Daemon** проверяемый файл должен быть доступен на чтение, а в случае почтовых файлов и использования действий `Cure` и `Delete` – необходимы и права на запись.

В корректно настроенной системе **Dr.Web Daemon** в большинстве случаев не требуется прав администратора.

Обрабатываемые сигналы

Dr.Web Daemon может принимать и обрабатывать следующие сигналы:

- `SIGHUP` — перезагрузка конфигурационного файла;
- `SIGTERM` — корректное завершение работы **Dr.Web Daemon**;
- `SIGKILL` — принудительное завершение работы **Dr.Web Daemon** (в случае проблем);
- `SIGUSR1` — инициирует сохранение в журнал статистики пула процессов.

Обратие внимание, что сигнал `SIGUSR1` должен посылаться только родительскому процессу, поскольку для дочерних процессов `SIGUSR1` приведет к завершению процесса.

Журнал работы и статистика пула процессов

Журнал работы

Поскольку **Dr.Web Daemon** является резидентной программой, информация о его работе может быть получена только из файла журнала (лога). Файл журнала содержит подробности обработки каждого запроса на сканирование, полученного **Dr.Web Daemon**. Имя файла журнала указывается в значении параметра конфигурационного файла **`LogFileName`**.

Dr.Web Daemon может выводить данные об обработке запросов на сканирование в разные файлы, в зависимости от клиента, который выслал запрос. В параметре **ClientsLogs** конфигурационного файла можно указать отдельные файлы журнала (или назначить службу журналирования **syslog**) для каждого из клиентских приложений **Dr.Web** (например, **Dr.Web для файловых серверов UNIX**).

Вне зависимости от параметра **ClientsLogs**, если клиентское приложение было распознано **Dr.Web Daemon**, результаты сканирования будут отмечены специальным префиксом при выводе в файл журнала. Возможны следующие префиксы:

- `<web>` – **Dr.Web ICAPD**;
- `<smb_spider>` – **Dr.Web Samba SpIDer**;
- `<mail>` – **Dr.Web MailD**;
- `<drwebdc>` – консольный клиент **Dr.Web Daemon**;
- `<kerio>` – **Dr.Web для интернет-шлюзов Kerio**;
- `<lotus>` – **Dr.Web для IBM Lotus Domino**.

В операционной системе **FreeBSD** вывод на консоль **Dr.Web Daemon** может быть перехвачен системной службой **syslog** и выведен в файл отчета посимвольно. Эта проблема проявляется, если в конфигурационном файле службы **syslog** `syslog.conf` установлен уровень подробности журналирования `*.info`.

Статистика пула процессов

Статистика текущего состояния пула процессов, который используется для обработки запросов на сканирование, может быть выведена в файл журнала по получению модулем **Dr.Web Daemon** сигнала `SIGUSR1` (сигнал должен посылаться только родительскому процессу, поскольку для дочерних процессов получение сигнала `SIGUSR1` приведет к завершению процесса). Накоплением статистики по пулу процессов управляет соответствующее значение **stat** (`yes` или `no`) в параметре **ProcessesPool**. Статистика не суммируется. В

каждом случае выводится состояние пула, накопленное между двумя последовательными сохранениями статистики.

Пример вывода записи со статистикой пула процессов:

```
Fri Oct 15 19:47:51 2010 processes pool
statistics: min = 1 max = 1024 (auto)
freetime = 121 busy max = 1024 avg =
50.756950 requests for new process = 94
(0.084305 num/sec) creating fails = 0 max
processing time = 40000 ms; avg = 118646 ms
curr = 0 busy = 0
```

где:

- `min` – минимальное количество процессов в пуле;
- `max` – минимальное количество процессов в пуле;
- `(auto)` – выводится, если ограничения пула процессов определяются автоматически;
- `freetime` – максимальное время бездействия процесса в пуле;
- `busy max` – максимальное количество одновременно занятых процессов, `avg` - среднее количество одновременно занятых процессов;
- `requests for new process` – количество запросов на создание дополнительных процессов (в скобках приводится частота запросов в секунду);
- `creating fails` – количество неудачных попыток создания процесса (обычно, по причине нехватки системных ресурсов);
- `max processing time` – максимальное время обработки одного запроса в миллисекундах;
- `avg` – среднее время обработки одного запроса в миллисекундах;
- `curr` – текущее общее количество процессов в пуле;
- `busy` – текущее количество занятых процессов.

Настройки

Можно запустить **Dr.Web Daemon** с настройками по умолчанию, но предпочтительнее настроить его в соответствии с требованиями и условиям эксплуатации. Конфигурационный файл `drweb32.ini` читается **Dr.Web Daemon** из каталога `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске **Dr.Web Daemon**.

Устройство конфигурационного файла и краткое описание правил задания параметров конфигурации приведены в разделе Конфигурационные файлы.

Секция [Daemon]

EnginePath = {путь к файлу}	Расположение модуля **drweb32.dll** (Антивирусное ядро **Dr.Web Engine**). Этот параметр также используется модулем обновления **Dr.Web Updater**. Значение по умолчанию: **EnginePath** = %bin_dir/lib/drweb32.dll
VirusBase = {список масок файлов}	Маски для подключаемых вирусных баз. Этот параметр также используется модулем обновления **Dr.Web Updater**. Допустимо перечисление нескольких масок через запятую. По умолчанию вирусные базы хранятся в файлах с расширением .vdb Значение по умолчанию: **VirusBase** = %var_dir/bases/*.vdb
UpdatePath = {путь к каталогу}	Каталог хранения обновлений. Этот параметр используется модулем обновления **Dr.Web Updater** и должен

	быть задан обязательно. Значение по умолчанию: **UpdatePath** = %var_dir/updates/
TempPath = {путь к каталогу}	Этот каталог используется Антивирусным ядром **Dr.Web Engine** для создания временных файлов. При нормальной работе каталог практически не используется, он нужен для распаковки некоторых видов архивов или когда в системе не хватает памяти. Значение по умолчанию: **TempPath** = %var_dir/spool/
Key = {список путей к файлам}	Расположение ключевых файлов. По умолчанию ключевой файл имеет расширение .key Ключевой файл может быть различным для **Dr.Web Daemon** и для **Dr.Web Scanner**. Соответственно, при необходимости нужно изменить настройки данного параметра. Параметр может задаваться несколько раз, указывая несколько лицензионных ключевых файлов. В таком случае **Dr.Web Daemon** пытается объединить права, предоставляемые различными лицензиями. Значение по умолчанию: **Key** = %bin_dir/drweb32.key
OutputMode = {Terminal | Quiet}	Режим вывода информации при запуске: • Terminal – вывод на консоль, • Quiet – отменяет вывод. Значение по умолчанию: **OutputMode** = Terminal

RunForeground = {логический}	Значение Yes запрещает **Dr.Web Daemon** переходить в режим демона, т. е. становиться фоновым процессом без управляющего терминала. Эта возможность может быть использована некоторыми средствами мониторинга (например, **Dr.Web Monitor**). Значение по умолчанию: **RunForeground** = No
User = {строка}	Пользователь, с правами которого работает **Dr.Web Daemon**. Рекомендуется завести в системе специального пользователя drweb, который будет использоваться **Dr.Web Daemon** и некоторыми фильтрами. Использовать **Dr.Web Daemon** с правами root нежелательно, хотя такое решение значительно проще настраивается. Значение этого параметра не изменяется во время процедуры перечитывания конфигурации "на лету" (обработки сигнала SIGHUP). Значение по умолчанию: **User** = drweb
PidFile = {путь к файлу}	Имя файла, в который при запуске **Dr.Web Daemon** записывается информация об идентификаторе его процесса (pid), а также сокет (если параметр **Socket** задает использование UNIX-сокета) или номер порта (если параметр **Socket** задает использование TCP-сокета). Если задано более одного параметра **Socket**, в данном файле будет присутствовать информация обо всех заданных сокетах (по одному в строке).

	Значение по умолчанию: **PidFile** = %var_dir/run/drwebd.pid
BusyFile = {путь к файлу}	Данный файл сигнализирует о занятости **Dr.Web Daemon**: он создается сканирующей "копией" **Dr.Web Daemon** при получении команды и уничтожается после передачи результата ее выполнения. Имя файла, создаваемого каждой "копией" **Dr.Web Daemon**, дополняется точкой и ASCII-представлением pid (например, /var/run/drwebd.bsy.123456). Значение по умолчанию: **BusyFile** = %var_dir/run/drwebd.bsy
ProcessesPool = {настройки пула процессов}	Настройки динамического пула процессов. Первым определяется количество процессов в пуле: • auto – количество процессов определяется автоматически в зависимости от загрузки системы; • N – целое неотрицательное число. Как минимум N процессов в пуле будут активны, а новые процессы будут создаваться по мере надобности; • N-M – целые положительное значения, и M>=N. Как минимум N процессов в пуле будут активны, а новые процессы будут создаваться по мере надобности, пока число процессов не достигнет значения M.

	Далее определяются дополнительные параметры: • **timeout** = {время в секундах} — если процесс не становится активным в течение заданного периода времени, процесс закрывается. Этот параметр не влияет на первые N процессов (ожидающих запросов бесконечно). • **stat** = {yes| no} — собирать ли статистику по процессам в пуле. В случае если этот параметр равен yes, при получении системного сигнала SIGUSR1 **Dr.Web Daemon** сохранит текущую накопленную статистику в файл журнала. В противном случае учет и сохранение статистики не производится. • **stop_timeout** = {время в секундах} — время ожидания остановки работающего процесса. Значение по умолчанию: **ProcessesPool** = auto, **timeout** = 120, **stat** = no, **stop_timeout** = 1
OnlyKey = {логический}	Подключение возможности запросить только ключевой файл от **Dr.Web Agent**, не запрашивая конфигурацию. При этом будет использоваться локальный конфигурационный файл. Если указан адрес сокета **Dr.Web Agent** и значение параметра **OnlyKey** установлено в No, то **Dr.Web Agent** будет отправляться статистика работы **Dr.Web Daemon** (после сканирования каждого файла **Dr.Web Daemon** будет отправлять информацию **Dr.Web Agent**).

