Dr.WEB®

Антивирус
для интернет-шлюзов UNIX

Защити созданное

Руководство администратора

Антивирус Dr.Web® для интернет-шлюзов UNIX
Версия 6.0.2
Руководство администратора
01.12.2014

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

Веб-сайт: www.drweb.com
Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Введение

В настоящей документации представлено описание следующих программных комплексов:

- **Антивирус Dr.Web® для интернет-шлюзов UNIX** для **Linux**;
- **Антивирус Dr.Web® для интернет-шлюзов UNIX** для **FreeBSD**;
- **Антивирус Dr.Web® для интернет-шлюзов 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 интернет-шлюзов UNIX** (далее – **Dr.Web для интернет-шлюзов UNIX**), а отличиям будут посвящены отдельные главы.

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

Проблема защиты интернет-шлюзов в UNIX-системах имеет три аспекта:

- Во-первых, это проверка всего входящего FTP- и HTTP-трафика на наличие вирусов, их диагностика и обезвреживание.

  При этом вирусы могут быть (и в большинстве случаев являются) отнюдь не специфичными для UNIX-систем. Через Интернет распространяются обычные Windows-вирусы, в том числе и макровирусы для **Word, Excel** и других офисных приложений.

- Во-вторых, это фильтрация доступа к HTML-ресурсам как по MIME-типу и размеру, так и по имени узла.
- В-третьих, это ограничение доступа к интернет-ресурсам благодаря использованию обновляемых тематических черных списков.

Программный комплекс **Dr.Web для интернет-шлюзов UNIX** выполняет все перечисленные функции.

Программный комплекс **Dr.Web для интернет-шлюзов 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** (**Dr.Web ESS**);

  По умолчанию в состав решения включен **Dr.Web Agent**, предназначенный для интеграции с **Dr.Web ESS** версии 6.0. Если вы хотите интегрировать ваш продукт с **Dr.Web ESS** версии 10.0, потребуется выполнить установку обновления для **Dr.Web Agent** и произвести дополнительную настройку. Подробнее см. в разделе Dr.Web Agent.

- **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 ICAP Daemon** (**Dr.Web ICAPD**) позволяет интегрировать все компоненты программного комплекса с приложениями, использующими протокол ICAP (как

правило, это HTTP/FTP прокси-сервер).

- **Веб-интерфейс управления** **Консоль Dr.Web для интернет-шлюзов UNIX** – модуль, интегрирующийся в системный компонент **Webmin** и используемый для управления и настройки **Dr.Web для интернет-шлюзов UNIX** через веб-интерфейс с любого браузера.

Структура компонентов **Dr.Web для интернет-шлюзов UNIX** изображена на рисунке ниже:

Рис. 1. Структура компонентов Dr.Web для интернет-шлюзов UNIX

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

- Общая характеристика продукта.
- Установка программного комплекса **Dr.Web для интернет-шлюзов UNIX**.
- Запуск программного комплекса **Dr.Web для интернет-шлюзов 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 ICAPD**.
- Работа с веб-интерфейсом **Консоль Dr.Web для интернет-шлюзов UNIX**.

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

Необходимо отметить, что продукты **Dr.Web** 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 **Dr.Web**. 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 **Dr.Web** или их компонентов.
Зеленое и подчеркнутое начертание	Ссылки на страницы руководства и веб-сайты.
`Моноширинный шрифт`	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
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
IP	Internet Protocol — маршрутизируемый межсетевой протокол сетевого уровня семейства TCP/IP

Сокращение	Расшифровка
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
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 компонентов **Dr.Web ICAPD** и **Консоль Dr.Web для интернет-шлюзов UNIX** используются следующие термины и сокращения:

Сокращение	Расшифровка
CGI	Common Gateway Interface — стандарт интерфейса, используемого для связи внешней программы с веб-сервером
FTP	File Transfer Protocol — стандартный протокол, предназначенный для передачи файлов по TCP-сетям, в т.ч. Интернет
HTTP	HyperText Transfer Protocol — протокол передачи гипертекста. Протокол прикладного уровня передачи данных (изначально в виде HTML-документов). Используется в Web для получения информации с Web-сайтов, а также в качестве транспорта для других протоколов прикладного уровня

Сокращение	Расшифровка
HTTPS	Hypertext Transfer Protocol Secure — расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS
ICAP	Internet Content Adaptation Protocol — протокол адаптпции контента. Используется для подулючения внешних фильтров и преобразователей web-трафика к web-прокси
JSON	JavaScript Object Notation — текстовый формат обмена данными, основанный на JavaScript
MIME	Multipurpose Internet Mail Extensions — стандарт, описывающий передачу различных типов данных по электронной почте, а также спецификация для кодирования информации и форматирования сообщений таким образом, чтобы их можно было пересылать через Интернет

Системные требования

Компоненты программного комплекса **Dr.Web для интернет-шлюзов 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.

Продукты, работающие под управлением операционной системы **FreeBSD** 6.x, не могут быть подключены к серверу **Dr.Web ESS** версии 10.

Пример:
Для поддержки 32-битных приложений в системах на основе **Debian**/**Ubuntu Linux** понадобится установить библиотеку `libc6-i386`, а для систем на основе **ALT Linux** – библиотеку `i586-glibc-core`.

Для успешной и стабильной работы **Dr.Web для интернет-шлюзов UNIX** требуются:

- Установленный и запущенный **Dr.Web Daemon** и Антивирусное ядро **Dr.Web Engine** версии не ниже 6.0.2.
- Установленный и запущенный **Squid** версии не ниже 3.0.STABLE1 или **SafeSquid** версии не ниже 3.0.
- Модуль обновления **Dr.Web Updater** требует установленный **Perl** 5.8.0 и выше.

С точки зрения аппаратного обеспечения требования программного комплекса **Dr.Web для интернет-шлюзов UNIX** совпадают с требованиями консольного (текстового) режима операционной системы, для которой он предназначен. Для установки требуется около 205 Мбайт дискового пространства.

Для работы графического инсталлятора **Dr.Web для интернет-шлюзов 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 интернет-шлюзов UNIX** в операционной системе **FreeBSD** старше восьмой версии необходимо наличие библиотеки `compat7x`.

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

Совместимость с дистрибутивами Linux

Программный комплекс **Dr.Web для интернет-шлюзов 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
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 продукта

По умолчанию **Dr.Web для интернет-шлюзов 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/lib/` – Различные служебные библиотеки, и вспомогательные файлы, 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 интернет-шлюзов UNIX** для подключения к **Webmin**.

`%etc_dir/` – Конфигурационные файлы программного комплекса, а также `enable`-файлы, управляющие запуском компонентов, работающих в режиме демонов*.

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

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

`%var_dir/bases/` – Вирусные базы (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.

`%var_dir/lib/` – Антивирусное ядро в виде подгружаемой библиотеки **`(drweb32.dll)`**.

*) Расположение `enable`-файлов зависит от способа установки **Dr.Web для интернет-шлюзов UNIX**:

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

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

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

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

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

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

Конфигурационные файлы

Общий формат конфигурационных файлов

Настройка большинства компонентов программного комплекса **Dr.Web для интернет-шлюзов 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, ..., значениеК
...
ПараметрN = значение1, ..., значениеК

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

--- 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 интернет-шлюзов 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"
```

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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 описании 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, то 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 интернет-шлюзов 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 выводится соответствующее предупреждение.

Некоторые параметры могут использовать в качестве значений регулярные выражения (для каждого параметра отмечается в его описании). По умолчанию используется синтаксис регулярных выражений **Perl**. С основами регулярных выражений вы можете ознакомиться, например, в **Wikipedia** (статья "Регулярные выражения").

Ведение журналов (логов)

Все компоненты программного комплекса **Dr.Web для интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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:

- `Move` — переместить файл в каталог **Карантина**, отправить пользователю HTML-страницу с уведомлением;
- `Truncate` — обрезать файл до нулевой длины и отправить его пользователю;
- `Pass` — пропустить файл к пользователю;
- `Report` — вывести информацию в журнал, отправить пользователю HTML-страницу с

уведомлением;

- `Cure` — попытаться вылечить зараженный объект и отправить его пользователю.

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.

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 интернет-шлюзов UNIX

Ниже описывается процедура установки, обновления и удаления программного комплекса **Dr.Web для интернет-шлюзов UNIX** из универсального пакета для UNIX-систем. Для осуществления этих операций необходимы права суперпользователя (`root`). Их можно получить, введя команду **`su`** или указав префикс **`sudo`**.

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 интернет-шлюзов 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.

Необходимо отметить, что если вы устанавливаете программный комплекс **Dr.Web для интернет-шлюзов UNIX** на компьютер, куда ранее из аналогичного универсального EPM-пакета был установлен какой-либо другой продукт **Dr.Web**, то при каждом использовании графического деинсталлятора вам будет предложено удалить абсолютно все модули **Dr.Web**, 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 интернет-шлюзов UNIX** распространяется в виде самораспаковывающегося архива `drweb-internet-gateways_[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 централизованной защиты с сервером **Dr.Web ESS** версии 6. Для установки требует пакеты drweb-agent, drweb-updater и drweb-scanner;
- drweb-agent10: пакет содержит исполняемые файлы и документацию обновленной версии **Dr.Web Agent** (предназначен для работы с сервером **Dr.Web ESS** версии 10).
- drweb-agent10-es: пакет содержит файлы для работы обновленной версии **Dr.Web Agent** с сервером **Dr.Web ESS** версии 10 в режиме централизованной защиты.
- 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-icapd: пакет содержит исполняемые файлы **Dr.Web ICAPD** и документацию к нему. Для установки требует пакеты drweb-common, drweb-libs и drweb-icapd-dws;
- drweb-icapd-dws: пакет содержит тематические черные и белые списки интернет-ресурсов. Для установки требует пакет drweb-common;
- drweb-icapd-web: пакет содержит веб-интерфейс **Dr.Web консоль для интернет-шлюзов UNIX**;
- drweb-internet-gateways-doc: пакет содержит документацию к **Dr.Web для интернет-шлюзов UNIX**.

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 интернет-шлюзов UNIX** разрешите исполнение архива, например, командой:

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

и затем запустите его на исполнение командой:

```
# ./drweb-internet-gateways_[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-internet-gateways_[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-internet-gateways_[номер версии]~[название ОС].run --noexec
```

Для продолжения установки с помощью графического инсталлятора запустите его командой:

```
# drweb-internet-gateways_[номер версии]~[название ОС]/install.sh
```

Для установки с использованием консольного инсталлятора потребуется выполнить команду:

```
# drweb-internet-gateways_[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 интернет-шлюзов UNIX**.

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

```
# setenforce 0
```

и перезапустите инсталлятор.

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

После успешного завершения установки run-файл и каталог `drweb-internet-gateways_[номер версии]~[название ОС]` можно удалить.

Пользовательский интерфейс графического инсталлятора

1. При запуске графического инсталлятора командой:

   ```
   # drweb-internet-gateways_[номер версии]~[название ОС]/install.sh
   ```

   открывается окно программы установки.

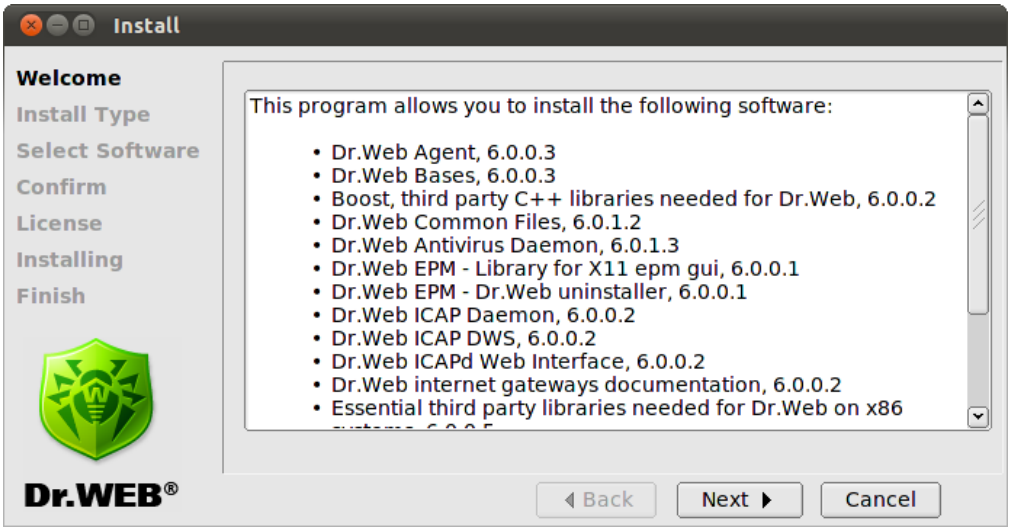


Рис. 2. Окно начала установки программы

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 Internet Gateways** со всеми компонентами по умолчанию или пользовательский.

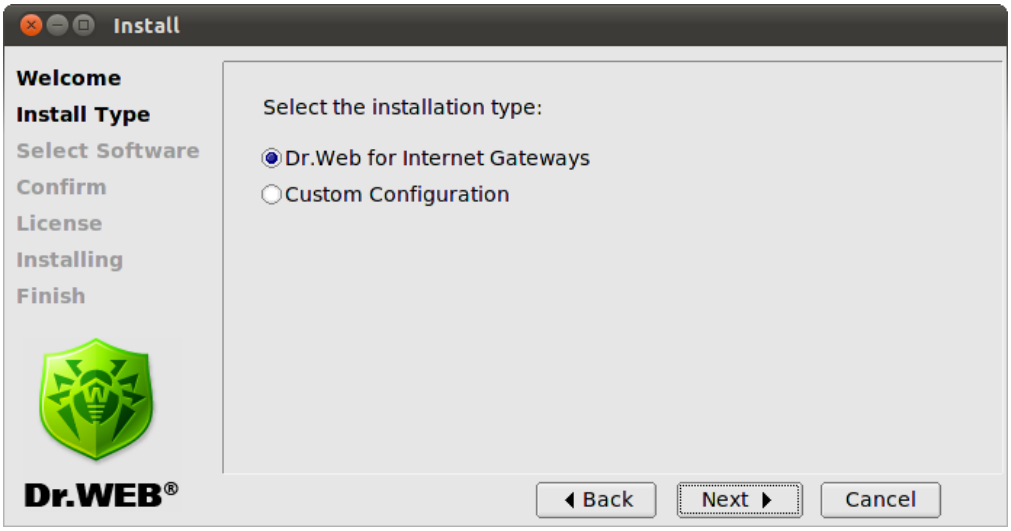


Рис. 3. Тип установки

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

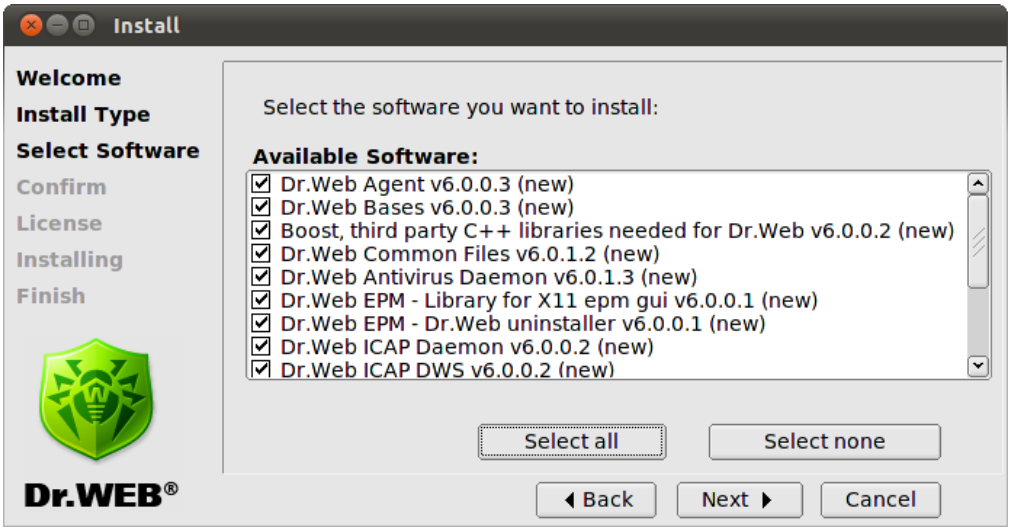


Рис. 4. Окно выбора компонентов для установки

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.

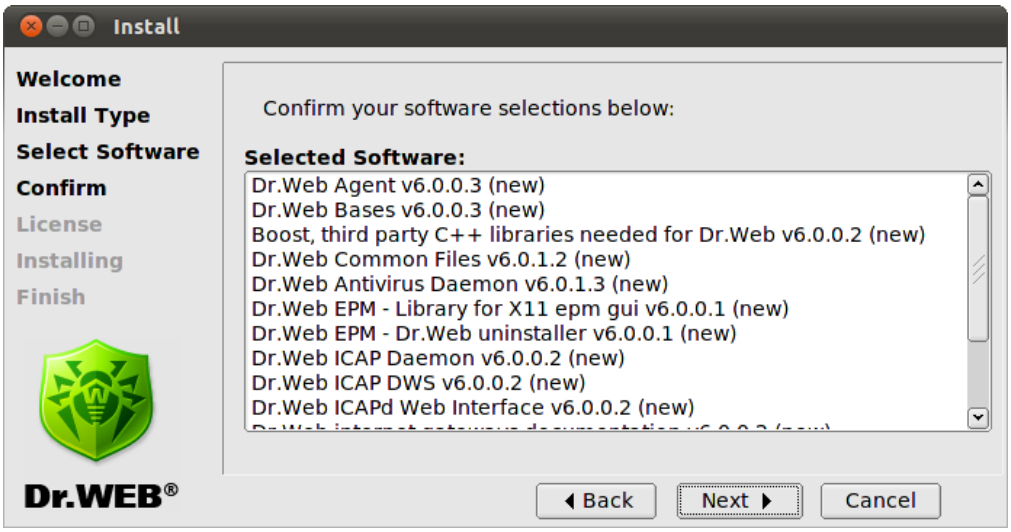


Рис. 5. Окно подтверждения установки компонентов

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**.

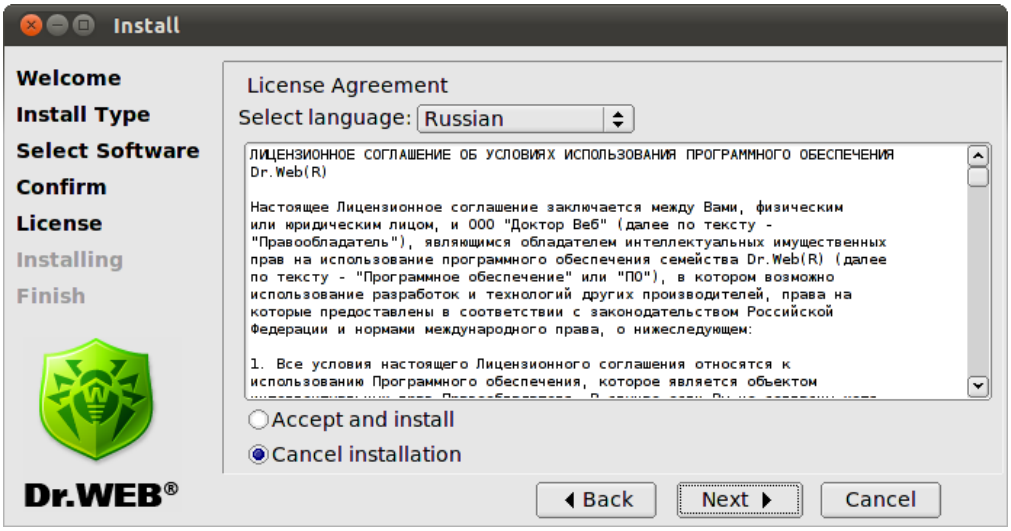


Рис. 6. Окно ознакомления с лицензионным соглашением

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

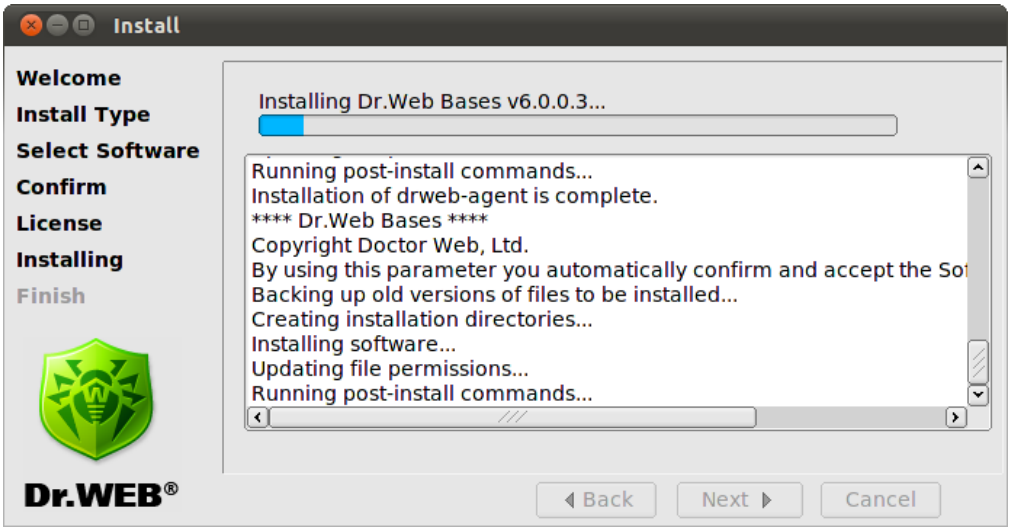


Рис. 7. Окно установки компонентов программы

Одновременно данный отчет копируется в файл `install.log`, расположенный в каталоге `drweb-internet-gateways_[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 интернет-шлюзов UNIX**.

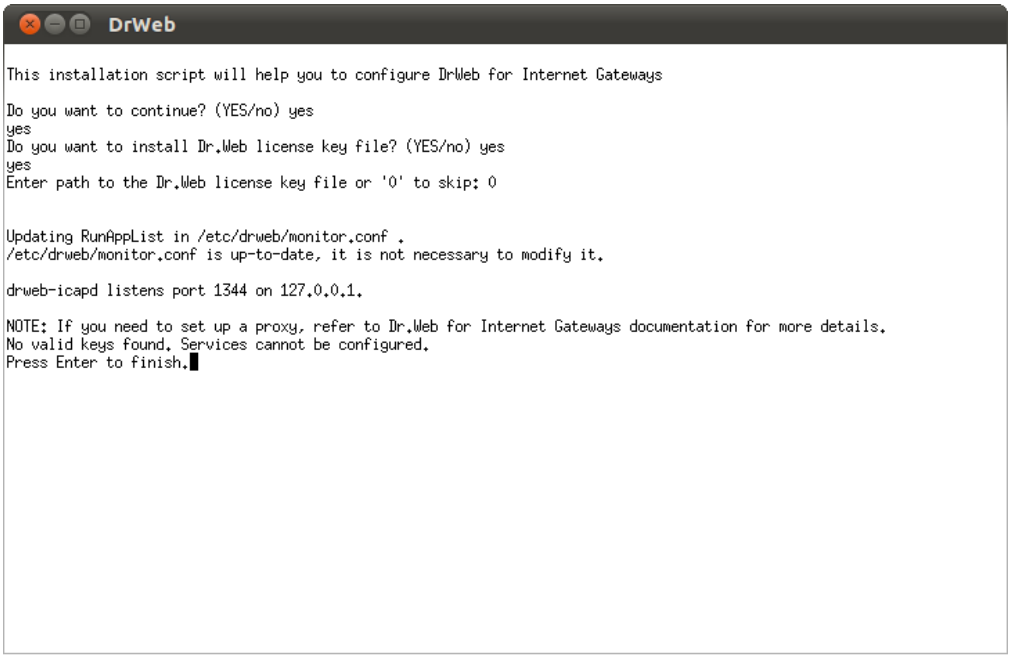


Рис. 8. Интерактивный установочный скрипт

Скрипт предложит указать путь к лицензионному ключевому файлу, установить порядок работы подключаемых модулей, и автоматически подключить необходимые для работы сервисы (**Dr.Web Daemon**, **Dr.Web Agent**, **Dr.Web Monitor**).

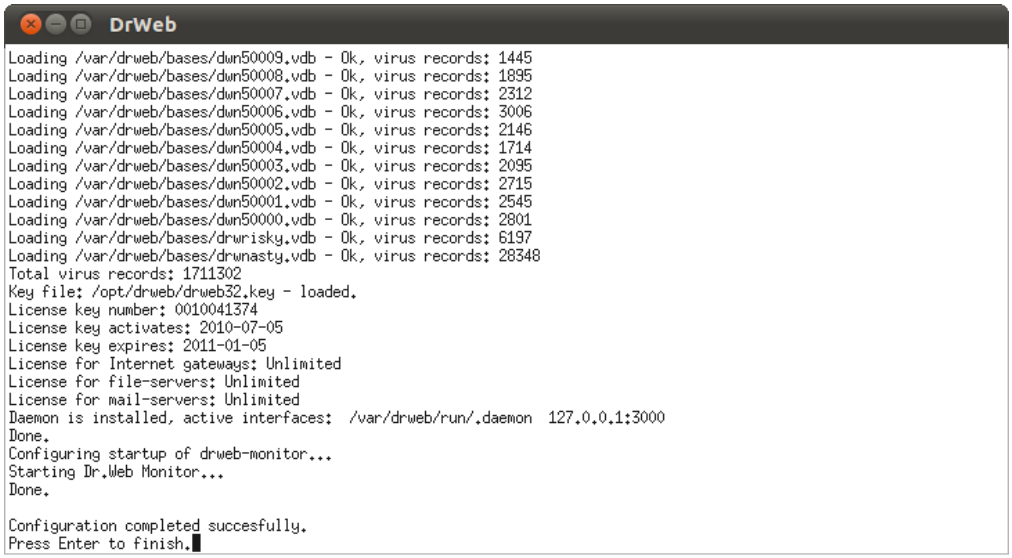


Рис. 9. Автоматический запуск сервисов

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.

