Dr.WEB®

Enterprise Security Suite

Защити созданное

Руководство администратора

© «Доктор Веб», 2004-2013. Все права защищены.

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

ТОВАРНЫЕ ЗНАКИ
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk и логотип Dr.WEB являются зарегистрированными товарными знаками «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

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

Dr.Web Enterprise Security Suite
Версия 6.0.4
Руководство администратора
05.07.2013

«Доктор Веб», Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

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

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Глава 1. Введение

1.1. Вступление

В настоящем Руководстве содержатся сведения, описывающие как общие принципы, так и детали реализации комплексной антивирусной защиты компьютеров компании с помощью **Dr.Web® Enterprise Security Suite** (далее кратко именуемого **Dr.Web ESS**). В Руководстве не описываются антивирусные пакеты **Dr.Web** для защищаемых компьютеров. За соответствующими сведениями обращайтесь к руководству **Антивирус Dr.Web® для Windows. Руководство пользователя.**

Данное Руководство адресовано *администратору антивирусной сети* — сотруднику организации, которому поручено руководство антивирусной защитой компьютеров (рабочих станций и серверов) этой сети.

Администратор антивирусной сети должен иметь полномочия системного администратора или сотрудничать с администратором локальной сети, быть компетентным в вопросах стратегии антивирусной защиты и детально знать антивирусные пакеты **Dr.Web** для всех используемых в сети ОС.

Ряд начальных глав Руководства будет полезен руководителю организации, принимающему решение о приобретении и установке системы комплексной антивирусной защиты.

Последняя часть документа (Приложения) содержит техническую информацию, описывающую параметры, необходимые для настройки компонентов Антивируса, а также синтаксис и значения инструкций, используемых при работе с ними.

Перед прочтением документа убедитесь, что это последняя версия **Руководства Администратора**. Руководство постоянно обновляется, и последнюю его версию можно найти на официальном веб-сайте компании **«Доктор Веб»** http://download.drweb.com/esuite/.

1.2. Условные обозначения и сокращения

Условные обозначения

В данном Руководстве используются обозначения, приведенные в таблице 1-1.

Таблица 1-1. Условные обозначения

Обозначение	Комментарий
 Заметьте, что	Важное замечание или указание.
 Внимание	Предупреждение о возможных ошибочных ситуациях, а так же важных моментах, на которые следует особо обратить внимание.
Dr.Web ESS	Названия подуктов и компонентов **Dr.Web**.
Антивирусная сеть	Термин в позиции определения или ссылки на определение.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Отмена	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

- ACL – списки контроля доступа (Access Control List),
- DFS – распределенная файловая система (Distributed File System),
- **Dr.Web ESS** – **Dr.Web Enterprise Security Suite**,
- GUI – графический пользовательский интерфейс (Graphical User Interface), GUI-версия программы — версия, использующая средства GUI,
- NAP – Network Access Protection,
- UDS – UNIX Domain Socket (доменный сокет UNIX),
- БД, СУБД – база данных, система управления базами данных,
- **ВСО Dr.Web** – **Всемирная система обновлений Dr.Web**,
- ЛВС – локальная вычислительная сеть,
- ОС – операционная система,
- ПО – программное обеспечение,
- РБНФ – расширенная форма Бэкуса-Наура.

1.3. Состав, назначение и основные функции Антивируса Dr.Web Enterprise Security Suite

Антивирус **Dr.Web Enterprise Security Suite** предназначен для организации и управления единой и надежной комплексной антивирусной защитой компьютеров вашей организации. При этом необязательно, чтобы компьютеры были объединены в локальную сеть, достаточно доступа в Интернет.

Dr.Web Enterprise Security Suite решает следующие задачи:

- централизованная (без необходимости непосредственного доступа персонала) установка антивирусных пакетов на защищаемые компьютеры,
- централизованная настройка параметров антивирусных пакетов,
- централизованное обновление вирусных баз и программного обеспечения на защищаемых компьютерах,
- мониторинг вирусных событий, а также состояния антивирусных пакетов и ОС на всех защищаемых компьютерах.

Dr.Web ESS позволяет как сохранить за пользователем защищаемых компьютеров права на настройку и управление антивирусными пакетами данных компьютеров, так и гибко ограничить их, вплоть до полного запрета.

Антивирусная сеть **Dr.Web ESS** имеет архитектуру *клиент-сервер*. Ее компоненты устанавливаются на компьютеры пользователей, администраторов и на компьютер(ы), выполняющий(ие) функции **Enterprise Сервера**, и обмениваются информацией, используя сетевые протоколы TCP/IP, IPX/SPX, NetBIOS. Совокупность компьютеров, на которых установлены взаимодействующие компоненты **Dr.Web ESS**, будем называть *антивирусной сетью*.

В состав антивирусной сети входят следующие компоненты:

Основные компоненты:

- *Dr.Web Enterprise Server (Enterprise Сервер)*. Этот компонент устанавливается на одном из компьютеров антивирусной сети. Хранит дистрибутивы антивирусных пакетов для различных ОС защищаемых компьютеров, обновления вирусных баз, антивирусных пакетов и **Enterprise Агентов**, пользовательские ключи и настройки пакетов защищаемых компьютеров и передает их по запросу **Enterprise Агентов** на соответствующие компьютеры. **Enterprise Сервер** ведет единый журнал событий антивирусной сети.
- *Центр Управления Dr.Web*. Этот компонент устанавливается автоматически вместе с **Enterprise Сервером** и предоставляет веб-интерфейс для удаленного управления **Enterprise Сервером** и антивирусной сетью путем редактирования настроек **Enterprise Сервера**, а также настроек защищаемых компьютеров, хранящихся на **Enterprise Сервере** и на защищаемых компьютерах.
- *Dr.Web Enterprise Agent (Enterprise Агент)*. Этот компонент устанавливается на защищаемом компьютере, после чего производит на нем установку антивирусного пакета. В дальнейшем **Enterprise Агент** производит регулярные обновления установленного антивирусного ПО, передает ему команды и настройки с **Enterprise Сервера**, а также отсылает **Enterprise Серверу** информацию о вирусных событиях и другие необходимые сведения о защищаемом компьютере.

Дополнительные компоненты:

- *Прокси-сервер*. Этот компонент может опционально включаться в состав антивирусной сети. Основная задача **Прокси-сервера** – обеспечение связи **Enterprise Сервера** и **Enterprise Агентов** в случае невозможности организации прямого доступа, например, если **Enterprise Сервер** и **Enterprise Агенты** расположены в различных сетях, между которыми отсутствует маршрутизация пакетов. За счет использования функции кэширования также может быть обеспечено уменьшение сетевого трафика и времени получения обновлений **Enterprise Агентами**.
- *NAP Validator.* Позволяет использовать технологию *Microsoft Network Access Protection (NAP)* для проверки работоспособности ПО защищаемых рабочих станций на основе соответствия политикам.

Enterprise Сервер можно установить на любом компьютере, а не только на компьютере, выполняющем функции сервера ЛВС. Основные требованием к этому компьютеру приведены в п. Системные требования.

Центр управления может быть открыт на любом компьютере, а не только на том, на котором установлен **Сервер**. Достаточно связи по сети с компьютером, на котором установлен **Сервер**.

В состав антивирусной сети может входить несколько **Enterprise Серверов**. Особенности такой конфигурации в настоящем Руководстве описываются в п. Особенности сети с несколькими антивирусными серверами.

В состав антивирусного пакета Dr.Web, устанавливаемого на защищаемые рабочие станции, входят следующие компоненты:

Основные компоненты:

- *Dr.Web Сканер для Windows* входит в состав обычного продукта **Dr.Web для Windows**. Настройки сканера задаются непосредственно для него (через групповые настройки или персональные для станции). Проверяет ПК по запросу пользователя или согласно локальному расписанию пользователя. Дополнительно включает в себя антируткит-модуль.
- *Dr.Web Enterprise Сканер для Windows* - это одна из функций **Enterprise Агента**. Это тоже антивирусный сканер, использует те же вирусные базы, то же поисковое ядро. Но функциональность эта "встроена" в **Enterprise Агента**. Предназначение **Dr.Web Enterprise Сканера для Windows** - выполнять антивирусную проверку по запросу: либо запуском по расписанию, либо непосредственным заданием **Сканировать** из **Центра Управления Dr.Web**. Какого-либо специального интерфейса и самостоятельных настроек работы у него нет, всё задается только через **Центр Управления** при запуске **Сканера** (при настройке запуска по расписанию или при ручном инициировании проверки).
- *Системный монитор SelfPROtect* обеспечивает защиту файлов и каталогов **Dr.Web ESS** от несанкционированного или невольного удаления или модификации пользователем, а также вредоносным ПО. При включенном системном мониторе доступ к указанным ресурсам имеют только программы **Dr.Web**.

Дополнительные компоненты:

- *SplDer Guard (файловый монитор)* постоянно находится в памяти и проверяет "на лету" все открываемые файлы на сменных дисках и открываемые на запись файлы на жестких дисках. Кроме того, сторож постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при их обнаружении блокирует процессы с выводом соответствующего сообщения пользователю.
- *SplDer Mail (почтовый монитор)* также постоянно находится в памяти. Программа перехватывает все обращения почтовых клиентов вашего ПК к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP и проверяет входящую (или исходящую) почту до ее приема (или отправки) почтовым клиентом.
- *SplDer Gate* (*HTTP-монитор)* постоянно находится в памяти компьютера и перехватывает все обращения к веб-сайтам по протоколу HTTP. Программа нейтрализует угрозы в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокирует доступ к подозрительным или некорректным ресурсам.
- *Dr.Web Офисный Контроль* постоянно находится в памяти компьютера и - при наличии соответствующих настроек - управляет доступом к сетевым и указанным локальным ресурсам. В частности, компонент позволяет контролировать доступ к веб-сайтам, разрешая или запрещая пользователям посещать определенные узлы сети Интернет. Программа позволяет не только контролировать целостность важных файлов от случайного изменения или заражения вирусами, но и запрещает служащим доступ к нежелательной информации.
- *Dr.Web FireWall (межсетевой экран)* предназначен для защиты компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети Интернет. Компонент позволяет контролировать подключение и передачу данных по сети Интернет и блокировать подозрительные соединения на уровне пакетов и приложений.