	Значение по умолчанию: **OnlyKey** = No
ControlAgent = {адрес}	Адрес сокета **Dr.Web Agent**. **Пример**: **ControlAgent** = inet:4040@127.0.0.1,local:/var/drweb/ipc/.agent **Dr.Web Daemon** получает через этот сокет от **Dr.Web Agent** лицензионный ключ (и конфигурационный файл, если в качестве значения параметра **OnlyKey** задано No. Кроме того, в этом случае через этот сокет **Dr.Web Daemon** отправляет **Dr.Web Agent** статистику проверки файлов).
	Значение по умолчанию: **ControlAgent** = local:%var_dir/ipc/.agent
MailCommand = {строка}	Команда shell, вызываемая **Dr.Web Daemon** и модулем обновления **Dr.Web Updater** для отсылки уведомлений пользователю (администратору) по электронной почте. **Dr.Web Daemon** использует этот механизм при каждом запуске (перезапуске, перезагрузке), если до истечения срока действия ключевого файла (одного из ключевых файлов) осталось менее дней, чем указано в параметре **NotifyPeriod**. Модуль обновления **Dr.Web Updater** использует этот механизм для рассылки пользователям информационных материалов, подготовленных компанией **Доктор Веб**, в том числе по вопросам, связанным с обновлениями файлов программы.

	Значение по умолчанию: **MailCommand** = "/usr/sbin/sendmail -i -bm -f drweb -- root"
NotifyPeriod = {числовое значение}	Значение данного параметра определяет, за сколько дней до окончания срока действия ключевого файла рассылаются уведомления о необходимости продления лицензии. Если указано значение 0, уведомления рассылаются сразу после окончания действия ключа. Значение по умолчанию: **NotifyPeriod** = 14
NotifyFile = {путь к файлу}	Путь к файлу с меткой времени последнего уведомления о продлении лицензии. Значение по умолчанию: **NotifyFile** = %var_dir/.notify
NotifyType = {Ever | Everyday | Once}	Регулярность отправления уведомления о продлении лицензии: • Once – уведомление посылается единожды. • Everyday – уведомление посылается каждый день. • Ever – уведомление посылается при каждой перезагрузке **Dr.Web Daemon** или обновлении баз. Значение по умолчанию: **NotifyType** = Ever
FileTimeout = {числовое значение}	Максимальное разрешенное время проверки одного файла в секундах. Если указано значение 0, время

	проверки файла не ограничивается. Значение по умолчанию: **FileTimeout** = 30
StopOnFirstInfected = {логический}	Прекращение проверки письма после первого обнаруженного вируса. Установка значения Yes может резко сократить нагрузку на почтовый сервер и время проверки писем. Значение по умолчанию: **StopOnFirstInfected** = No
ScanPriority = {числовое значение}	Приоритет сканирующих процессов **Dr.Web Daemon**. Значение параметра должно быть в диапазоне от высшего значения (-20) до низшего (19 для **Linux**, 20 для остальных ОС). Значение по умолчанию: **ScanPriority** = 0
FilesTypes = {список расширений файлов}	Типы файлов, которые будут проверяться при сканировании по типу, т.е. когда параметр **ScanFiles** (см. ниже) имеет значение ByType. Допускаются символы маски '*' и '?'.

	Значение по умолчанию: **FilesTypes** = EXE, COM, SYS, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, VXD, 386, DLL, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, AR?, ZIP, R??, PP?, OBJ, LIB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SHS, SHB, PIF, SO, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, BMP, MPP, OCX, DVB, CPY, MSG, EML
FilesTypesWarnings = {логический}	Предупреждение о файлах неизвестных типов. Значение по умолчанию: **FilesTypesWarnings** = Yes
ScanFiles = {All | ByType}	Дополнительное ограничение на файлы, подлежащие проверке. При задании значения ByType учитываются расширения файлов, значения которых заданы или по умолчанию, или в параметре (параметрах) **FilesTypes**. Внутри почтовых файлов всегда действует режим All. Значение ByType может быть использовано только в режиме **локального сканирования**. Значение по умолчанию: **ScanFiles** = All
CheckArchives = {логический}	Проверка файлов, содержащихся в архивах. Поддерживаются архивы форматов ZIP (WinZip, InfoZIP и др.), RAR, ARJ, TAR, GZIP, CAB и др.

	Значение по умолчанию: **CheckArchives** = Yes
CheckEMailFiles = {логический}	Проверка файлов в почтовых (e-mail) форматах. Значение по умолчанию: **CheckEMailFiles** = Yes
ExcludePaths = {список путей (масок)}	Маски для тех файлов, которые не должны проверяться. Значение по умолчанию: **ExcludePaths** = /proc,/sys,/dev
FollowLinks = {логический}	Следование символическим ссылкам при сканировании. Значение по умолчанию: **FollowLinks** = No
RenameFilesTo = {маска}	Маска для переименования файлов, если сработало действие Rename. Значение по умолчанию: **RenameFilesTo** = #??
MoveFilesTo = {путь к каталогу}	Путь к каталогу **Карантина**. Значение по умолчанию: **MoveFilesTo** = %var_dir/infected/
BackupFilesTo = {путь к каталогу}	Каталог для сохранения зараженных файлов, которые были вылечены. Значение по умолчанию: **BackupFilesTo** = %var_dir/infected/

Параметры регистрации событий:

LogFileName = {syslog | путь к файлу}	Имя файла журнала или syslog, если нужно использовать системный сервис **syslog**. Значение по умолчанию: **LogFileName** = syslog
SyslogFacility = {метка syslog}	Метка записи при использовании системного сервиса **syslog**. Значение по умолчанию: **SyslogFacility** = Daemon
SyslogPriority = {уровень подробности}	Уровень подробности ведения журнала при использовании системного сервиса **syslog**. Допускается использование следующих уровней: • Error • Alert • Warning • Info • Notice Значение по умолчанию: **SyslogPriority** = Info
LimitLog = {логический}	Ограничение размера файла журнала. Игнорируется при использовании системного сервиса **syslog**. Ограничение размера файла журнала реализуется следующим образом: при запуске или получении сигнала HUP **Dr.Web Daemon** проверяет размер файла журнала, и если он превышает значение, заданное в параметре **MaxLogSize**, файл журнала стирается и ведение журнала начинается с нуля.

	Значение по умолчанию: **LimitLog** = No
MaxLogSize = {числовое значение}	Максимальный размер файла журнала в килобайтах. Имеет смысл только если не используется **syslog** и **LimitLog** = Yes. Если указано значение 0, размер файла журнала проверяться не будет. Значение по умолчанию: **MaxLogSize** = 512
LogScanned = {логический}	Вывод в файл журнала информации обо всех проверяемых объектах, независимо от того, обнаружены вирусы или нет. Значение по умолчанию: **LogScanned** = Yes
LogPacked = {логический}	Вывод в файл журнала дополнительной информации о файлах, упакованных утилитами DIET, PKLITE и др. Значение по умолчанию: **LogPacked** = Yes
LogArchived = {логический}	Вывод в файл журнала дополнительной информации об архиваторах. Значение по умолчанию: **LogArchived** = Yes
LogTime = {логический}	Вывод в файл журнала времени каждой записи. Параметр не имеет смысла при использовании системного сервиса **syslog**

	Значение по умолчанию: **LogTime** = Yes
LogProcessInfo = {логический}	Вывод в файл журнала перед каждой записью данных о pid сканирующего процесса и адресе фильтра (имени хоста или IP-адресе), с которого инициирована проверка. Значение по умолчанию: **LogProcessInfo** = Yes
RecodeNonprintable = {логический}	Перекодировка при выводе в файл журнала символов, не являющихся отображаемыми для данного терминала (см. следующие два параметра). Значение по умолчанию: **RecodeNonprintable** = Yes
RecodeMode = {Replace | QuotedPrintable}	При **RecodeNonprintable** = Yes задает метод перекодировки неотображаемых символов. При **RecodeMode** = Replace все такие символы заменяются на значение параметра **RecodeChar** (см. ниже). При **RecodeMode** = QuotedPrintable производится перекодировка неотображаемых символов в формат Quoted Printable. Значение по умолчанию: **RecodeMode** = QuotedPrintable
RecodeChar = {"?" | "_" | ...}	При **RecodeMode** = Replace задает символ, на который будут заменены все неотображаемые символы. Значение по умолчанию: **RecodeChar** = "?"