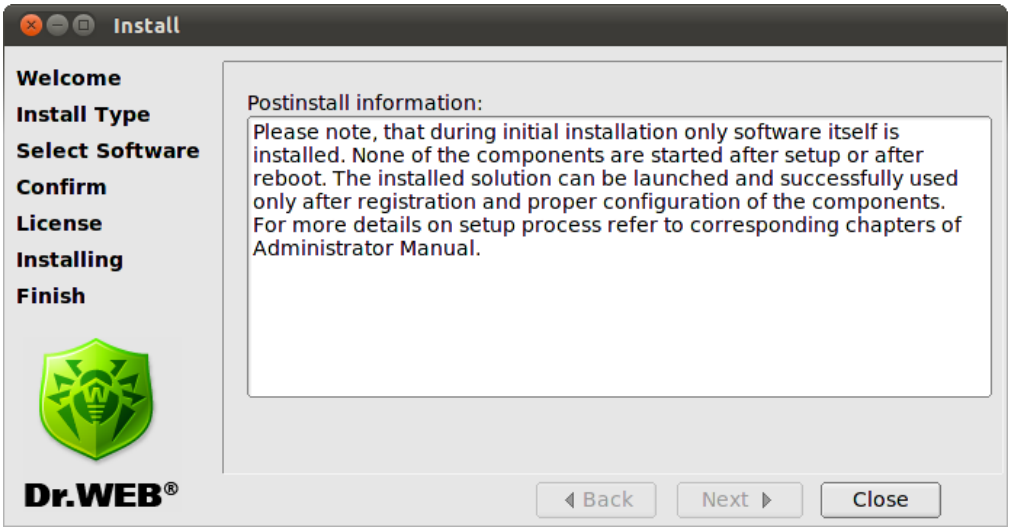


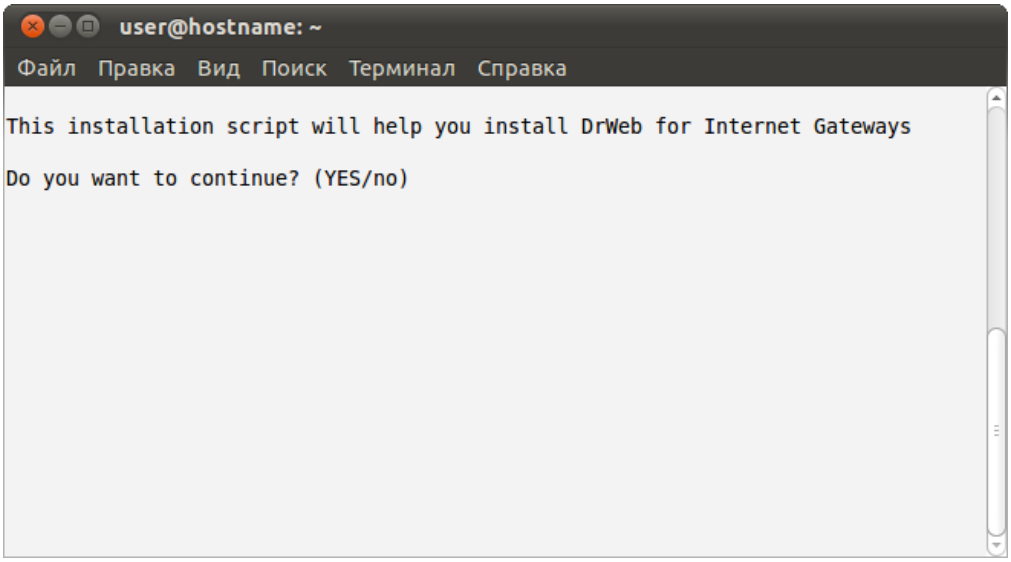
Рис. 10. Окно завершения установки программы

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 (для получения прав `root` воспользуйтесь командой **`su`** или **`sudo`**):

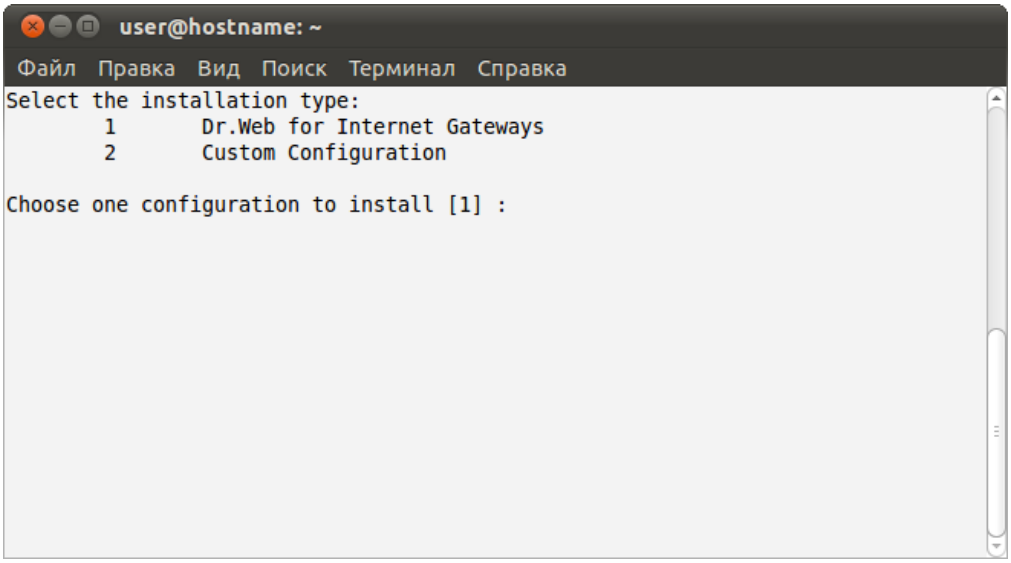
```
# drweb-internet-gateways_[номер версии]~[название ОС]/setup.sh
```

Откроется диалоговое окно консольного инсталлятора.

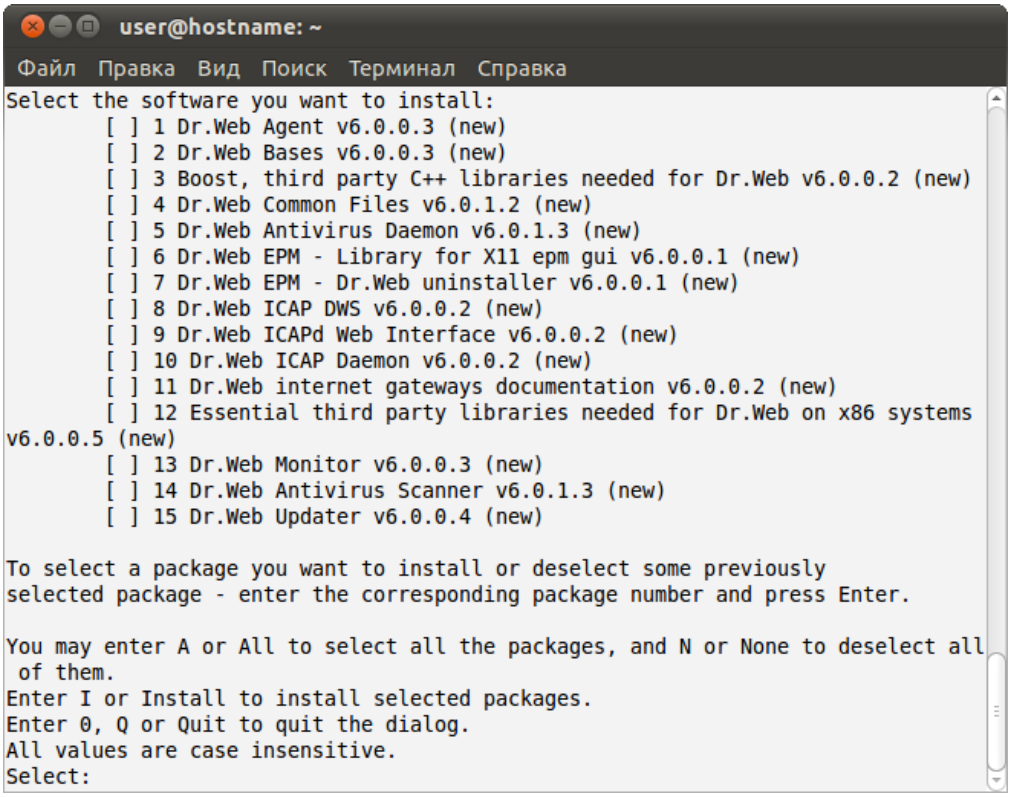


Если вы хотите установить **Dr.Web для интернет-шлюзов UNIX**, укажите **Y** или **Yes** в строке ввода (значения регистронезависимы) и нажмите клавишу ENTER. В противном случае введите **N** или **No**.

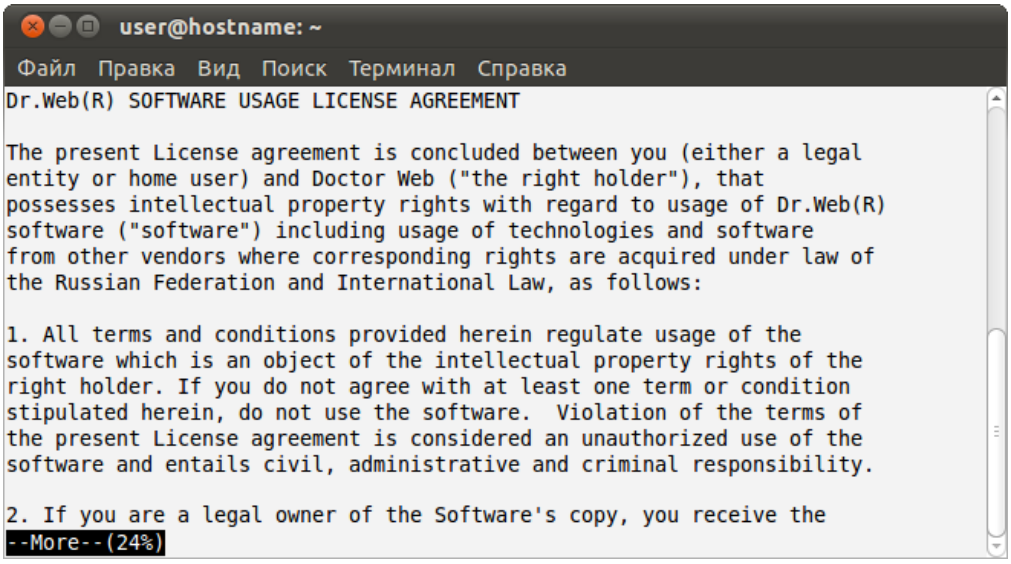
Затем вам будет предложено выбрать тип установки. Укажите номер соответствующего пункта в меню и нажмите ENTER.



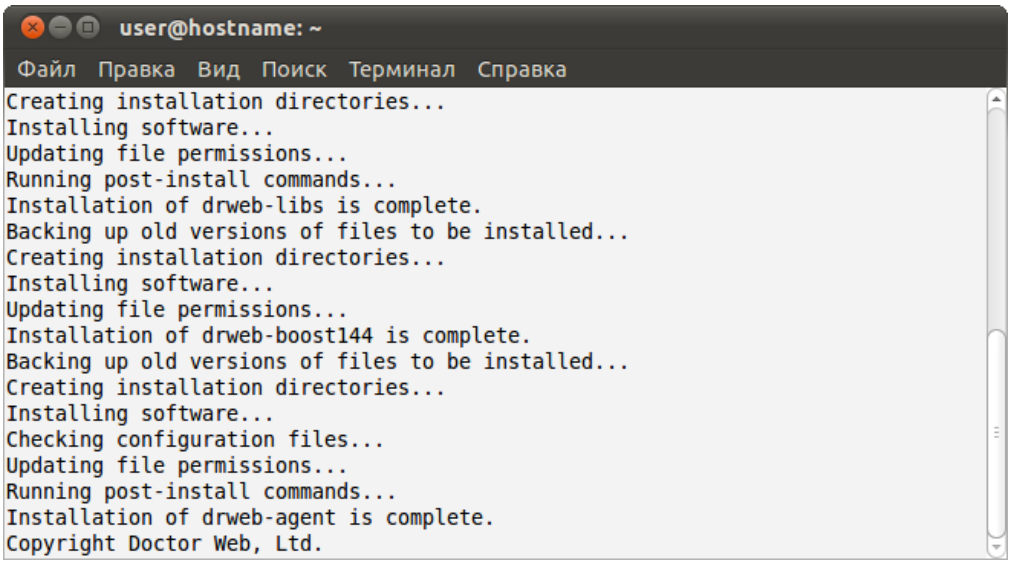
Если вы выбрали пункт **Custom Configuration**, то на следующем этапе вам будет предложено указать необходимые компоненты для установки. Укажите номер соответствующего компонента в меню и нажмите ENTER.



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 интернет-шлюзов 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**).

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.

Пользовательский интерфейс графического деинсталлятора

1. При запуске графического деинсталлятора командой:

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

открывается окно программы удаления компонентов.

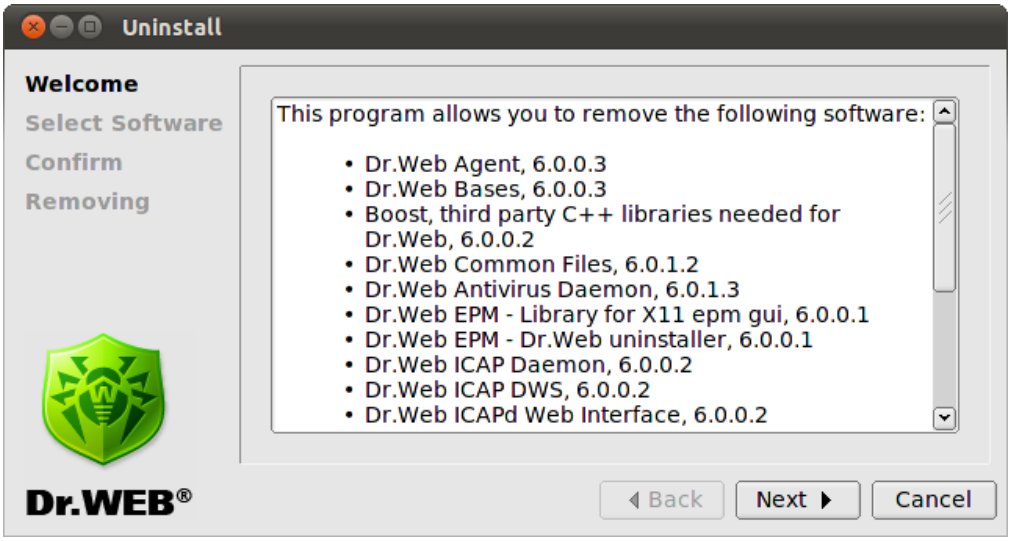


Рис. 11. Окно начала удаления программы

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.

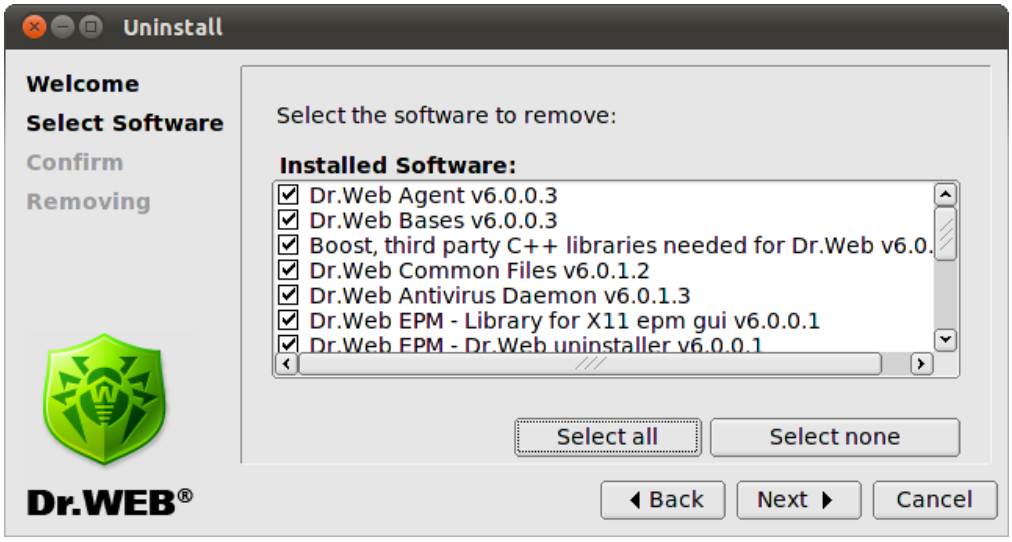


Рис. 12. Окно выбора компонентов для удаления

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.

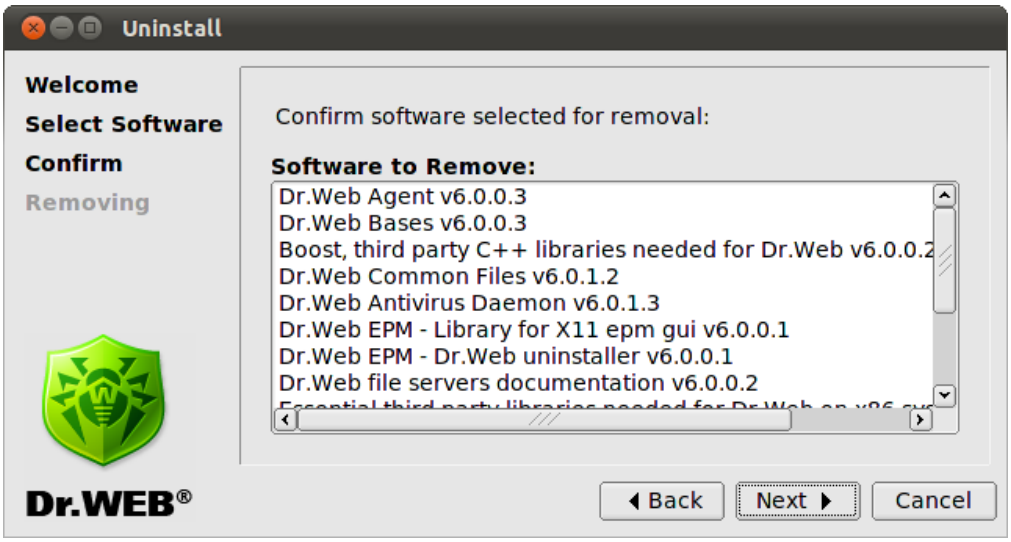


Рис. 13. Окно подтверждения удаления компонентов

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

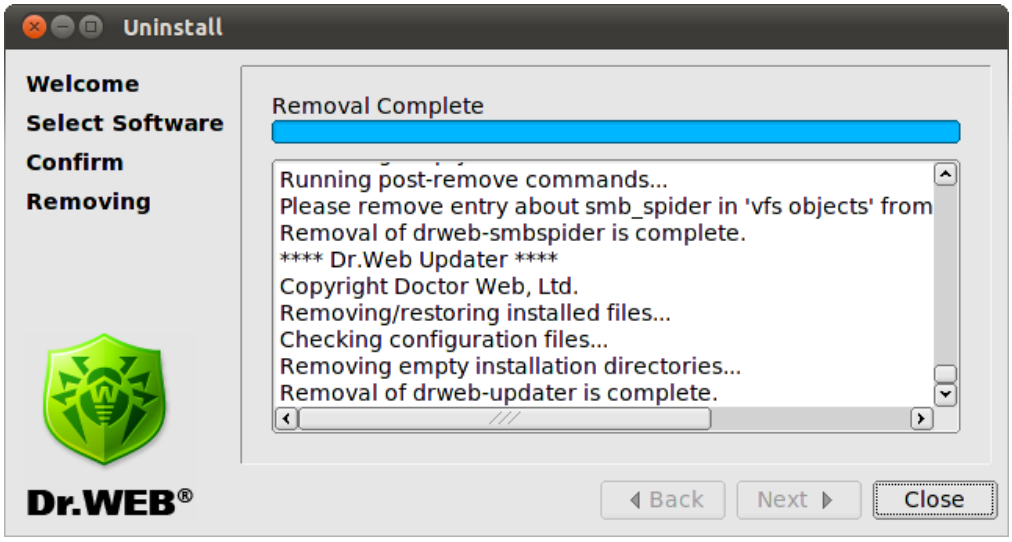


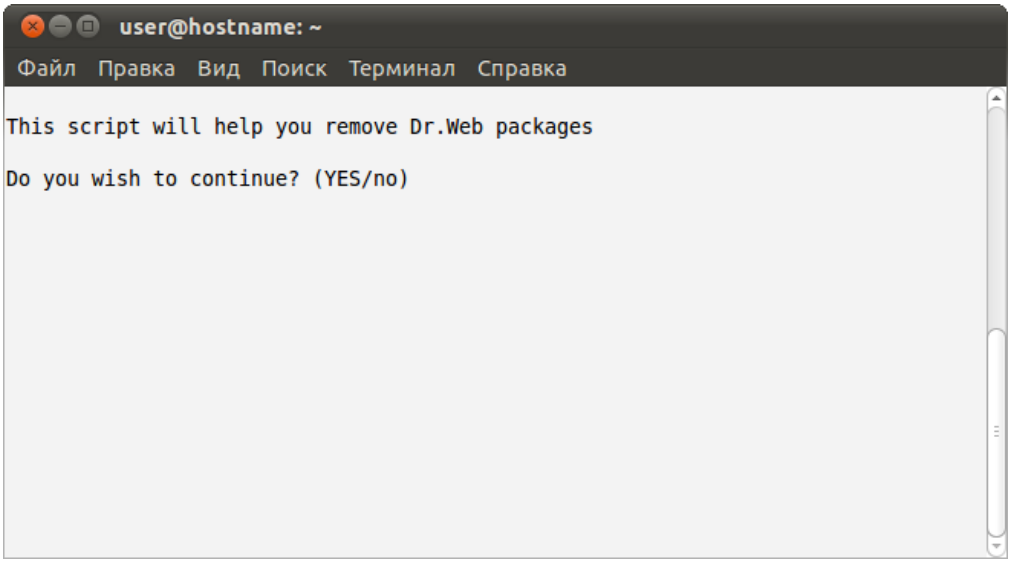
Рис. 14. Окно удаления компонентов программы

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

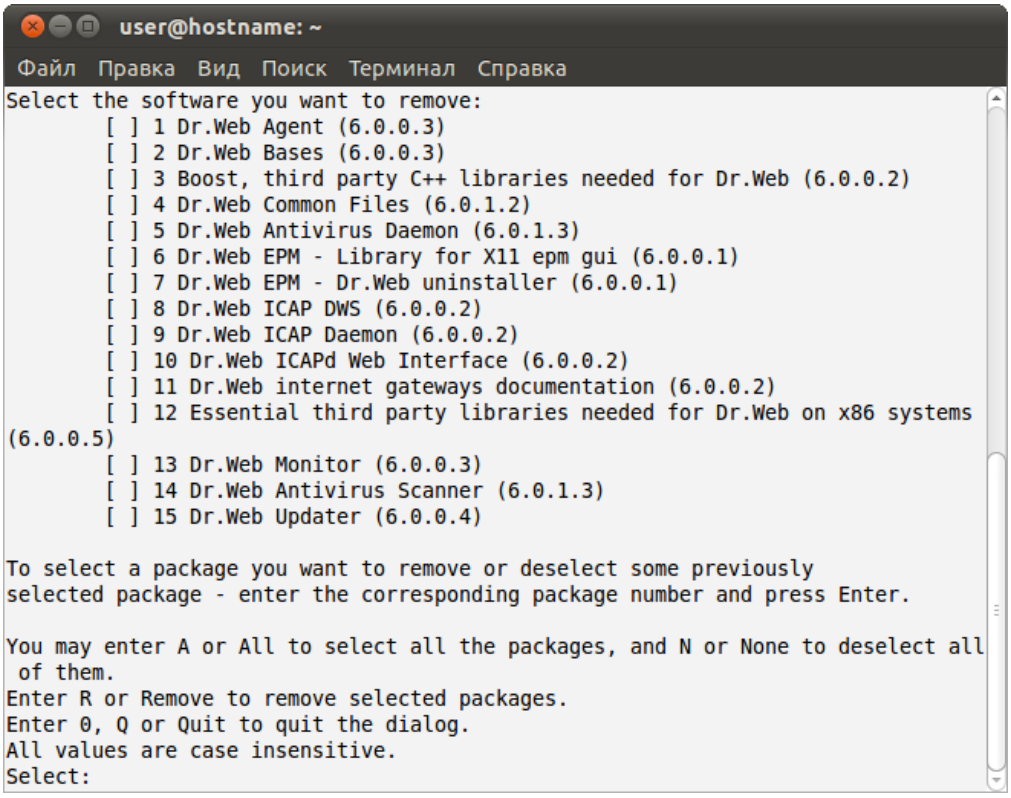
Использование консольного деинсталлятора

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

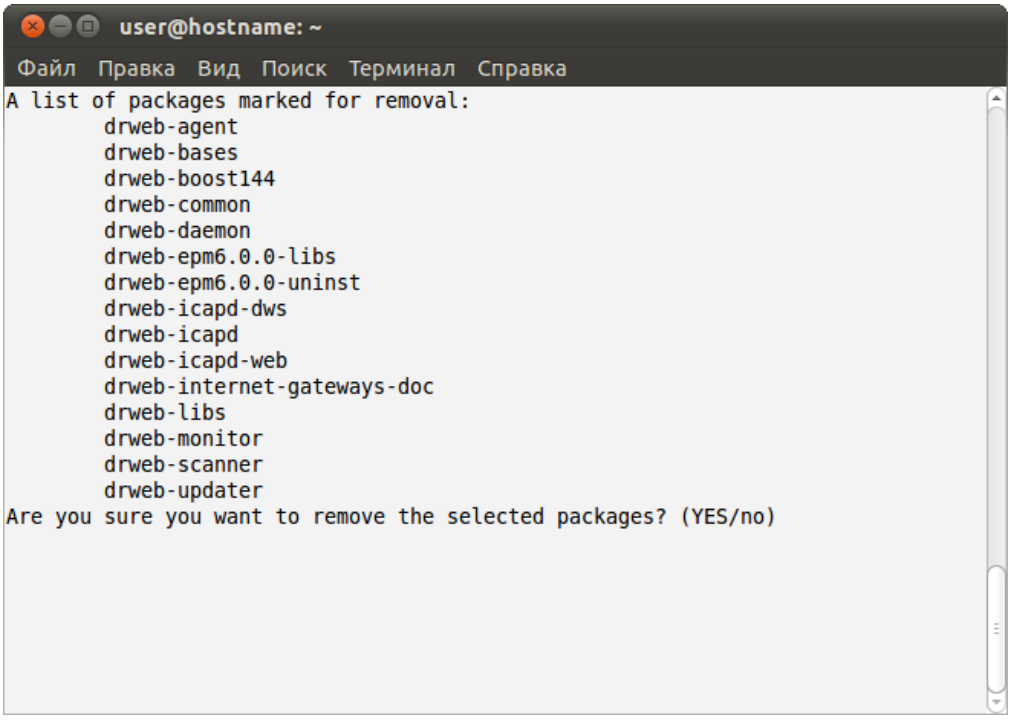
Откроется диалоговое окно консольного деинсталлятора.