1.4. Преимущества

- Кросс-платформенность серверного программного обеспечения, позволяющего использовать в качестве **Enterprise Сервера** машину под управлением как ОС Microsoft® Windows®, так и ОС семейства UNIX®.
- Кросс-платформенность агентского программного обеспечения, позволяющего осуществлять антивирусную защиту компьютеров под управлением ОС семейств Microsoft Windows, ОС Android, Microsoft® Windows Mobile®, Novell® NetWare®, ОС семейства UNIX, Mac OS X.
- Антивирусная защита почтовой системы Microsoft® Outlook®, а также почтовой системы, построенной на основе сервера IBM® Lotus® Domino® или Microsoft® Exchange Server.
- Минимальный сетевой трафик локальных сетей, построенных на основе протоколов TCP/IP, IPX и NetBIOS, с возможностью применения специальных алгоритмов сжатия.
- Возможность шифрования данных при обмене между различными компонентами системы.
- Упрощенное управление рабочими станциями антивирусной сети за счет использования механизма групп.
- Возможность управления антивирусной защитой (при помощи **Центра Управления Dr.Web**) практически с любого компьютера под управлением любой операционной системы.
- Возможность удаленной установки и удаления компонентов пакета системным администратором непосредственно через **Центр Управления.**
- Централизованная установка **Enterprise Агентов** (с возможностью настройки ПО **Enterprise Агентов** на **Enterprise Сервере** до его установки на клиентские машины).
- Возможность использования спам-фильтра на антивирусной станции (при условии, что приобретенная лицензия позволяет использование такой функции).
- Быстрое и эффективное распространение **Сервером** обновлений вирусных баз и программных модулей на

защищаемые рабочие станции.

- Функция резервного копирования критических данных **Сервера** (базы данных, конфигурационных файлов и др.).

В отличие от других антивирусных продуктов, **Антивирус Dr.Web ESS** может быть установлен даже на зараженных компьютерах пользователей.

1.5. Системные требования

Для установки и функционирования Dr.Web ESS требуется:

- чтобы **Enterprise Сервер** был установлен на компьютер, имеющий доступ в Интернет, для автоматического получения обновлений с серверов **ВСО** (Всемирной системы обновления) **Dr.Web**;
- чтобы компьютеры антивирусной сети имели доступ в Интернет для связи с **Enterprise Сервером** либо **Прокси-сервером** или находились в одной локальной сети с ним;
- для совместной работы антивирусных компонентов на используемых компьютерах должны быть открыты все необходимые порты и сокеты:

Номер	Протокол	Назначение
порты 2193, 2371	TCP, UDP	Для связи антивирусных компонентов с **Сервером**.
сокет 2371	IPX/SPX	Для связи антивирусных компонентов с **Сервером**.
порты 2193, 2372	UDP	Для работы Сканера Сети.
порты 139, 445	TCP, UDP	Для работы **Сетевого инсталлятора**.
порт 9080	http	Для работы Центра Управления Dr.Web.
порт 9081	https	Для работы Центра Управления Dr.Web.

Порт 2371 необходим для связи (по протоколам TCP и UDP) с компонентами версии **4.XX**. Используется для обеспечения совместимости, в частности, в процессе обновления компонентов антивирусной сети.

Для работы Dr.Web Enterprise Server требуется:

- процессор Intel® Pentium® III с частотой 667 МГц или выше,
- объем оперативной памяти 512 МБ (1 ГБ при использовании встроенной БД),
- объем свободной (доступной) памяти на жестком диске до 12 ГБ: до 8 ГБ для встроенной базы данных (каталог установки), до 4 ГБ в системном временном каталоге (для рабочих файлов),

При установке **Сервера** необходимо, чтобы на системном диске (вне зависимости от места установки самого **Сервера**) было не менее 2,5 ГБ свободной памяти для полного дистрибутива или 650 МБ для облегченного дистрибутива - для запуска инсталлятора и распаковки временных файлов.

- ОС Windows, ОС Linux®, ОС FreeBSD® или ОС Solaris™. Полный список поддерживаемых версий ОС приведен в Приложении. А,
- при установке **Enterprise Сервера** под ОС семейства UNIX требуется наличие библиотек: `libiconv` версии `1.8.2` и старше, `pcre`, `ncurses`, `openssl`, `libcrypto` и `libssl` (разделяемые библиотеки, обычно входят в состав `openssl`), `libxml2`, `libpq` (только для использования с базой **PostgreSQL**; при установке через generic-пакеты, библиотека уже входит в их состав), `libcurl` версии `7.20.0` и старше, `libldap`.

Для работы Прокси-сервера требуется:

- процессор Intel Pentium III с частотой 667 МГц или выше,
- объем оперативной памяти не менее 512 МБ,
- объем свободной (доступной) памяти на жестком диске: не

менее 1 ГБ,

- ОС Windows 2000 и выше, ОС Linux, ОС FreeBSD или ОС Solaris (аналогично **Enterprise Серверу**, см. Приложение А. Полный список поддерживаемых версий ОС),
- при установке **Прокси-Сервера** под ОС семейства UNIX требуется наличие библиотек: `libiconv` версии `1.8.2` и старше, `pcre`, `libxml2`.

Библиотеку `libiconv` можно загрузить с сервера ftp://ftp.freebsd.org.

Для работы NAP требуется:

Для сервера:

- ОС Windows Server 2008.

Для агентов:

- ОС Windows XP SP3, ОС Windows Vista, ОС Windows Server 2008.

Для работы Центра Управления Dr.Web требуется:

- Веб-браузер Windows® Internet Explorer® 7 и выше или веб-браузер Mozilla® Firefox® 3.0 и выше.

Также возможно использование веб-браузеров Opera® 10 и выше, Safari® 4 и выше, Chrome® 7 и выше. Однако возможность работы под данными веб-браузерами не гарантируется.

При установке **Сервера** на компьютер, в названии которого присутствует символ "_" (подчеркивание), работа с **Сервером** через **Центр Управления** в браузере Windows Internet Explorer будет невозможна.

В таком случае необходимо использовать другой веб-браузер.

Для корректной работы **Центра управления** под веб-браузером Windows Internet Explorer, IP-адрес и/или DNS-имя машины, на которой установлен **Enterprise Сервер**, должны быть добавлены в доверенные сайты браузера, в котором открывается **Центр управления**.

Для корректного открытия **Центра управления** через меню **Пуск** при использовании веб-браузера Windows Internet Explorer под ОС Windows 8 и ОС Windows Server 2012 с плиточным интерфейсом необходимо установить следующие настройки веб-браузера: **Свойства браузера** → **Программы** → **Открытие Internet Explorer** установить флаг **Всегда в Internet Explorer в классическом виде**.

- Подключаемый модуль **Dr.Web Browser-Plugin** для полноценной работы с **Центром Управления**. Модуль поставляется вместе с дистрибутивом **Сервера** и устанавливается по запросу браузера в процессе работы с элементами **Центра Управления**, требующими подгрузку модуля (для **Сканера сети**, при удаленной установке антивирусных компонентов).

Для работы подключаемого модуля **Dr.Web Browser-Plugin** на странице **Сканера сети** как под ОС Windows, так и под ОС семейства GNU/Linux, необходимы права администратора (root).

При использовании веб-браузера Safari подключаемый модуль **Dr.Web Browser-Plugin** доступен только для версий, работающих под ОС Windows.

При использовании веб-браузеров Mozilla Firefox, Opera и Chrome подключаемый модуль **Dr.Web Browser-Plugin** доступен только для версий, работающих под ОС Windows и ОС семейства Linux.

- Рекомендуемое разрешение экрана для работы с **Центром Управления** 1280x1024 px.

Для работы Dr.Web Enterprise Agent и полного антивирусного пакета требуется:

1. Минимальные требования:
   - процессор Intel Pentium IV с частотой 1.6 ГГц;
   - объем оперативной памяти 512 МБ.
2. Рекомендуемые требования:
   - процессор Intel Pentium IV с частотой 2.4 ГГц и выше;
   - объем оперативной памяти не менее 1 ГБ.
3. Свободное место на жестком диске: не менее 250 МБ для исполняемых файлов + дополнительно для протоколов работы и временных файлов;
4. Операционные системы (см. Прил. А. Полный список поддерживаемых версий ОС):
   a) ОС Windows 98, ОС Windows Me, ОС Windows NT4 (SP6) и выше. При этом, в зависимости от ОС, могут быть установлены следующие компоненты:

Компонент	ОС
SpIDer Gate, **SelfPROtect**, **Офисного Контроль**, **Dr.Web Browser-Plugin для Outlook**	Windows 2000 с SP4 и выше.
SpIDer Guard NT4, **Dr.Web Сканер NT4**	• Windows 98, • Windows ME, • Windows NT4 (SP6a), • Windows 2000 с SP4 без Update Rollup1, • Windows XP без SP, а также с SP1, • Windows 2003 без SP.
FireWall, **SpIDer Guard G3**, **Dr.Web Сканер**	• Windows 2000 с SP4 и Update Rollup1, • Windows XP с SP2 и выше,

Компонент	ОС
	• Windows 2003 с SP1 и выше, • Windows Vista и выше.
SpIDer Mail NT4	• Windows 98, • Windows NT4 с SP6a.
SpIDer Mail	Все поддерживаемые ОС, старше систем для версии **SpIDer Mail NT4**.

b) ОС Microsoft® Windows Mobile®;

c) ОС Novell NetWare;

d) ОС семейства UNIX: Linux, FreeBSD и Solaris 10 (только для платформы Intel);

e) ОС Android;

f) Mac OS X.