Socket = {список адресов}	Описание сокета, который будет использован для связи с **Dr.Web Daemon**.
	Пример:
	`Socket = inet:3000@127.0.0.1, local:%var_dir/.daemon`
	Также можно адрес каждого из сокетов указывать в отдельном параметре в формате `ПОРТ [интерфейсы] | ФАЙЛ [доступ]`. Соответственно, для TCP-сокета: ПОРТ - десятичный номер порта, интерфейсы - список имен интерфейсов или IP-адресов, на которых **Dr.Web Daemon** будет принимать запросы.
	Пример:
	`Socket = 3000 127.0.0.1, 192.168.0.100`
	Для UNIX-сокета: ФАЙЛ - имя сокета, доступ - восьмеричное значение прав доступа к нему.
	Пример:
	`Socket = %var_dir/.daemon 0660`
	Количество значений в списке **Socket** не ограничено, **Dr.Web Daemon** будет работать со всеми из описанных сокетов.
	Чтобы **Dr.Web Daemon** принимал запросы через все доступные интерфейсы, для параметра следует задать значение `3000 0.0.0.0`.
	Значение по умолчанию:
	`Socket = %var_dir/run/.daemon`

SocketTimeout = {числовое значение}	Время в секундах, отведенное для приема/передачи всех данных через сокет (время сканирования файла не

	учитывается). Если указано значение 0, время не будет ограничено. Значение по умолчанию: **SocketTimeout** = 10

Следующие параметры могут быть использованы для уменьшения времени проверки архивов (за счет отказа от проверки некоторых объектов в архиве). Если объект подпадает под ограничения, созданные этими параметрами, то к нему применяется действие **ArchiveRestriction**, которое задано в файлах конфигурации различных фильтров.

MaxCompressionRatio = {числовое значение}	Максимальный коэффициент сжатия, т. е. отношение длины файла в распакованном виде к длине файла в запакованном виде (внутри архива). Если коэффициент превышает данное значение, файл не будет извлечен и, соответственно, не будет проверен. Параметр может принимать только натуральные значения. Если указано значение 0, проверка коэффициента сжатия проводиться не будет. Значение по умолчанию: **MaxCompressionRatio** = 5000
CompressionCheckThreshold = {числовое значение}	Минимальный размер файла внутри архива в килобайтах, начиная с которого будет производиться проверка коэффициента сжатия (если это предписано параметром **MaxCompressionRatio**). Если указано значение 0, проверка производиться не будет. Значение по умолчанию: **CompressionCheckThreshold** = 1024

MaxFileSizeToExtract = {числовое значение}	Максимальный размер файла в килобайтах, извлекаемого из архива. Если размер файла внутри архива превышает это значение, он будет пропущен. Если указано значение 0, максимальный размер не ограничен. Значение по умолчанию: **MaxFileSizeToExtract** = 40960
MaxArchiveLevel = {числовое значение}	Максимальный уровень вложенности архивов (когда архив вложен в архив, который тоже вложен в архив и т.д.). При превышении этого уровня архив будет пропущен (не будет проверен). Если указано значение 0, уровень вложенности архивов не будет ограничиваться. Значение по умолчанию: **MaxArchiveLevel** = 8
ClientsLogs = {список строк}	Параметр разделения файлов журнала. Если при обращении к **Dr.Web Daemon** клиент передает в расширенных опциях свой идентификатор, файл журнала клиента заменяется на тот, который указан в параметре ClientsLogs. Описания логов разделяются запятыми или пробелами. В случае задания в параметре больше шести файлов журнала строка конфигурационного файла считается неверной.

	Файлы отчета клиентов задаются в виде: `ClientsLogs=<имя клиента1>: <путь к файлу>,<имя клиента2>: <путь к файлу>.` Имя клиента может быть одним из следующих: • `web` — **Dr.Web ICAPD**; • `smb_spider` — **Dr.Web Samba SpIDer**; • `mail` — **Dr.Web MailD**; • `drwebdc` — консольный клиент **Демона Dr.Web**; • `kerio` — **Dr.Web для интернет-шлюзов Kerio**; • `lotus` — **Dr.Web для IBM Lotus Domino**. **Пример**: **drwebdc:** `/var/drweb/log/drwebdc.log`, **smb:** `syslog`, **mail:** `/var/drweb/log/drwebmail.log` Значение по умолчанию: **ClientsLogs** =
MaxBasesObsolescencePeriod = {числовое значение}	Максимальный период времени (в часах) с момента последнего обновления, в течение которого вирусные базы считаются "свежими". По истечении этого времени, в консоли выводится уведомление о том, что базы устарели. Если установлено значение 0, то актуальность вирусных баз не проверяется.

	Значение по умолчанию: **MaxBasesObsolescencePeriod =** 24
MessagePatternFileName = {путь к файлу}	Путь к файлу шаблона сообщения об истечении срока действия лицензии. Позволяет пользователю определить сообщение об истечении срока действия лицензии в удобном для него виде. В шаблоне сообщения могут быть использованы следующие переменные, вместо которых будут автоматически подставлены следующие значения: • $EXPIRATIONDAYS — количество дней до истечения срока лицензии; • $KEYFILENAME — путь к лицензионному ключевому файлу; • $KEYNUMBER — номер лицензии; • $KEYACTIVATES — дата активации лицензии; • $KEYEXPIRES — дата завершения срока действия лицензии. Если пользовательский шаблон отсутствует, используется сообщение по умолчанию на английском языке.
	Значение по умолчанию: **MessagePatternFileName =** % etc_dir/templates/drwebd/msg.tmpl
MailTo = {адрес электронной почты}	Почтовый адрес администратора для отправки сообщений об истечении срока действия лицензии, устаревании вирусных баз и пр.
	Значение по умолчанию: **MailTo =**

Модуль интеграции с файловым сервером Samba

Интеграция сервиса резидентной антивирусной проверки, осуществляемой компонентом **Dr.Web Daemon**, с сервером файловой службы **Samba** осуществляется через специальный компонент **Dr.Web Samba VFS SpIDer**, задача которого состоит в том, чтобы отправлять на антивирусную проверку модулю **Dr.Web Daemon** файлы, к которым обращаются клиенты файловой службы **Samba**.

Требования

Для интеграции файловой службы **Samba** с сервисом антивирусной защиты **Dr.Web** необходимо наличие следующих компонентов:

- Установленный и настроенный сервер файловой службы **Samba** версии не ниже 3.0.END (3.0.x — 3.5.x).
- Установленный и запущенный **Dr.Web Daemon** и Антивирусное ядро **Dr.Web Engine** версии 6.0.2;
- Подключаемый модуль **Dr.Web Samba SpIDer**, собранный с поддержкой тех же опций, которые использует **Samba**.
- Для использования **Консоли управления** (веб-интерфейс) необходимо наличие в системе установленного компонента **Webmin**.

Подключение модуля Dr.Web Samba SpIDer

К конфигурационному файлу **Samba** (`/etc/samba/smb.conf` по умолчанию) необходимо добавить раздел, пример которого приведен ниже, и отредактировать его в соответствии с используемыми путями.

```
[drweb_audit]
comment = Dr.Web protected directory
path = /каталог/который/нужно/защитить/
vfs objects = smb_spider
smb_spider: config = <путь к конфигурационному файлу
 или адрес сокета Агента>
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

После этого необходимо перезапустить файловый сервер **Samba**.

Если вы хотите, чтобы для каждого защищаемого разделяемого ресурса можно было задавать свой файл настроек, добавьте строку с путем к конфигурационному файлу

```
smb_spider: config = %etc_dir/smp_spider.conf
```

в секцию для каждого из ресурсов.

Dr.Web Samba VFS SpIDer может также получать необходимые настройки от модуля **Dr.Web Agent**. Для подключения этой возможности в конфигурационном файле `smb.conf` замените строку с путем к конфигурационному файлу `smb_spider.conf` для каждого защищаемого ресурса на следующую:

```
smb_spider: config = <адрес сокета Dr.Web Agent>
```

Пример:

UNIX сокет (используется **Dr.Web Agent** запущенный на локальной машине):

```
smb_spider: config = local:%var_dir/ipc/.agent
```

TCP-сокет (используется **Dr.Web Agent** запущенный на удаленной машине в сети):

```
smb_spider: config = inet:4040@127.0.0.1
```

Обратите внимание, что если вы укажете адрес **Dr.Web Agent** в `smb_spider: config`, то **Dr.Web Samba SpIDer** также будет посылать статистику **Dr.Web Agent**. Для корректной работы функции сбора и отсылки статистики соответствующая строка с адресом **Dr.Web Agent** должна быть добавлена в каждую из секций для каждого из разделяемых ресурсов.

Запуск

Монитор **Dr.Web Samba SpIDer** активизируется, когда какой-нибудь из клиентов пытается открыть ресурс общего доступа на сервере. При его инициализации производятся следующие действия:

- проверяется версия интерфейса **Dr.Web Samba SpIDer** и сервера **Samba**;
- **Dr.Web Samba SpIDer** читает файл конфигурации (`%etc_dir/smb_spider.conf` по умолчанию);
- **Dr.Web Samba SpIDer** отслеживает файловые операции, производимые клиентами.

На первом и втором этапах **Dr.Web Samba SpIDer** выводит информацию в системный журнал **syslog**. По умолчанию используются следующие значения параметров управляющих работой системного сервиса `syslogd`:

```
SyslogFacility = Daemon
SyslogPriority = Info
```

Взаимодействующие элементы рекомендуется запускать в таком порядке:

- **Dr.Web Daemon**;
- **Dr.Web Samba VFS SpIDer**.

Для обеспечения оптимальной производительности рекомендуется обратить особое внимание на настройку прав доступа **Dr.Web Daemon** к ресурсам.

Если **Dr.Web Daemon** запущен с правами, которые не обеспечивают ему доступ на чтение (для поиска вирусов) и на запись (для удаления, лечения и т.д.) к файлам на разделяемом ресурсе, он по умолчанию будет работать в режиме нелокального сканирования и получать нужные ему файлы через сокет. Это значительно снизит скорость работы.

Dr.Web Daemon не может сканировать файлы размером больше 2 гигабайт, поэтому **Dr.Web Samba VFS SpIDer** не будет отправлять такие файлы на сканирование.

Настройки

Можно запустить **Dr.Web Samba VFS SpIDer** с настройками по умолчанию, но лучше настроить его для соответствия необходимым требованиям и условиям эксплуатации. Конфигурационный файл `smb_spider.conf` по умолчанию читается из директории `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать в конфигурационном файле `smb.conf`, добавив туда следующую строку:

```
smb_spider: config = /my/new/path/smb_spider.conf
```

Устройство конфигурационного файла и краткое описание его параметров приведены в разделе Конфигурационные файлы.

Секция [`DaemonCommunications`]

`Address` = {список адресов}	Список адресов сокетов для связи с **Dr.Web Daemon**. Адреса в списке разделяются запятыми. Значение по умолчанию: **`Address`** = `pid:%var_dir/run/drwebd.pid`
`Cache` = {логический}	Хранить ли в памяти IP-адрес узла, на котором работает **Dr.Web Daemon**. Если установлено в `No`, то IP-адрес узла будет запрашиваться каждый раз при возникновении необходимости проверить тот или иной файл на вирусы. Этот параметр используется только в случае, когда связь с **Dr.Web Daemon** осуществляется через TCP-сокеты (см. предыдущий параметр). Значение по умолчанию: **`Cache`** = `Yes`

Timeout = {числовое значение}	Время в секундах, отведенное для сканирования одного файла. Если значение этого параметра равно 0, время сканирования не ограничено. Значение по умолчанию: **Timeout** = 120
UseTcpNodelay = {логический}	Возможность использовать опцию TCP_NODELAY для настройки работы TCP-сокета, по которому осуществляется связь с **Dr.Web Daemon**. Этот параметр используется только в случае каких-либо проблем с устойчивостью сетевого соединения. Значение по умолчанию: **UseTcpNodelay** = No

Секция [Scanning]

HeuristicAnalysis = {Off | On}	Включение/отключение использования **Эвристического анализатора**. Эвристический анализ делает возможным обнаружение неизвестных вирусов по априорным соображениям об устройстве вирусного кода. Особенностью этого типа поиска вирусов является вероятностный характер обнаружения заражения, что позволяет говорить не о зараженных, а о подозрительных объектах. При отключении этого режима осуществляется только поиск известных вирусов по вирусным базам **"Доктор Веб"** Целый класс программ ввиду использования сходного с вирусами кода может вызывать ложные срабатывания **Эвристического анализатора**. Кроме того, данный режим может

	незначительно увеличить время проверки. Данные обстоятельства могут быть доводами в пользу отключения **Эвристического анализатора**. Вместе с тем, включение этого типа анализа увеличивает надежность антивирусной защиты. Все файлы, обнаруженные **Эвристическим анализатором**, лучше всего отправить разработчикам через сайт http://vms.drweb.com/sendvirus/ (предпочтительнее) или по электронной почте на адрес newvirus@drweb.com. Отправку подозрительных файлов рекомендуется производить следующим образом: запаковать файл в архив с паролем, пароль сообщить в теле письма, при этом желательно приложить отчет **Dr.Web Daemon** или **Dr.Web Scanner**
	Значение по умолчанию: **HeuristicAnalysis** = On
StripPath = {числовое значение}	Позволяет удалить заданное количество сегментов из начала пути для сканирования. Если задано значение 0, то используется полный путь. При значении, равном 1, из пути убирается сегмент до первого разделителя пути — символа "/" (слеш) — включительно. При значении, равном 2, из пути убирается сегмент до второго разделителя пути включительно. **Пример:** Допустим, в качестве пути для сканирования задан path = /некий/путь/к/file.ext Тогда при StripPath = 1 путь примет следующий вид: path = некий/путь/к/file.ext

	При `StripPath = 2` путь примет вид: `path = путь/к/file.ext.` Значение по умолчанию: **`StripPath`** `= 0`

`PrefixPath` =
`{путь к каталогу}`
	Задает сегмент пути, который добавляется к началу пути для сканирования, после того как этот путь был обработан параметром `StripPath`.
	Значение данного параметра не должно оканчиваться символом "/" (слеш). Необходимый разделитель пути будет добавлен программой автоматически.
	Пример:
	Допустим, в качестве пути для сканирования задан
	`path = /некий/путь/к/file.ext`
	Он был обработан параметром StripPath со значением 2 и принял вид:
	`path = путь/к/file.ext`
	Тогда после автоматической подстановки разделителя пути "/" и обработки параметром `PrefixPath = /совсем/другой`, путь примет следующий вид:
	`path = /совсем/другой/путь/к/file.ext`
	Значение по умолчанию:
	`PrefixPath` =

`MaxFileSizeToScan` = `{числовое значение}`	Устанавливает максимальный размер файла для сканирования в килобайтах. При значении 0 сканироваться будут файлы любого размера. Значение по умолчанию: **`MaxFileSizeToScan`** `= 0`

ScanMode = {onWrite | onRead | onAccess}	Возможны следующие значения данного параметра: • onAccess — файлы будут сканироваться при попытке открытия или запуска и при закрытии (после создания или изменения). • onRead — файлы будут сканироваться только при попытке открытия или запуска. Этот режим позволяет увеличить скорость работы системы, но снижает уровень антивирусной защиты, поскольку файлы не будут проверятся при копировании на сервер. Хотя зараженные файлы не могут быть запущены удаленными пользователями в этом режиме, такие файлы могут быть запущены пользователями с локальным доступом к общей директории (т.е. в обход сервера **Samba**). • onWrite — файлы будут сканироваться только при закрытии, после создания или изменения. Этот режим позволяет еще больше увеличить скорость работы системы, но существенно снижает уровень защиты, поскольку файлы будут запускаться без проверки. Пользователь, имеющий локальный доступ к общей директории (т.е. в обход сервера **Samba**), может скопировать туда зараженный файл, который может быть впоследствии запущен удаленными пользователями. Значение по умолчанию: **ScanMode** = onAccess
RewriteDataBase = {логический}	При значении Yes данного параметра базы заблокированных (инфицированных) и разрешенных

	(чистых) файлов перезаписываются, как только к директории общего доступа обращается новый пользователь. Значение по умолчанию: **RewriteDataBase** = Yes
BlockedCacheSize = {числовое значение}	Устанавливает размер базы заблокированных (инфицированных) файлов в байтах. При значении параметра равном 0, база заблокированных файлов не создается. При значении, отличном от нуля, в базу записываются md5 хеш-суммы содержимого файлов, уже проверенных **Dr.Web Daemon**, и признанных инфицированными. При последующих попытках открытия этих файлов их md5 хеш-суммы сверяются с хранящимися в базе, и в случае совпадения файл признается инфицированным без отсылки его на проверку **Dr.Web Daemon**. Значение по умолчанию: **BlockedCacheSize** = 4096