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 интернет-шлюзов 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 интернет-шлюзов UNIX** из нативных пакетов для распространенных дистрибутивов **Linux** или **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 интернет-шлюзов 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 интернет-шлюзов UNIX** выполните команды:

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

2. Удаление:

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

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

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

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

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

```
apt-get autoremove
```

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

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

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

ALT Linux, PCLinuxOS (apt-rpm)

1. 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 интернет-шлюзов UNIX** выполните команды:

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

2. Удаление:

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

Установка и удаление пакетов также могут осуществляться с помощью альтернативных менеджеров (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 интернет-шлюзов UNIX** выполните команды:

```
urpmi.update drweb
urpmi drweb-internet-gateways
```

2. Удаление:

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

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

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

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

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

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

Установка и удаление пакетов также могут осуществляться с помощью альтернативных менеджеров (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 интернет-шлюзов UNIX** выполните команду:

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

2. Удаление:

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

```
yum remove drweb-internet-gateways
```

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

Установка и удаление пакетов также может осуществляться с помощью альтернативных менеджеров (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 интернет-шлюзов UNIX** выполните команды:

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

2. Удаление:

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

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

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

```
zypper remove drweb*
```

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

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

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

FreeBSD

Установка:

Загрузите архив `drweb-internet-gateways_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 интернет-шлюзов UNIX**. При установке **Dr.Web для интернет-шлюзов 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-internet-gateways_current-current~freebsd_all.tar.gz
make install -I /usr/ports/Mk/
```

Запуск Dr.Web для интернет-шлюзов UNIX

В данном разделе описана процедура запуска **Dr.Web для интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов UNIX**:

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

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

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

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

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

  Файлы располагаются в каталоге `%etc_dir/sysconfig` и называются
  `drweb-icapd.enable`,
  `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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов UNIX** из нативных пакетов в **Solaris**, запуск комплекса производится с помощью системы управления сервисами SMF:

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

Для остановки сервиса введите:

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

7. Запустить прокси-сервер.

Модули **drwebd** и **drweb-icapd** могут быть запущены 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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.
6. Запустить прокси-сервер.

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.

Настройка политик безопасности SELinux

Если используемый вами дистрибутив **Linux** оснащен подсистемой безопасности **SELinux** (`Security-Enhanced Linux` – **Linux** с улучшенной безопасностью), то для того, чтобы антивирусные компоненты (сканирующий демон **Dr.Web Daemon** и консольный сканер **Dr.Web Console Scanner**) работали корректно после установки компонентов приложения, вам потребуется внести изменения в политики безопасности, используемые **SELinux.**

Кроме того, при включенном **SELinux** установка продукта из универсальных пакетов (`.run`) может окончиться неудачей, поскольку будет заблокирована попытка создания пользователя `drweb`, от имени которого работают модули **Dr.Web для интернет-шлюзов UNIX**.

Перед началом установки рекомендуется проверить режим работы **SELinux**, для этого выполните команду **`getenforce`**. Эта команда выводит на экран текщий режим зашиты:

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

Если **SELinux** работает в режиме `Enforced`, следует временно (на период установки продукта и последующей настройки политик безопасности) перевести ее в режим `Permissive`. Для этого выполните команду **`setenforce 0`**, которая временно (до первой перезагрузки системы) переведет **SELinux** в режим `Permissive`. Чтобы вернуть систему в режим `Enforced`, следует выполнить команду
`setenforce 1`.

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

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

Чтобы при работающем **SELinux** антивирусные компоненты могли успешно функционировать, необходимо скомпилировать специальные политики безопасности сразу после установки программного продукта, по завершении работы инсталлятора или установщика нативных пакетов.

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

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 двумя способами:

   1) **С помощью утилиты `audit2allow`**. Это наиболее простой способ. 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.

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

Пример использования:

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

ИЛИ

```
# cat /var/log/audit/audit.log | audit2allow -M drweb
```

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

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

В данном примере утилита **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`.

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

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

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

Пример создания политик при помощи policygentool:

- Для модуля **Dr.Web Console Scanner**:

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

- Для сканирующего демона **Dr.Web Daemon**:

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

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

`[module_name].te`, `[module_name].fc` и `[module_name].if`.

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

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

Пример использования:

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

После перезагрузки операционной системы подсистема безопасности **SELinux** будет настроена для корректной работы **Dr.Web для интернет-шлюзов UNIX**.

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

Регистрация продукта

Права на использование программного комплекса **Dr.Web для интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 **Dr.Web** 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 интернет-шлюзов 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.

В штатном режиме обновления выполняются автоматически, с правами пользователя `drweb`.

Не следует запускать обновление с правами суперпользователя `root`, т.к. в этом случае все последующие попытки автоматического обновления будут завершаться ошибкой из-за попыток доступа к файлам, которые в результате предыдущего обновления сменили своего владельца на суперпользователя `root`.

Обновление антивируса и вирусных баз

Компоненты программного комплекса **Dr.Web для интернет-шлюзов UNIX** нуждаются в регулярном обновлении баз данных вирусов.

Вирусные базы **Dr.Web для интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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.

Тематические черные и белые списки адресов интернет-ресурсов состоят из файлов с расширением `dws`:

- `dwfXXXNN.dws` – черный список, где `XXX` – трехбуквенное сокращение темы списка, а `NN` - порядковый номер списка из одной темы;
- `white_dwfXXX.dws` – белый список, где `XXX` – трехбуквенное сокращение темы списка.

На серверах **BCO Dr.Web** эти файлы также могут храниться в lzma-архивах. Если обновлять эти списки не требуется, то следует удалить или переместить файл `icapd.drl` из каталога, содержащего `drl`-файлы (путь к нему можно узнать из параметра **`DrlDir`** секции `[Updater]` конфигурационного файла `drweb32.ini`).

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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 подключаемых модулей. 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 **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: **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 подключаемых модулей. 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. Если здесь указано пусто значение, прокси-сервер не используется. Значение по умолчанию: **ProxyServer** =
ProxyLogin = {текст}	Имя пользователя прокси-сервера (если сервер требует аутентификации). Значение по умолчанию: **ProxyLogin** =
ProxyPassword = {текст}	Пароль пользователя прокси-сервера (если сервер требует аутентификации).

	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
IcapdPidFile = {путь к файлу}	Путь к PID-файлу для **Dr.Web ICAPD**. Значение по умолчанию: **IcapdPidFile** = %var_dir/run/drweb_icapd.pid
BlacklistPath = {путь к каталогу}	Путь к каталогу с файлами .dws. Значение по умолчанию: **BlacklistPath** = %var_dir/dws
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`, или тот, который указан при помощи аргумента командной строки `--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 **ВСО 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 ответ от выбранного сервера в течение периода времени, указанного в параметре **`Timeout`**).
5. Модуль запрашивает с сервера **ВСО 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 интернет-шлюзов 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 **Dr.Web**, либо на сервер централизованной защиты, под управлением которого работает **Dr.Web Agent**. Когда происходит запуск компонентов **Dr.Web для интернет-шлюзов UNIX**, или происходит изменение настроек, **Dr.Web Agent** шлет компонентам необходимые настройки.

Обратите внимание, что модуль **drweb-agent** в режиме централизованной защиты (**enterprise mode**) предназначен для работы только с **Dr.Web ESS** версии 6. Если вы хотите обеспечить подключение к серверу централизованной защиты **Dr.Web ESS** версии 10, вам следует установить и настроить новую версию агента, реализованную в виде модуля **drweb-agent10**. Об установке и настройке версии **drweb-agent10** см. в разделе Переход на использование Dr.Web ESS версии 10.

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 интернет-шлюзов 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 режиме централизованной защиты не требует установки дополнительного программного обеспечения или удаления **Dr.Web для интернет-шлюзов 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 централизованной защиты (**enterprise mode**), когда защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки **Dr.Web для интернет-шлюзов UNIX** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл с сервера централизованной защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется. Статистика вирусных инцидентов отсылается на управляющий сервер централизованной защиты.

Обратите внимание, что модуль **drweb-agent** в режиме централизованной защиты (**enterprise mode**) предназначен для работы только с **Dr.Web ESS** версии 6. Если вы хотите обеспечить подключение к серверу централизованной защиты **Dr.Web ESS** версии 10, вам следует установить и настроить новую версию агента, реализованную в виде модуля **drweb-agent10**. Об установке и настройке версии **drweb-agent10** см. в разделе Переход на использование Dr.Web ESS версии 10.

Чтобы использовать режим централизованной защиты:

1. Свяжитесь с системным администратором вашей сети, чтобы получить файл с открытым ключом и параметры соединения с сервером централизованной 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 централизованной защиты, установите `Yes` в качестве значения параметра **UseEnterpriseMode**.

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

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

Чтобы **Dr.Web для интернет-шлюзов UNIX** полностью поддерживал режим централизованной защиты, **Dr.Web Monitor** также должен работать в режиме централизованной 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 интернет-шлюзов UNIX** будут разблокированы и вы вновь получите доступ ко всем функциям и настройкам **Dr.Web для интернет-шлюзов UNIX**.

Для работы в одиночном режиме **Dr.Web для интернет-шлюзов UNIX** необходим действующий лицензионный ключ. Ключевые файлы, полученные с сервера централизованной защиты, не могут быть использованы в этом режиме.

Совместное использование Dr.Web для интернет-шлюзов UNIX и Антивируса Dr.Web для Linux в режиме централизованной защиты

Ввиду особенностей реализации, одновременное использование в режиме централизованной защиты **Dr.Web для интернет-шлюзов UNIX** и **Антивируса Dr.Web для Linux**, установленных на одном компьютере, невозможно. Для включения режима централизованной

защиты **Dr.Web для интернет-шлюзов 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 **Антивирус Dr.Web для Linux** в режим централизованной защиты. В таком случае, отключите режим централизованной защиты **Dr.Web для интернет-шлюзов 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 интернет-шлюзов UNIX**		
`-f`	`--update-failed`	
Описание: Запуск процесса обновления для тех компонентов **Dr.Web для интернет-шлюзов 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		
`-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 централизованной защиты **Dr.Web Enterprise Server**		
`-s`	`--socket`	`<путь к файлу>`
Описание: Использование компонентом для коммуникации с управляемыми модулями сокета, указанного в аргументе		

Краткий вариант	Расширенный вариант	Аргументы
-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 интернет-шлюзов 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 интернет-шлюзов 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 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 интернет-шлюзов 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 сжимать • Possible – если возможно • No – не сжимать 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 вниманиме, 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 (.amc). 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 файлов мета-конфигурации (`.amc`). В этих файлах описывается конфигурация компонентов и параметры, значения которых **Dr.Web Agent** выдает компонентам. Эти файлы располагаются в каталоге, определяемом параметром **`MetaConfDir`** (по умолчанию – `%etc_dir/agent`). Как правило, в одном файле указывается описание конфигурации и параметров одного компонента, а имя файла совпадает с именем компонента **Dr.Web для интернет-шлюзов UNIX**.

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 ICAPD для Linux:

```
Application "ICAPD"
      id  49
      ConfFile  "/etc/drweb/drweb-icapd.ini"
      Components
                  drweb-icapd  Icapd
    EndComponents
EndApplication
```

Интеграция с Dr.Web Enterprise Security Suite

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

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

Для того, чтобы **Dr.Web для интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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`, `ICAPD`).

Пример:

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

Запуск комплекса

Чтобы запустить комплекс:

- Через веб-интерфейс **Центра Управления Dr.Web** в настройках **Dr.Web Monitor** установите флаги **Daemon** и **ICAP** для запуска соответствующих компонентов комплекса;
- 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
  ```

Интеграция с Dr.Web ESS версии 10

В состав продукта **Dr.Web для интернет-шлюзов UNIX** версии 6.0.2 входит две версии компонента **Dr.Web Agent**:

- **Dr.Web Agent**, представленный модулем **drweb-agent**, в режиме **enterprise mode** может взаимодействовать только с сервером **Dr.Web ESS** версии 6.
- **Dr.Web Agent**, представленный модулем **drweb-agent10**, в режиме **enterprise mode** может взаимодействовать только с сервером **Dr.Web ESS** версии 10.

Чтобы перейти на использование сервера централизованной защиты **Dr.Web ESS** версии 10, следует, помимо настройки интеграции, выполнить ряд дополнительных настроек.

Продукты, работающие под управлением операционной системы **FreeBSD** 6.x, не могут быть подключены к серверу **Dr.Web ESS** версии 10.

Настройка программного продукта для подключения к Dr.Web ESS версии 10

Так как **Dr.Web ESS** версии 10 не поддерживает управление компонентами **Dr.Web Monitor** и **Dr.Web Daemon**, в дополнение к стандартному файлу конфигурации `%etc_dir/agent.conf`, модуль **drweb-agent10** использует два дополнительных файла конфигурации: `es_monitor.conf` и `es_daemon.conf`, расположенных в том же каталоге. Эти файлы хранят параметры конфигурации модулей **Dr.Web Monitor** и **Dr.Web Daemon**, которые будут использоваться агентом для настройки работы этих модулей в режиме **enterprise mode**.

В каждой строке файла указывается значение некоторого параметра конфигурации соответствующего модуля в формате `<section>/<parameter> <value>`, где `<section>` – имя секции из конфигурационного файла компонента, `<parameter>` – имя параметра, а `<value>` – задаваемое значение параметра.

Пример (файл `es_monitor.conf`, задающий настройки для работы компонента **Dr.Web Monitor** в режиме **enterprise mode**):

```
Monitor/RunAppList DAEMON
```

В этой строке задается значение параметра **RunAppList**, находящегося в секции `[Monitor]` файла конфигурации **Dr.Web Monitor**. Данное значение параметра будет использовано, когда программный комплекс будет запущен в режиме **enterprise mode**. В этом случае **Dr.Web Monitor** запустит только компонент **Dr.Web Daemon**.

Пример (файл `es_daemon.conf`, задающий настройки для работы компонента **Dr.Web Daemon** в режиме **enterprise mode**):

```
Daemon/MaxCompressionRatio 500
```

В этой строке задается значение параметра **MaxCompressionRatio**, находящегося в секции `[Daemon]` файла конфигурации **Dr.Web Daemon**. Данное значение параметра будет использовано, когда программный комплекс будет запущен в режиме **enterprise mode**. В этом случае **Dr.Web Daemon** будет использовать 500 в качестве порогового значения коэффициента сжатия.

Для подключения программного продукта **Dr.Web для интернет-шлюзов UNIX** к серверу централизованной защиты **Dr.Web ESS** версии 10 следует:

1. Открыть файл мета-конфигурации `agent.mmc` (используется **Dr.Web Monitor** для взаимодействия с **Dr.Web Agent**) и заменить указанное в нем имя бинарного файла **drweb-agent** на **drweb-agent10**.

2. В файле `es_monitor.conf` указать требуемые для запуска компоненты, задав строку **`Monitor/RunAppList`**. Состав запускаемых компонентов должен совпадать составом компонентов, запускаемых программным комплексом в режиме **standalone** (указан непосредственно в параметре **`RunAppList`**, находящегося в секции `[Monitor]` файла конфигурации **Dr.Web Monitor**). В случае если должно быть запущено более одного компонента, они указываются через запятую, причем использование пробелов не допускается. Например:

```
Monitor/RunAppList DAEMON,ICAPD
```

   В качестве имен компонентов указываются имена, заданные в секции `Application` mmc-файлов.

3. При необходимости изменить в файле `es_daemon.conf` значения параметров, которые будут использованы **Dr.Web Daemon** в режиме **enterprise mode**.
4. Если ранее использовался режим **standalone**, следует переключить **Dr.Web Agent** и **Dr.Web Monitor** в режим **enterprise mode**, задав соответствующие настройки в файлах конфигурации этих модулей, как показано в разделе Настройка компонентов для работы в режиме Enterprise.
5. Перезапустить модуль **Dr.Web Monitor**, выполнив команду:

```
# service drweb-monitor restart
```

Работа с вирусной статистикой

При работе программного комплекса **Dr.Web для интернет-шлюзов 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**. Обратите внимание, что если на компьютере одновременно установлено несколько антивирусных продуктов **Dr.Web**, работающих под управлением **Dr.Web Agent**, то он будет собирать и отправлять статистику по каждому из работающих продуктов.

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 интернет-шлюзов 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.

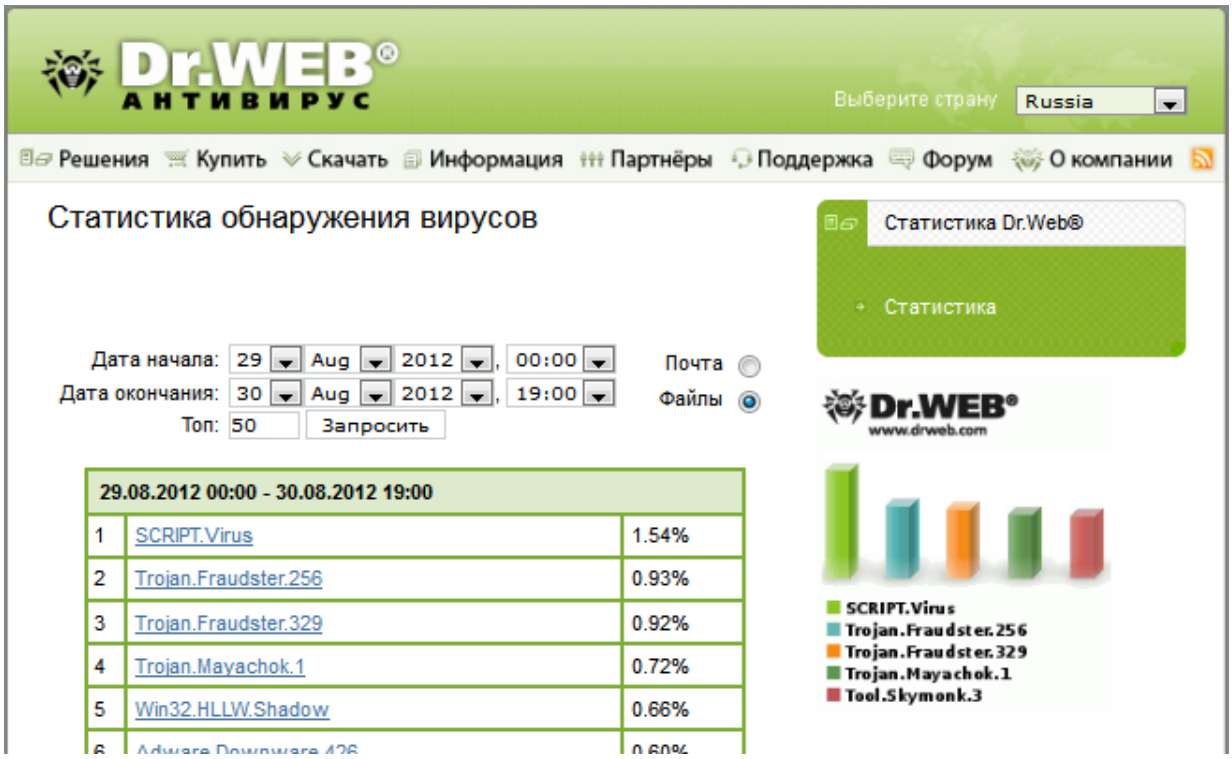


Рис. 15. Вирусная статистика

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 интернет-шлюзов 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 режиме централизованной защиты не требует установки дополнительного программного обеспечения или удаления **Dr.Web для интернет-шлюзов 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 централизованной защиты (**enterprise mode**), когда защитой компьютера управляет сервер централизованной защиты **Dr.Web Enterprise Server**. В этом режиме некоторые функции и настройки **Dr.Web для интернет-шлюзов UNIX** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл, получаемый от сервера централизованной защиты **Dr.Web Enterprise Server**. Персональный лицензионный ключевой файл на локальном компьютере не используется.

Чтобы использовать режим централизованной защиты

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

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

Чтобы **Dr.Web для интернет-шлюзов UNIX** полностью поддерживал режим централизованной защиты, **Dr.Web Agent** также должен работать в режиме централизованной 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 интернет-шлюзов UNIX** будут разблокированы, и вы вновь получите доступ ко всем функциям и настройкам **Dr.Web для интернет-шлюзов UNIX**.

Для работы в одиночном режиме **Dr.Web для интернет-шлюзов UNIX** необходим действующий лицензионный ключ. Ключевые файлы, полученные от сервера централизованной 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 интернет-шлюзов 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 интернет-шлюзов UNIX**		
-c	--conf	<путь к файлу>
Описание: Использование при запуске указанного конфигурационного файла		
-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 интернет-шлюзов 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 интернет-шлюзов 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 интернет-шлюзов 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** (.mmc).

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 интернет-шлюзов UNIX**:

- Установка при помощи **универсального пакета для UNIX**:
  Файлы располагаются в каталоге `%etc_dir` и называются
  `drweb-icapd.enable`,
  `drwebd.enable`,
  `drweb-monitor.enable`.
- Установка из **нативных DEB-пакетов**:
  Файлы располагаются в каталоге `/etc/defaults` и называются
  `drweb-icapd`,
  `drwebd`,
  `drweb-monitor`.
- Установка из **нативных RPM-пакетов**:
  Файлы располагаются в каталоге `/etc/sysconfig` и называются
  `drweb-icapd.enable`,
  `drwebd.enable`,
  `drweb-monitor.enable`.

Взаимодействие с компонентами программного комплекса

Взаимодействие с компонентами программного комплекса осуществляется с помощью файлов мета-конфигурации (.mmc). Эти файлы включены в пакеты тех продуктов, компоненты которых могут работать под управлением **Dr.Web Monitor**, и располагаются в каталоге, определяемом параметром **MetaConfDir** (по умолчанию – %etc_dir/monitor). В этих файлах описывается состав компонентов, расположение бинарных файлов, порядок их запуска и параметры запуска. Как правило, в одном файле указывается описание одного компонента, а имя файла совпадает с именем компонента **Dr.Web для интернет-шлюзов UNIX**.

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, передаваемые модулю при запуске (могут быть заключены в кавычки);
  - Максимальное время в секундах, отводимое на запуск компонента (StartTimeout);
  - Максимальное время в секундах для остановки (StopTimeout);
  - 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 журнал).

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

Пример mmc-файла для Dr.Web Daemon:

```
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
```

Пример mmc-файла для Dr.Web ICAPD:

```
Application "ICAPD"
 FullName    "Dr.Web (R) icapd"
 Path        "/opt/drweb/"
 Depends     "AGENT"
 Components
  # name  args  MaxStartTime  MaxStopTime  NotifyType  User:Group
  drweb-icapd   "-m -f local:/var/drweb/ipc/.agent"  5  5  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. В соответствии с соглашениями UNIX-систем, праметры должны быть отделены от указанного путя для проверки пробелои и начинаться с дефиса ("-"). 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

Параметр	Описание
	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** 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 каталогах.
-fl	Указывает следовать символическим ссылкам как для файлов, так и для каталогов. 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 (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,

Параметр	Описание
	производится только информирование пользователя. Если параметр дополняется модификатором `d`, `m` 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 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.

Параметр	Описание
-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**.
-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 консольный сканер **Dr.Web Scanner** использует конфигурационный файл drweb32.ini (этот файл совместно используется компонентами **Dr.Web Daemon**, **Dr.Web Scanner** и **Dr.Web Updaer**). Компонент использует параметры, расположенные в секции [Scanner]. Перечень параметров, задаваемых в секции и их назначение аналогичны параметрам, указанным в секции [Daemon].
-lng = {путь к файлу}	Задает использование указанного альтернативного языкового файла. По умолчанию используется английский язык.
-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.

Параметр	Описание
-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 анализа*, 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 анализа*).

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 анализа.* *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 анализа*. Кроме того, данный режим может незначительно увеличить время проверки. Данные обстоятельства могут быть доводами в пользу отключения использования *Эвристического анализа*. Вместе с тем, включение этого типа анализа увеличивает надежность антивирусной защиты. Все файлы, обнаруженные методом *Эвристического анализа*, 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, писем, HTML-страниц и прочих контейнеров), если они содержат зараженные объекты. Важно понимать, что при наличии данного разрешения будет удален весь составной объект целиком, а не только содержащийся в нем вредоносный элемент. 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 и других контейнерах, применяется к соответствующему контейнеру 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 (если сработал *Эвристический анализ*). 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

Коды возврата

По окончании работы **Dr.Web Scanner** возвращает код возврата, по которому можно определить, с каким результатом завершено сканирование.

Код возврата всегда образуется как комбинация (сумма) кодов, сопоставленных определенным событиям в процессе сканирования. Возможные значения кодов и соответствующие им события следующие:

Код	Событие
1	Обнаружены известные вирусы
2	Обнаружены модификации известных вирусов
4	Обнаружены подозрительные на вирус объекты

Код	Событие
8	В архиве, контейнере или почтовом ящике обнаружены известные вирусы
16	В архиве, контейнере или почтовом ящике обнаружены модификации известных вирусов
32	В архиве, контейнере или почтовом ящике обнаружены подозрительные на вирус объекты
64	Успешно выполнено лечение хотя бы одного зараженного вирусом объекта
128	Выполнено удаление/переименование/перемещение хотя бы одного зараженного файла

Результирующий код возврата, формируемый по завершению проверки, равен сумме кодов тех событий, которые произошли во время проверки (и его слагаемые могут однозначно быть по нему восстановлены). Например, код возврата 9 = 1 + 8 означает, что во время проверки обнаружены известные вирусы (вирус), в том числе в архиве; обезвреживание не проводилось; больше никаких «вирусных» событий не было.

Если в процессе сканирования ни одного из указанных инцидентов не было, **Dr.Web Scanner** возвращает 0.

Одна из известных особенностей поведения **Dr.Web Scanner** состоит в том, что в случае отсутствия инцидентов при сканировании он может вернуть код 128. Возврат этого кода равносилен возврату кода 0.

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 интернет-шлюзов UNIX** является готовым решением по интеграции **Dr.Web Daemon** с приложениями, использующими протокол ICAP.

Обратите внимание, что **Dr.Web Daemon** не может проверять содержимое зашифрованных файлов, поскольку для анализа их содержимого требуется знание пароля. Поэтому такие файлы пропускаются без проверки, а **Dr.Web Daemon** возвращает специальный код ответа вызвавшему его клиентскому приложению.

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		
-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	

Краткий вариант	Расширенный вариант	Аргументы
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).

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 журнале **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 (суперпользователя `root`).

При необходимости, имя пользователя, от имени которого должен работать **Dr.Web Daemon**, задается при помощи параметра конфигурации **`User`** в настройках **Dr.Web Daemon**. Кроме того, вы можете настроить пользователя и группу, используемые для запуска модуля, отредактировав соответствующий `mmc`-файл у компонента **Dr.Web Monitor**, если он используется для управления работой компонентов **Dr.Web для интернет-шлюзов UNIX**.

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 журнала (лога). Журнал 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 интернет-шлюзов 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` – максимальное 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** (информация будет отправляться **Dr.Web Agent** после сканирования каждого файла). 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 **Dr.Web**, 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 и не может быть меньше 2.
	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**). Должен быть указан размер больше 0.
	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.
	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).
	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 Dr.Web ICAPD

Модуль **Dr.Web ICAPD** (**drweb-icapd**) позволяет интегрировать все компоненты программного комплекса **Dr.Web для интернет-шлюзов UNIX** с приложениями, использующими протокол ICAP. На данный момент поддержка протокола ICAP включена в прокси-серверы **Squid** и **SafeSquid**.

Dr.Web ICAPD соединяет поддерживающий протокол ICAP прокси-сервер с **Dr.Web Daemon** для проверки всего входящего FTP- и HTTP-трафика на наличие вирусов. Кроме того, он позволяет фильтровать доступ к HTML-ресурсам как по MIME-типу и размеру соответствующих файлов, так и по имени хоста. Также с его помощью можно ограничивать доступ к страницам благодаря использованию как обновляемых тематических черных списков, так и черных и белых списков, определенных пользователем (администратором комплекса).

Принципы работы:

1. Клиент выполняет запрос некоторого ресурса (HTTP-запрос GET);
2. Прокси-сервер запрашивает у **Dr.Web ICAPD** по протоколу ICAP возможность обращения к указанному серверу;
3. Если доступ к указанному серверу не должен быть заблокирован (сервер находится в пользовательском белом списке, не находится в пользовательском черном списке, не подпадает под активные тематические списки или если для запроса сработали разрешающие доступ правила), то **Dr.Web ICAPD** разрешает прокси-серверу выполнить HTTP-запрос. В противном случае **Dr.Web ICAPD** предписывает прокси-серверу вернуть клиенту сгенерированную **Dr.Web ICAPD** HTML-страницу с уведомлением о блокировке ресурса;
4. Если доступ к удаленному серверу был разрешен, то прокси-сервер получает от него ответ, который по протоколу ICAP передает **Dr.Web ICAPD** на антивирусную проверку;
5. Если хост, от которого получен ответ, не входит в доверенный список (т.е. список хостов, файлы от которых не подлежат проверке), то модуль **Dr.Web ICAPD** проверяет выполнение правил контент-фильтрации, и если для контента выполняется действие **scan**, отправляет полученный файл на проверку сканирующему демону **Dr.Web Daemon**;
6. По результатам проверки на вирусы к файлу могут быть применены следующие действия:
   a) **pass** – **Dr.Web ICAPD** разрешает прокси-серверу вернуть ответ клиенту;
   b) **report** – **Dr.Web ICAPD** предписывает прокси-серверу вернуть клиенту сгенерированную **Dr.Web ICAPD** HTML-страницу с уведомлением об отклонении запрошенного файла;
   c) **move** – **Dr.Web ICAPD** помещает исходный файл в **Карантин** и предписывает прокси-серверу вернуть клиенту сгенерированную **Dr.Web ICAPD** HTML-страницу с уведомлением о помещении запрошенного файла в **Карантин**;
   d) **truncate** – **Dr.Web ICAPD** предписывает прокси-серверу вернуть клиенту пустой файл.

   Эти же действия (за исключением перемещения в **Карантин**) могут быть указаны и в самих правилах контент-фильтрации, таким образом, например, можно разрешить пропускать без проверки, или наоборот, безусловно отвергать данные некоторых типов (например, потоковое видео). Однако для этого требуется, чтобы был активизирован и корректно настроен режим ICAP preview.

Настройка Squid для взаимодействия с drweb-icapd

Общая схема взаимодействия **Squid**, **drweb-icapd** и клиента:

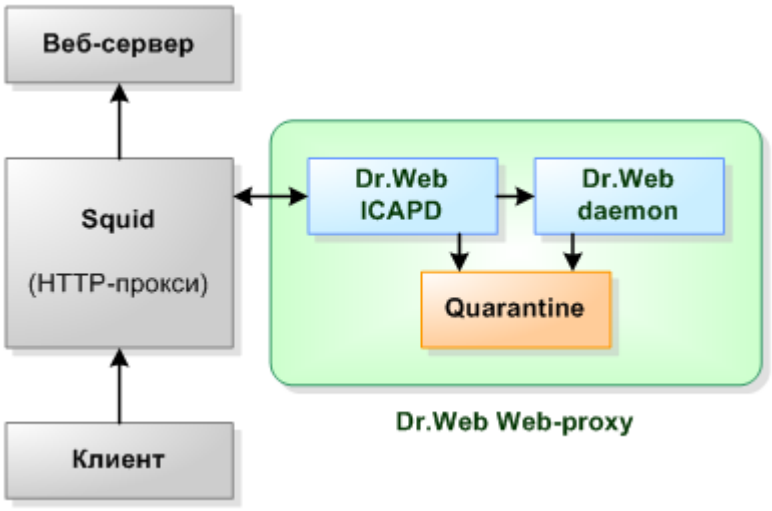


Рис. 16. Общая схема взаимодействия прокси-сервера, drweb-icapd и клиента

В данной схеме клиент взаимодействует с HTTP-сервером через прокси-сервер. При этом прокси-сервер является одновременно ICAP-клиентом по отношению к ICAP-серверу **drweb-icapd**. Модуль **drweb-icapd**, в свою очередь, является клиентом по отношению к **Dr.Web Daemon**. Модуль **drweb-icapd** позволяет проверять на наличие вирусов с помощью **Dr.Web Daemon** весь исходящий от HTTP-сервера HTTP-трафик, переданный прокси-сервером по протоколу ICAP. Заметим, что данная схема не позволяет проверять FTP-трафик. Организация такой проверки с использованием **Squid** описана далее.

Также следует уточнить, что проверка HTTPS-трафика не производится, поскольку этот протокол передает данные в зашифрованном виде, и их невозможно расшифровать, не имея открытого ключа сервера, осуществившего передачу.

Для обеспечения взаимодействия между **Squid** и **Dr.Web ICAPD** требуется отредактировать конфигурационный файл `squid.conf` с целью подключения возможности использования ICAP-протокола (этот файл обычно находится в каталоге `/usr/local/squid/etc/`).

Порядок настройки ICAP-взаимодействия зависит от используемой версии сервера **Squid**.

Если нижеприведенные строки уже есть в конфигурационном файле, то нужно раскомментировать их и исправить значения по умолчанию в случае необходимости. В противном случае нужно добавить данные настройки в конец файла.

1. Подключение возможности использования протокола ICAP:

```
icap_enable on
```

2. Регистрация новой службы ICAP:

для Squid 3.0:

```
icap_service service_1 respmod_precache 0 icap://127.0.0.1:1344/respmod
icap_class class_1 service_1
icap_access class_1 allow all
```

для Squid 3.1:

```
icap_service service_1  respmod_precache  bypass=0  icap:// 127.0.0.1:1344/respmod
adaptation_access service_1 allow all
```

Обратите внимание, что адрес и порт, указанные в **icap_service**, должны совпадать с адресом и портом, указанными в параметрах **BindAddress** и **BindPort** конфигурационного файла **Dr.Web ICAPD.**

При использовании возможности ICAP preview необходимы дополнительные настройки.

3. Подключение возможности использования режима ICAP preview:

```
icap_preview_enable on
```

4. Установка размера тела сообщения (в байтах), посылаемого в ICAP preview:

```
icap_preview_size 0
```

Обратите внимание, что для прокси-сервера **Squid** установка любого другого значения этого параметра, кроме `0` при включенном `ICAP preview`, и `-1` при выключенном, не имеет никакого эффекта (т.е. в данный момент не имеется возможность регулировать размер предпросматриваемых объектов).

5. Для вывода в файл отчета информации об IP-адресе клиента, запрашивающего ресурс:

```
icap_send_client_ip on
```

6. Для поддержки постоянных соединений между drweb-icapd и Squid, что повышает производительность:

```
icap_persistent_connections on
```

В связи с тем, что на данный момент в **Squid** не реализован режим `respmod-postcache`, при использовании данного прокси-сервера невозможно произвести проверку контента после того, как он попал в кэш.

Настройка SafeSquid для взаимодействия с drweb-icapd

Для обеспечения взаимодействия между **SafeSquid** и **drweb-icapd** требуется отредактировать файл `config.xml` или воспользоваться web-интерфейсом.

При использовании web-интерфейса следует выбрать секцию **ICAP** из выпадающего меню, затем выбрать пункт **Add** и добавить новый ICAP-интерфейс. В появившейся форме нужно заполнить следующие поля:

- **Enabled** = true;
- **Host** = IP-адрес или имя хоста, на котором запущен **drweb-icapd** (по умолчанию 127.0.0.1);
- **File** = /respmod;
- **Port** = номер порта, который использует **drweb-icapd** (по умолчанию 1344);
- **Applies to** = responses;

Затем следует нажать на кнопку **Submit.**

Также можно самостоятельно отредактировать файл `config.xml`. Для этого, к примеру, можно добавить блок

```
<icap>
  <enabled>true</enabled>
  <icap>
      < enabled>true</enabled>
      < comment>Dr.Web icap server</comment>
      < profiles></profiles>
      < host>127.0.0.1</host>
      < file>/respmod</file>
      < port>1344</port>
      < which>responses</which>
  </ icap>
</icap>
```

в секцию <**safesquid**></**safesquid**>.

Обратите внимание, что значения параметров Host и Port должны совпадать со значениями параметров **BindAddress** и **BindPort** конфигурационного файла **Dr.Web ICAPD.**

Передача FTP-трафика через drweb-icapd с использованием Squid

Передача FTP-трафика через **Dr.Web ICAPD** возможна только с использованием прокси-сервера **Squid**. Проверка FTP-трафика возможна с использованием любой из двух нижеприведенных схем:

1. Использование цепочки из двух прокси-серверов **Squid**.
2. Использование цепочки из FTP-прокси **Frox** (выполняет конвертирование FTP/HTTP), и прокси-сервера **Squid**.

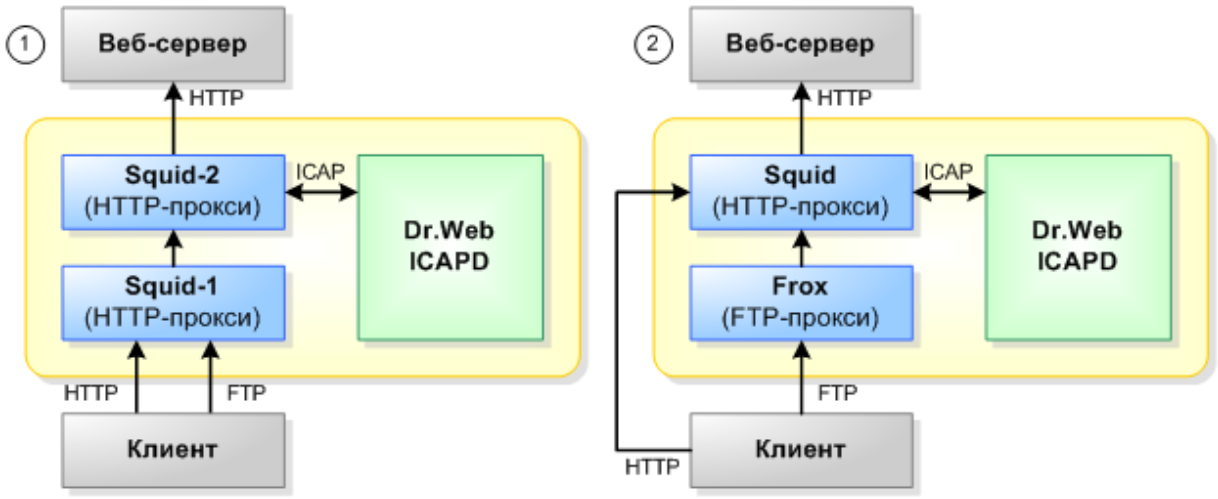


Рис. 17. Организация проверки HTTP- и FTP-трафика

1. Использование цепочки из двух прокси-серверов Squid:

При этой схеме как HTTP-трафик, так и FTP-трафик из сети Интернет будет проверяться посредством **Dr.Web ICAPD**, т.к. в обоих случаях для **Squid-2** данный трафик является HTTP-трафиком. Для реализации данной схемы требуется выполнить следующее:

1. Установить два независимых прокси-сервера **Squid** в различные каталоги;

2. Изменить параметр **http_port** у **Squid-1**, установив новое значение порта (например, 3129);
3. Настроить **Squid-2** на работу с **Dr.Web ICAPD**, как описано выше;
4. Изменить настройки **Squid-2** для взаимодействия со **Squid-1**, установив следующий параметр:

```
cache_peer localhost parent 3129 3130 default connect-timeout=80000
```

Здесь:

- 3129 - номер порта, установленного для **Squid-1**,
- localhost - хост, на котором установлен **Squid-1**,
- 80000 - значение таймаута, которое должно быть достаточно большим для поддержания связи между **Squid-2** и **Squid-1**;

5. Настроить клиенты на работу через прокси **Squid-2** как по HTTP-трафику, так и по FTP-трафику;
6. Запустить оба прокси-сервера **Squid** и **Dr.Web ICAPD**.

2. Использование цепочки Frox - Squid:

При этой схеме как HTTP-трафик, так и FTP-трафик из сети Интернет будет проверяться посредством **Dr.Web ICAPD**, т.к. в обоих случаях для **Squid** данный трафик является HTTP-трафиком. Для реализации данной схемы требуется выполнить следующее:

1. Установить прокси-серверы **Frox** и **Squid**;
2. Настроить FROX на передачу трафика на **Squid** (FTP-трафик клиентов будет учитываться, как HTTP-трафик, исходящий от **Frox**);
3. Настроить **Squid** на работу с **Dr.Web ICAPD**, как описано выше;
4. Настроить клиенты на работу через прокси **Squid** по HTTP-трафику и через **Frox** по FTP-трафику;
5. Запустить оба прокси-сервера (**Squid** и **Frox**), а также **Dr.Web ICAPD**.

Режим ICAP preview

Режим **ICAP preview** позволяет задавать в правилах контент-фильтрации файлы, которые не требуют проверки и, соответственно, закачки ICAP-сервером (к примеру, потоковое видео и аудио). Кроме того, он позволяет значительно уменьшить как внешний трафик при использовании возможности фильтрации доступа по MIME-типу и размеру или по имени хоста, так и внутренний за счет использования режимов **Allow** 204 и **preview_size** = 0. При этом повышается общая скорость и комфортность работы конечного пользователя.

Перечень правил определения файлов, требующих и не требующих проверки (в зависимости от типа содержимого и размера) задается в конфигурационном файле. Подробнее см. в разделе Настройки контент-фильтрации.

При использовании версии **Squid** из ветки 2.* *настоятельно рекомендуется* выключить режим preview как в **drweb-icapd (UsePreview** = No), так и в **Squid (icap_preview_enable** off и **icap_preview_size** -1).

Обратите внимание, что для прокси-сервера **Squid** установка любого другого значения этого параметра, кроме 0 при включенном ICAP preview, и -1 при выключенном, не имеет никакого эффекта (т.е. в данный момент не имеется возможность регулировать размер предпросматриваемых объектов).

На данный момент в прокси-сервере **SafeSquid** вместо режима **ICAP preview** реализован вывод общего числа скачанных байт информации.

Черные и белые списки доступа

Dr.Web ICAPD поддерживает списки доступа, представляющие собой наборы адресов интернет-ресурсов, доступ к которым может быть разрешен или запрещен. Помимо автоматически пополняемых компанией **«Доктор Веб»** тематических черных списков ресурсов, поставляемых вместе с **Dr.Web ICAPD**, пользователь может создать и произвольное количество пользовательских списков.

Обратите внимание, что пользователь может задавать не только черные (запрещающие), но и белые (разрешающие) списки.

Тематические черные списки

Dr.Web ICAPD поддерживает тематические черные списки. Данные списки представляют собой наборы адресов интернет-ресурсов, разбитые по темам. Каждый из этих списков обновляется в автоматическом режиме компонентом **Dr.Web Updater**. В комплект входят списки адресов ресурсов по следующим темам:

- **Adult** – ссылки на сайты и веб-ресурсы, относящиеся к категории "сайты для взрослых" (эротические рассказы, соответствующие темы на форумах, фото- и видео-материалы и страницы со ссылками на них, интернет-магазины товаров для взрослых и любые другие ресурсы эротического и порнографического характера);
- **Violence** – ссылки на фото- и видео-материалы, посвященные авто- и авиа-катастрофам, стихийным бедствиям, войнам, террористическим актам, казням, пыткам, хирургическим операциям, травмам, физическим недостаткам;
- **Weapon** – ссылки на текстовые описания, фото- и видео-материалы по всем типам оружия (от холодного до оружия массового поражения) и по изготовлению взрывчатых веществ;
- **Gamble** – ссылки на интернет-казино и разнообразные интернет-игры на деньги;
- **Drugs** – ссылки на ресурсы, где ведется пропаганда употребления наркотических веществ, публикуются отчеты об употреблении наркотических веществ и полученных ощущениях, содержатся описания процесса изготовления тех или иных наркотиков, осуществляется распространение наркотических веществ;
- **Obscenity** – ссылки на ресурсы, которые содержат нецензурную лексику (в названиях разделов, статьях и т.п.; комментарии пока не учитываются);
- **Chats** – все чаты;
- **Terrorism** – ссылки на ресурсы с материалами агрессивно-агитационного характера, с текстовыми описаниями террористических актов, их подготовки и последствий, с описаниями технологий изготовления взрывчатых веществ;
- **Email** – ссылки на сайты, предоставляющие возможность бесплатной регистрации почтового ящика;
- **SocialNetwork** – сайты знакомств, деловые социальные сети, тематические социальные сети (объединения людей по интересам, например, кулинария, авто и т.п.), корпоративные социальные сети;
- **SocialEngineering** – нерекомендумые сайты, которые могут использоваться для фишинга и мошенничества;
- **MalwareLinks** – ссылки на сайты, содержащие вирусы.
- **CopyrightNotices** – ссылки на ресурсы, добавленные по обращениям правообладателей этих ресурсов.

Обратите внимание, что один и тот же ресурс может входить в различные тематические списки. В этом случае доступ к нему будет блокироваться, если он входит хотя бы в один из блокируемых списков. Если требуется разрешить доступ к такому ресурсу, нужно разрешить доступ к ресурсам всех тематических списков, к которым он относится.

Блокировку каждой из этих тем можно включать или выключать независимо с помощью параметров конфигурации **Block<NAME>**, где **<NAME>** – тема (имя) списка. Кроме того, вы можете создать правила для разрешения доступа к ресурсам из тематических списков в зависимости от условий.

Если требуется безусловно разрешить доступ к некоторому ресурсу вне зависимости от того, в какие категории он входит, его можно добавить в пользовательский белый разрешающий список.

Тематические черные списки содержатся в файлах с расширением `dws`.

Пользовательские списки

Возможно задание для **Dr.Web ICAPD** пользовательских черных и белых списков. Черные списки запрещают доступ к хостам (так же, как и тематические списки), а белые пользовательские списки есть двух видов:

- **Доверенный список WhiteHosts.** Для хостов, находящихся в этом списке, отключается антивирусная проверка (файлы, получаемые от них, не проверяются).
- **Разрешающий список WhiteDWS.** Разрешается доступ к хостам, находящимся в этом списке, даже если они находятся в тематических черных списках, но не в пользовательском черном.

Обратите внимание, что:

- если некоторый хост находится в доверенном списке **WhiteHosts**, то доступ к нему регулируется как обычно – проверкой на нахождение в тематических списках с учетом правил, а также в черном пользовательсокм списке.
- если некоторый хост находится в черном списке **BlackHosts**, то доступ к нему блокируется безусловно, т.е. нельзя создать переопределяющего правила, разрешающего доступ к этому хосту. Кроме того, этот список имеет приоритет над разрешающим белым списком, т.е. если один и тот же хост указан в пользовательском черном списке и в разрешающем белом, то доступ к нему будет блокирован.

Создание пользовательских черных и белых списков

Пользовательские черные и белые списки могут задаваться:

- С помощью веб-интерфейса;
- Вручную.

Чтобы создать или отредактировать пользовательские списки вручную, выполните следующее:

- Создайте текстовый файл со списком имен или IP-адресов хостов, доступ к которым необходимо разрешить или запретить. Каждый хост указывается на новой строке.
- Настройте требуемую реакцию:
  - **Чтобы добавить адреса в пользовательский черный список,** укажите путь к файлу со списком, где указаны данные хосты, в значении параметра **BlackHosts** конфигурационного файла **Dr.Web ICAPD**. Возможно указание нескольких списков через запятую.

Пример:

```
BlackHosts = /home/user/host_list_1, /home/user/host_list_2
```

В данном случае, хосты, указанные в файлах `host_list_1` и `host_list_2` будут занесены в чёрный список и доступ к ним будет запрещён.

- **Чтобы добавить хосты в пользовательский белый разрешающий список,** т.е. в список хостов, доступ к которым разрешен в обход тематических списков, укажите путь к файлу со списком, содержащему данные адреса, в значении параметра **`WhiteDWSFiles`** конфигурационного файла **Dr.Web ICAPD.** Обратите внимание, что при занесении одних и тех же хостов в черный список и разрешающий белый список, **доступ к ним будет запрещен.**

  Пример:

  ```
  WhiteDWSFiles = /home/user/host_list_1, /home/user/host_list_3
  ```

  В приведенном примере пользователи будут иметь доступ только к хостам, указанным в файле `host_list_3`, несмотря на то, что список `host_list_1` указан в значении параметра **`WhiteDWSFiles`**. Однако, при нахождении одного и того же адреса в тематическом черном списке и в разрешающем белом списке, **доступ к нему будет разрешен.**

- **Чтобы добавить хосты в пользовательский белый доверенный список,** т.е. в список хостов, не требующих проверки на вирусы, укажите путь к файлу со списком, где указаны данные хосты, в значении параметра **`WhiteHosts`** конфигурационного файла **Dr.Web ICAPD.**

  Пример:

  ```
  WhiteHosts = /home/user/host_list_1, /home/user/host_list_2, /home/user/
  host_list_3
  ```

  В данном случае хосты, указанные в списках `host_list_1`, `host_list_2` и `host_list_3`, проверяться на вирусы не будут.

Обратите внимание, что параметр **`WhiteHosts`** лишь отключает антивирусную проверку файлов, поступающих от хостов, но не разрешает доступ к самим хостам. Таким образом, для привёденного примера в целом, с учетом параметров **`BlackHosts`** и **`WhiteDWSFiles`**, доступ будет открыт только к адресам из списка `host_list_3`, причем контент, получаемый от хостов из этого списка, проверяться на вирусы не будет.

Параметры командной строки

На данный момент исполняемый модуль **Dr.Web ICAPD** **`(drweb-icapd)`** поддерживает следующие параметры командной строки:

Краткий вариант	Расширенный вариант	Аргументы
`-h`	`--help`	
Описание: Вывод краткой справки о параметрах командной строки и завершение работы		
`-v`	`--version`	
Описание: Вывод информации о версии **`drweb-icapd`** и завершение работы		
`-d`		
Описание: Вывод debug-журнала на терминал		
`-f`		`<путь к файлу | путь к сокету Агента>`

Краткий вариант	Расширенный вариант	Аргументы
Описание: Задание нового пути к конфигурационному файлу **drweb-icapd** или к сокету **Dr.Web Agent**, если **Dr.Web ICAPD** будет получать конфигурационный файл от него (см. описание **Dr.Web Agent**)		
-m		
Описание: **drweb-icapd** запускается под управлением **Dr.Web Monitor** (см. описание **Dr.Web Monitor**)		

Настройки

Dr.Web ICAPD может использоваться с настройками по умолчанию, но предпочтительнее настроить его в соответствии с требованиями и условиям эксплуатации. Конфигурационный файл `drweb-icapd.ini` расположен в каталоге `%etc_dir`.

Файл состоит из одной обязательной секции `[Icapd]`, задающей основные параметры работы **Dr.Web ICAPD**, а также из набора дополнительных секций `[match]` и `[def]`, используемых для переопределения параметров работы **Dr.Web ICAPD** для групп пользователей или в зависимости от заданных условий.

- Правила записи параметров в основной секции конфигурационного файла и краткое описание типов параметров приведены в разделе Конфигурационные файлы.
- Перечень параметров, задаваемых в основной секции `[Icapd]`, рассмотрен в разделе Параметры конфигурации.
- Правила настройки фильтрации файлов по их содержимому рассмотрены в разделе Настройки контент-фильтрации.
- Способы переопределения разрешающих и запрещающих параметров **Dr.Web ICAPD** для групп пользователей или в зависимости от заданных условий рассмотрено в разделе Переопределение параметров для групп пользователей.

Параметры конфигурации

Общие настройки компонента фильтрации Интернет-трафика **Dr.Web ICAPD** задается в конфигурационном файле `drweb-icapd.ini`, в секции `[Icapd]`. В этой секции задаются следующие параметры:

Logfile = {имя файла | syslog}	Имя файла журнала или `syslog`, если используется системный сервис **syslog** Значение по умолчанию: **Logfile** = syslog
SyslogFacility = {метка syslog}	Метка записи при использовании системного сервиса **syslog** Значение по умолчанию: **SyslogFacility** = Daemon
SyslogPriority = {уровень подробности}	Уровень подробности сохранения событий в журнал при использовании системного сервиса **syslog**. Допускается использование следующих уровней: • Alert • Warning • Info • Notice

	Значение по умолчанию: **SyslogPriority** = Info
Loglevel = {числовое значение}	Устанавливает уровень подробности ведения журнала работы. Представляет собой число, являющееся суммой произвольной комбинации следующих значений: • 0 – выводить информацию об ошибках и обнаруженных вирусах; • 1 – выводить информацию уровня Info: о проверенных чистых файлах и прочую служебную информацию; • 2 – выводить общие сообщения; • 4 – выводить сообщения о результатах разбора фрагментов данных (chunks of data); • 8 – выводить расширенные сообщения по фрагментам данных; • 16 – выводить протокол работы синтаксического анализатора; • 32 – выводить прочие отладочные сообщения. Например, если требуется выводить в журнал общие сообщения (2), сообщения синтаксического анализатора (16) и информацию об ошибках и обнаруженных вирусах (0), то значение **LogLevel** образуется следующим образом: 0 + 2 + 16 = 18 Максимально подробный вывод информации, включающий вывод всех данных, включается, таким образом, если **Loglevel** = 63. Обратите внимание, что если **Loglevel** = -1, то это означает отключение вывода информации в журнал.
	Значение по умолчанию: **Loglevel** = 1
MaxLogSize = {размер}	Максимальный размер файла журнала. Если при запуске **Dr.Web Daemon** размер файла журнала будет больше заданного, то он будет перезаписан заново. При **MaxLogSize** = 0 размер файла журнала при старте не проверяется.
	Значение по умолчанию: **MaxLogSize** = 1m
Hostmaster = {адрес e-mail}	Почтовый адрес администратора.
	Значение по умолчанию: **Hostmaster** = root@localhost

Параметры, задающие реакцию **Dr.Web ICAPD** на обнаружение тех или иных объектов в файлах, отправленных на вирусное сканирование:

Infected = {действие}	Задает реакцию на обнаружение файла, зараженного известным вирусом. Допустимые значения параметра: Cure, Move, Truncate, Report
	Значение по умолчанию: **Infected** = Cure

Incurable = {действие}	Задает реакцию на обнаружение файла, который заражен и не может быть вылечен (если ранее к этому объекту применялось действие Cure, не приведшее к успеху). Допустимые значения параметра: Move, Truncate, Report Значение по умолчанию: **Incurable** = Report
Suspicious = {действие}	Задает реакцию на обнаружение подозрительного файла методом *Эвристического анализа.* Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **Suspicious** = Report
Adware = {действие}	Задает реакцию на обнаружение файла, содержащего программу для показа рекламы (adware). Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **Adware** = Report
Dialers = {действие}	Задает реакцию на обнаружение файла, содержащего программу автоматического дозвона. Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **Dialers** = Report
Jokes = {действие}	Задает реакцию на обнаружение файла, содержащего программу-шутку, которая может пугать или раздражать пользователя. Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **Jokes** = Pass
Riskware = {действие}	Задает реакцию на обнаружение файла, содержащего потенциально опасную программу, которая может быть использована не только ее владельцем, но и злоумышленниками. Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **Riskware** = Pass
Hacktools = {действие}	Задает реакцию на обнаружение файла, содержащего программу, которая используется для взлома компьютеров. Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **Hacktools** = 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, Move, Truncate, Report Значение по умолчанию: **ArchiveRestriction** = Report
DaemonError = {действие}	Действие, совершаемое с файлами, вызывающими у **Dr.Web Daemon** ошибки в процессе проверки. Например, **Dr.Web Daemon** может перестать хватать памяти или у него не окажется нужных прав для дальнейшей работы. Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **DaemonError** = Report
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, Move, Truncate, Report Значение по умолчанию: **SkipObject** = Pass
LicenseError = {действие}	Действие, совершаемое с файлами, при проверке которых произошла ошибка лицензии (например, когда срок действия лицензии истек). Допустимые значения параметра: Pass, Move, Truncate, Report Значение по умолчанию: **LicenseError** = Report
Heuristic = {логический}	Включение использования *Эвристического анализа.* *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 анализа.* Кроме того, данный режим может незначительно увеличить время проверки. Данные обстоятельства могут быть доводами в пользу отключения эвристического анализа. Вместе с тем, включение этого типа анализа увеличивает надежность антивирусной защиты. Все файлы, обнаруженные методом *Эвристического анализа*, лучше всего отправить разработчикам через сайт http://vms.drweb.com/sendvirus/.

	Обратите внимание, что положительный вердикт *Эвристического анализа* приводит к срабатыванию события **Suspicious**. Значение по умолчанию: **Heuristic** = Yes

Глобальные параметры блокирования интернет-ресурсов, находящихся в тематических списках (могут быть переопределены для различных условий):

BlockAdult = {логический}	Блокировать или нет интернет-ресурсы "для взрослых", находящиеся в тематическом черном списке Adult. Значение по умолчанию: **BlockAdult** = Yes
BlockViolence = {логический}	Блокировать или нет интернет-ресурсы, посвященные жестокости и насилию, находящиеся в тематическом черном списке Violence. Значение по умолчанию: **BlockViolence** = Yes
BlockWeapon = {логический}	Блокировать или нет интернет-ресурсы, посвященные всем типам вооружений, находящиеся в тематическом черном списке Weapon. Значение по умолчанию: **BlockWeapon** = Yes
BlockGamble = {логический}	Блокировать или нет интернет-ресурсы, посвященные азартным играм на деньги, находящиеся в тематическом черном списке Gamble. Значение по умолчанию: **BlockGamble** = Yes
BlockDrugs = {логический}	Блокировать или нет интернет-ресурсы, посвященные наркотическим веществам, находящиеся в тематическом черном списке Drugs. Значение по умолчанию: **BlockDrugs** = Yes
BlockObscenity = {логический}	Блокировать или нет интернет-ресурсы, содержащие нецензурную лексику, находящиеся в тематическом черном списке Obscenity. Значение по умолчанию: **BlockObscenity** = Yes
BlockChats = {логический}	Блокировать или нет все чаты, находящиеся в тематическом черном списке Chats. Значение по умолчанию: **BlockChats** = No
BlockTerrorism = {логический}	Блокировать или нет интернет-ресурсы, посвященные терроризму, находящиеся в тематическом черном списке Terrorism. Значение по умолчанию: **BlockTerrorism** = Yes

BlockEmail = {логический}	Блокировать или нет интернет-ресурсы, предоставляющие бесплатную регистрацию почтового ящика, находящиеся в тематическом черном списке Email. Значение по умолчанию: **BlockEmail** = No
BlockSocialNetwork = {логический}	Блокировать или нет доступ к разнообразным социальным сетям, находящимся в тематическом черном списке SocialNetwork. Значение по умолчанию: **BlockSocialNetwork** = No
BlockSocialEngineering = {логический}	Блокировать или нет нерекомендумые сайты, которые могут использоваться для фишинга и мошенничества, находящиеся в тематическом черном списке SocialEngineering. Значение по умолчанию: **BlockSocialEngineering** = Yes
BlockMalwareLinks = {логический}	Блокировать или нет интернет-ресурсы, содержащие вирусы и другие вредоносные программы, находящиеся в тематическом черном списке MalwareLinks. Значение по умолчанию: **BlockMalwareLinks** = Yes
BlockDueToCopyrightNotice = {логический}	Блокировать или нет интернет-ресурсы, ссылки на которые по обращению правообладателей этих ресурсов добавлены в тематический черный список CopyrightNotices. Значение по умолчанию: **BlockDueToCopyrightNotice** = Yes
BlockAll = {логический}	Блокировать или нет все запросы от пользователей к сети Интернет, как к запрещенным, так и не запрещенным ресурсам. Обратите внимание, что действие этого параметра не равносильно выставлению одновременно всех параметров **Block<Name>** в Yes или в No: • Если параметр установлен в Yes, то блокируются все запросы пользователей к Интернет, вне зависимости от того, следуют они на ресурсы, внесенные в черные или белые списки, или нет. • Если параметр установлен в No, то пользователям разрешен доступ в Интернет, но только на те ресурсы, которые не блокируются (т.е. не содержатся в активных черных списках или содержатся в белом разрешающем пользовательском списке). Если требуется разрешить доступ ко всем ресурсам в сети Интернет, вне зависимости от того, принадлежат они черным спискам или нет, следует не только установить **BlockAll**=No, но и выставить значение No для всех параметров **Block<Name>**, включающих тематические списки **<Name>**, а также очистить пользовательский черный список, задаваемый в параметре **BlackHosts**.

	Значение по умолчанию: **BlockAll** = No

Далее перечислены списки, определенные пользователем:

WhiteDwsFiles = {список путей к файлам}	Разрешающий белый пользовательский список. Содержит список имен текстовых файлов через запятую, в каждом из которых содержится список хостов, которые не будут проверяться на блокировку в черных списках (как активных тематических, так и пользовательском черном), но контент от них будет проверяться на вирусы. Данный параметр необходим, когда черные списки блокируют доступ на нужный сайт. Формат этих файлов следующий: host1 host2 ... Также вы можете воспользоваться переопределением параметров доступа для условного разрешения доступа. Если требуется разрешить пропускать контент, следующий от хоста, без проверки на вирусы, следует указать этот хост в параметре **WhiteHosts** (доверенный белый пользовательский список). Значение по умолчанию: **WhiteDwsFiles** =
WhiteHosts = {список путей к файлам}	Доверенный белый пользовательский список. Содержит список путей к файлам через запятую, в каждом из которых содержится список хостов, которые не будут проверяться на наличие вирусов (но при этом эти хосты проверяются на наличие в черных списках, как в тематических, так и в пользовательском). Чтобы разрешить обращение к хосту, его нужно указать в разрешающем белом пользовательском списке (в параметре **WhiteDwsFiles**). Данный параметр используется для предотвращения ложного срабатывания антивирусного модуля **Dr.Web Daemon**. Отказ от проверки на вирусы разрешается как по имени хоста, так и по всем его IP-адресам. Значение по умолчанию: **WhiteHosts** =
BlackHosts = {список путей к файлам}	Черный пользовательский список. Содержит список путей к файлам через запятую, в каждом из которых содержится список хостов, доступ к которым требуется запретить. Блокировка происходит как по имени хоста, так и по всем его IP-адресам. Обратите внимание, что если хост включен в этот черный список, то доступ к нему запрещается безусловно, и не может быть разрешен при помощи переопределения параметров в правилах. Значение по умолчанию: **BlackHosts** =

Прочие настройки:

SendUrlsWithViruses = {логический}	Возможность автоматически отсылать в **Dr.Web** адреса зараженных интернет-ресурсов и имена вирусов, найденных на этих веб-страницах. Для осуществления данной операции необходимо, чтобы был установлен компонент **Dr.Web Agent**. Значение по умолчанию: **SendUrlsWithViruses** = No
MaxBlocksize = {размер}	Максимальный размер блока памяти, который **Dr.Web ICAPD** пытается выделить за один раз. При достаточном количестве оперативной памяти значение данного параметра можно увеличить для повышения производительности. Значение по умолчанию: **MaxBlocksize** = 10m
LocalScan = {логический}	Выбор режима передачи файлов на сканирование **Dr.Web Daemon**. При **LocalScan** = Yes **Dr.Web Daemon** будет сканировать файлы в локальном режиме (ему будет передаваться только путь к файлу), в противном случае ему будет передаваться само содержимое файла. Параметр **LocalScan** может быть Yes только в том случае, если **Dr.Web Daemon** расположен на той же машине, на которой работает **Dr.Web ICAPD**. Значение по умолчанию: **LocalScan** = Yes
User = {строка}	Пользователь, с правами которого работает **Dr.Web ICAPD**. Рекомендуется завести в системе специального пользователя drweb, который будет использоваться **Dr.Web ICAPD**. Значение по умолчанию: **User** = drweb
Cache = {путь к каталогу}	Путь к каталогу, в котором создаются и хранятся временные файлы. Значение по умолчанию: **Cache** = %var_dir/cache/
DwsDirectory = {путь к каталогу}	Путь к каталогу, в котором находятся файлы, содержащие тематические черные списки (dws-файлы). Значение по умолчанию: **DwsDirectory** = %var_dir/dws/
Templates = {путь к каталогу}	Путь к каталогу, в котором хранятся шаблоны уведомлений для пользователей и администратора. Значение по умолчанию: **Templates** = %etc_dir/templates/icapd
PidFile = {путь к файлу}	Имя файла, в который при запуске **Dr.Web ICAPD** 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/drweb_icapd.pid
Key = {путь к файлу}	Расположение ключевого файла (лицензионного или демонстрационного). Обычно это файл с расширением .key Значение по умолчанию: **Key** = %bin_dir/drweb32.key
BindPort = {числовое значение}	Номер порта, к которому должны подключаться ICAP-клиенты (например, **Squid)** при попытке соединения с **Dr.Web ICAPD**. Значение должно совпадать со значением, указанным у прокси-сервера. Значение по умолчанию: **BindPort** = 1344
BindAddress = {IP-адрес или имя хоста}	Хост, на котором находится **drweb-icapd.** Значение должно совпадать с адресом, указанным у прокси-сервера. Значение по умолчанию: **BindAddress** = 127.0.0.1
DrwebAddress = {список адресов}	Список адресов сокетов для связи с **Dr.Web Daemon.** Адреса в списке разделяются запятыми. **Примеры**: **DrwebAddress** = inet:3000@localhost **DrwebAddress** = local:%var_dir/.daemon **DrwebAddress** = pid:/usr/local/drweb/run/drwebd.pid Если вы используете **Dr.Web Daemon**, запущенный на удаленной машине, параметр **LocalScan** должен быть установлен в No. Когда первым в списке стоит адрес сокета или PID-файла **Dr.Web Daemon**, обеспечивающего локального сканирование, то при невозможности установить соединение по этому адресу, режим локального сканирования принудительно отключается. Если список пуст, то **Dr.Web ICAPD** работает без подключения к **Dr.Web Daemon**, и проверка на вирусы не производится. Значение по умолчанию: **DrwebAddress** = pid:%var_dir/run/drwebd.pid
PathToQuarantine = {путь к каталогу}	Путь к каталогу **Карантина**. Значение по умолчанию: **PathToQuarantine** = %var_dir/infected/
QuarantineFilesMode = {права доступа}	Права доступа к файлам, находящимся в **Карантине**. Значение по умолчанию: **QuarantineFilesMode** = 0660

Timeout = {числовое значение}	Максимальное время в секундах, в течение которого сокет может находиться в режиме ожидания. При получении/отсылке хотя бы одного байта счетчик обнуляется. Если указано значение 0, время ожидания не ограничивается. Значение по умолчанию: **Timeout** = 300
SendMail = {логический}	Следует ли посылать администратору уведомления при попытках загрузки вредоносных объектов. Уведомления высылаются на адрес, указанный в значении параметра **Hostmaster**. Значение по умолчанию: **SendMail** = No
SendMailDwsBlock = {логический}	Следует ли посылать администратору уведомления при попытках загрузки страниц, заблокированных с помощью тематических черных списков. Уведомления высылаются на адрес, указанный в значении параметра **Hostmaster**. Значение по умолчанию: **SendMailDwsBlock** = No
MailCommand = {строка}	Команда shell, выполняемая для отправления почтовых уведомлений администратору. Параметр %s в указанной команде заменяется на значение параметра **Hostmaster**. Значение по умолчанию: **MailCommand** = "/usr/sbin/sendmail -i -bm -f drweb -- %s"
MailCache = {числовое значение}	Промежуток времени в секундах, в течение которого не высылаются уведомления администратору об одном и том же инциденте (повторные попытки открытия "плохой" страницы или загрузки зараженного файла). При **MailCache** = 0 уведомление высылается при каждом блокировании страницы. Значение по умолчанию: **MailCache** = 60
AclList = {список путей к файлам}	Список файлов через запятую, содержащих IP-адреса и имена хостов, которым разрешен доступ к **Dr.Web ICAPD** по протоколу ICAP. Если список пуст или в указанных файлах не найдено ни одного адреса, то **Dr.Web ICAPD** принимает соединения от всех клиентов. Значение по умолчанию: **AclList** =
SendStat = {логический}	Следует ли отправлять модулю **Dr.Web Agent** статистику по найденным вирусам. Значение по умолчанию: **SendStat** = No

KeepAlive = {логический}	Следует ли поддерживать постоянное соединение с прокси-сервером. Значение по умолчанию: **KeepAlive** = Yes
UsePreview = {логический}	Использование режима предпросмотра ICAP preview. Если прокси-сервер некорректно работает с режимом предпросмотра, можно отключить эту возможность, указав **UsePreview** = No. Значение по умолчанию: **UsePreview** = Yes
Hostmaster = {адрес электронной почты}	Почтовый адрес администратора для отправки уведомлений. Значение по умолчанию: **Hostmaster** = root@localhost

Обратите внимание, что один и тот же ресурс может входить в различные тематические списки и черный список пользователя. В этом случае доступ к нему будет блокироваться, если он входит хотя бы в один из активных черных списков. Если требуется разрешить доступ к такому ресурсу, нужно отключить все черные списки, к которым он относится.

В конце секции параметров располагается раздел определения правил фильтрации файлов на основе анализа их содержимого. Этот раздел всегда начинается со строки **MimeStart**, заканчивается строкой **MimeEnd** и содержит правила фильтрации файлов, по одному на строку. Подробнее о правилах фильтрации см. в разделе Настройки фильтрации MIME.

Переопределение параметров для групп пользователей

Существует возможность для разных пользователей (или групп пользователей) задавать индивидуальные настройки доступа к интернет-ресурсам, указывая для некоторых параметров из основной секции файла конфигурации значения, отличные от базовых. Такое переопределение параметров осуществляется с помощью специальных правил.

В текущей версии **Dr.Web для интернет-шлюзов UNIX** можно переопределять следующие параметры:

- **BlockAdult**
- **BlockViolence**
- **BlockWeapon**
- **BlockGamble**
- **BlockDrugs**
- **BlockObscenity**
- **BlockChats**
- **BlockTerrorism**
- **BlockEmail**
- **BlockSocialNetwork**
- **BlockSocialEngineering**
- **BlockMalwareLinks**
- **BlockDueToCopyrightNotice**
- **BlockAll**

Правила задаются в секции `[match]` конфигурационного файла `drweb-icapd.ini`. Функции, используемые в правилах, задаются в секции `[def]` в том же конфигурационном файле. Порядок данных секций может быть произвольным, но любая используемая в правилах функция должна быть предварительно определена в секции `[def]`. Соответствующие выражения для правил и функций внутри секций `[match]` и `[def]` могут быть разбиты на несколько строк.

Один и тот же ресурс может одновременно входить в различные тематические списки и черный список пользователя. В этом случае доступ к нему будет блокироваться, если он входит хотя бы в один из активных черных списков. Если требуется разрешить доступ к такому ресурсу, нужно отключить все черные списки, к которым он относится.

Однако, чтобы в этом случае заодно не разрешить доступ к остальным запрещенным ресурсам этих категорий, крайне рекомендуется включать в разрешающее условие как проверку на URL ресурса, к которому разрешается доступ, так и проверку свойств клиента (таких, как IP-адрес), которому этот доступ предоставляется.

Обратите внимание, что если ресурс включен в пользовательский черный список, то разрешить доступ к нему при помощи разрешающего условия невозможно.

Переменные

Каждый запрос, направляемый от клиента прокси-серверу, имеет ряд уникальных параметров. Эти параметры можно использовать в правилах, указав их как переменные:

Имя переменной	Тип переменной	Описание
`request_url`	строка (string)	URL запроса
`request_username`	строка (string)	Имя пользователя, под которым он авторизовался на прокси-сервере. Оно берется из заголовка `X-Client-Username`, а если этот заголовок отсутствует, то значение переменной берется равным пустой строке.
`request_ip`	IP-адрес с маской сети (CIDR)	IP-адрес пользователя, от которого пришел запрос на прокси-сервер. Он берется из заголовка `X-Client-IP`, а если такой заголовок отсутствует, то переменная принимает значение `undefined`.
`system_time`	время (time)	Текущее системное время (часы и минуты).

Обратите внимание, что для использования переменных **`request_ip`** и **`request_username`** нужно обеспечить соответствующую настройку HTTP прокси-сервера **Squid**.

Логические выражения

Логические выражения – это операции сравнения и вызова функций, объединенные логическими операторами **`&&`** ("логическое И", "AND"), **`||`** ("логическое ИЛИ", "OR"), **`!`** ("логическое отрицание", "NOT"). Для группировки операций и изменения их приоритета могут использоваться скобки.

Обратите внимание, что логические операции задаются только при помощи операторов **`&&`**, **`||`** и **`!`**.

Обозначения **`AND`**, **`OR`** и **`NOT`** не используются.

Синтаксис логических выражений BOOL_EXPR:

```
func_name() | COMPARE |
(BOOL_EXPR) | !BOOL_EXPR |
BOOL_EXPR && BOOL_EXPR |
BOOL_EXPR || BOOL_EXPR
```

Где func_name() – вызов функции с именем func_name, а COMPARE – одна из перечисленных ниже операций сравнения. Функция должна быть определена заранее в секции [def].

Используемые обозначения при определении операций сравнения COMPARE:

Обозначение	Комментарий
string_var cidr_var time_var	Переменная соответствующего типа (STRING, CIDR или TIME)
TIME	Строка в формате "ЧЧ:ММ" или "Ч:ММ" (часы, минуты), в кавычках
STRING	Произвольная строка в кавычках
REGEX	Регулярное выражение формата POSIX extended, в кавычках
FILE_NAME	Путь к файлу, в кавычках
CIDR	IPv4-адрес в кавычках (возможно, с маской сети, указанной через слеш). Если маска сети не указана, то подразумевается /32. Пустая строка "" означает специальное значение undefined

Поддерживаемые операции сравнения для переменных типа string:

Операция	Комментарий
string_var == STRING	Переменная совпадает со строкой
string_var != STRING	Переменная не совпадает со строкой
string_var ~ REGEX	Переменная содержит подстроку, которая проверяется на совпадение с регулярным выражением (используется метод search)
string_var == file:FILE_NAME	Переменная совпадает хотя бы с одной строкой из указанного файла
string_var ~ file:FILE_NAME	Переменная соответствует хотя бы одному регулярному выражению из указанного файла

Операции == и ~ для строк регистронезависимы.

Поддерживаемые операции сравнения для переменных типа cidr:

Операция	Комментарий
cidr_var <<= CIDR	IP-адрес входит в сеть указанного диапазона
cidr_var <<= file:FILE_NAME	IP-адрес входит хотя бы в одну из сетей, перечисленных в указанном файле

Если для операции <<= оба аргумента имеют значение undefined, то результатом операции считается true. Если же только один из аргументов имеет значение undefined, то результат этой операции – false.

Поддерживаемые операции сравнения для переменных типа time:

Операция	Комментарий
time_var > TIME time_var >= TIME time_var < TIME time_var <= TIME	Сравнение времени

Каждая операция сравнения имеет определенный приоритет относительно других операций. В порядке убывания приоритета операции сравнения распределяются следующим образом:

1. `!` ("логическое НЕ", "NOT")
2. `<` ("меньше"), `<=` ("меньше или равно"), `>` ("больше"), `>=` ("больше или равно")
3. `==` ("совпадает"), `!=` (не "совпадает"), `~` ("соответствует"), `<<=` ("входит в группу")
4. `&&` ("логическое И", "AND")
5. `||` ("логическое ИЛИ", "OR")

Операции, перечисленные в одной строке, имеют одинаковый приоритет и вычисляются слева направо.

Для некоторых операций возможно чтение массива значений из файла (с указанием префикса `file:`). Строки, начинающиеся с символов "#" или ";", а также пустые строки – пропускаются при чтении значений. Содержимое файла `file:FILE_NAME` читается при обработке конфигурационного файла, соответственно, при изменении содержимого файла со значениями или пути к нему необходимо заставить **`drweb-icapd`** перечитать конфигурацию, например, послав ему сигнал `SIGHUP`.

Переопределение параметров - секции [match]

Правила задаются в секциях `[match]` конфигурационного файла `drweb-icapd.ini`. При задании правил используются специальные `if`-операторы.

Синтаксис оператора `if`:

```
if BOOL_EXPR {
      блок_конфигурации
}
```

Где `BOOL_EXPR` – логическое выражение, а `блок_конфигурации` – список параметров, которым присвоены новые значения, отличные от "глобальных" значений, указанных в конфигурационном файле.

Как определяется значение параметра с учетом правил из секции `[match]`:

1. **Dr.Web ICAPD** с помощью тематических черных списков интернет-ресурсов определяет, относится ли запрашиваемый ресурс к категории блокируемых.
2. Если соответствующий URL найдет в черных списках (например, в списке **Terrorism**), то **Dr.Web ICAPD** запрашивает значение параметра **`Block<NAME>`**, где **`<NAME>`** – тема списка (например, **`BlockTerrorism`**).
3. Сперва поиск значения соответсвующего параметра осуществляется в секции `[match]`. Используется следующий алгоритм:
   - вычисляется значение выражения оператора `if` для значений переменных запроса,
   - если оно истинно, то осуществляется поиск требуемого параметра в соответствующем блоке конфигурации,
   - если такой параметр найден, то возвращается его значение и поиск завершается,
   - если параметр не найден, либо если переменная не удовлетворяет критериям, заданным конкретным выражением оператора `if`, то осуществляется переход к следующему оператору `if`.
4. Если в секции `[match]` ни одно из правил не может быть применено к данному запросу, либо не содержит необходимого параметра, возвращается глобальное значение этого параметра (или значение по умолчанию, если параметр не определен в конфигурационном файле).

Поиск значения параметра осуществляется до первого совпадения, и, соответственно, возвращается первое найденное значение (из блоков конфигурации тех операторов `if`, выражения в которых имеют значение `true`).

Функции - секции [def]

Функции можно использовать в любых логических выражениях, но каждая функция должна быть определена перед использованием. Функции определяются в секции `[def]`. В одной секции может быть определено несколько функций, кроме того, самих секций `[def]` в конфигурационном файле может быть несколько (объявленные в них функции будут объеденены в единый список при чтении конфигурации).

Синтаксис определения функции:

```
func_name = { BOOL_EXPR }
```

Где `BOOL_EXPR` – логическое выражение.

Все функции возвращают логическое значение, аргументы не поддерживаются. По сути, функция – это просто сокращенная запись выражения.

Пример:

Определяем функции `is_localhost` и `local_ip`: данные функции будет иметь значение `true`, если запрос пришел с одного из указанных IP-адресов или с одного из IP-адресов, перечисленных в файле.

```
[def]
is_localhost = { request_ip <<= "127.0.0.0/8" }

local_ip = {
      request_ip <<= "127.0.0.0/8"
      || request_ip <<= "192.168.0.0/16"
      || request_ip <<= "172.16.0.0/12"
      || request_ip <<= file:"/tmp/icapd/other_local_ips.txt"
}
```

Определяем функцию `worktime()`: данная функция будет иметь значение `true`, если текущее системное время попало в промежуток от 9:30 до 13:00 и от 14:00 до 18:15.