5. Для подключаемого модуля **Dr.Web для Outlook** необходим установленный клиент Microsoft Outlook из состава MS Office:
   - Outlook 2000 (Outlook 9),
   - Outlook 2002 (Outlook 10 или Outlook XP),
   - Office Outlook 2003 (Outlook 11),
   - Office Outlook 2007,
   - Office Outlook 2010.
6. Для корректной работы контекстной справки **Dr.Web Агент для Windows** необходим Windows Internet Explorer 6.0 и выше.

На рабочих станциях антивирусной сети, управляемой с помощью **Dr.Web**, не должно использоваться другое антивирусное ПО (в том числе ПО других версий антивирусных программ **Dr.Web**).

Описание функциональности **Агента** под ОС Windows Mobile и Novell NetWare приведено в руководствах пользователя **Dr.Web Агент для Windows Mobile** и **Dr.Web Агент для Novell NetWare**.

1.6. Комплект поставки

Дистрибутив Dr.Web Enterprise Security Suite поставляется в двух вариантах в зависимости от ОС выбранного Enterprise Сервера:

1. Для установки под управлением ОС семейства UNIX – в виде файлов архивного формата `bzip2` или пакетов установки для соответствующей версии ОС следующих компонентов:
   - **Dr.Web Enterprise Server**,
   - **Прокси-сервер**.
2. Для установки под управлением ОС Windows — в виде исполняемых файлов мастера установки для следующих компонентов:
   - **Dr.Web Enterprise Server**,
   - **Прокси-сервер**,
   - **Dr.Web Enterprise Agent** для Active Directory,
   - **NAP Validator**.

Дистрибутив Enterprise Сервера поставляется в двух вариантах:

1. *Полный дистрибутив* - включает дистирубивы всех корпоративных продуктов, предоставляемых для установки на защищаемые станции, управляемые всеми поддерживаемыми ОС.
2. *Облегченный дистрибутив* - дистрибутив, состав которого аналогичен составу дистрибутива предыдущих версий **Dr.Web Enterprise Security Suite**.

   Подходит при установке антивирусной защиты, управляемой

при помощи **Dr.Web Enterprise Security Suite**, на станции только с ОС Windows.

В состав дистрибутива Enterprise Сервера входят следующие компоненты:

- ПО **Сервера Dr.Web Enterprise Server** для соответствующей ОС,
- ПО **Агентов Dr.Web Enterprise Agent** и антивирусных пакетов для поддерживаемых ОС,
- ПО **Центра Управления Dr.Web**,
- вирусные базы,
- документация, шаблоны и примеры.

Кроме самого дистрибутива поставляются также серийные номера, после регистрации которых вы получите файлы с серверным ключом и ключом для рабочих станций.

1.7. Ключевые файлы

Права на использование **Dr.Web Enterprise Security Suite** регулируются при помощи следующих ключевых файлов:

1. Ключевой файл для **Сервера** - `enterprise.key`.
2. Ключевой файл для рабочих станций - `agent.key`.

Ключевой файл имеет формат, защищенный от редактирования при помощи механизма электронной подписи. Редактирование файла делает его недействительным. Чтобы избежать случайной порчи ключевого файла, не следует модифицировать ключевой файл и/или сохранять его после просмотра в текстовом редакторе.

Состав и стоимость лицензии на использование антивирусного решения **Dr.Web ESS** зависят от количества защищаемых станций в сети (в т.ч. серверов, входящих в состав сети **Dr.Web ESS** как защищаемые станции).

Эту информацию необходимо обязательно сообщать продавцу лицензии при покупке решения **Dr.Web ESS**. Вам также следует указать количество **Enterprise Серверов**, необходимых для создания антивирусной сети. Количество используемых независимых (не связанных друг с другом) **Enterprise Серверов** не влияет на увеличение стоимости лицензии (см. также п. Создание антивирусной сети).

Обратите внимание, что при создании антивирусной сети с несколькими **Серверами** (см. п. Особенности сети с несколькими Серверами), при подсчете защищаемых станций необходимо учитывать соединения между **Enterprise Серверами**, поскольку такие соединения требуют дополнительной лицензии. При этом, для каждого **Enterprise Сервера** каждая межсерверная связь, вне зависимости от ее типа (см. п. Строение сети с несколькими Серверами) требует отдельной лицензии, т.е. при связи двух **Серверов** дополнительная лицензия на межсерверную связь нужна обоим.

Лицензионные ключевые файлы могут входить в комплект антивируса **Dr.Web ESS** при покупке. Однако, как правило, поставляются только серийные номера.

Лицензионные ключевые файлы высылаются пользователям по электронной почте, как правило, после регистрации серийного номера на специальном веб-сайте (адрес сайта регистрации http://products.drweb.com/register/, если иной адрес не указан в регистрационной карточке, прилагаемой к продукту). Зайдите на указанный сайт, заполните форму со сведениями о покупателе и введите в указанное поле регистрационный серийный номер (находится на регистрационной карточке). Архив с ключевыми файлами будет выслан по указанному вами адресу. Вы также сможете загрузить его непосредственно с указанного сайта.

Ключевые файлы поставляются пользователю в виде zip-архива, содержащего ключевые файлы для **Сервера** и рабочих станции.

Пользователь может получить ключевые файлы одним из следующих способов:

- по электронной почте (обычно после регистрации на веб-сайте, см. выше);
- вместе с дистрибутивом продукта, если лицензионные файлы были включены в состав дистрибутива продукта при его комплектации;
- на отдельном носителе в виде файла.

Рекомендуется сохранять лицензионный ключевой файл до истечения срока его действия и использовать его при переустановке или восстановлении компонентов программы. В случае утраты лицензионного ключевого файла вы можете повторить процедуру регистрации на указанном сайте и снова получить лицензионный ключевой файл. При этом необходимо указывать тот же регистрационный серийный номер и те же сведения о покупателе, что и при первой регистрации; может измениться только адрес электронной почты. В этом случае лицензионный ключевой файл будет выслан по новому адресу.

Для ознакомления с антивирусом можно использовать демонстрационные ключевые файлы. Такие ключевые файлы обеспечивают полную функциональность основных антивирусных компонентов, но имеют ограниченный срок действия. Для того чтобы получить демонстрационные ключевые файлы, следует заполнить форму, расположенную на странице http://download.drweb.com/demoreq/. Ваш запрос будет рассмотрен в индивидуальном порядке. В случае положительного решения архив с ключевыми файлами будет выслан по указанному вами адресу.

Использование полученных ключевых файлов в процессе установки программы описывается в п. Установка Dr.Web Enterprise Server.

Использование ключевых файлов для уже развернутой антивирусной сети описано в разделе Обновление серверного ключа и ключа для рабочих станций.

Глава 2. Установка и удаление компонентов Dr.Web Enterprise Security Suite

2.1. Создание антивирусной сети

Чтобы создать антивирусную сеть:

1. Составьте план структуры антивирусной сети, включив в него все защищаемые компьютеры и определив, какие из них будут выполнять функцию **Enterprise Сервера**.
2. Установите ПО **Enterprise Сервера** (вместе с ним установится **Центр Управления Dr.Web**) на выбранный компьютер или компьютеры.
3. Используя **Центр Управления** произведите обновление репозитория.
4. Настройте ПО рабочих станций и **Сервера** (**Серверов**).
5. При необходимости установите и настройте **Прокси-сервер**.
6. Установите ПО **Enterprise Агента** на рабочие станции.

Сразу после установки на компьютеры **Агенты** автоматически устанавливают соединение с **Сервером**. Авторизация антивирусных станций на **Сервере** происходит в соответствии с выбранной вами политикой (см. п. Политика подключения станций).

7. Используя **Центр Управления**, настройте и запустите необходимые модули.

На этапе планирования структуры антивирусной сети, прежде всего, необходимо выбрать компьютер, который будет выполнять функции **Enterprise Сервера**.

Enterprise Сервер можно установить на любом компьютере, а не только на компьютере, выполняющем функции сервера ЛВС. Основные требованием к этому компьютеру приведены в п. Системные требования.

Центр Управления и **Сервер** могут находиться на разных компьютерах. Достаточно связи по сети между ними.

В состав антивирусной сети может входить несколько **Enterprise Серверов**. Особенности такой конфигурации описаны в п. Особенности сети с несколькими Серверами.

Для установки **Enterprise Сервера** и **Enterprise Агента** требуется однократный доступ (физический или с использованием средств удаленного управления и запуска программ) к соответствующим компьютерам. Все дальнейшие действия выполняются с рабочего места администратора антивирусной сети (в том числе, возможно, извне локальной сети) и не требуют доступа к **Enterprise Серверам** или рабочим станциям.

2.2. Установка Dr.Web Enterprise Server

Установка **Enterprise Сервера** является первым шагом развертывания антивирусной сети. До ее успешного завершения никакие другие компоненты антивирусной сети установить невозможно.

Ход процесса установки **Enterprise Сервера** зависит от того, какая версия **Сервера** (для ОС Windows или для ОС семейства UNIX) устанавливается. Тем не менее, состав настраиваемых в ходе установки параметров и структура установленного ПО совпадают.

Все параметры, задаваемые при установке, могут быть впоследствии изменены администратором антивирусной сети в процессе работы **Сервера**.

Если у вас уже установлено ПО **Сервера**, обратитесь к разделам Обновление Dr.Web ESS для ОС Windows® или Обновление Dr.Web ESS для ОС семейства UNIX® соответственно.

Если перед установкой ПО **Сервера** осуществлялось удаление **Сервера**, установленного ранее, то в процессе инсталляции будет удалено содержимое репозитория, и установлена его новая версия. Если по какой-либо причине был сохранен репозиторий предыдущей версии, необходимо вручную удалить все содержимое репозитория перед установкой новой версии **Сервера** и произвести полное обновление репозитория после установки **Сервера**.