AllowedCacheSize = {числовое значение}	Устанавливает размер базы разрешенных (чистых) файлов в байтах. При значении параметра, равном 0, база разрешенных файлов не создается. При значении, отличном от нуля, в базу записываются md5 хеш-суммы уже проверенных Демоном и признанных чистыми файлов. При последующих попытках открытия этих файлов их md5 хеш-суммы сверяются с хранящимися в базе, и в случае совпадения файл признается чистым без отсылки его на проверку **Dr.Web Daemon**. Значение по умолчанию: **AllowedCacheSize** = 4096

LocalScan = {логический}	Режим локального сканирования, когда **Dr.Web Daemon** передается только путь к файлу для проверки. При LocalScan = Yes **Dr.Web Daemon** будет сканировать файлы в локальном режиме. Значение по умолчанию: **LocalScan** = yes

Dr.Web Samba VFS SpIDer может самостоятельно совершать действия с файлами в случае, когда **Dr.Web Daemon** по какой-либо причине не хватило прав, либо если используется режим нелокального сканирования.

Секция [Actions]

LicenseLimit = {действие}	Действие, совершаемое с файлами, при проверке которых произошла ошибка лицензии (например, когда срок действия лицензии истек). Допустимые значения параметра: pass, reject. Значение по умолчанию: **LicenseLimit** = reject
Infected = {действие}	Действие при обнаружении файла, зараженного известным вирусом. Допустимые значения параметра: cure, rename, discard, quarantine, reject. Значение по умолчанию: **Infected** = quarantine
Suspicious = {действие}	Действие при обнаружении подозрительного файла (возможно, зараженного неизвестным вирусом).

	Допустимые значения параметра: `pass, rename, discard, quarantine, reject.` Значение по умолчанию: **`Suspicious`** = `quarantine`
`Incurable` = `{действие}`	Действие при обнаружении файла, который заражен и не может быть вылечен. Допустимые значения параметра: `rename, discard, quarantine, reject.` Значение по умолчанию: **`Incurable`** = `quarantine`
`Adware` = `{действие}`	Действие при обнаружении программы для показа рекламы (adware). Допустимые значения параметра: `pass, rename, discard, quarantine, reject.` Значение по умолчанию: **`Adware`** = `quarantine`
`Dialers` = `{действие}`	Действие при обнаружении программы автоматического дозвона. Допустимые значения параметра: `pass, rename, discard, quarantine, reject.` Значение по умолчанию: **`Dialers`** = `quarantine`
`Jokes` = `{действие}`	Действие при обнаружении программы-шутки, которая может пугать или раздражать пользователя.

	Допустимые значения параметра: `pass, rename, discard, quarantine, reject.` Значение по умолчанию: **`Jokes`** = `quarantine`
`Riskware` = `{действие}`	Действие при обнаружении потенциально опасной программы, которая может быть использована не только ее владельцем, но и злоумышленниками. Допустимые значения параметра: `pass, rename, discard, quarantine, reject.` Значение по умолчанию: **`Riskware`** = `quarantine`
`Hacktools` = `{действие}`	Действие при обнаружении программы, которая используется для взлома компьютеров. Допустимые значения параметра: `pass, rename, discard, quarantine, reject.` Значение по умолчанию: **`Hacktools`** = `quarantine`
`Archives` = `{действие}`	Действие при обнаружении архива, содержащего зараженные файлы. Допустимые значения параметра: `rename, discard, quarantine, reject.` Для того чтобы получить возможность удалять эти архивы, необходимо указать значение `Yes` для параметра **`EnableDeleteArchiveAction`** в главном конфигурационном файле `drweb32.ini`.

	Значение по умолчанию: **Archives** = quarantine
SkipObject = {действие}	Действие, совершаемое с файлами, которые не могут быть проверены **Dr.Web Daemon** (защищенные паролем или испорченные архивы, символические ссылки, файлы нестандартных форматов и т.п.). Допустимые значения параметра: pass, reject. Значение по умолчанию: **SkipObject** = pass
ArchiveRestriction = {действие}	Действие, совершаемое с архивами, которые не могут быть проверены **Dr.Web Daemon** по причине превышения значений ряда параметров (степени сжатия, размера запакованных объектов, степени вложенности), заданных в главном конфигурационном файле. Допустимые значения параметра: pass, reject. Значение по умолчанию: **ArchiveRestriction** = pass
ScanningErrors = {действие}	Действие, совершаемое с файлами, вызывающими у **Dr.Web Daemon** ошибки в процессе проверки. Например, нехватка памяти или недостаток прав для работы. Допустимые значения параметра: pass, reject. Значение по умолчанию: **ScanningErrors** = reject

ProcessingErrors = {действие}	Действие, совершаемое с файлами, при проверке которых произошла ошибка обработки (например, **Dr.Web Samba SpIDer** был неправильно настроен, либо истекло время ожидания ответа от **Dr.Web Daemon**). Допустимые значения параметра: pass, reject. Значение по умолчанию: **ProcessingErrors** = reject
ShellScriptForBlockedFile = {путь к файлу}	Путь к скрипту командной оболочки, который будет запускаться при блокировке файла. **Dr.Web Samba VFS SpIDer** передает скрипту следующие параметры: • FileName — имя зараженного файла; • UserName — имя, под которым вошел в систему пользователь, пытающийся получить доступ к заблокированному файлу; • UserHost — узел, с которого зашел в систему пользователь, пытающийся получить доступ к заблокированному файлу; • DaemonReport — отчет **Dr.Web Daemon**. Пример такого скрипта (файл smb_script.sh) расположен в каталоге %bin_dir/doc/samba/ Значение по умолчанию: **ShellScriptForBlockedFile** =
Quarantine =	Путь к каталогу **Карантина**.

	Значение по умолчанию: **Quarantine** = %var_dir/infected/
QuarantineFilesMode = {права доступа}	Права доступа к файлам, находящимся в **Карантине**. Значение по умолчанию: **QuarantineFilesMode** = 0660

Секция [Logging]

LogFileName = {syslog | путь к файлу}	Имя файла журнала или syslog, если нужно использовать системный сервис **syslog**. Значение по умолчанию: **LogFileName** = syslog
Level = {уровень подробности}	Уровень подробности ведения журнала. Допускается использование следующих уровней: • Quiet • Errors • Alerts • Info • Debug • Verbose Значение по умолчанию: **Level** = Info
SyslogFacility = {метка syslog}	Метка записи при использовании системного сервиса **syslog**. Значение по умолчанию: **SyslogFacility** = Daemon

SyslogPriority = {уровень подробности}	Уровень подробности ведения журнала системным сервисом **syslog**. Допускается использование следующих уровней: • Alert • Info • Notice • Debug
	Значение по умолчанию: **SyslogPriority** = Info

Dr.Web консоль для файловых серверов UNIX

Настройка программного комплекса **Dr.Web для файловых серверов UNIX** может быть осуществлена через веб-интерфейс **Dr.Web консоль для файловых серверов UNIX**. Он реализован в виде дополнения к интерфейсу **Webmin** (подробная информация об интерфейсе **Webmin** доступна на официальном сайте производителя: http://www.webmin.com/).