```
[def]
worktime = {
 (system_time>="9:30" && system_time<="13:00")
 ||
 (system_time>="14:00" && system_time<"18:15")
}
```

Примеры использования

Если требуется заблокировать доступ к интернет-ресурсам из списков **Adult** и **Email** в рабочее время для пользователей из локальной сети, а также для пользователей с определенного IP-адреса, то можно использовать следующее правило:

```
[match]
if (local_ip() ||
    request_ip <<= "87.249.57.20") &&
    worktime()
{
  BlockAdult = yes
  BlockEmail = yes
}
```

Если требуется заблокировать доступ к интернет-ресурсам из списка **Terrorism** в ночное время (с 23:00 до 8:00) для пользователей с определенных IP-адресов, то можно задать следующее правило:

```
[match]
if (request_ip <<= "93.185.182.46" ||
    request_ip <<= "195.98.93.66") &&
    (system_time>="23:00" ||
    system_time<="8:00")
{
  BlockTerrorism = yes
}
```

Чтобы запретить пользователю "edx" доступ к сети Интернет в нерабочее время:

```
[match]
if request_username=="edx" && !worktime()
{
  BlockAll = yes
}
```

Обратите внимание, что функции `local_ip()` и `worktime()`, используемые в примерах, должны быть предварительно определены в секции `[def]`.

Чтобы запретить доступ к конкретному интернет-ресурсу всем пользователям, чьи имена удовлетворяют регулярному выражению `"vasya.*"`, либо удовлетворяют любому из регулярных выражений, перечисленных в файле, либо совпадают с одной из строк в файле, используйте следующее правило:

```
[match]
if (request_username ~ "vasya.*" ||
 request_username ~ file:"/tmp/icapd/users_re_block.txt"
 || request_username == file:"/tmp/icapd/users_block.txt")
 && (request_url == "http://example.com/mega_music.mp3")
{
  BlockAll = yes
}
```

Обратите внимание, что установка в правиле **BlockAll** в `No` не означает, что в результате срабатывания условия будет обеспечен беспрепятственный доступ к запрошенному ресурсу. В этом случае доступ к ресурсу разрешается, если он попадает в пользовательский белый разрешающий список или не попадает в активные черные списки (как тематические списки `<Name>`, включение и выключение которых определяется значением соответствующих параметров **Block<Name>**, так и пользовательский черный список).

В случае если в обычном режиме доступ к ресурсам из некоторых тематических списков запрещен, но нужно разрешить доступ к некоторому ресурсу (или, например, разрешить доступ к сайтам из некоторого тематического списка), следует создать соответствующее разрешающее правило.

Например, пусть требуется разрешить посещать ресурс **socialnetwork.com** пользователям, IP-адреса которых принадлежат подсети `192.168.1.1/32`, не смотря на то, что он относится к блокируемым тематическим спискам **SocialNetworks** и **Chats**:

```
if (request_ip <<= "192.168.1.1/32") && (request_url ~ "socialnetwork.com")
{
  BlockSocialNetwork = no
  BlockChats = no
}
```

Данное правило разрешает доступ к ресурсам, находящимся в тематических списках **SocialNetworks** и **Chats**, только в том случае, если:

- IP-адрес запросившего доступ клиента относится к подсети `192.168.1.1/32`;
- URL, запрошенный клиентом, содержит подстроку `socialnetwork.com`.

При выполнении указанных условий доступ к ресурсу будет открыт. Во всех остальных случаях применяются глобальные настройки блокировки, указанные в конфигурационном файле. Обратите внимание, что если ресурс принадлежит более чем одному списку, то чтобы обеспечить к нему доступ, следует отключить блокировку для всех списков, в которые он входит.

Настройка Squid для работы с переменными

Для получения возможности использовать переменные `request_username` и `request_ip` необходима дополнительная настройка прокси-сервера **Squid**. Для этого требуется отредактировать его конфигурационный файл (обычно это файл `/usr/local/squid/etc/squid.conf`).

Если нижеприведенные строки уже есть в конфигурационном файле, то нужно раскомментировать их и исправить значения по умолчанию в случае необходимости. В противном случае нужно добавить данные настройки в конец файла.

Для использования переменной request_ip:

```
# request_ip
icap_send_client_ip on
```

Для использования переменной request_username:

```
# request_username
icap_send_client_username on
icap_client_username_header X-Client-Username
icap_client_username_encode off
```

Настройки контент-фильтрации

Правила контент-фильтрации файлов в зависимости от их MIME-типа и размера задаются в конце основной секции `[Icapd]` конфигурационного файла. Этот раздел всегда начинается со строки **MimeStart**, заканчивается строкой **MimeEnd** и содержит правила фильтрации файлов, по одному на строку.

Для использования данной возможности необходимо, чтобы прокси-сервер поддерживал режим ICAP preview, а также убедитесь, чтобы параметр **UsePreview** был установлен в значение `Yes`.

Для правил фильтрации используется следующий синтаксис (элементы выражения разделяются пробелами):

```
<MIME-тип> <действие1> <размер> <действие2>
```

где

- `MIME-тип` – MIME-тип файла, например:
  - `*` – файл любого типа;
  - `application` – исполняемые и архивированные файлы, документы в формате PDF, MS Word и др.;
  - `audio` – аудиофайлы (`mp3`, `wav`, `wma` и др.);
  - `image` – изображения (`gif`, `jpg`, `png`, `svg` и др.);

- message – сообщения между веб-серверами и клиентами;
- multipart – контейнеры (почтовые файлы, запакованные файлы);
- text – текст или исходный код (html, xml, css и др.);
- video – видеофайлы (mpeg-1, mp4, wma);
- model – файлы трехмерных моделей.

При необходимости может быть указано как целое семейство MIME, так и конкретный тип (например: video – любые видеофайлы, а video/mpeg – видео типа MPEG).

Обратите внимание, что для объекта всегда применяется правило, заданное для MIME-типа, наиболее близкого MIME-типу объекта, таким образом, правило для MIME-типа "*", подходящее любому типу, применяется, только если не имеется правил с более близким классом типов MIME.

- <действие1> – наименование действия (scan, pass, reject), которое следует выполнить в случае, если размер объекта данного MIME-типа не превосходит размер, указанный в поле <размер>.
- <размер> – пороговый размер. Если размер объекта данного MIME-типа не будет превосходить пороговый, то к нему применится действие <действие1>, иначе к нему будет применено действие <действие2>.
- <действие2> – наименование действия (scan, pass, reject), которое следует выполнить в случае, если размер объекта превосходит указанный.

Если в качестве размера указать ключевое слово **all**, то это означает, что первое действие будет применяться ко всем объектам данного MIME-типа, вне зависимости от их размера. В этом случае <действие2> не указывается.

Обозначение действий:

- scan – Отправить файл на вирусное сканирование;
- pass – Пропустить файл к пользователю без проверки;
- reject – Заблокировать файл. Обратите внимание, что это действие должно указываться с дополнительным ключом, определяющим, какие данные возвращаются пользователю:
  - -report – Вернуть пользователю вместо запрошенного файла HTML-уведомление о блокировке;
  - -trunc – Вернуть пользователю запрошенный файл, усеченный до нулевой длины.

Обратите внимание, что без уточняющего ключа действие reject указывать нельзя!

Порядок следования правил в секции не имеет значения.

Примеры правил:

```
MimeStart
  *                          scan 1M pass
  application                scan 1M pass
  image                      scan 1M pass
  message                    scan 1M pass
  multipart                  scan 1M reject -report
  text                       scan 1M pass
  audio                      pass all
  video                      pass all
  application/x-mms-framed   pass all
MimeEnd
```

Первое правило в приведенном списке применяется к объектам, тип которых не соответствует ни одному из указанных ниже. Если размер файла окажется меньше 1 MB, то файл будет отправлен на сканирование, в противном случае он будет пропущен к пользователю без сканирования. Правило, относящееся к multipart, требует отвергать составные объекты, размер которых больше 1 MB, возвращая вместо них пользователю HTML-страницу с сообщением об отказе.

Последнее правило применяется ко всем объектам типа `application/x-mms-framed`, и предписывает пропускать их без проверки вне зависимости от их размера.

Обратите внимание, что файл будет отправлен на сканирование только в том случае, если к нему применено действие `scan` (в этом случае он также может быть отвергнут по результатам вирусного сканирования, в зависимости от заданных настроек). Если к файлу применено действие `reject` (с ключом `-report` или `-trunc`), то сканирования не происходит, а пользователь сразу получает соответствующее уведомление в виде HTML-страницы или пустой файл.

Взаимодействие с компонентами Dr.Web Agent и Dr.Web Monitor

Dr.Web ICAPD имеет возможность взаимодействовать с компонентами **Dr.Web Agent** и **Dr.Web Monitor**.

Dr.Web ICAPD получает от **Dr.Web Agent** конфигурационную информацию и ключи. Таким образом, если **Dr.Web ICAPD** запущен под управлением **Dr.Web Agent**, то значение параметра **`Key`** из конфигурационного файла `drweb-icapd.ini` игнорируется и используется путь к ключу, указанный в конфигурационном файле **Dr.Web Agent** (по умолчанию это файл `%etc_dir/agent.conf`).

Dr.Web ICAPD имеет возможность отсылать **Dr.Web Agent** информацию о найденных вирусах (отправка статистики контролируется параметром **`SendStat`** конфигурационного файла `drweb-icapd.ini`).

Dr.Web Agent, в свою очередь, может отсылать полученную информацию на сайт **«Доктор Веб»**. Для этого в параметре **`UUID`** конфигурационного файла **Dr.Web Agent** следует указать md5-сумму ключевого файла.

Доступ к собранной статистике осуществляется по адресу http://stat.drweb.com/view/<md5sum>/, где `<md5sum>` – значение из параметра **`UUID`**.

Подключить **Dr.Web Agent** можно, указав путь к его сокету в параметре командной строки `-f` при запуске **`drweb-icapd`**.

Кроме того, с помощью **Dr.Web Agent** можно в автоматическом режиме отправлять адреса зараженных вирусами интернет-ресурсов на анализ в **«Доктор Веб»**, что позволит в дальнейшем улучшить качество работы антивируса.

Dr.Web Monitor позволяет автоматизировать запуск **Dr.Web ICAPD** и контролировать его работу. При запуске **Dr.Web ICAPD** с помощью **Dr.Web Monitor** он автоматически запускается с использованием **Dr.Web Agent**.

Для запуска **Dr.Web ICAPD** с помощью **Dr.Web Monitor** следует добавить значение `ICAPD` в параметр **`RunAppList`** конфигурационного файла **Dr.Web Monitor** (по умолчанию это файл `%etc_dir/monitor.conf`) либо указать значение `ICAPD` в параметре командной строки `-r` при запуске **Dr.Web Monitor**. Также необходимо удалить скрипт автоматического запуска **Dr.Web ICAPD** из системных путей, так как теперь **Dr.Web Monitor** будет отвечать за запуск и остановку компонента.

С дополнительной информацией о компонентах **Dr.Web Agent** и **Dr.Web Monitor** вы можете ознакомиться в разделах **Dr.Web Agent** и **Dr.Web Monitor** данного документа.

Запуск

Рекомендуемым порядком запуска взаимодействующих элементов является следующий:

1. **Dr.Web Daemon**;
2. **Dr.Web ICAPD**;
3. Используемый прокси-сервер.

Независимо от порядка запуска элементов не будет пропущен ни один непроверенный объект, так как либо прокси-сервер заблокирует передачу данных при отсутствии связи с **Dr.Web ICAPD**, либо сам **Dr.Web ICAPD** заблокирует получение информации при отсутствии связи с **Dr.Web Daemon** (при этом пользователю будет возвращаться страница с соответствующим уведомлением).

Проверка работоспособности Dr.Web ICAPD

Для проверки работоспособности **Dr.Web ICAPD** нужно выполнить следующие действия:

1. Убедиться, что параметры **Infected**, **Suspicious** и **Incurable** в файле `drweb-icapd.ini` установлены в значение `Report`;
2. Зайти на страницу http://eicar.org/download/eicar.com – в окне браузера должно появиться уведомление о зараженном файле.

Если уведомление не появилось, нужно проверить следующее:

- для доступа к http-трафику браузер использует прокси **Squid**, настроенный на взаимодействие с **Dr.Web ICAPD**;
- шаблоны уведомлений скопированы в подкаталог `/templates/icapd/` каталога `%etc_dir`, и пути к ним в файле `drweb-icapd.ini` заданы правильно.

Адреса сайтов проектов Squid и Shweby

Проект **Squid**:

http://squid-cache.org/

Поддержка протокола ICAP для **Squid**:

http://squid.sourceforge.net/projects.html#icap

Проект **SafeSquid**:

http://safesquid.com/

Шаблоны уведомлений

Dr.Web ICAPD использует два типа шаблонов уведомлений – HTML-шаблоны и mail-шаблоны.

1) **HTML-шаблоны** используются для формирования уведомлений, показываемых клиенту в браузере в ответ на попытку обращения к заблокированному ресурсу или загрузки вредоносного или подозрительного объекта, если в результате проверки полученных от удаленного сервера данных было применено "предотвращающее" действие `Move` или `Report`.
2) **mail-шаблоны** используются для формирования почтовых уведомлений, отправляемых администратору при возникновении инцидентов (в зависимости от разрешений на отправку уведомлений, заданных в настройках).

Все шаблоны представляют собой обычные текстовые файлы, расположенные в каталоге `%etc_dir/templates/icapd[_lng]`, где `_lng` – суффикс в имени каталога, указывающий, какой язык используется в шаблонах, находящихся в этом каталоге (например, `ru` для русского языка, `ja` для японского и т.д.). Подкаталог `/icapd` без добавленного суффикса хранит шаблоны уведомлений на английском языке и должен присутствовать всегда.

При необходимости можно изменить используемый каталог с шаблонами, указав путь к нему в параметре **`Templates`**. В каталоге шаблонов должны быть представлены следующие файлы шаблонов (имена файлов изменять нельзя):

Имя файла	Описание
`ERR_FAILED_CHECK`	HTML-шаблон с отчетом об ошибке сканирования файла
`ERR_DOWNLOAD_BLOCK`	HTML-шаблон с отчетом об ошибке доступа к заблокированной веб-странице (из черного списка)
`ERR_ACCESS_DENIED`	HTML-шаблон с отчетом об ошибке загрузки файла с запрещенным содержимым. Данный отчет генерируется в случае, когда соответствующим параметром задано действие **информировать** (`Report`)
`ERR_ACCESS_DENIED_MOVED`	HTML-шаблон с отчетом об ошибке загрузки файла с запрещенным содержимым. Данный отчет генерируется в случае, когда соответствующим параметром задано действие **переместить** (`Move`)
`email.templ`	mail-шаблон почтового сообщения, которое посылается администратору на почтовый адрес, указанный в праметре **`Hostmaster`**

1. HTML-шаблоны

Все HTML-шаблоны по внутренней структуре представляют собой корректный HTML-файл, который может включать в себя, в том числе, стилевые таблицы и даже JavaScript, но не должен включать в себя внедренные объекты и изображения, а также URL любых ресурсов, расположенных вне файла (например, нельзя подключать стилевую таблицу из CSS-файла).

В текст HTML-шаблона могут быть внедрены (в любое место внутри HTML-структуры) специальные маркеры-заместители, которые при генерации HTML-страницы на основе данного шаблона будут заменены на соответствующий текст. В HTML-шаблонах разрешается использование следующих маркеров:

Маркер	Описание
`$DAEMON_REPORT$`	Заменяется на строку отчета от **Dr.Web Daemon**, содержащую причину возникшего инцидента (например, был найден вирус или файл не мог быть проверен вследствие установленных ограничений и т.п.)
`$DATE$`	Заменяется на строку даты и времени генерации уведомления
`$FILE_NAME_ERROR$`	Заменяется на путь к файлу, помещенному в **Карантин**
`$HOSTMASTER$`	Заменяется на почтовый адрес администратора (значение параметра **`Hostmaster`** из настроек)
`$MANUAL_SUBMIT$`	Заменяется на форму, содержащую кнопку, нажатие которой приводит к отправке в **Доктор Веб** информации об инциденте. Текст на кнопке задается строкой, следующей непосредственно после маркера, например: `$MANUAL_SUBMIT$Отправить!`
`$RELEASE$`	Заменяется на информацию о текущем установленном релизе продукта (включает название и версию продукта, а также **Антивирусного ядра**).
`$URL$`	Заменяется на полный URL исходного запрошенного ресурса

Маркер	Описание
URL_SHORT	Заменяется на укороченный URL исходного запрошенного ресурса
$VERSION$	Заменяется на номер текущей версии Dr.Web ICAPD

Пример HTML-шаблона:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <title>Blocked by Dr.Web ICAPD</title>
 </head>
 <body>
  <H1>Content blocked!</H1>
  <p>Access to this resource is denied due to administration policy.<br/>
     Please save content of this page and ask your
     <a href="mailto:$HOSTMASTER$">system administrator</a>
     for further instructions.
  </p>
  <H2>Details:</H2>
  <p><strong>Restricted URL: </strong><a href="$URL$">$URL_SHORT$</a></p>
  <p><strong>Reason: </strong><pre>$DAEMON_REPORT$</pre></p>
  <H2>Product information:</H2>
  <p><strong>Release: </strong><pre>$RELEASE$</pre></p>
  <p><strong>Version: </strong><pre>Dr.Web ICAPD $VERSION$</pre></p>
  <p>$MANUAL_SUBMIT$Notify Dr.Web</p>
 </body>
</html>
```

2. mail-шаблоны

В текущей версии Dr.Web ICAPD использует только один mail-шаблон: шаблон **email.templ** письма администратору о произошедшем инциденте. По внутренней структуре этот шаблон представляет собой структуру корректного письма в формате MIME `multipart/mixed`.

В текст шаблона письма могут быть внедрены (в любое место внутри структуры письма, например, как значения заголовков и в текстовую часть) специальные маркеры-заместители, которые при генерации отправляемого письма на основе данного шаблона будут заменены на соответствующий текст. В mail-шаблонах разрешается использование следующих маркеров:

Маркер	Описание
$ACTION$	Заменяется на название действия, примененного к объекту
$HOSTMASTER$	Заменяется на почтовый адрес администратора (значение параметра **Hostmaster** из настроек)
$HTML_PAGE$	Заменяется на содержимое страницы уведомления, которая была показана пользователю
IP	Заменяется на IP-адрес пользователя, запросившего запрещенный объект
$REASON$	Заменяется на причину инцидента (например, был найден вирус или файл не мог быть проверен вследствие установленных ограничений и т.п.)
$SIZE$	Заменяется на размер запрещенного объекта
$TIME$	Заменяется на строку даты и времени генерации уведомления
URL	Заменяется на полный URL исходного запрошенного ресурса

Пример mail-шаблона:

```
From: "DrWeb-ICAP" <drweb-icapd>
To: "System Administrator" <$HOSTMASTER$>
Subject: $REASON$
Content-Type: multipart/mixed;
              boundary="001-DrWeb-Icapd-Notification"
MIME-Version: 1.0
Precedence: junk
X-Antivirus-Ticket: Dr.Web notification.

--001-DrWeb-Icapd-Notification
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 7bit

Url: $URL$
Reason: $REASON$
Action: $ACTION$
Time: $TIME$
Client-IP: $IP$
Object size: $SIZE$

--001-DrWeb-Icapd-Notification
Content-Type: text/html; charset=iso-8859-1
Content-Transfer-Encoding: 7bit

$HTML_PAGE$
--001-DrWeb-Icapd-Notification--
```

Настоятельно не рекомендуется изменять структуру mail-шаблона без крайней необходимости, чтобы не нарушить внутреннюю структуру MIME-частей и заголовков письма.

Имеется возможность изменить содержимое шаблонов прямо на специальной странице веб-интерфейса **Dr.Web консоль для интернет-шлюзов UNIX**.

Dr.Web консоль для интернет-шлюзов UNIX

Настройка программного комплекса **Dr.Web для интернет-шлюзов UNIX** может быть осуществлена через веб-интерфейс **Dr.Web консоль для интернет-шлюзов 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 интернет-шлюзов 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;
- **CGI::Carp** — модуль для работы с журналом ошибок;
- **Cwd** — модуль для определения текущем рабочем каталоге 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()`;
- **Encode** и **Encode::Detect** — модули для преобразования кодировки ;
- **perl-devel** (или **libperl-dev**, в зависимости от дистрибутива);
- **File::Basename** — модуль для преобразования имен файлов;
- **File::Stat** — объектно-ориентированный интерфейс для вызова функции `stat()`;
- **POSIX** — интерфейс для функций, определенных стандартом POSIX;
- **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 интернет-шлюзов UNIX** необходимо:

- установить **Webmin**;
- подключить модуль **Dr.Web консоль для интернет-шлюзов UNIX** к **Webmin** (расположен в каталоге `%bin_dir/web/`).

Подключение модулей, а также настройка дополнительных параметров самого **Webmin**

осуществляется через его веб-интерфейс.

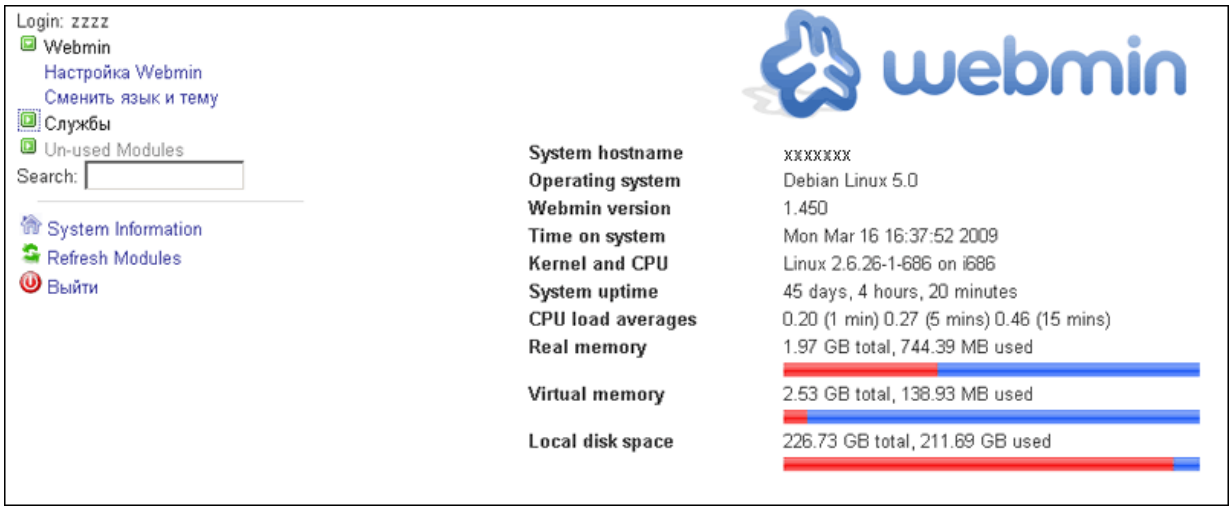


Рис. 18. Главная страница Webmin

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

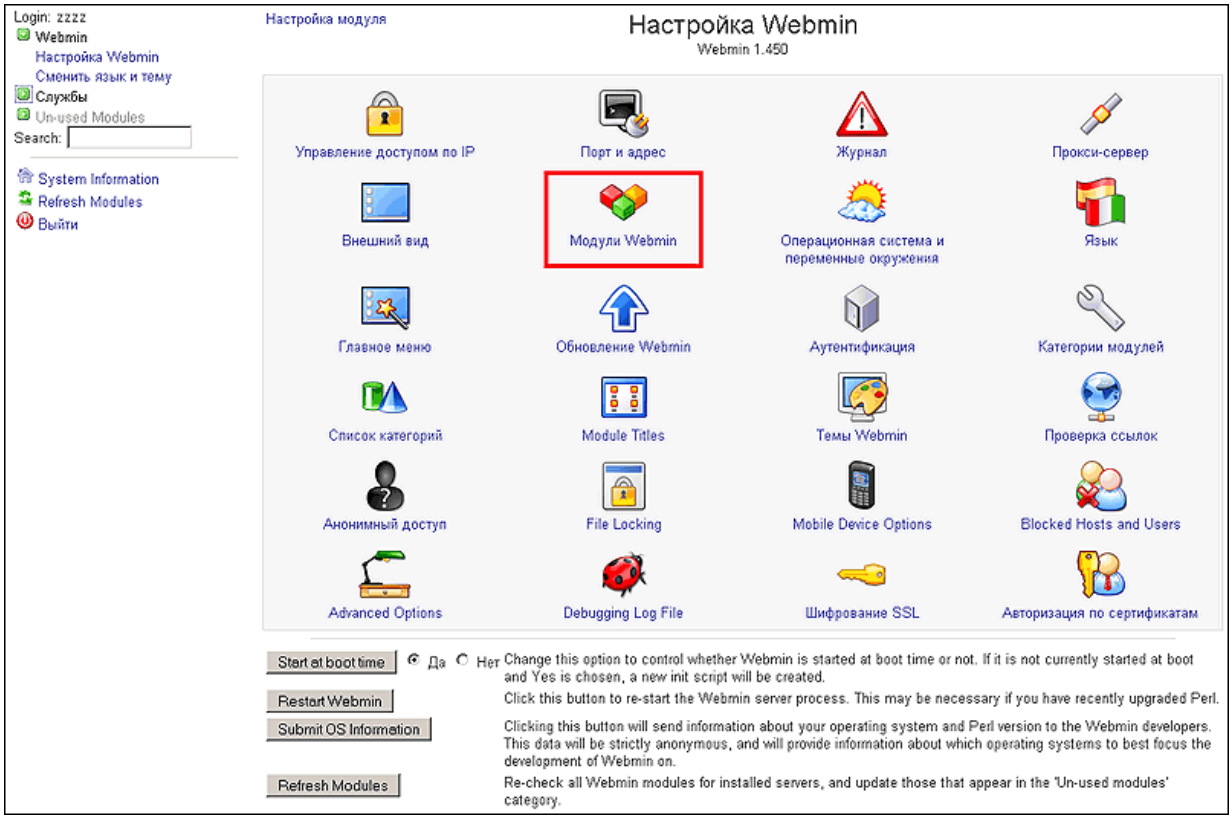


Рис. 19. Настройка Webmin

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 каталогов вашей системы, в котором вы сможете выбрать соответствующий установочный пакет (`%bin_dir/web/drweb-icapd-web.wbm.gz` по умолчанию).

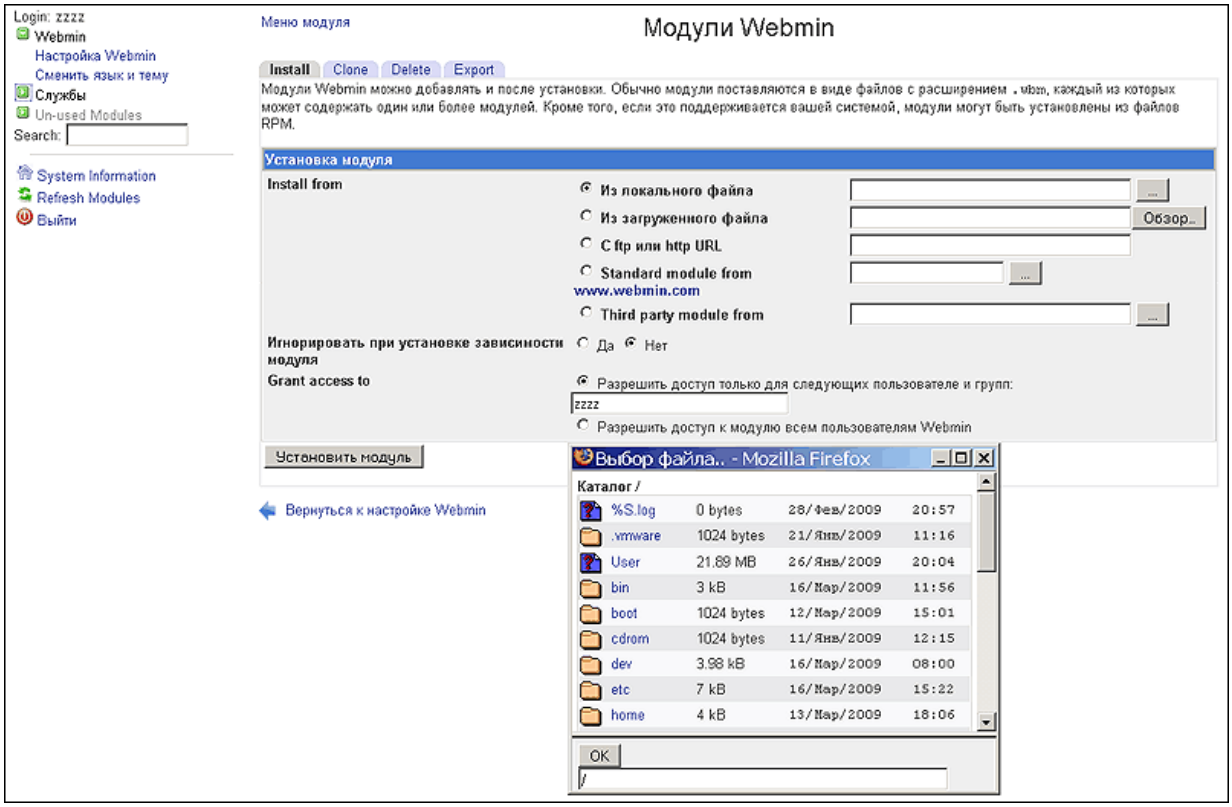


Рис. 20. Добавление модулей Webmin

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 каталога он 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 интернет-шлюзов Unix**.

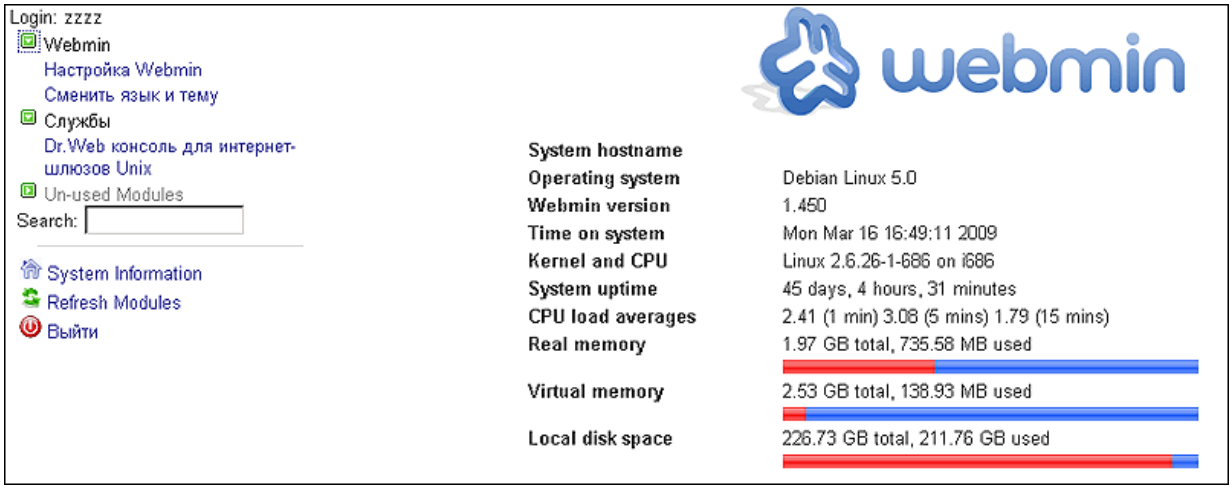


Рис. 21. Новый пункт меню "Dr.Web консоль для интернет-шлюзов Unix"

Кроме того, для **Webmin** версии 1.680 или старше, требуется также добавить в файл конфигурации **Webmin** (как правило, это файл `/etc/webmin/config`) следующую строчку:

```
no_content_security_policy=1
```

Настройка

Базовые настройки модуля **Dr.Web консоль для интернет-шлюзов UNIX** можно открыть, нажав нажав в верхнем меню навигации веб-интерфейса. На открывшейся странице вы сможете указать путь к конфигурационному файлу `drweb-icapd.ini`, пути к init-скрипту и каталогу для черных и белых списков, количество файлов, отображаемых на странице карантина, а также режим работы **Консоли**.