Язык названия каталога, в который ставится **Сервер**, должен совпадать с языком, указанным в языковых настройках ОС Windows для программ, не использующих Unicode. В противном случае установка **Сервер** не будет запущена.

Исключение - английский язык в названии каталога инсталляции.

Вместе с **Enterprise Сервером** автоматически устанавливается **Центр Управления Dr.Web**, который служит для управления антивирусной сетью и настройки **Сервера**.

По умолчанию **Enterprise Сервер** после установки запускается автоматически (для версии под ОС семейства UNIX это указывается в настройках инсталлятора).

2.2.1. Установка Dr.Web Enterprise Server для ОС Windows®

Ниже описывается установка **Enterprise Сервера** для ОС Windows. Состав и последовательность шагов могут несколько различаться в зависимости от версии дистрибутива.

Перед началом установки Dr.Web Enterprise Server рекомендуется принять во внимание следующую информацию:

Если в ОС Windows установлены службы **Terminal Services,** установка ПО должна осуществляться только с помощью мастера **Установка и удаление программ** на **Панели управления** ОС Windows.

Файл дистрибутива и другие файлы, запрашиваемые в процессе установки программы, должны находиться на локальных дисках компьютера, на который устанавливается ПО **Сервера**. Права доступа должны быть настроены так, чтобы эти файлы были доступны для пользователя **LOCALSYSTEM**.

Установка **Enterprise Сервера** должна выполняться пользователем с правами администратора данного компьютера.

После установки **Enterprise Сервера** необходимо произвести обновление всех компонентов **Dr.Web ESS** (см. п. Ручное обновление компонентов Dr.Web ESS).

При использовании внешней БД необходимо предварительно создать БД и настроить соответствующий драйвер (см. Приложение B. Настройки, необходимые для использования СУБД. Параметры драйверов СУБД).

На Рис. 2-1. приведена блок-схема процесса установки **Enterprise Сервера** при помощи инсталлятора. Разделение установки по шагам соответствует подробному текстовому описанию процедуры, приведенному ниже.

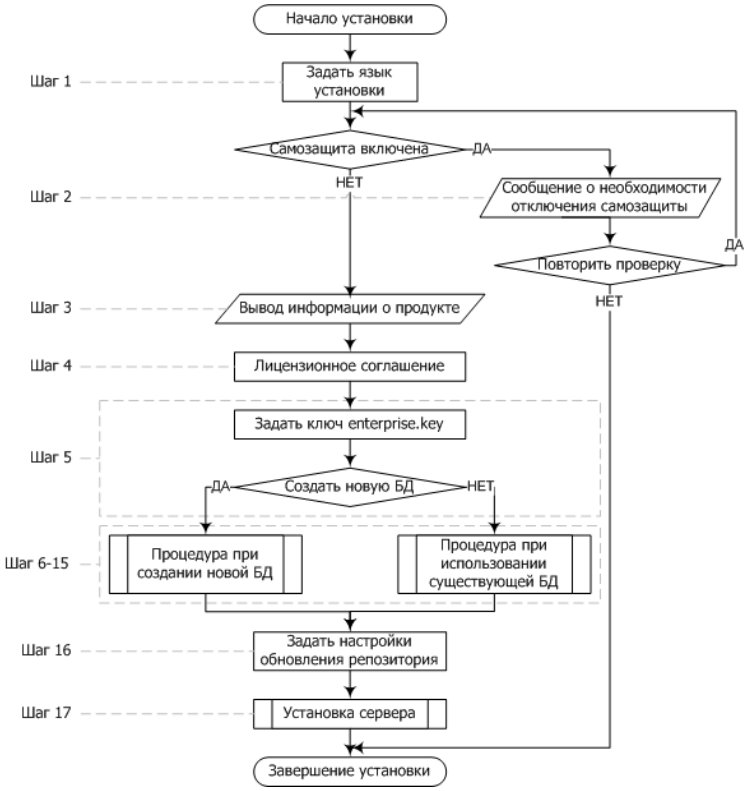


Рисунок 2-1. Схема процесса установки Dr.Web Enterprise Server (Нажмите на блок схемы для перехода к описанию)

Блок-схема содержит три встроенные процедуры. Процедура **Установка Сервера** (шаг 17) не требует вмешательства пользователя (см. описание ниже) и осуществляется непосредственно инсталлятором.

Блок-схемы процедур **при создании новой БД** и **при использовании существующей БД** приведены на Рис. 2-2. и Рис. 2-3.

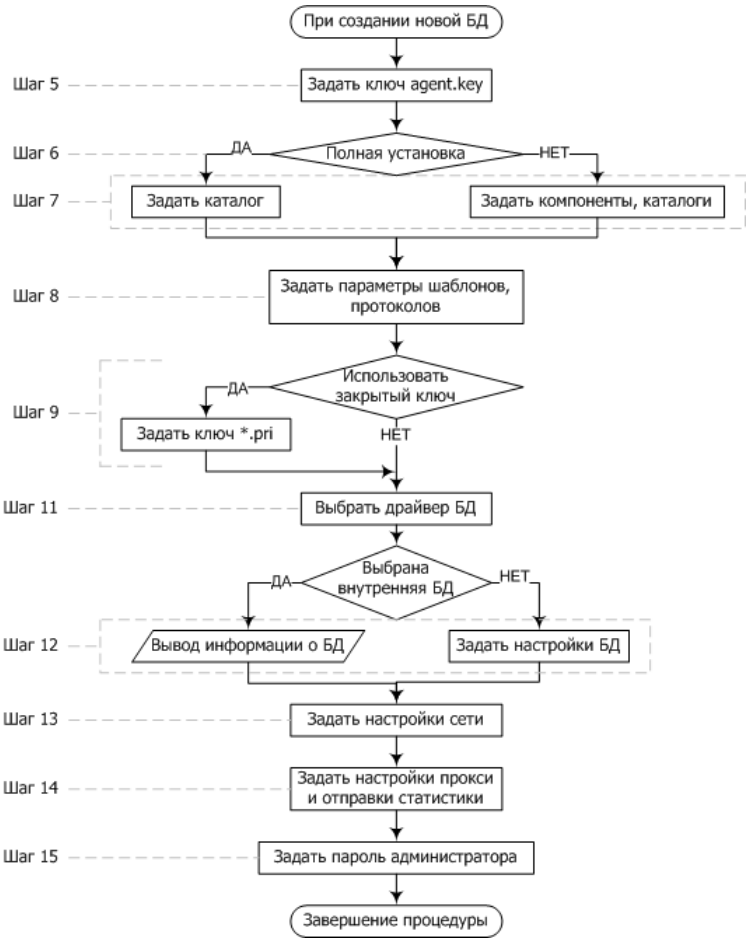


Рисунок 2-2. Схема процедуры инсталляции при создании новой БД (Нажмите на блок схемы для перехода к описанию)

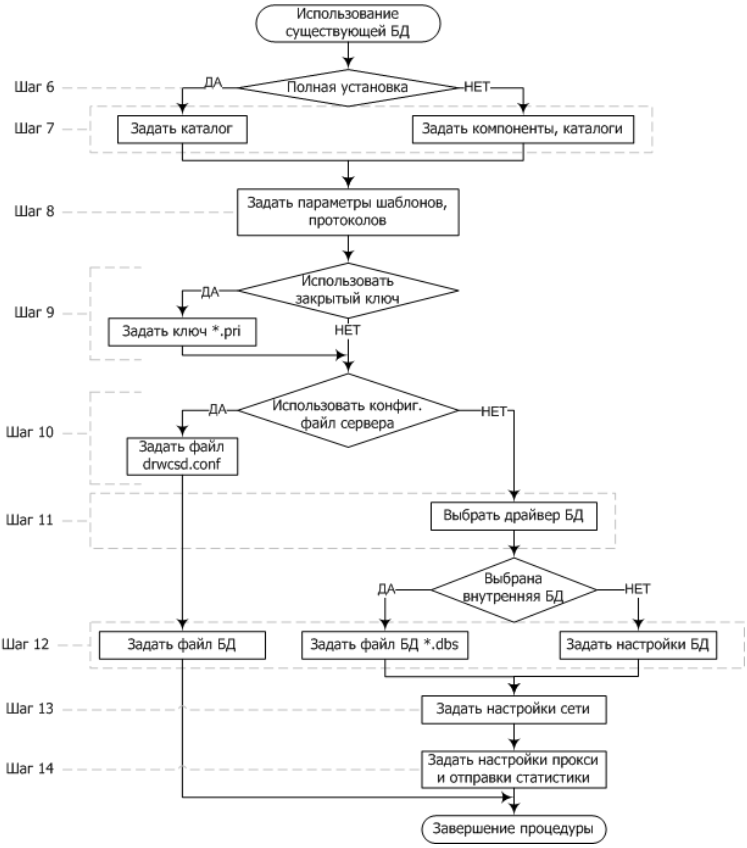


Рисунок 2-3. Схема процедуры установки Dr.Web Enterprise Server при использовании существующей БД (Нажмите на блок схемы для перехода к описанию)

Для установки Dr.Web Enterprise Server на компьютер с ОС Windows:

1. Запустите файл дистрибутива. Откроется окно выбора языка, на котором будет производиться дальнейшая установка продукта. Выберите **Русский** и нажмите на кнопку **Далее**.
2. Далее, если на компьютере с **Enterprise Сервером**

установлен **Enterprise Агент** со включенной самозащитой, то будет выдано сообщение об активности компонента самозащиты **Dr.Web**. Отключите данный компонент через настройки **Агента** и нажмите на кнопку **ОК** для продолжения процедуры или на кнопку **Cancel** - для отмены установки **Сервера**.

3. Откроется окно **InstallShield Wizard** с информацией об устанавливаемом продукте. Нажмите на кнопку **Далее**.
4. Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора в группе кнопок выбора в нижней части окна выберите **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее**.
5. Откроется окно выбора лицензионных ключевых файлов.