Для успешной работы веб-интерфейса **Dr.Web консоль для файловых серверов UNIX** необходимо, чтобы в системе были установлены следующие модули **Perl:**

- **XML::Parser** — модуль для преобразования документов в формате XML;
- **XML::XPath** — набор модулей для преобразования инструкций Xpath;
- **CGI** — модуль для работы с Common Gateway Interface;
- **Cwd** — модуль для определения текущей рабочей директории какого-либо процесса;
- **Data::Dumper** — модуль для записи произвольных структур данных в память и чтения их из памяти;
- **Text::Iconv** — модуль для управления функцией преобразования кодировки `iconv()`;
- **perl-devel** (или **libperl-dev**, в зависимости от дистрибутива) — пакет для сборки `Text::Iconv`;
- **JSON** — модуль для преобразования данных в формате JSON (JavaScript Object Notation).
- **Encode::CN** – модуль для работы с китайской кодировкой.
- **Encode::HanExtra** – модуль с дополнительным набором китайских кодировок.
- **Switch** – модуль для использования конструкций `switch-case`.

Недостающие модули рекомендуется устанавливать из командной строки. Для установки требуются права `root`. Имена модулей могут различаться, однако, как правило, они содержатся в пакетах `perl-Convert-BinHex`, `perl-IO-stringy`, `perl-MIME-tools`, `perl-XML-Parser`, `perl-XML-XPath`. Для установки в `rpm` системах рекомендуется выбирать `noarch.rpm` пакеты.

При запуске в разных браузерах и при использовании разных версий **Webmin** во внешнем виде веб-интерфейса могут наблюдаться отличия от приведенных скриншотов.

Ввиду особенности реализации **Webmin**, интерфейс **Консоли** не может быть корректно отображен в браузере **Internet Explorer** 7. В случае возникновения проблем с отображением страниц, попробуйте воспользоваться **Internet Explorer** 8 или 9 (и более поздними версиями), или использовать другой браузер.

Установка

Для начала работы с **Dr.Web консоль для файловых серверов UNIX** необходимо:

- установить **Webmin**;
- подключить модуль **Dr.Web консоль для файловых серверов UNIX** к **Webmin** (расположен в директории `%bin_dir/web/`).

Подключение модулей, а также настройка дополнительных параметров самого **Webmin** осуществляется через его веб-интерфейс.

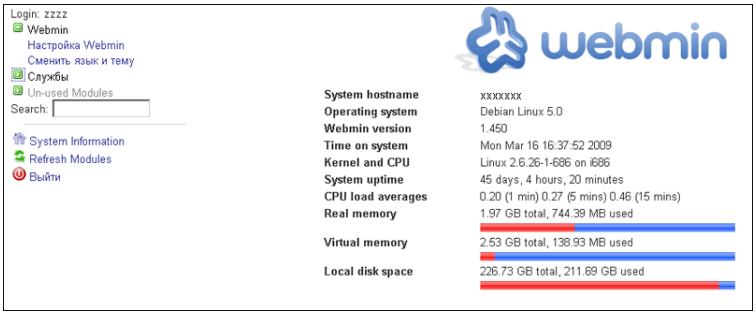


Рис. 15. Главная страница Webmin

Установка дополнительных модулей происходит в разделе **Настройка Webmin** секции **Webmin** основного меню, в подразделе Модули **Webmin**.

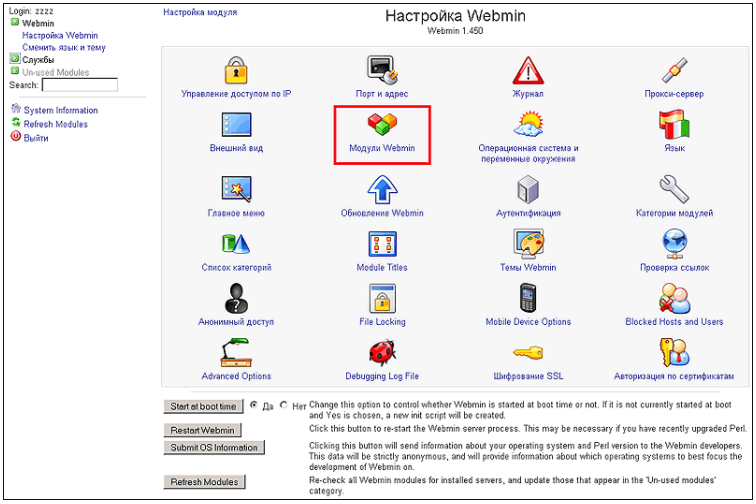


Рис. 16. Настройка Webmin

Чтобы установить нужный модуль, в открывшемся окне **Модули Webmin** нажмите кнопку **Обзор** напротив строки **Из локального файла**. Откроется отдельное окно браузера для

навигации по списку файлов и директорий вашей системы, в котором вы сможете выбрать соответствующий установочный пакет (`%bin_dir/web/drweb-samba-web.wbm.gz` по умолчанию).

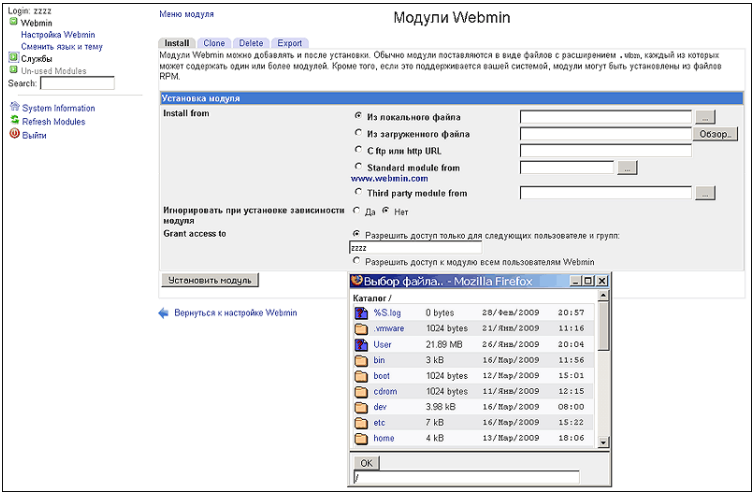


Рис. 17. Добавление модулей Webmin

После одного клика левой кнопкой мыши на какой-либо элемент списка в строке ввода прописывается путь к этому элементу.

После повторного клика левой кнопкой мыши на иконку или название директории, последняя открывается.

Повторным кликом левой кнопкой мыши на иконку или название файла вы выбираете соответствующий модуль для установки в **Webmin**. Соответственно, окно выбора файла закрывается, а путь к этому файлу появляется в поле **Из локального файла**. Также вы можете нажать кнопку **OK** после того, как выбор нужного файла будет сделан.

Выбрав необходимый файл, нажмите кнопку **Установить модуль**. По завершении установки в секции **Службы** основного меню появится ссылка на новый раздел **Dr.Web консоль для**

файловых серверов Unix.

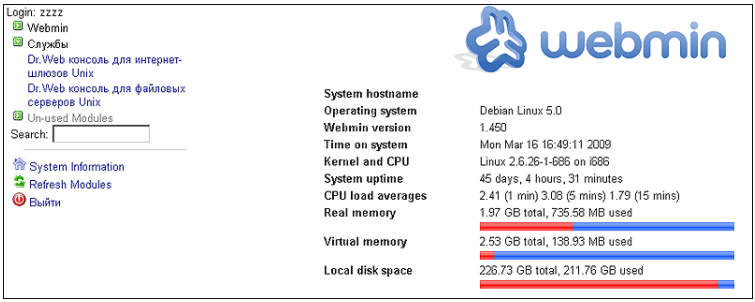


Рис. 18. Новый пункт меню "Dr.Web консоль для файловых серверов Unix"

Настройка

Настроить язык веб-интерфейса **Webmin** и **Dr.Web консоль для файловых серверов UNIX** можно в разделе **Сменить язык и тему** секции **Webmin** основного меню.

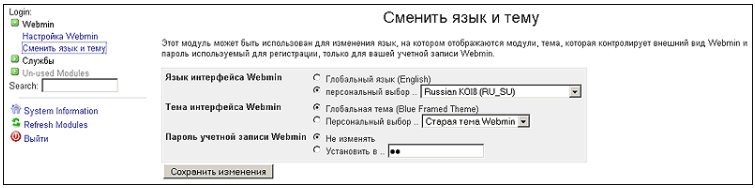


Рис. 19. Смена языка и темы

Если вы хотите, чтобы были русифицированы оба веб-интерфейса, то в меню раздела "**Язык интерфейса Webmin -> Персональный выбор..**" необходимо выбрать пункт **Russian KOI8 (RU_SU)** или **Russian CP1251 (RU_RU)**. Если вы выберете **Russian UTF-8 (RU.UTF-8)**, то русифицирован будет только веб-интерфейс **Dr.Web консоль для файловых серверов UNIX**.

На той же странице можно поменять оформление веб-

интерфейса **Webmin** (в меню раздела **Тема интерфейса Webmin** -> **Персональный выбор..**) и установить новый пароль для доступа к системе (в меню раздела **Пароль учетной записи Webmin** -> **Установить в..**).

Для того, чтобы изменения были применены к интерфейсу **Webmin**, после нажатия кнопки **Сохранить изменения** необходимо обновить страницу.

Базовые настройки модуля **Dr.Web консоль для файловых серверов UNIX** можно найти, нажав  в шапке страницы веб-интерфейса. На открывшейся странице вы сможете указать путь к конфигурационному файлу `smb_spider.conf`, количество файлов на странице **Карантина** и режим работы **Консоли**.

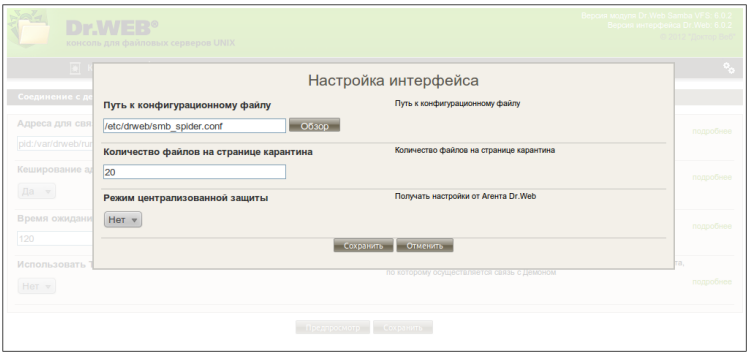


Рис. 20. Настройка модуля

Пользовательский интерфейс

При навигации внутри раздела **Dr.Web консоль для файловых серверов UNIX** невозможно перейти на предыдущую страницу при помощи стандартной функции браузера **Назад**. Если вы нажмете кнопку **Назад** или соответствующую комбинацию клавиш, вы попадете к предыдущему разделу главного меню.

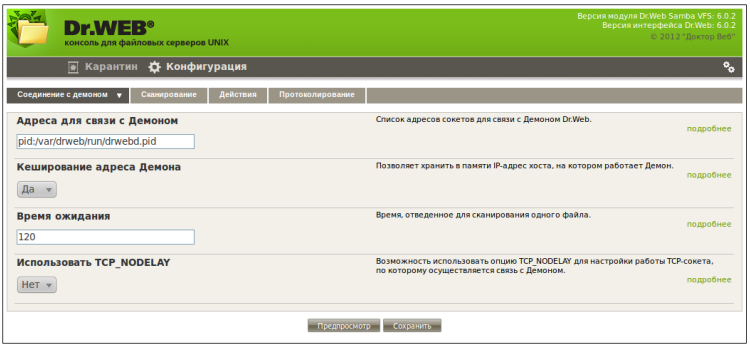


Рис. 21. Dr.Web консоль для файловых серверов UNIX

Справа от заголовка модуля вы найдете информацию о текущей версии **Dr.Web Samba VFS SpIDer** и веб-интерфейса **"Доктор Веб"**.

Под заголовком модуля расположены две секции: **Карантин** и **Конфигурация**. По умолчанию при входе в раздел открывается вкладка **Соединение с демоном** секции **Конфигурация**.

Нужные значения параметров на каждой вкладке могут быть выбраны из раскрывающихся списков либо заданы вручную в соответствующих полях ввода. Подробное описание каждого параметра вы найдете в интерактивной справке по ссылке **подробнее**.

Конфигурация

Вы можете выбирать нужные значения параметров из раскрывающихся списков либо задавать эти значения вручную в соответствующих полях ввода.

После того, как вы изменили значение какого-либо параметра, вы можете одним щелчком мыши по соответствующей иконке рядом с параметром немедленно отменить изменение или восстановить настройки по умолчанию. Последняя операция доступна всегда, даже после сохранения изменений.