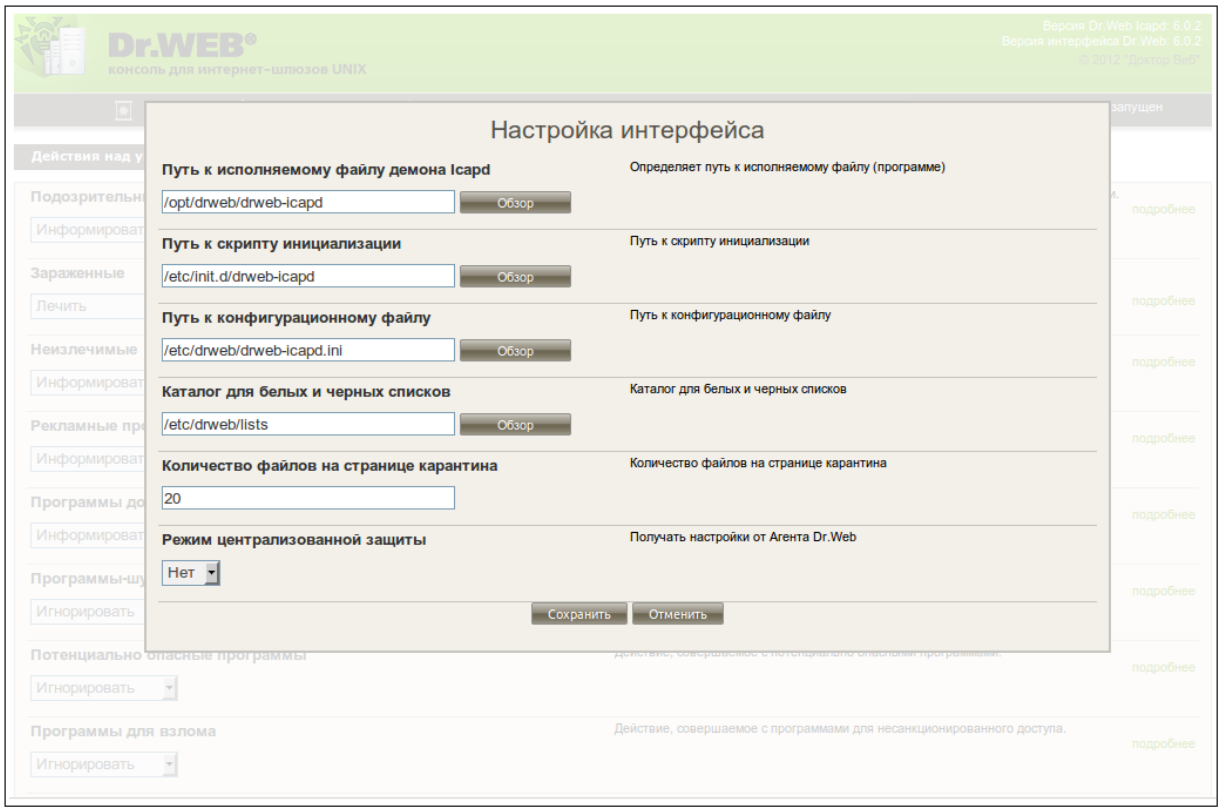


Рис. 22. Настройка модуля

Пользовательский интерфейс

Пожалуйста, обратите внимание на то, что при навигации внутри раздела **Dr.Web консоль для интернет-шлюзов 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.

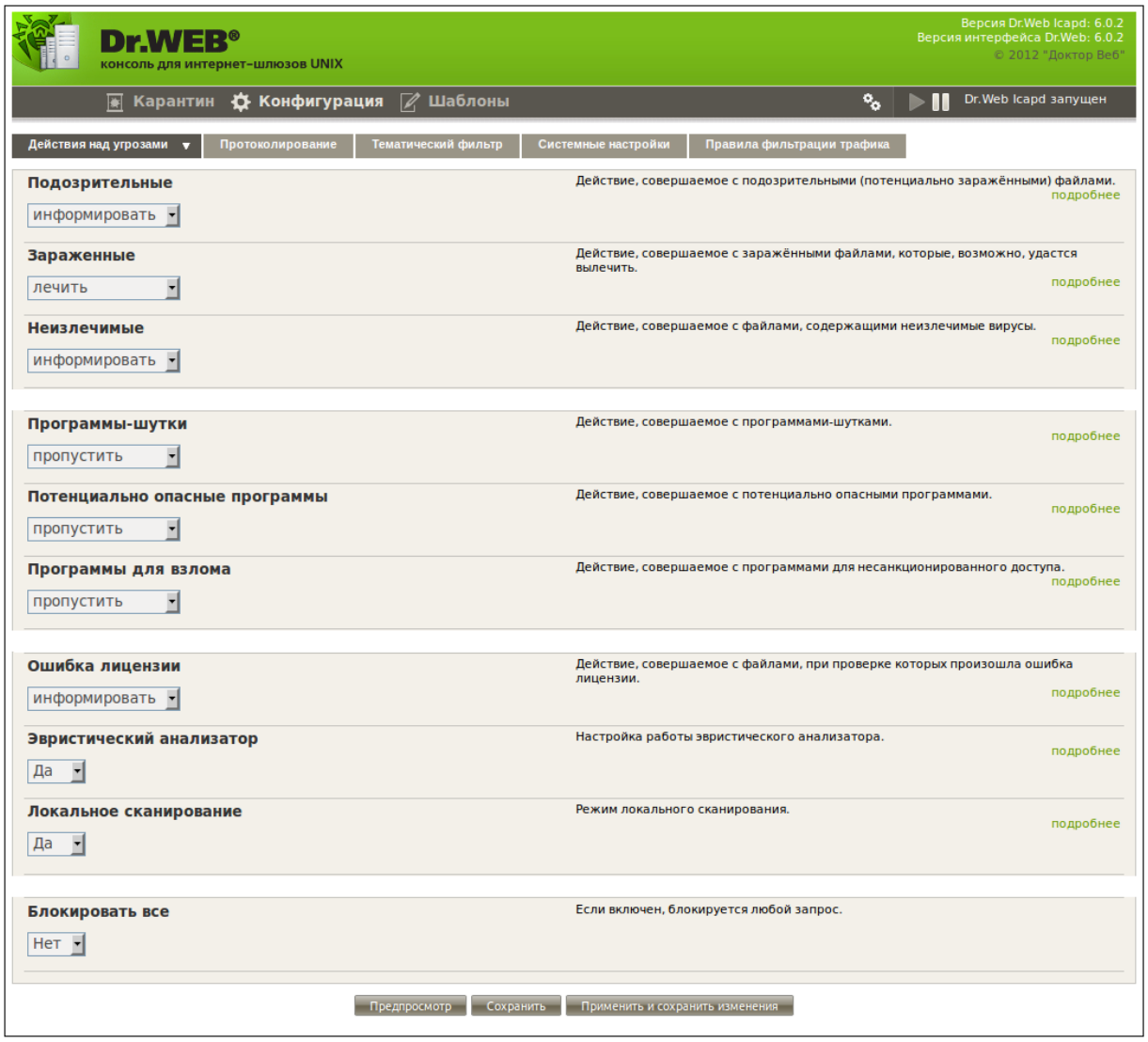


Рис. 23. Dr.Web консоль для интернет-шлюзов UNIX

Справа от заголовка модуля вы найдете информацию о текущей версии **Dr.Web ICAPD** и веб-интерфейса **Dr.Web для интернет-шлюзов UNIX**.

Под заголовком модуля расположены три секции: **Карантин**, **Конфигурация** и **Шаблоны**. По умолчанию при входе в раздел открывается вкладка **Действия над угрозами** секции **Конфигурация**.

Рядом с заголовками секций расположены три кнопки: **Настройка интерфейса**, **Запустить Dr.Web Icapd** и **Остановить Dr.Web Icapd**, а также отображается текущее состояние **Dr.Web ICAPD**.

Конфигурация

На вкладке **Конфигурация** представлены следующие разделы по управлению работой **Dr.Web для интернет-шлюзов UNIX**:

- Действия над угрозами — настройка действий для различных типов обнаруженных угроз, например для неизлечимых или подозрительных файлов;
- Протоколирование — настройка ведения отчета о работе **Dr.Web для интернет-шлюзов UNIX**;

- Тематический фильтр — настройка блокировки веб-страниц по тематике их содержимого (например, сайтов для взрослых или иного нежелательного содержания);
- Системные настройки — настройка пользовательских белых и черных списков интернет-ресурсов, путей к ключевому файлу и каталогу **Карантина**, отправления уведомлений администратору;
- Правила фильтрации трафика — правила обработки файлов в зависимости от их типа и размера.

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

При задании параметров в соответствующих секциях вы можете выбирать нужные значения из раскрывающихся списков, либо нажимать кнопку для добавления значений параметров, либо задавать эти значения вручную в соответствующих полях ввода. После изменения значения какого-либо параметра вы можете щелчком мыши по соответствующей иконке рядом с параметром отменить изменение или восстановить настройки по умолчанию .

Для того чтобы просмотреть все сделанные изменения нажмите кнопку **Предварительный Просмотр**.

На появившейся странице вы можете выбрать те изменения, которые желаете сохранить, установив соответствующие флажки. Если вы хотите внести дополнительные изменения, вы можете вернуться к предыдущей странице, нажав на кнопку **Продолжить Редактирование**. Если вы хотите отменить изменения, то нажмите кнопку **Отменить изменения**. Если сделанные изменения вас устраивают, нажмите на кнопку **Сохранить** или **Применить и сохранить изменения**.

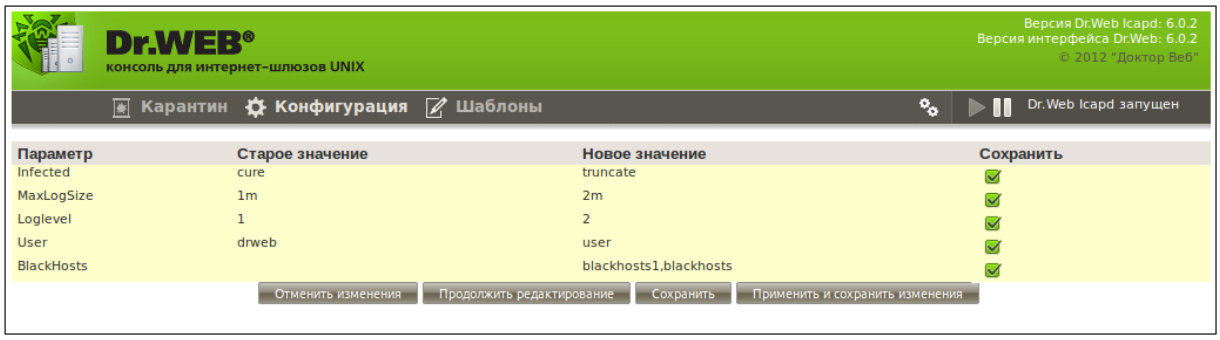


Рис. 24. Страница предпросмотра

Когда вы нажимаете на кнопку **Сохранить** или **Сохранить и применить**, появляется уведомление о том, что конфигурация сохранена. Щелкните по нему мышкой, чтобы вернуться к странице настроек.

Действия над угрозами

В этом разделе вы можете настроить действия при обнаружении различных типов угроз или при возникновении ошибок.

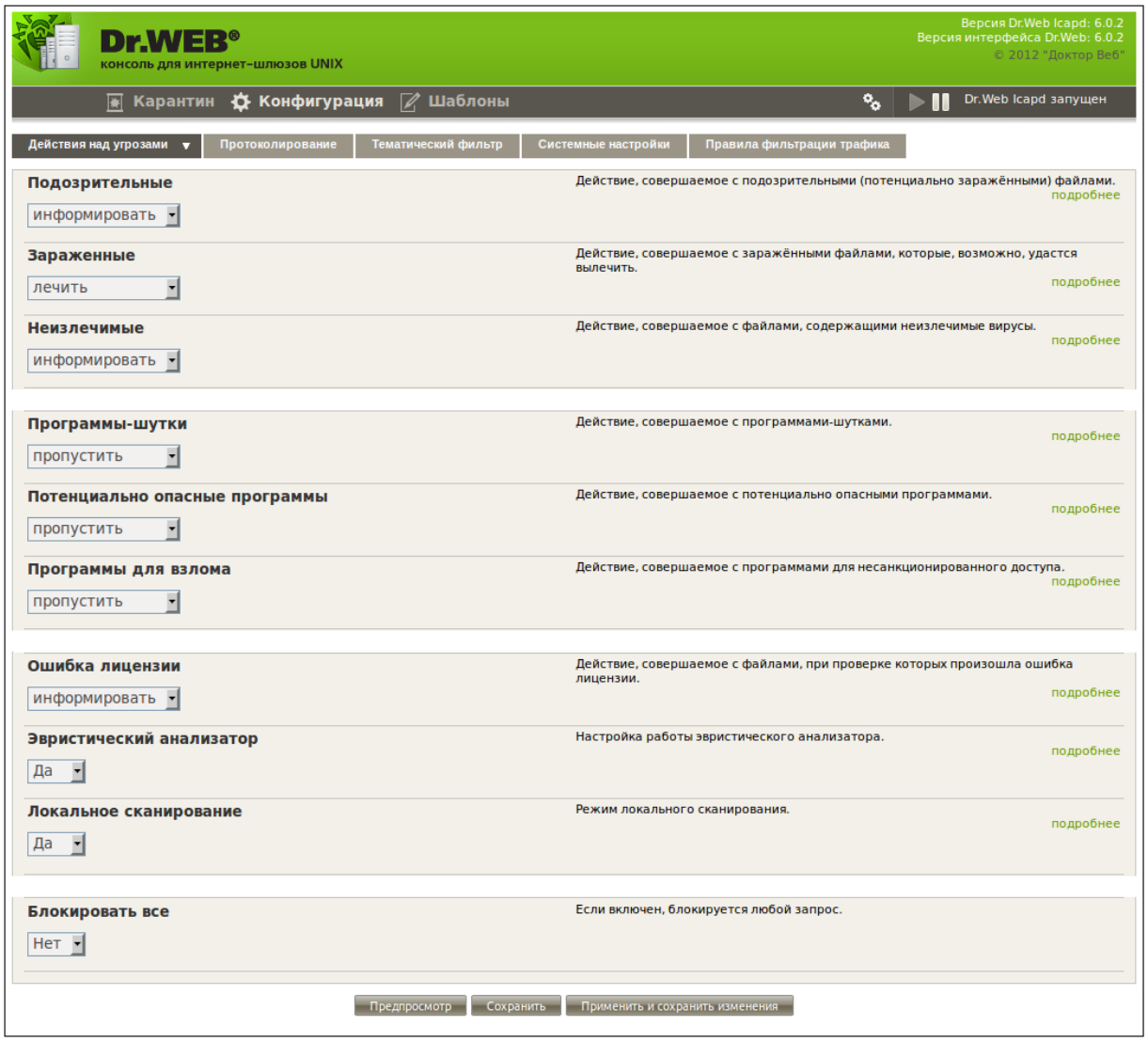


Рис. 25. Действия над угрозами

У каждого параметра на этой вкладке имеется раскрывающееся меню со списком возможных значений. Подробное описание каждого параметра вы найдете в интерактивной справке по ссылке **подробнее**.

Протоколирование

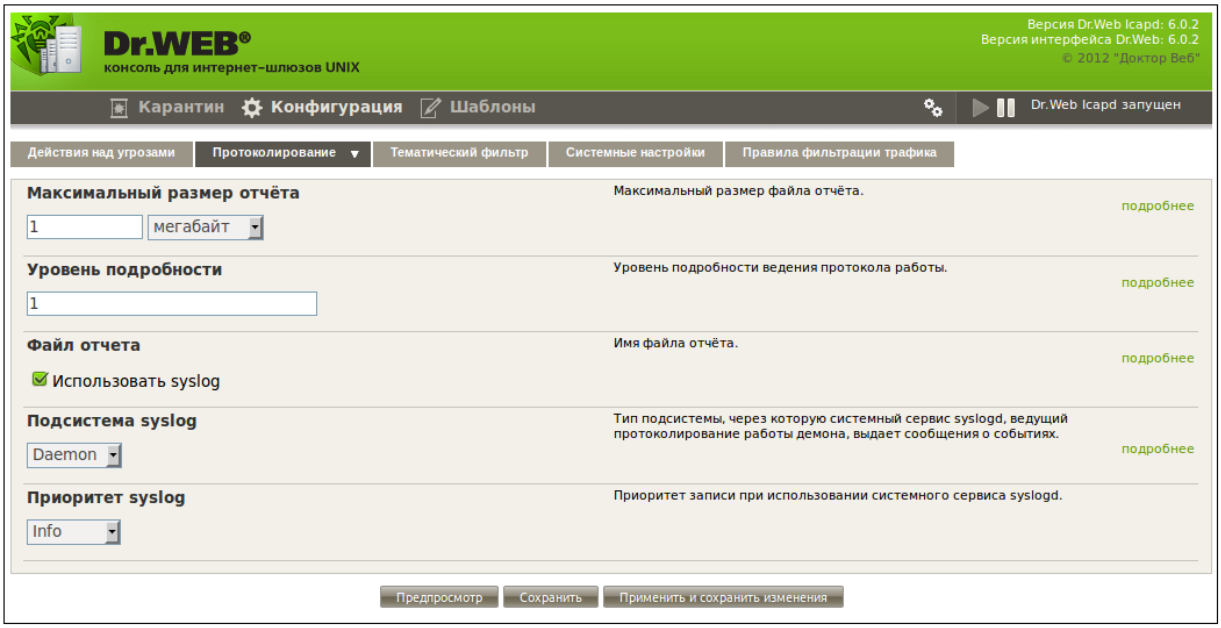


Рис. 26. Протоколирование

Значения параметров на этой вкладке могут быть выбраны из раскрывающихся списков или заданы вручную в соответствующих полях ввода.

Если вы хотите самостоятельно выбрать файл для хранения отчетов о работе системы, уберите галочку из ячейки **Использовать syslog** и нажмите кнопку **Обзор**. Откроется отдельное окно браузера для навигации по списку файлов и каталогов вашей системы, в котором следует выбрать имя файла, в который будет сохраняться протокол работы.

Тематический фильтр

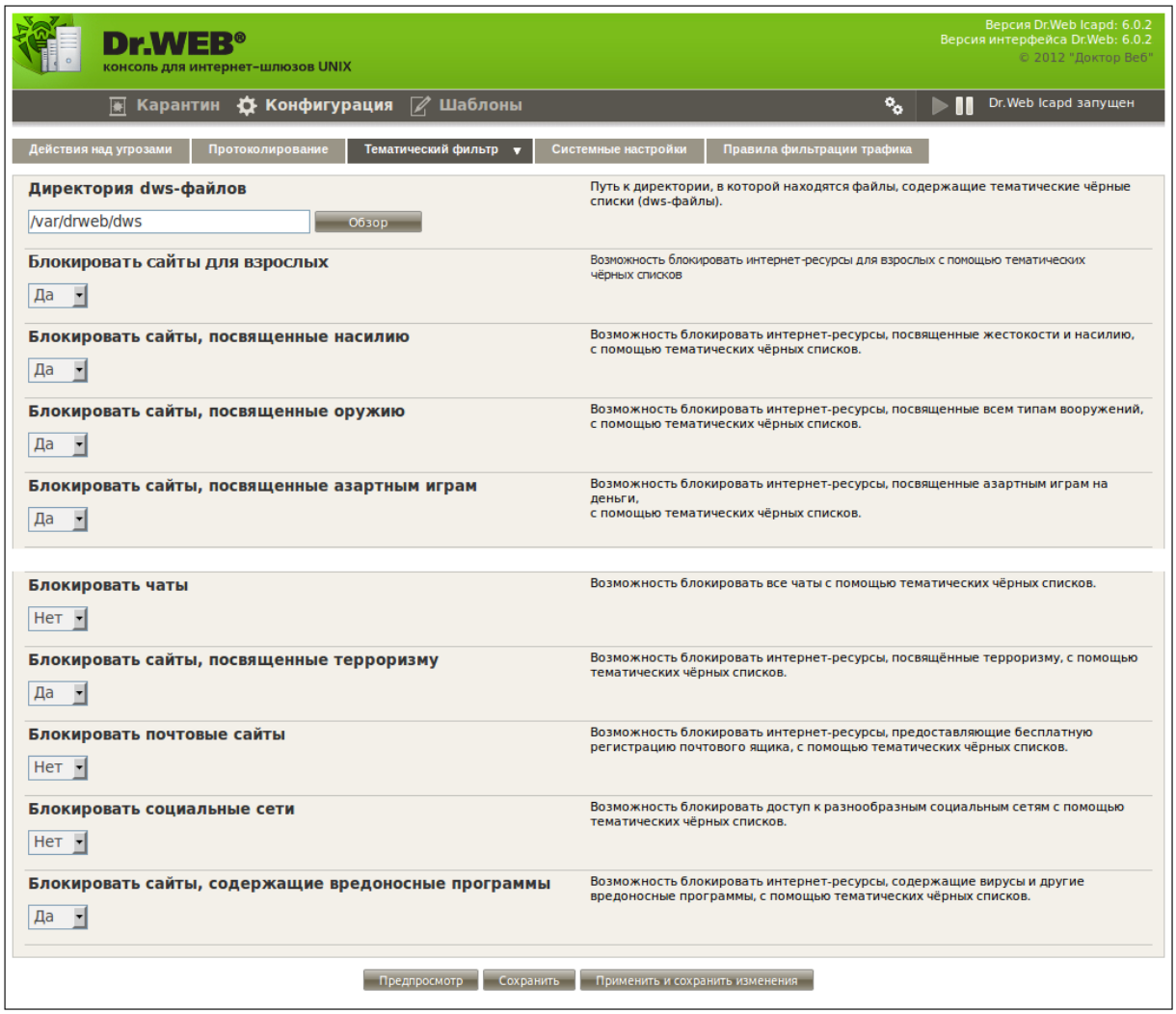


Рис. 27. Тематический фильтр

На данной вкладке вы можете настроить блокировку веб-страниц по типу их содержимого: например, заблокировать сайты "для взрослых" или сайты с информацией про наркотики. Значения параметров на этой вкладке могут быть выбраны из раскрывающихся списков. Доступные значения: **Да** и **Нет**.

Задать путь к каталогу, в котором хранятся обновляемые тематические черные списки, можно либо вручную, указав нужный путь в соответствующем поле ввода для параметра **Каталог dws-файлов,** либо нажав кнопку **Обзор** и выбрав нужный каталог в открывшемся навигационном окне.

Системные настройки

В этом разделе вы можете настроить пользовательские белые и черные списки интернет-ресурсов, пути к ключевому файлу и каталогу **Карантина**, указать почтовый адрес администратора, настроить отправку уведомлений о попытках открытия заблокированных веб-страниц.

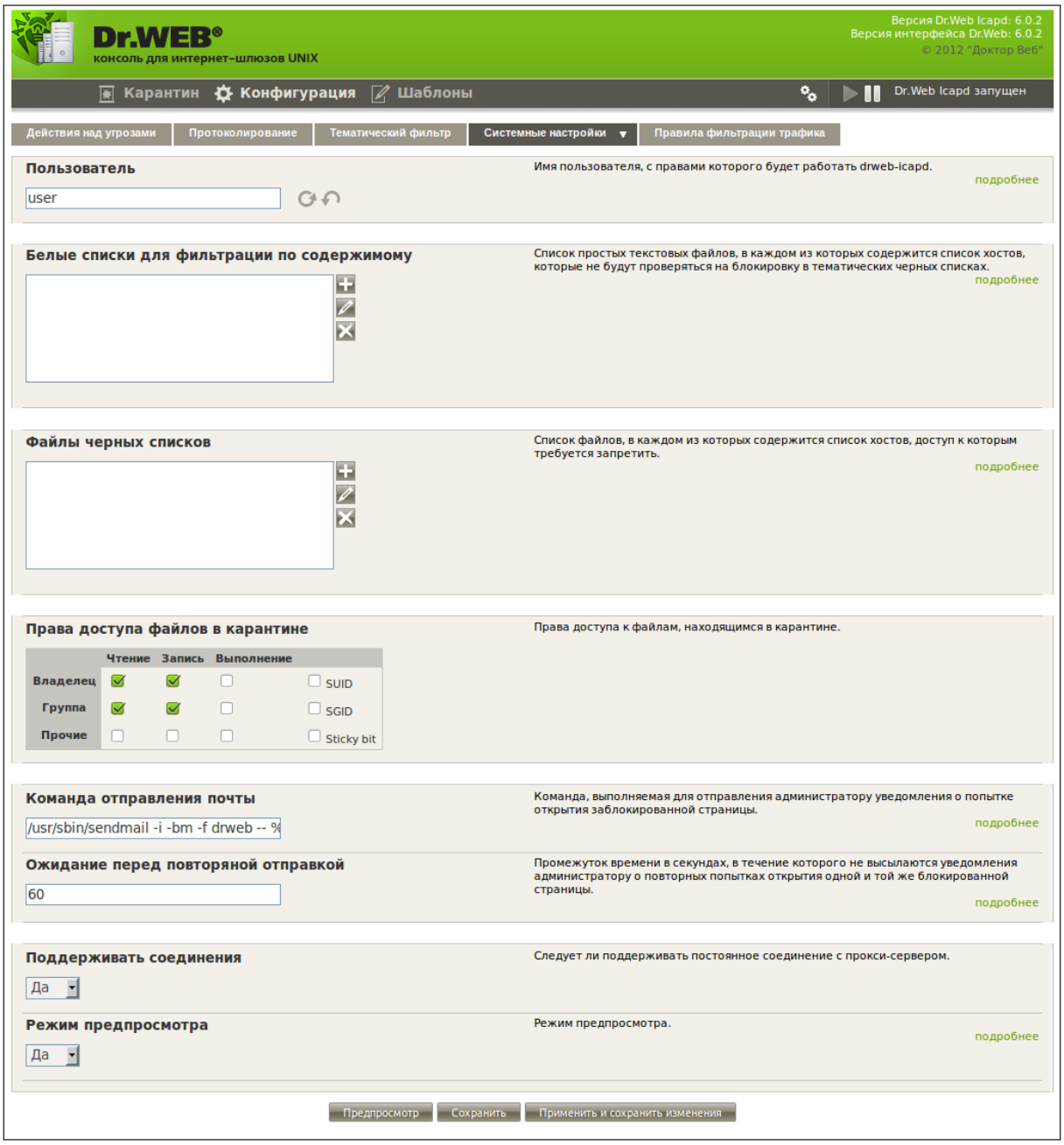


Рис. 28. Системные настройки

В секции **Файлы черных списков** могут создаваться пользовательские черные списки. Для того, чтобы создать такой список, нажмите кнопку , введите новое имя списка (без пробелов) и поочередно имена хостов, которые вы желаете заблокировать.