   Рядом с полем **Ключ для Dr.Web Enterprise Server** нажмите на кнопку **Обзор,** после чего в стандартном окне ОС Windows укажите местонахождение лицензионного ключевого файла для **Сервера** `enterprise.key`.

   При первой установке **Сервера** выберите **Создать новую базу данных** и в поле **Создать базу, используя данный ключ для Dr.Web Enterprise Agent** укажите файл ключа для ПО рабочей станции (`agent.key`).

   Если вы хотите сохранить базу данных **Сервера** от предыдущей установки, в группе кнопок выбора базы данных выберите **использовать имеющуюся базу данных**. Файл базы данных вы сможете указать позднее (см. шаг **10**).

   Для ознакомления с продуктом можно использовать демонстрационные ключевые файлы. Нажмите на кнопку **Демо ключи** для перехода на веб-сайт компании **«Доктор Веб»** и получения демонстрационных ключевых файлов (см. Демонстрационные ключевые файлы).

   Нажмите на кнопку **Далее**.

6. Откроется окно выбора типа установки. При выборе типа **Полная** будут установлены все компоненты **Enterprise**

Сервера, при указании типа **Выборочная** вы сможете на следующем шаге задать компоненты, которые вы хотите установить. После выбора типа установки нажмите на кнопку **Далее**.

Если вы планируете использовать в качестве внешней базы данных ODBC для Oracle, выберите пункт **Выборочная** и в открывшемся окне отмените установку встроенного клиента для СУБД Oracle (в разделе **Database support** - **Oracle database driver**).

В противном случае работа с БД Oracle будет невозможна из-за конфликта библиотек.

7. Если на предыдущем шаге был указан тип установки **Полная**, то откроется окно выбора каталога установки. Если необходимо изменить каталог установки по умолчанию, нажмите на кнопку **Изменить** и выберите каталог установки. Нажмите на кнопку **Далее**.

   Если на предыдущем шаге был указан тип установки **Выборочная**, то откроется окно выбора устанавливаемых компонентов и каталогов для каждого из них. В контекстном меню компонентов вы можете изменить способ их установки: установить компонент на локальной машине или для запуска по сети (доступно не для всех) или отменить установку компонента. Если необходимо изменить каталог установки выбранного в списке компонента, нажмите на кнопку **Изменить** и укажите каталог установки. Нажмите на кнопку **Далее**.

8. В следующем окне вы можете выбрать язык шаблонов сообщений, задать режим использования и наименование системного разделяемого ресурса для каталога установки **Агента** (по умолчанию задается скрытое имя разделяемого ресурса) и задать настройки ведения файла протокола установки.

   Если вы хотите автоматически запустить **Сервер** после установки, установите флаг **Запустить службу в процессе установки**.

   Если вы ходите добавить **Сервер** в исключения сетевого

экрана операционной системы (кроме ОС Windows 2000), установите флаг **Добавить в исключения брандмауэра порты и интерфейсы сервера**.

9. В следующем окне при первой установке **Сервера** просто нажмите на кнопку **Далее**. Ключи шифрования будут автоматически сгенерированы в процессе установки.

   Если вы устанавливаете **Сервер** для имеющейся антивирусной сети, установите флаг **Использовать существующие ключи шифрования** и укажите файл с закрытым ключом, после чего будет создан файл с открытым ключом (содержание открытого ключа будет совпадать с содержанием предыдущего открытого ключа). Это позволит **Агентам** опознать устанавливаемый **Сервер**. В противном случае после установки потребуется скопировать новый открытый ключ шифрования на все рабочие станции, на которых ранее были установлены **Enterprise Агенты**.

10. Далее, если вы на шаге **4** выбрали существующую базу данных, появится диалоговое окно, в котором вы можете указать заранее подготовленный конфигурационный файл **Сервера**.

    В серии следующих диалоговых окон задаются основные настройки, хранящиеся в конфигурационном файле **Сервера** (см. Приложение G1. Конфигурационный файл Dr.Web Enterprise Server).

11. В диалоговом окне, посвященном конфигурации базы данных, настраиваются параметры используемой базы данных, которые зависят от выбора типа базы на шаге **4** и от наличия конфигурационного файла **Сервера**, задаваемого на шаге **9**.

    При создании новой БД или в случае, если не был задан конфигурационный файл **Сервера** (для существующей БД), укажите драйвер, который следует использовать. Вариант **Драйвер базы данных IntDB** предписывает использовать встроенные средства **Enterprise Сервера**. Остальные варианты подразумевают использование соответствующей внешней БД. Настройки параметров СУБД подробно описаны

в приложениях (см. Приложение В. Настройки, необходимые для использования СУБД. Параметры драйверов СУБД).

Нажмите на кнопку **Далее**.

12. Если для создания новой БД на предыдущем шаге вы выбрали **Драйвер базы данных IntDB**, то в следующем окне будет выведена информация о создании новой БД.

    Если при использовании существующей БД вы на предыдущем шаге задали конфигурационный файл **Сервера** или выбрали **Драйвер базы данных IntDB**, то в следующем окне необходимо будет указать файл БД. Для этого нажмите на кнопку **Обзор**. Установите флаг **Запустить проверку внутренней базы данных во время установки** для проверки целостности БД в процессе установки **Сервера**.

    Если на предыдущем шаге вы указали один из вариантов внешних СУБД, то в следующем окне необходимо указать соответствующие параметры для настройки доступа к БД.

13. Далее, если вы на шаге **4** задали создание новой базы или на шаге **9** (для существующей БД) не задали конфигурационный файл **Сервера** от предыдущей установки, будет показано диалоговое окно, посвященное конфигурации сети, в котором настраивается сетевой протокол для **Сервера** (разрешается задать только один сетевой протокол; дополнительные протоколы можно настроить в дальнейшем).

    В полях **Интерфейс** и **Порт** задайте соответствующие значения для обращения к **Серверу**. По умолчанию задан интерфейс `0.0.0.0`, это означает, что к **Серверу** возможен доступ по всем интерфейсам.

По умолчанию используется порт `2193`, однако, для совместимости с антивирусным ПО предыдущих версий, также поддерживается порт `2371`.

Чтобы ограничить локальный доступ к **Серверу**, установите

флаг **Ограниченный доступ к Dr.Web Enterprise Серверу.** Доступ инсталлятору, **Агентам** и другим **Серверам** (в случае уже существующей антивирусной сети, построенной с помощью **Dr.Web Enterprise Security Suite)** будет запрещен. В дальнейшем эти настройки можно будет изменить через меню **Центра Управления Администрирование**, пункт **Конфигурация Dr.Web Enterprise Server**, вкладка **Модули**.

Установите флаг **Служба обнаружения сервера**, если хотите, чтобы **Сервер** отвечал на широковещательные и многоадресные запросы других **Серверов**.

Чтобы задать настройки сети по умолчанию, нажмите внизу окна на кнопку **Стандартная**. Чтобы ограничить работу **Сервера** только внутренним сетевым интерфейсом – `127.0.0.1` – нажмите на кнопку **Ограниченная**. При этих настройках управление **Сервером** возможно только из **Центра Управления**, запущенного на том же компьютере, а также к **Серверу** может подключиться только **Агент**, запущенный на том же компьютере. В дальнейшем, после отладки настроек **Сервера**, настройки сети можно будет изменить.

Нажмите на кнопку **Далее**.

14. Если на шаге **4** вы выбрали создание новой БД или на шаге **9** (для существующей БД) не задали конфигурационный файл **Сервера** от предыдущей установки, то в следующем окне будет выведен запрос на отправку статистики по вирусным событиям в компанию **«Доктор Веб»**. Для этого установите флаг **Разрешить отправку статистики** и заполните соответствующие поля. **Сервер** статистики – `stat.drweb.com`, **URL** – `\update`. Также вы можете заполнить поля **Пользователь** и **Пароль** при необходимости идентификации отправляемой статистики (получить имя пользователя и пароль можно в **Службе Технической Поддержки «Доктор Веб»**). В поле **Отправлять каждые** введите интервал отправки статистики в минутах. Обязательными полями являются только адрес сервера

статистики и интервал отправки статистики.

Также в данном окне в случае использования прокси-сервера вы можете указать его параметры. Для этого установите флаг **Использовать прокси** и введите адрес прокси-сервера (обязательный), имя пользователя и пароль для доступа к нему.

Флаг **Использовать прокси** будет доступен только в том случае, если каталог установки **Сервера** не содержит конфигурационных файлов от предыдущей установки.

15. Если на шаге **4** вы выбрали создание новой БД, то в следующем окне задайте пароль администратора антивирусной сети.

При задании пароля администратора не допускается использование национальных символов.

Нажмите на кнопку **Далее**.

16. Далее рекомендуется задать обновление репозитория во время установки. Для этого установите флаг **Обновить репозиторий**. Нажмите на кнопку **Далее**.
17. Нажмите на кнопку **Установить**. Дальнейшие действия программы установки не требуют вмешательства пользователя.
18. После завершения установки нажмите на кнопку **Готово**.

После установки **Сервера**, для корректного формирования ссылок при создании установочных пакетов **Агента**, отредактируйте параметр **ServerName** в конфигурационном файле `webmin.conf`, расположенном в подкаталоге `etc` каталога установки **Enterprise Сервера**. Раскомментируйте данный параметр и вместо www.example.com укажите IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**, а также номер порта в формате:

`ServerName` *<Адрес_Сервера>*`:`*<номер_порта>*

Сохраните изменения и перезапустите **Enterprise**

Сервер.

При использовании кластерной системы **Enterprise Серверов**, а также при использовании на **Enterprise Сервере** нестандартного порта, отредактируйте соответствующие параметры в конфигурационном файле `download.conf`, расположенном в подкаталоге `etc` каталога установки **Enterprise Сервера** (см. также Приложение G3. Конфигурационный файл download.conf).