Если **Dr.Web для файловых серверов UNIX** используется в режиме центральной защиты, администратор сервера центральной защиты может заблокировать настройки. В таком случае вы не сможете изменять настройки **Dr.Web для файловых серверов UNIX**.

Для того, чтобы просмотреть все сделанные изменения, используйте кнопку **Предпросмотр**. На появившейся странице вы можете выбрать те изменения, которые желаете сохранить, отметив соответствующую ячейку. Если вы хотите внести дополнительные изменения, вы можете вернуться к предыдущей странице, нажав на кнопку **Продолжить редактирование**.

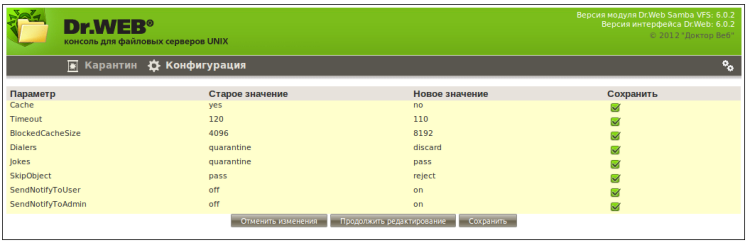


Рис. 22. Страница предпросмотра

Когда вы нажимаете на кнопку **Сохранить**, появляется уведомление **Конфигурация сохранена**. Щелкните по нему мышкой, чтобы вернуться к странице настроек.

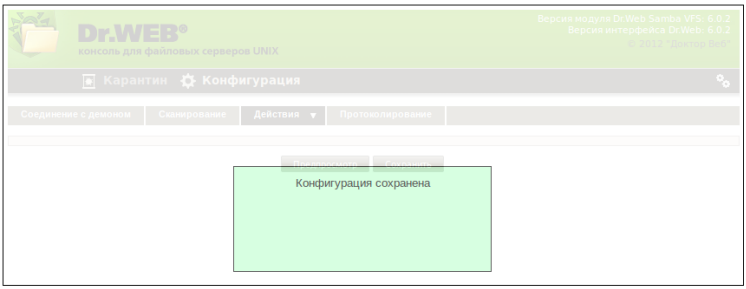


Рис. 23. Уведомление о сохранении

Изменения во вкладках **Сканирование** и **Действия** будут применены только после перезапуска сервера **Samba** или открытии новой пользовательской сессии.

Вкладка "Соединение с демоном"

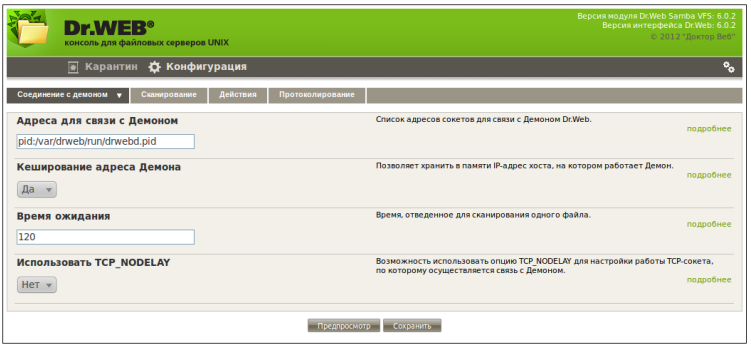


Рис. 24. Соединение с демоном

На данной вкладке вы можете настроить параметры работы с **Dr.Web Daemon** (например, указать адрес сокета **Dr.Web Daemon**, на котором он будет ожидать и принимать соединения, и максимальное время для сканирования одного файла).

Вкладка "Сканирование"

На данной вкладке вы можете подключить **Эвристический анализатор**, указать, в каком режиме будет осуществляться антивирусная проверка, задать ограничения на размер файла для сканирования, настроить пути к проверяемым каталогам.

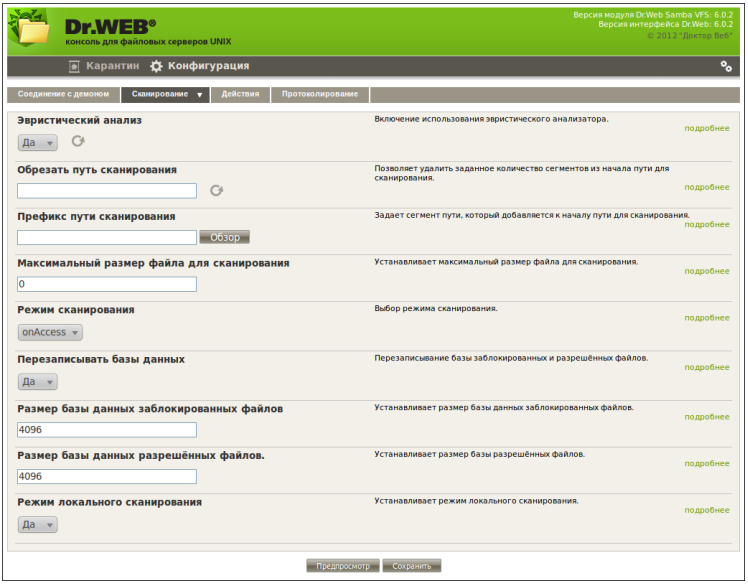


Рис. 25. Сканирование

Изменения во вкладках **Сканирование** и **Действия** будут применены только после перезапуска сервера **Samba** или открытии новой пользовательской сессии.

Вкладка "Действия"

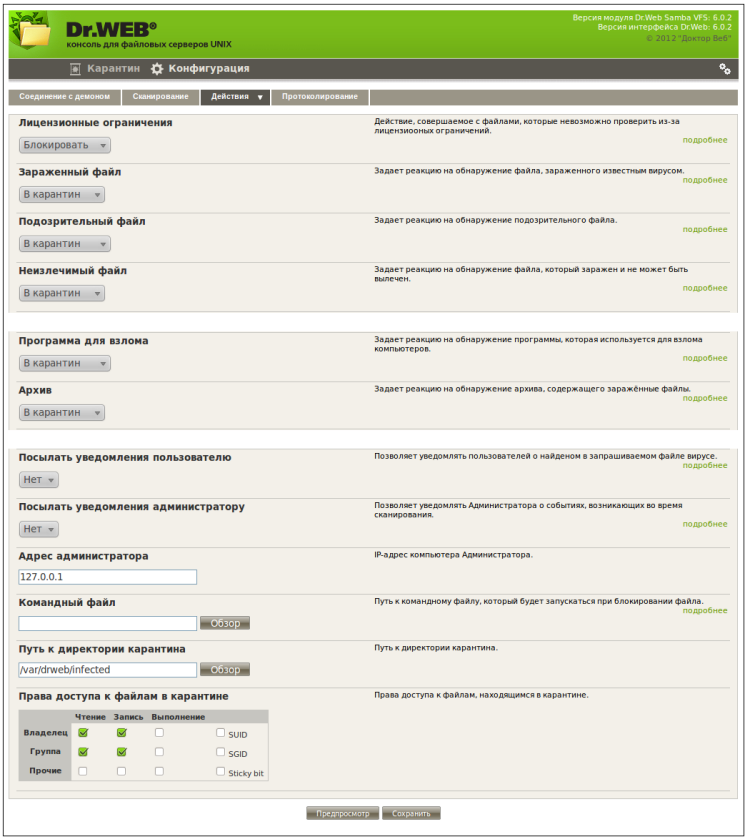


Рис. 26. Действия

На этой вкладке осуществляется настройка действий, применяемых антивирусным модулем к различным обнаруженным угрозам и к файлам, вызвавшим ошибки сканирования. Здесь вы также можете указать путь к каталогу **Карантина** и права доступа к перемещенным в **Карантин** файлам.

Изменения во вкладках **Сканирование** и **Действия** будут применены только после перезапуска сервера **Samba** или открытии новой пользовательской сессии.

Вкладка "Протоколирование"

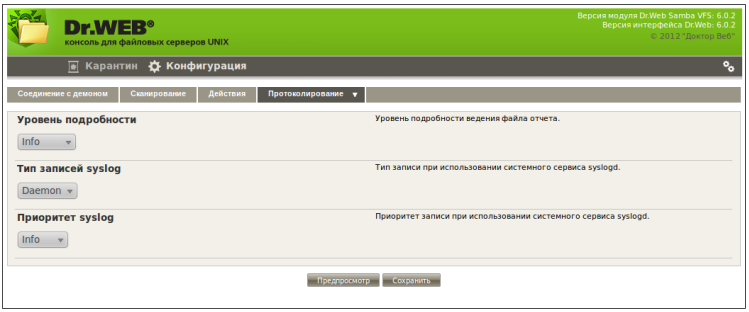


Рис. 27. Протоколирование

На данной вкладке вы можете настроить порядок ведения отчетов о работе **Dr.Web для файловых серверов UNIX**.

Карантин

Если для параметров из вкладки **Действия** указано значение `quarantine`, соответствующие заблокированные объекты помещаются в **Карантин**. Подозрительные файлы помещаются в **Карантин** целиком, а имена их создаются по специальным правилам. На главной странице секции **Карантин** представлен список ссылок на эти файлы, по которым их можно загрузить, чтобы ознакомиться с содержимым.

Рис. 28. Карантин

Чтобы удалить какой-либо файл из каталога **Карантина**, нужно отметить его и нажать кнопку **Удалить**.

Работа в Enterprise-режиме

Для начала работы **Консоли** в режиме централизованной защиты, необходимо произвести настройку **Dr.Web Agent**, описанную в соответствующем разделе. После внесения необходимых изменений откройте базовые настройки **Консоли**, нажав кнопку  в верхнем меню навигации web-интерфейса. В открывшемся окне настроек установите `Да` в качестве значения параметра `Режим централизованной защиты`.

Параметр `Режим централизованной защиты` может принимать 2 значения:

- `Нет` – в данном режиме **Консоль** работает с локальными конфигурационными файлами и не имеет доступа к конфигурации, получаемой **Dr.Web Agent** от **Dr.Web Enterprise Server**. Изменения конфигурации, внесенные в данном режиме, вступят в силу только после перевода **Dr.Web Agent** в режим `Standalone`.

- Да – **Консоль** получает конфигурационные данные из сокета **Dr.Web Agent**. В случае, если при этом **Dr.Web Agent** работает в Standalone режиме, будет выведено предупреждение вида:

  Ошибка получения настроек: не удаётся установить соединение с Агентом Dr.Web.

При возникновении проблем подключения к серверу **Dr.Web Enterprise Server**, возможны следующие варианты поведения **Консоли**:

- Если при первом подключении (т.е. в случае, если вы ранее не работали с данным сервером) сервер недоступен, либо авторизация прошла неудачно, **Dr.Web Agent** завершит свою работу. В этом случае проверьте настройки и попробуйте перезапустить **Dr.Web Agent** и **Консоль**.
- Если ранее вы уже подключались к серверу централизованной защиты, но в данный момент он недоступен (например, в случае проблем с соединением), **Dr.Web Agent** использует резервные копии конфигурационных файлов, полученных от сервера во время предыдущего подключения. Данные файлы зашифрованы и не предназначены для правки пользователем. Попытка изменить их вручную приведёт к их неработоспособности.

Настройка прав доступа

При работе в режиме Enterprise, администратор **Центра Управления Dr.Web** может частично либо полностью заблокировать возможность настройки пользователем компонентов **Dr.Web**, установленных на рабочей станции.

Чтобы установить права пользователя рабочей станции:

- Войдите в **Центр Управления Dr.Web**. Обратите внимание, что для редактирования настроек антивирусного ПО **Dr.Web** на рабочей станции, а также редактирования прав доступа к настройкам, администратор должен обладать достаточными правами.

- Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции. В открывшемся управляющем меню (панель слева) выберите пункт **Права**. Откроется окно настройки прав.

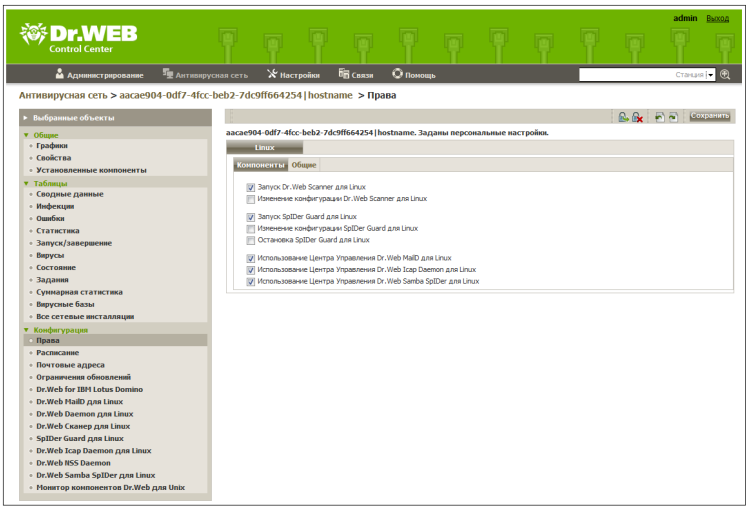


Рис. 29. Окно настройки прав пользователя рабочей станции

- В пункте **Компоненты** выберите компоненты, которые будут доступны для изменения пользователю рабочей станции. Например, чтобы разрешить изменение конфигурации **Dr.Web для файловых серверов UNIX** пользователем рабочей станции, установите флажок **Использование Центра Управления Dr.Web Samba SpIDer для Linux** и нажмите **Сохранить.**
- Чтобы отключить возможность изменения конфигурации **Dr.Web для файловых серверов UNIX** пользователем рабочей станции, снимите флажок **Использование Центра Управления Dr.Web Samba SpIDer для Linux** и нажмите кнопку **Сохранить.** При этом в окне **Консоли** пользователя рабочей станции будет выведено

соответствующее предупреждение, а кнопки **Предпросмотр** и **Сохранить** блокируются.