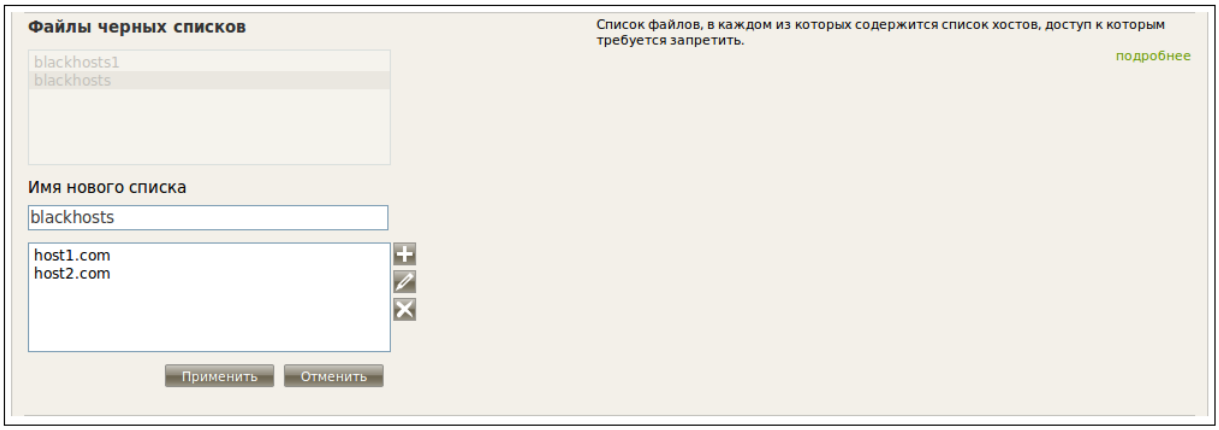


Рис. 29. Создание пользовательского списка

Порядок создания и задания пользовательских белых списков в секциях **Файлы белых списков** и **Белые списки для фильтрации по содержимому** аналогичен вышеописанному.

Обратите внимание, что:

- Хосты, перечисленные в файлах из списка **Файлы белых списков**, не будут проверяться на наличие вирусов.
- Хосты, перечисленные в файлах **Белые списки для фильтрации по содержимому**, не будут проверяться на блокировку в тематических черных списках.

Правила фильтрации трафика

На данной вкладке вы можете вы можете настроить и создать правила обработки файлов в зависимости от их MIME-типа - идентификатора типа файла, используемого в Интернет.

Идентификатор MIME состоит из двух частей: основной и дополнительной. Например, `application/octet-stream` соответствует исполняемым файлам с расширениями `.com` и `.exe`; `image/any` соответствует любым файлам с изображениями; `audio/mpeg` соответствует аудиофайлам в форматах `mp1`, `mp2` и `mp3`.

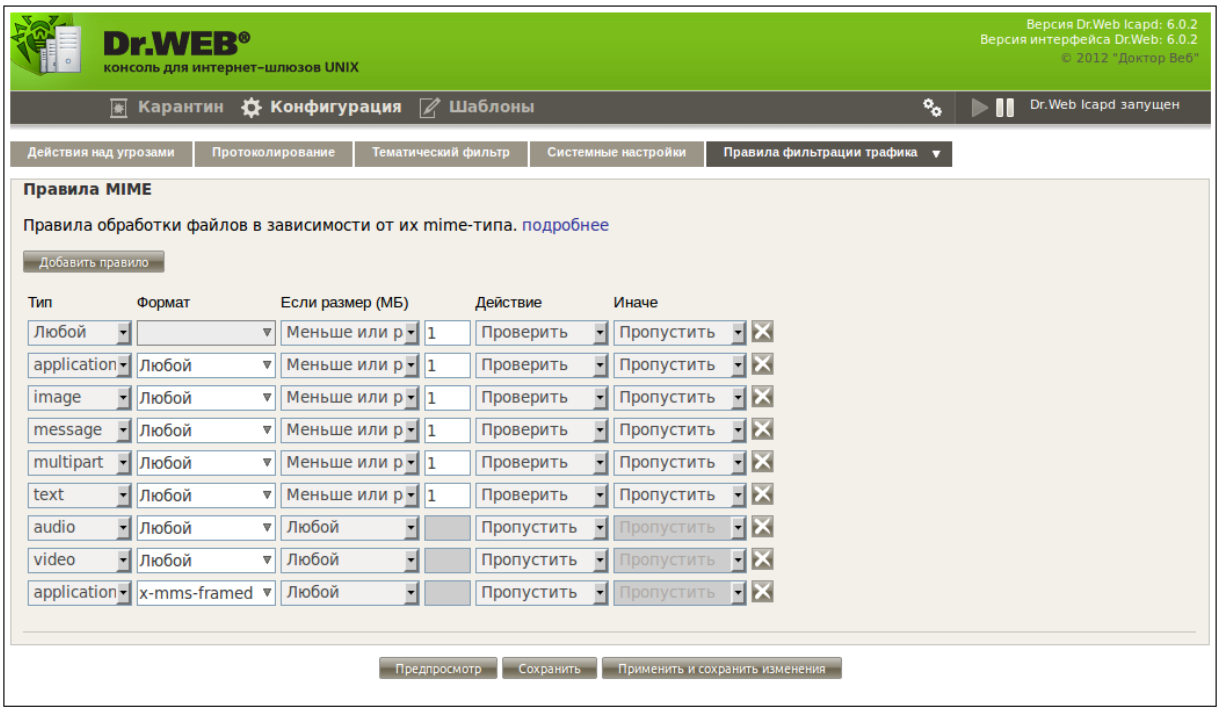


Рис. 30. Правила обработки скачиваемых файлов

Нажмите **Добавить правило**, чтобы добавить новое правило. Чтобы удалить правило нажмите кнопку рядом с правилом, которое необходимо удалить.

Каждое правило состоит из следующих полей:

- **Тип** - основной MIME-тип файла.
  - **Любой** - файл любого типа;
  - **application** - исполняемые и архивированные файлы, документы в формате PDF, MS Word и др.;
  - **audio** - аудиофайлы (mp3, wav, wma и др.);
  - **image** - изображения (gif, jpg, png, svg и др.);
  - **message** - сообщения между веб-серверами и клиентами;
  - **multipart** - контейнеры (почтовые файлы, запакованные файлы);
  - **text** - текст или исходный код (html, xml, css и др.);
  - **video** - видеофайлы (mpeg-1, mp4, wma);
  - **model** - файлы трехмерных моделей.
- **Формат** - дополнительный MIME-тип файла. Может быть выбран из списка или введен вручную.
- **Если размер** - укажите, требуется ли фильтровать файлы по размеру и, если требуется, введите размер в мегабайтах в соответствующем поле.
- **Действие** - укажите действия для файлов указанного размера.
- **Иначе** - укажите действия для всех остальных файлов данного типа.

Для правил фильтрации трафика используется следующий синтаксис:

```
<MIME-тип> <действие1> <размер> <действие2>
```

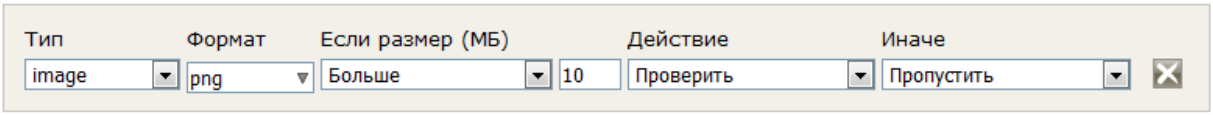
К файлу, имеющему тип `<MIME-тип>`, применяется `<действие1>`, если его размер в мегабайтах не превышает значения параметра `<размер>`. В противном случае к данному файлу

применяется `<действие2>`.

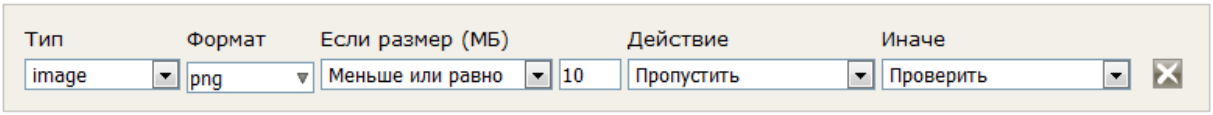
В таком виде правила фильтрации трафика записываются в конфигурационный файл и отображаются в веб-интерфейсе **Консоли**. Если при записи правила поле **Если размер** установлено в положение **Больше,** правило будет приведено к описанной выше форме.

Пример:

Задано правило, согласно которому изображения формата png размером больше 10 мегабайт проверяются на вирусы. Если размер изображения меньше или равно 10 мегабайт, оно пропускается.



После сохранения правило приводится к описанной выше форме и отображается следующим образом:



Таким образом, несмотря на другую форму записи, данное правило ведет себя аналогично первоначальной записи.

Карантин

На вкладке **Карантин** представлен список ссылок на заблокированные файлы. Подозрительные файлы помещаются в **Карантин** целиком, а их имена создаются по специальным правилам из адресов тех веб-страниц, с которой файл был загружен.

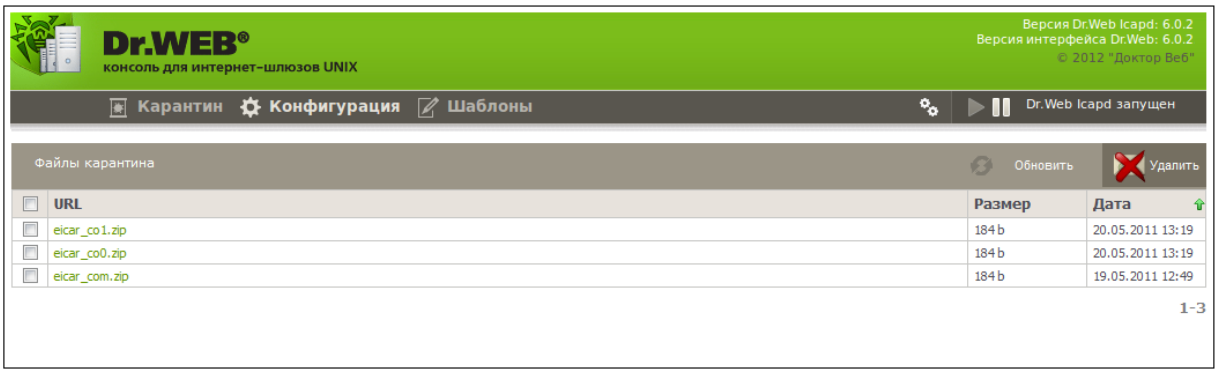


Рис. 31. Карантин

Чтобы удалить файл из **Карантина**, нужно выделить его и нажать кнопку **Удалить**.

Шаблоны

В этой секции содержатся шаблоны веб-страниц, которые генерируются и показываются конечному пользователю в ответ на попытку доступа к заблокированному содержимому (когда для соответствующих параметров в секции конфигурации заданы действия **информировать** или **переместить**), а также шаблон письма, отправляемого администратору при возникновении инцидентов.

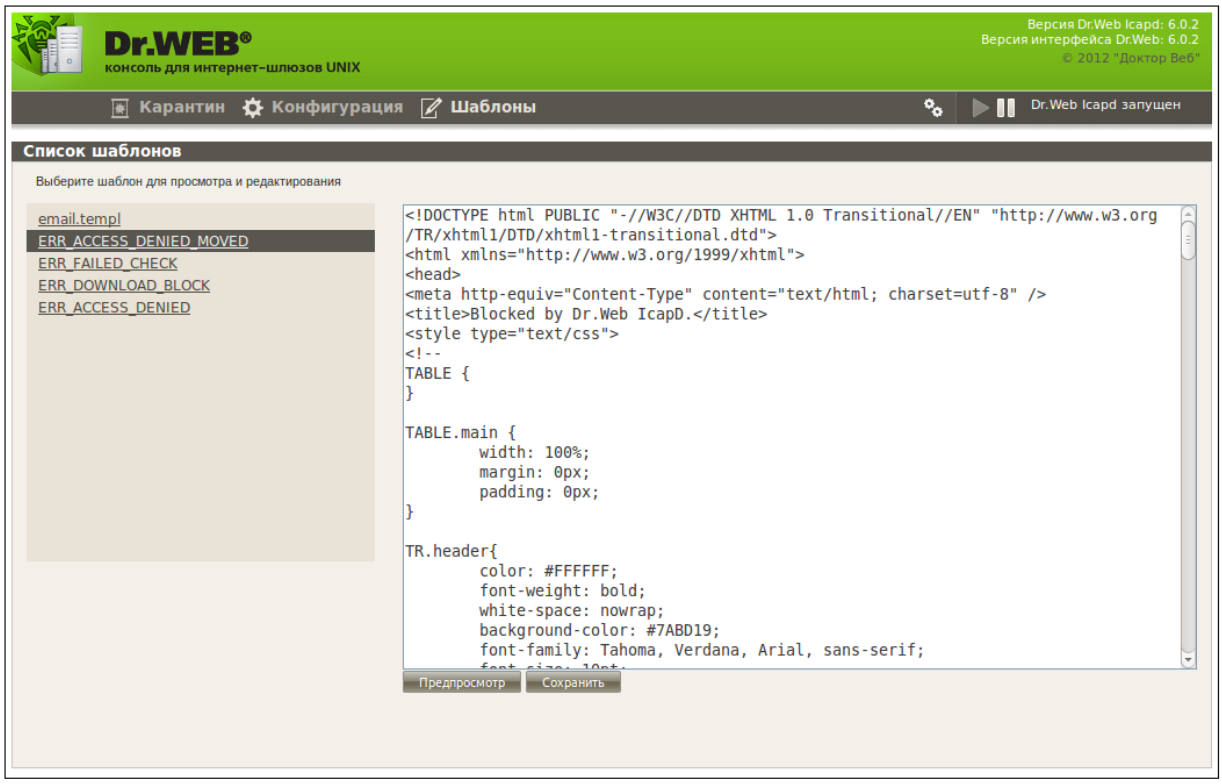


Рис. 32. Шаблоны

Название шаблона	Описание
ERR_FAILED_CHECK	Шаблон с отчетом об ошибке сканирования файла
ERR_DOWNLOAD_BLOCK	Шаблон с отчетом об ошибке доступа к заблокированной веб-странице (из черного списка)
ERR_ACCESS_DENIED	Шаблон с отчетом об ошибке загрузки файла с запрещенным содержимым. Данный отчет генерируется в случае, когда соответствующим параметром задано действие **информировать**
ERR_ACCESS_DENIED_MOVED	Шаблон с отчетом об ошибке загрузки файла с запрещенным содержимым. Данный отчет генерируется в случае, когда соответствующим параметром задано действие **переместить**
email.templ	Шаблон почтового сообщения, которое посылается системному администратору при попытке доступа к заблокированному содержимому

При необходимости Вы можете изменить структуру и содержимое шаблонов. Подробнее о шаблонах см. в разделе Шаблоны уведомлений.

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.

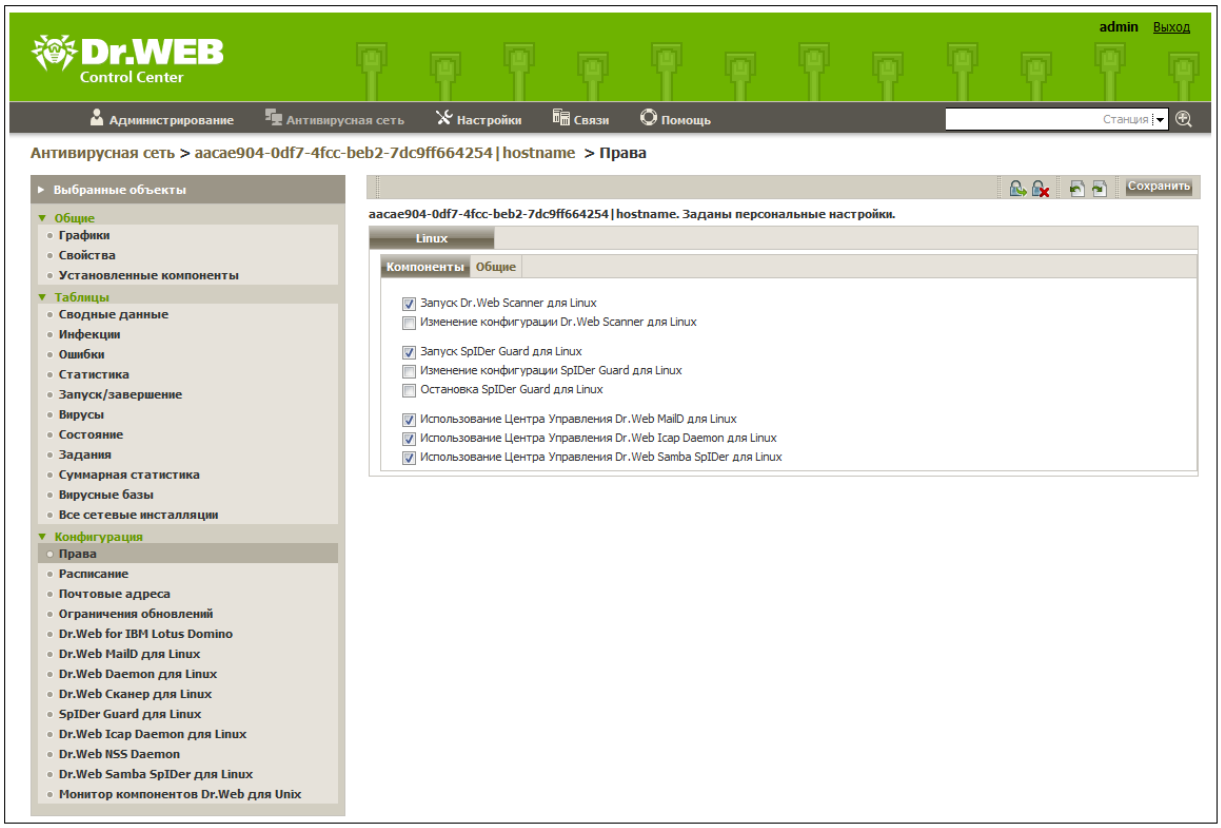


Рис. 33. Окно настройки прав пользователя рабочей станции

- В пункте **Компоненты** выберите компоненты, которые будут доступны для изменения пользователю рабочей станции. Например, чтобы разрешить изменение конфигурации **Dr.Web для интернет-шлюзов UNIX** пользователем рабочей станции, установите флажок **Использование Центра Управления Dr.Web Icap Daemon для Linux** и нажмите **Сохранить.**
- Чтобы отключить возможность изменения конфигурации **Dr.Web для интернет-шлюзов UNIX** пользователем рабочей станции, снимите флажок **Использование Центра Управления Dr.Web Icap Daemon для Linux** и нажмите кнопку **Сохранить.** При этом в окне **Консоли** пользователя рабочей станции будет выведено соответствующее предупреждение, а кнопки **Применить и сохранить изменения, Предпросмотр** и **Сохранить** блокируются.

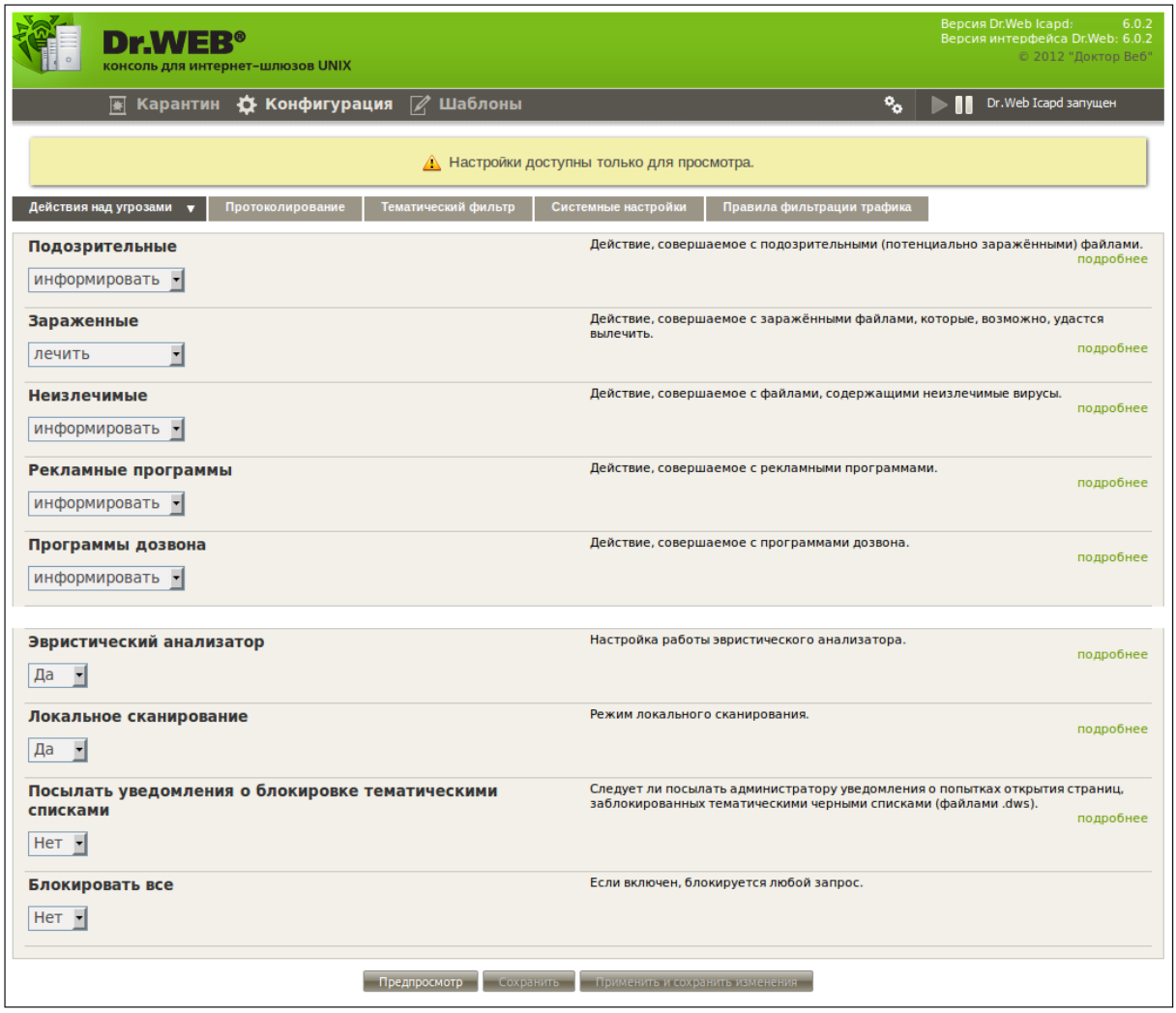


Рис. 34. Запрет на изменение конфигурации пользователем рабочей станции

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** выберите 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.

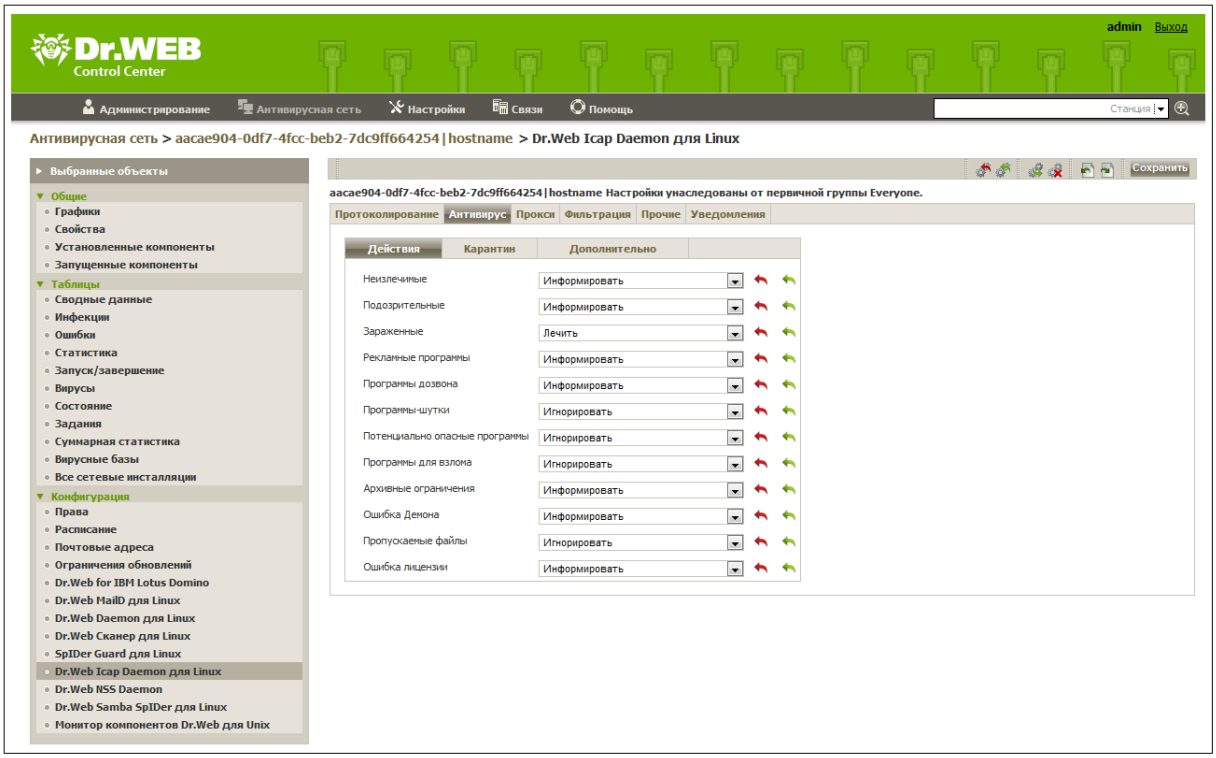


Рис. 35. Настройка Dr.Web Icap Daemon для Linux через интерфейс Центра Управления Dr.Web

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 интернет-шлюзов 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 интернет-шлюзов UNIX**;
- конфигурационные файлы компонентов;
- файлы журнала компонентов и отчеты и статистику, если имеются.

Приложение. Пользовательские лицензии

Программный комплекс **Антивирус Dr.Web® для интернет-шлюзов 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 интернет-шлюзов

Данная лицензия для компонентов **Dr.Web Daemon** и **Dr.Web ICAPD** позволяет использовать **Dr.Web Daemon** для проверки входящего HTTP-трафика, проходящего через прокси-сервер, поддерживающий протокол ICAP (**Squid** и **SafeSquid**). Возможна также проверка входящего FTP-трафика для прокси-сервера на базе **Squid**.

Программный комплекс лицензируется по количеству пользователей, которые будут работать через интернет-шлюз. Минимальная лицензия – на 25 пользователей.

Компоненты продолжают работать еще 24 часа после завершения лицензии.

Страница продукта находится по адресу: http://products.drweb.com/gateway/unix/?lng=ru