Как правило, управление установленным **Enterprise Сервером** производится при помощи **Центра Управления Dr.Web**. Инсталлятор также помещает в главное меню ОС Windows элементы, позволяющие осуществлять настройку и управление **Сервером**.

В меню **Пуск** → **Программы** помещается каталог **Dr.Web Enterprise Server**, содержащий следующие элементы:

- Каталог **Управление сервером** - содержит команды запуска, перезапуска и завершения работы **Сервера**, а также команды настройки протоколирования и другие команды **Сервера**, подробнее описанные в Приложении H5. Dr.Web Enterprise Server.
- Пункт **Веб-интерфейс** - для открытия **Центра Управления** и подключения к **Серверу**, установленному на данном компьютере (по адресу http://localhost:9080).
- Пункт **Документация** - для открытия документации администратора в формате HTML.

Каталог установки Dr.Web Enterprise Server имеет следующую структуру:

- `bin` – исполняемые файлы **Enterprise Сервера**.
- `etc` – каталог содержит файлы основных настроек компонентов антивирусной сети, а также лицензионные ключи **Сервера** (`enterprise.key`) и **Агента** (`agent.key`).

- `Installer` – содержит инсталлятор для установки **Антивируса** на защищаемый компьютер и открытый ключ шифрования (`drwcsd.pub`).
- `update-db` – скрипты, необходимые для обновления структуры баз данных **Сервера**.
- `var` – каталог содержит подкаталоги:
  - `backup` – служит для хранения бэкапов БД и других критичных данных;
  - `extensions` – содержит пользовательские скрипты, предназначенные для автоматизации выполнения определенных заданий, все скрипты по умолчанию отключены;
  - `repository` – так называемый каталог обновлений, в который помещаются актуальные обновления вирусных баз, файлов антивирусных пакетов и компонентов антивирусной сети. Каталог содержит подкаталоги для отдельных функциональных компонентов ПО, а внутри них — подкаталоги для отдельных ОС. Каталог должен быть доступен на запись пользователю, от имени которого запускается **Сервер** (в ОС семейства UNIX это, как правило, пользователь **drwcs**, в ОС Windows — **LocalSystem**);
  - `templates` – шаблоны отчетов.
- `webmin` – каталог содержит элементы **Центра Управления Dr.Web**: документацию, значки, модули.

Содержимое каталога обновлений `\var\repository` загружается с сервера обновлений по протоколу HTTP автоматически, по установленному для **Сервера** расписанию, также администратор антивирусной сети может вручную помещать обновления в эти каталоги.

2.2.2. Установка Dr.Web Enterprise Server для ОС семейства UNIX®

Все действия по установке необходимо выполнять из консоли от имени суперпользователя (**root**).

Чтобы установить Dr.Web Enterprise Server для ОС семейства UNIX:

1. Чтобы запустить установку пакета `drweb-esuite`, выполните следующую команду:

Для Сервера под		Команда
ОС FreeBSD		`pkg_add` *<файл_дистрибутива>*`.tbz`
ОС Solaris		1. `bzip2 -d` *<файл_дистрибутива>*`.bz2` 2. `pkgadd -d` *<файл_дистрибутива>*
ОС Linux	Debian® Ubuntu®	`dpkg -i` *<файл_дистрибутива>*`.deb`
	rpm-пакеты	`rpm -i` *<файл_дистрибутива>*`.rpm`

Если у вас уже установлено ПО **Enterprise Сервера**, вы можете произвести обновление установленных компонентов. Для этого запустите дистрибутив, используя следующую команду:

- для **rpm**-дистрибутивов:

  `rpm -U` *<имя_файла_дистрибутива>*`.rpm`

- для **deb**-пакетов:

  `dpkg -i` *<имя_файла_дистрибутива>*`.deb`

Также существуют так называемые `generic`-пакеты, которые могут быть установлены на любую операционную

систему семейства Linux, в том числе не входящую в список официально поддерживаемых.

При установке `generic`-пакетов на ОС семейства Linux необходимо наличие библиотеки `glibc` той же версии, что и версия `generic`-пакета.

Установка осуществляется при помощи включенного в пакет инсталлятора. Используйте следующую команду:

```
tar -xjf <имя_файла_дистрибутива>.tar.bz2
```

Затем от имени суперпользователя выполните скрипт:

```
./drweb-esuite-install.sh
```

Установку **Сервера** можно прервать в любой момент, отправив процессу установки любой из следующих сигналов: `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` и `SIGWINCH` (в операционной системе **FreeBSD** изменение размеров окна терминала влечет отправку сигнала `SIGWINCH`). При прерывании процесса установки производится полный откат изменений в файловой системе до начала установки. Установка rpm-пакета может быть прервана нажатием клавиш CTRL + C

Нажатие кнопки ESC в процессе инсталляции **Сервера** позволяет вернуться к предыдущему шагу установки. При этом, на шаге 2 (первое окно инсталлятора с лицензионным соглашением) кнопка ESC прерывает работу инсталлятора.

Имя администратора антивирусной сети по умолчанию **admin**.

2. В следующих окнах (количество и последовательность их появления зависит от семейства ОС) выводятся сообщения об авторских правах и текст лицензионного соглашения. Для продолжения установки вам необходимо принять лицензионное соглашение.

3. Далее вам будет предложено задать группу и пользователя, от имени которого будет работать **Сервер**. Этот же пользователь будет являться владельцем файлов **Enterprise Сервера**.

   На запрос создания пользователя выберите пункт **new**, чтобы создать нового пользователя, от имени которого будет запускаться комплекс. В следующем меню рекомендуется оставить значение по умолчанию и нажать **OK**. В меню выбора группы создайте новую группу. В следующем запросе оставьте значение по умолчанию.

4. Далее будет предложено указать пути к ключевым файлам **Сервера** (`enterprise.key`) и **Агента** (`agent.key`), которые поставляются вместе с дистрибутивом, или, в случае обновления с более ранней версии, сохранены по умолчанию в `/root/esuite_backup` или в указанной вами директории.

При инсталляции в консольном режиме количество попыток задания ключей (при неверном их указании) ограничено:

- для ОС FreeBSD - 3 попытки;
- для ОС Solaris - 2 попытки.

При неверном задании ключей, по истечении допустимого числа попыток, работа инсталлятора будет прекращена.

5. Далее:
   - В случае установки ПО под ОС **Solaris**: вам будет предложено создать новую базу данных **Сервера**. Если вы производите обновление **Сервера**, и у вас есть сохраненная база данных, введите `no`, нажмите ENTER и укажите путь к сохраненному файлу с БД.
     Если же это первая установка **Enterprise Сервера**, нажмите ENTER и укажите пароль администратора (пользователь **admin**), который будет иметь доступ к **Серверу**. Вы можете оставить пароль по умолчанию - **root**. При задании собственного пароля, из соображений безопасности, вводимый пароль никак не

отображается на экране. Пароль следует ввести дважды (в случае различия введенных паролей процедуру придется повторить сначала – следуйте появляющимся инструкциям). Пароль должен быть не короче 4 символов.

Далее вам будет предложено создать новые ключи шифрования. Если у вас есть сохраненные ключи `drwcsd.pri` и `drwcsd.pub`, откажитесь от создания новых (наберите `no`, нажмите ENTER) и укажите полный путь к существующим файлам. Если же ключей нет, нажмите ENTER для создания новых ключей шифрования.

- В случае установки через **deb**-пакеты: вам будет предложено ввести пароль администратора (пользователь **admin**). Вы можете оставить пароль по умолчанию - **root**. При задании собственного пароля, из соображений безопасности, вводимый пароль никак не отображается на экране. Пароль следует ввести дважды (в случае различия введенных паролей процедуру придется повторить сначала – следуйте появляющимся инструкциям). Пароль должен быть не короче 4 символов.
- В остальных случаях: вам будет предложено ввести пароль администратора (пользователь **admin**). При задании пароля, из соображений безопасности, вводимый пароль никак не отображается на экране. Пароль следует ввести дважды (в случае различия введенных паролей процедуру придется повторить сначала – следуйте появляющимся инструкциям). Пароль должен быть не короче 8 символов.

При задании пароля администратора не допускается использование национальных символов.

При обновлении и при инициализации БД вручную пароль администратора сбрасывается в значение по умолчанию.

В целях соблюдения политик безопасности настоятельно рекомендуется не оставлять регистрационные данные, принятые по умолчанию. Регистрационные данные (имя пользователя и пароль) требуются при подключении к **Серверу** с помощью **Центра Управления**.

6. При наличии интерпретатора perl, в зависимости от используемой ОС, может быть предложено произвести настройку некоторых параметров **Сервера**. При запросе на настройку определенного типа параметров вариант `no` задается по умолчанию (по клавише ENTER), это означает, что для данных параметров будут заданы предустановленные значения. При вводе `yes` будет предложено указать значения предлагаемых параметров (при этом значения параметров по умолчанию представлены в квадратных скобках, для их задания достаточно нажать клавишу ENTER).

   Процедуру настройки параметров **Сервера** можно инициировать вручную (для этого также необходимо, чтобы был установлен интерпретатор perl). Для этого достаточно запустить скрипт `configure.pl`, который находится в:

   - в директории `/usr/local/drwcs/bin/` для ОС **FreeBSD**,
   - в директории `/opt/drwcs/bin/` для ОС **Linux** и ОС **Solaris**.

   Параметры использования скрипта `configure.pl` приведены в приложении H5.9. Настройка Dr.Web Enterprise Server для ОС семейства UNIX.

7. Далее будет произведена установка ПО, в ходе которой инсталлятор может попросить подтверждения ваших действий от имени администратора.