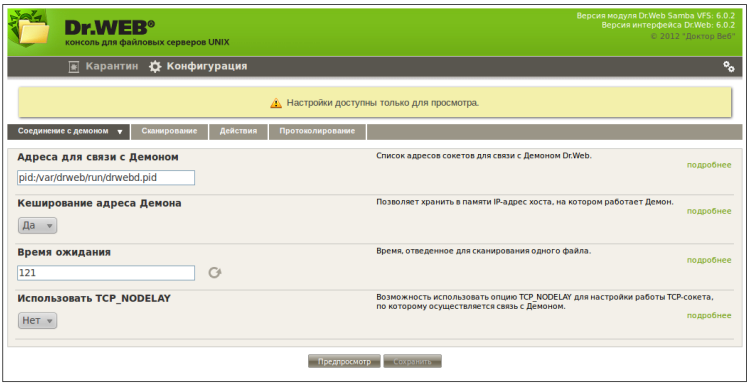


Рис. 30. Запрет на изменение конфигурации пользователем рабочей станции

Настройка конфигурации рабочей станции

При создании новой рабочей станции элементы ее конфигурации заимствуются от одной из групп, в которую она входит. Такая группа называется *первичной*. При изменениях в настройках первичной группы эти изменения наследуются входящими в группу станциями, за исключением случаев, когда станциям были заданы персональные настройки. При создании станции вы можете указать, какая из групп будет считаться первичной. По умолчанию это группа **Everyone**.

В условиях вложенных групп, если для станции не заданы персональные настройки, наследование элементов конфигурации осуществляется в соответствии со структурой вложенных групп. Поиск осуществляется вверх по иерархическому дереву, начиная с первичной группы станции, ее родительской группы и далее до корневого элемента дерева. Если при этом не были обнаружены персональные настройки, то наследуются элементы конфигурации группы **Everyone.**

Пример:

Структура иерархического списка представляет собой дерево следующего вида:

Группа `Group4` является первичной для станции `Station1`. При этом при наследовании настроек станцией `Station1` будет осуществляться поиск настроек в следующем порядке: `Station1 -> Group4 -> Group3 -> Group2 -> Group1 -> Everyone`.

Изменение конфигурации, унаследованной от первичной группы, возможно двумя способами:

- Через интерфейс **Центра Управления Dr.Web**. Для этого в интерфейсе **Центра Управления Dr.Web** в ыберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции. В открывшемся управляющем меню (панель слева) выберите компонент, который хотите настроить. Обратите внимание, что для редактирования настроек, вы должны обладать соответствующими правами. Процесс настройки аналогичен настройке посредством Консоли. После изменения настроек нажмите **Сохранить,** чтобы сохранить изменения.

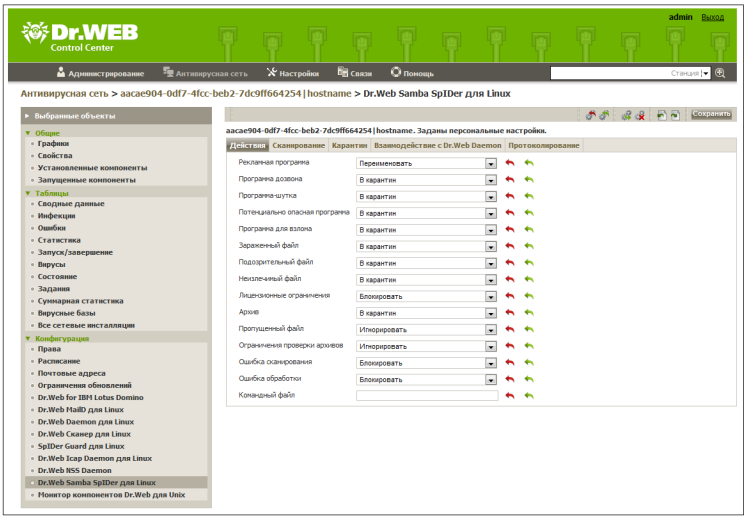


Рис. 31. Настройка Dr.Web Samba SpIDer для Linux через интерфейс Центра Управления Dr.Web

- При соответствующих настройках прав доступа параметры могут быть переопределены с помощью **Консоли**. Процесс настройки аналогичен работе в режиме Standalone. В случае недостатка прав у пользователя рабочей станции, **Консоль** предоставит доступ к настройкам в режиме «только для чтения».

Типы учетных записей администраторов

Учетные записи администраторов антивирусной сети делятся на 4 группы:

- *Администраторы с полными правами* имеют исключительные права на управление **Dr.Web Enterprise Server** и **Антивирусной сетью** в целом. Они могут просматривать и редактировать конфигурацию **Антивирусной сети**, а также создавать новые административные учетные записи. Администратор с такими правами также имеет полные права на управление антивирусным ПО на рабочей станции. При этом он может

ограничить, вплоть до полного запрета, вмешательство пользователя рабочей станции в управление антивирусным ПО.

Администратор с полными правами может просматривать и редактировать список имеющихся административных учетных записей.

- *Администраторы с правами "только для чтения"* могут только просматривать настройки **Антивирусной сети** в целом и отдельных ее элементов, но не менять их.
- *Администраторы групп с полными правами* имеют доступ ко всем системным группам и к тем пользовательским группам, управление которыми для них разрешено (включая вложенные). Возможно создание данных учетных записей только для пользовательских групп (подробнее см. Руководство администратора **Антивирусной сети Dr.Web® Enterprise Security Suite**). Для такого администратора в иерархическом дереве будут отображаться только те группы, к которым он имеет доступ.

  Администраторы групп не могут просматривать список имеющихся административных учетных записей.
- *Администраторы групп с правами "только для чтения"* могут обладать как полными правами для редактирования доступных им групп, так и правами "только для чтения".
- *Администраторы по умолчанию*. После установки **Dr.Web Enterprise Server** автоматически создается учетная запись **admin** - администратор с полными правами.

Таким образом, *Администраторы с полными правами* могут:

- Создавать новые и удалять имеющиеся учетные записи администраторов.
- Редактировать настройки всех администраторов **Антивирусной сети**.

Администраторы групп и *администраторы с правами "только для чтения"* могут:

- Редактировать часть настроек только своей учетной записи.

Контакты

Программный комплекс **Dr.Web для файловых серверов UNIX** находится в постоянном развитии. Наиболее свежую информацию о его обновлениях, а также новости можно получить на сайте:

http://www.drweb.com/

Отдел продаж:

http://buy.drweb.com/

Техническая поддержка:

http://support.drweb.com/

В письме необходимо предоставить следующую дополнительную информацию, которая поможет лучше разобраться в ситуации:

- полное название и версию дистрибутива UNIX-системы;
- версии компонентов программного комплекса **Dr.Web для файловых серверов UNIX**;
- конфигурационные файлы компонентов;
- файлы отчета компонентов.

Приложение. Пользовательские лицензии

Программный комплекс **Антивирус Dr.Web® для файловых серверов UNIX** доступен как в качестве отдельного продукта, так и в составе универсального и экономичного комплектов. Соответственно различаются и варианты лицензий.

Все лицензии могут быть приобретены на определенные сроки, например, на 1, 2 или 3 года, а также различаться по количеству защищаемых файловых серверов. Конкретные предложения по срокам, а также по другим количественным возможностям и ограничениям могут варьироваться для отдельных региональных партнеров компании **"Доктор Веб"**, а также могут быть в будущем пересмотрены компанией **"Доктор Веб"**. Для уточнения всех вопросов лицензирования следует обращаться к конкретному партнеру компании **"Доктор Веб"**. Контактные данные каждого из них можно найти на сайте компании **"Доктор Веб"** (http://partners.drweb.com/).

При покупке лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов **Всемирной Системы Обновлений Dr.Web** (**ВСО Dr.Web**), а также получать стандартную техническую поддержку компании и ее партнеров.

Защита файловых серверов

Программный комплекс лицензируется по количеству файловых серверов. Минимальная лицензия — на 1 файловый сервер.

Компоненты комплекса продолжают работать еще 24 часа после завершения срока действия лицензии.

Страница продукта находится по адресу: http://products.drweb.com/fileserver/unix/?lng=ru

© 2013 "Доктор Веб"