После установки **Сервера**, для корректного формирования ссылок при создании установочных пакетов **Агента**, отредактируйте параметр **ServerName** в конфигурационном файле `webmin.conf`, расположенном в каталоге:

- `/var/drwcs/etc` для ОС **FreeBSD** и ОС **Solaris**
- `/var/opt/drwcs/etc` для ОС **Linux**

Раскомментируйте данный параметр и вместо www.example.com укажите IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**, а также номер порта в формате:

`ServerName` *<DNS_имя>*`:`*<номер_порта>*

Сохраните изменения и перезапустите **Enterprise Сервер.**

При использовании кластерной системы **Enterprise Серверов**, а также при использовании на **Enterprise Сервере** нестандартного порта, отредактируйте соответствующие параметры в конфигурационном файле `download.conf`, расположенном в каталоге:

- `/var/drwcs/etc` для ОС **FreeBSD** и ОС **Solaris**
- `/var/opt/drwcs/etc` для ОС **Linux**

(см. также Приложение G3. Конфигурационный файл download.conf).

В процессе установки ПО под ОС **FreeBSD** создается `rc`-скрипт:

`/usr/local/etc/rc.d/drwcsd.sh`.

Используйте команды:

- `/usr/local/etc/rc.d/drwcsd.sh stop` - для ручной остановки **Сервера**;
- `/usr/local/etc/rc.d/drwcsd.sh start` - для ручного запуска **Сервера**.

В процессе установки ПО под ОС **Linux** и ОС **Solaris** будет создан `init`-скрипт для запуска и остановки **Сервера**: `/etc/init.d/drwcsd`, который использует `/opt/drwcs/bin/drwcs.sh`. Последний не предназначен для запуска вручную.

2.2.3. Установка подключаемого модуля Dr.Web Browser-Plugin

Установка подключаемого модуля **Dr.Web Browser-Plugin** для веб-браузеров Mozilla Firefox, Opera и Chrome возможна только для версий, работающих под ОС Windows и ОС семейства Linux.

Подключаемый модуль **Dr.Web Browser-Plugin** необходим для полноценной работы с **Центром Управления** (см. также Системные требования для Центра Управления Dr.Web).

Модуль поставляется вместе с дистрибутивом **Сервера** и может быть установлен:

1. Автоматически, по запросу Веб-браузера в процессе работы с **Центром Управления**, в частности с элементами требующими подгрузку модуля (для **Сканера сети**, при удаленной установке антивирусных компонентов).
2. Вручную, через инсталлятор модуля **Dr.Web Browser-Plugin**.

Установка Dr.Web Browser-Plugin вручную

Чтобы скачать инсталлятор модуля Dr.Web Browser-Plugin для установки вручную:

1. Откройте **Центр Управления**. Если **Dr.Web Browser-Plugin** еще не установлен для используемого веб-браузера, то под главным меню будет приведена рекомендация об установке подключаемого модуля.
2. Перейдите по ссылке **Установить Dr.Web Browser-Plugin**.

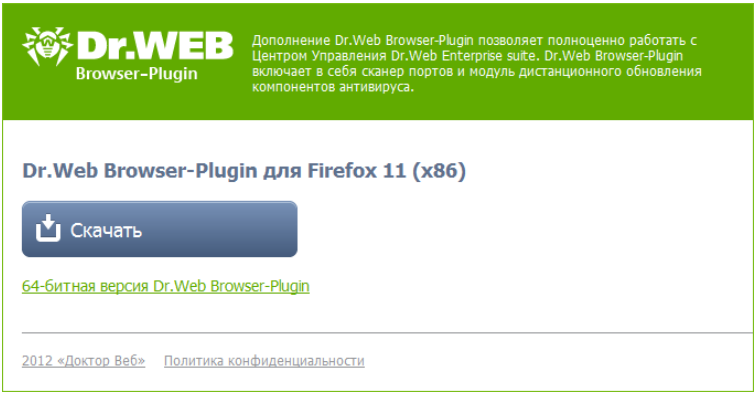


Рисунок 2-4. Раздел для загрузки модуля Dr.Web Browser-Plugin

3. В разделе скачивания подключаемого модуля приводится версия текущего веб-браузера и предлагаемая битность (x86 или x64) модуля.

   Для ОС семейства UNIX также предлагается выбрать из выпадающего списка версию дистрибутива для соответствующей ОС.

4. Для загрузки и сохранения модуля нажмите на кнопку **Скачать**. После этого вы можете установить его вручную.
5. Для того чтобы переключиться на версию с другой битностью, нажмите на ссылку под кнопкой загрузки, после чего инсталлятор можно скачать как описано на шаге **4**.

Для установки модуля Dr.Web Browser-Plugin под ОС Windows:

1. Запустите файл дистрибутива. Откроется окно **InstallShield Wizard**, извещающее вас об устанавливаемом продукте. Нажмите на кнопку **Далее**.
2. Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора в группе кнопок выбора укажите **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее**.

3. Откроется окно выбора каталога установки. Если необходимо изменить каталог установки, заданный по умолчанию, нажмите на кнопку **Change** и выберите каталог установки. Нажмите на кнопку **Далее**.
4. В следующем окне нажмите на кнопку **Установить** для начала процесса инсталляции. Дальнейшие действия программы установки не требуют вмешательства пользователя.
5. После завершения установки нажмите на кнопку **Готово**.

Для установки модуля Dr.Web Browser-Plugin под ОС семейства UNIX:

Выполните следующую команду:

- для **deb**-пакетов:

  `dpkg -i drweb-esuite-plugins-linux-`*<версия_дистрибутива>*`.deb`

- для **rpm**-пакетов:

  `rpm -i drweb-esuite-plugins-linux-`*<версия_дистрибутива>*`.rpm`

- для остальных систем (пакеты **tar.bz2** и **tar.gz**):

  1. Распакуйте архив с подключаемым модулем.
  2. Создайте директорию для подключаемых модулей, если она еще не создана.

  Например, для браузера Mozilla Firefox: `mkdir /usr/lib/mozilla/plugins`

  3. Скопируйте в директорию для подключаемых модулей распакованную на шаге 1 библиотеку.

  Например, для браузера Mozilla Firefox: `cp libnp*.so /usr/lib/mozilla/plugins`

После установки подключаемого модуля **Dr.Web Browser-Plugin** под ОС семейства UNIX перезапустите веб-браузер, если он был запущен.

2.3. Установка Dr.Web Enterprise Agent для ОС Windows®

Установка **Enterprise Агента** должна выполняться пользователем с правами администратора данного компьютера.

Если на рабочей станции уже установлен **Агент**, то перед началом новой инсталляции необходимо удалить установленный **Агент**.

Установка Enterprise Агента и антивирусного пакета может быть осуществлена двумя способами:

1. Удаленно: на **Enterprise Сервере** через ЛВС. Производится администратором антивирусной сети. При этом вмешательство пользователя не требуется. Подробное описание приведено в разделе Удаленная установка Dr.Web Enterprise Agent для ОС Windows®.
2. Локально: на машине пользователя непосредственно. Может производится как администратором, так и пользователем. При этом для установки может использоваться (см. также п. Инсталляционные файлы):
   - Инсталляционный пакет `esinst.exe`.
   - Сетевой инсталлятор **Агента** `drwinst`.

При установке Enterprise Агентов на сервера ЛВС и компьютеры кластера необходимо учесть:

- В случае установки на компьютеры, выполняющие роль терминальных серверов (в ОС Windows установлены службы **Terminal Services**), для обеспечения работы **Агентов** в терминальных сессиях пользователей установка **Агентов** должна осуществляться только локально с помощью мастера установки и удаления программ на **Панели управления** ОС Windows.
- На сервера, выполняющие важные сетевые функции (домен-контроллеры, сервера раздачи лицензий и т.д.), не

рекомендуется устанавливать компоненты **SpIDer Gate**, **SpIDer Mail** и **Dr.Web Firewall** во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса **Dr.Web**.

- Установка **Агента** на кластер должна выполняться отдельно на каждый узел кластера.
- Принципы функционирования **Агента** и компонентов антивирусного пакета на узле кластера аналогичны таковым на обычном сервере ЛВС, поэтому не рекомендуется устанавливать на узлы кластера компоненты **Dr.Web Firewall**, **SpIDer Mail**, **SpIDer Gate**.
- Если доступ к кворум-ресурсу кластера строго ограничен, рекомендуется исключить его из проверки сторожем **SpIDer Guard** и ограничиться регулярными проверками ресурса при помощи **Сканера**, запускаемого по расписанию или вручную.

2.3.1. Инсталляционные файлы

Инсталляционный пакет (esinst)

При создании новой учетной записи пользователя генерируется инсталляционный пакет `esinst` для установки **Агента**.

Ссылка для скачивания инсталляционного пакета **Агента** для конкретной станции доступна:

1. Сразу после создания новой станции (см. шаг **11** в разделе Создание новой учетной записи).
2. В любое время после создания станции:
   - в разделе свойств станции,
   - в разделе **Выбранные объекты** при выборе станции в иерархическом списке.

Сетевой инсталлятор (drwinst)

Сетевой инсталлятор **Агента** `drwinst`, а также открытый ключ шифрования `drwcsd.pub` располагаются в каталоге `Installer` (по умолчанию скрытый разделяемый ресурс) каталога установки **Enterprise Сервера**. Сетевая доступность ресурса задается на шаге 8 при установке **Enterprise Сервера**. В дальнейшем вы можете изменить данный ресурс по своему усмотрению.

Также инсталлятор для установки **Агента** и открытый ключ шифрования доступны на инсталляционной странице **Центра Управления Dr.Web**.

Инсталляционная страница

На инсталляционной странице **Центра Управления Dr.Web** вы можете скачать:

1. Сетевой инсталлятор **Агента** `drwinst`.

   Инсталляторы для различных ОС располагаются в каталогах с соответствующими названиями.

2. Открытый ключ шифрования `drwcsd.pub`.

Инсталляционная страница доступна на любом компьютере, имеющем сетевой доступ к **Enterprise Серверу**, по адресу:

`http://`*<Адрес_Сервера>*`:`*<номер_порта>*`/install/`

где в качестве *<Адрес_Сервера>* укажите IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**. В качестве *<номер_порта>* укажите порт номер `9080` (или `9081` для https).

2.3.2. Установка Dr.Web Enterprise Agent при помощи Инсталляционного пакета

Для установки Агента при помощи инсталляционного пакета необходимо:

1. При помощи **Центра Управления**:
   - Создать учетную запись нового пользователя на **Сервере**.
   - Получить ссылку для загрузки инсталлятора **Агента**.
2. Отправить пользователю ссылку на инсталлятор **Агента**.
3. Произвести установку Агента на рабочую станцию. Как правило, установка ПО **Enterprise Агента** осуществляется самим пользователем.
4. Авторизация новой антивирусной станции на **Сервере** по умолчанию осуществляется автоматически (также см. п. Политика подключения новых станций).

2.3.2.1. Создание новой учетной записи

Чтобы создать учетную запись или несколько учетных записей новых пользователей, воспользуйтесь Центром Управления Dr.Web.

Убедитесь, что для параметра **ServerName** в конфигурационном файле `webmin.conf` задано значение:

<Адрес_Сервера>`:9080`,

где *<Адрес_Сервера>* - IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**.

При создании учетной записи пользователя необходимо, чтобы подключение **Центра Управления** к **Серверу** осуществлялось по IP-адресу для домена, в котором создается учетная запись. В противном случае, при установке пакета будет невозможно подключиться к **Серверу**, поскольку при создании установочного пакета **Enterprise Агента**, в нем прописывается адрес **Сервера,** по которому подключен **Центр Управления**.

При подключении **Центра Управления** к **Серверу** с локальной машины проследите, чтобы адрес **Сервера** не был задан как loopback (`127.0.0.1`).

Для создания нового пользователя через Центр Управления Dr.Web:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**.
2. На панели инструментов нажмите на кнопку **Добавить станцию или группу**. В открывшемся подменю выберите пункт **Создать станцию**. В правой части окна **Центра Управления** откроется панель создания учетной записи пользователя.
3. В поле **Количество** укажите количество пользователей, которое вам нужно создать.
4. В поле **Идентификатор** автоматически генерируется уникальный идентификатор создаваемой станции. При необходимости, вы можете его изменить.
5. В поле **Название** задайте имя станции, которое будет отображаться в иерархическом списке антивирусной сети. В дальнейшем, после соединения станции с **Сервером**, данное имя может быть автоматически заменено на название станции, заданное локально.
6. В полях **Пароль** и **Еще раз пароль** укажите пароль для доступа станции к **Серверу**.

При создании более одной учетной записи поля **Идентификатор**, **Название** и **Пароль** (**Еще раз пароль**) будут заданы автоматически и недоступны для изменений на этапе создания станций.

7. В поле **Описание** введите дополнительную информацию о пользователе. Данный параметр не обязателен.
8. В разделе **Группа** выберите группы, в которые будет входить создаваемая антивирусная станция. По умолчанию станция входит в группу **Everyone**. В случае наличия пользовательских групп, вы можете включить в них создаваемую станцию. Для этого нажмите на название группы в разделе **Известные группы**. Для исключения станции из пользовательских групп, в которые она включена, нажмите на название группы в разделе **Членство в**.

   Для того чтобы назначить первичную группу для создаваемой станции, нажмите на значок нужной группы в разделе **Членство в**. При этом на значке группы появится **1.**

   Нельзя исключить станцию из группы **Everyone** и из первичной группы.
9. При необходимости заполните раздел **Безопасность**. Описание настроек данного раздела приведено в п. Настройка конфигурации рабочей станции.
10. При необходимости заполните раздел **Расположение**.
11. Нажмите **Сохранить** в правом верхнем углу. Откроется окно об удачном создании новой станции, в котором будет также указан идентификационный номер и ссылка для загрузки дистрибутива **Агента**.

Ссылка для скачивания инсталлятора **Агента** также доступна:

- в свойствах станции после ее создания,
- в разделе **Выбранные объекты** при выборе созданной станции в иерархическом списке.

Также см. п. Инсталляционные файлы.

12. Действия по установке ПО **Агента** описаны ниже.

Установка **Enterprise Агента** должна выполняться пользователем с правами администратора данного компьютера.

Если на рабочей станции уже установлено антивирусное ПО, то перед началом установки инсталлятор предпримет попытку его удалить. В случае, если такая попытка окажется неудачной, пользователю нужно будет самостоятельно удалить используемое на рабочей станции антивирусное ПО.

2.3.2.2. Установка Dr.Web Enterprise Agent и антивирусного пакета

Для установки Dr.Web Enterprise Agent и антивирусного пакета на рабочей станции:

1. Скачайте установочный файл **Агента**. Для этого перейдите по ссылке, полученной при создании станции в **Центре Управления**.
2. Запустите на станции скачанный файл `esinst.exe`. Откроется окно мастера установки антивируса **Dr.Web**.
3. Перед началом инсталляции мастер установки попросит подтвердить, что у вас не установлены антивирусные программы. Убедитесь, что на вашем компьютере не используется другое антивирусное ПО (в том числе ПО других версий антивирусных программ **Dr.Web**), после чего установите флаг **У меня на компьютере нет других антивирусов**. Нажмите на кнопку **Далее**.
4. В следующем окне будет предложен выбор варианта установки:
   - **Быстрая (рекомендуется)** - наиболее простой вариант установки. Все параметры задаются автоматически. Далее перейдите к шагу **8**.
   - **Выборочная** - вариант установки, при котором пользователь может выбрать компоненты антивирусного ПО, устанавливаемого на компьютер.

- **Административная** - наиболее полный вариант установки. Позволяет задать/изменить все параметры инсталляции и устанавливаемого антивирусного ПО.

5. Для вариантов установки **Выборочная** и **Административная**: в следующем окне вам будет предоставлен выбор компонентов антивирусного пакета **Dr.Web**. Установите флаги напротив тех компонентов, которые вы хотите установить на ваш компьютер.

   В разделе **Путь каталога установки** вы можете задать каталог, в который будет установлено антивирусное ПО. По умолчанию - это каталог `Dr.Web Enterprise Suite`, расположенный в каталоге `Program files` на системном диске. Для задания/изменения пути по умолчанию, нажмите на кнопку **Обзор** и укажите требуемый путь.

   Нажмите на кнопку **Далее**.

   Далее для варианта установки **Выборочная** перейдите к шагу **8**.

6. Для варианта установки **Административная**: в следующем окне задайте настройки **Сетевого инсталлятора**:
   - В поле **Dr.Web Enterprise Server** задается сетевой адрес **Enterprise Сервера**, с которого будет производиться установка **Агента** и антивирусного пакета. Если при запуске инсталлятора вы задали адрес **Сервера**, то он будет автоматически занесен в данное поле.

При установке **Enterprise Агента** при помощи инсталлятора, созданного в **Центре Управления**, автоматически заполняется поле **Dr.Web Enterprise Server**.

Если вы заведомо не знаете адрес **Сервера**, нажмите на кнопку **Поиск**. Будет выведено окно для поиска активных **Enterprise Серверов** сети. Задайте необходимые параметры (в формате *<имя_сервера>*@*<IP-адрес>*/*<префикс_сети>*:*<порт>*) и нажмите кнопку **Поиск**. В списке найденных **Серверов** выберите тот, с которого будет устанавливаться антивирусное ПО, и нажмите на кнопку **ОК**.

- В поле **Dr.Web Enterprise Server публичный ключ** задается полный путь к открытому ключу шифрования (`drwcsd.pub`), расположенному на компьютере пользователя (при запуске инсталлятора с **Сервера** по сети, ключ копируется во временные файлы ОС, а после перемещается в каталог установки).
- В разделе **Использовать сжатие при закачке** выберите нужный для вас вариант компрессии трафика: **Да** - использовать сжатие, **Нет** - не использовать, **Возможно** - использование сжатия трафика зависит от настроек на **Сервере**.
- Флаг **Добавить Dr.Web Агент в список исключений Windows Firewall** предписывает добавление портов и интерфейсов, используемых **Агентом**, в список исключений сетевого экрана операционной системы. Рекомендуется установить данный флаг. Это поможет избежать ошибок, например, при автоматическом обновлении компонентов антивируса и вирусных баз.
- При необходимости установите флаг **Зарегистрировать агент в списке установленных программ**.

Данная опция позволяет, в том числе, осуществлять удаление **Агента** и антивирусного пакета штатными средствами ОС Windows (см. п. Удаление компонентов ПО для ОС Windows®).

7. Для варианта установки **Административная**: в следующем окне задайте настройки **Агента**:

- В разделе **Авторизация** задаются параметры авторизации **Агента** на **Сервере**. При выборе варианта **Автоматически (по умолчанию)** параметры авторизации (идентификатор и пароль) будут автоматически сгенерированы на **Сервере**, при этом режим доступа станции будет определяться на **Сервере** (см. п. Политика подключения станций). При выборе варианта **Ручная** необходимо задать параметры авторизации станции: ее **Идентификатор** на **Сервере** и **Пароль** доступа к нему. При этом станция получит доступ без ручного подтверждения администратором на **Сервере**.

При установке **Enterprise Агента** при помощи инсталлятора, созданного в **Центре Управления**, автоматически заполняются поля **Идентификатор** и **Пароль** для варианта авторизации **Ручная**.

- В разделах **Сжатие** и **Шифрование** задаются соответствующие режимы для трафика между **Сервером** и **Агентом** (подробнее см. п. Использование шифрования и сжатия трафика).

Нажмите **Далее**.

8. Начнется установка **Агента** и антивирусных компонентов (не требует вмешательства пользователя).
9. После завершения инсталляции мастер установки сообщит о необходимости перезагрузить компьютер. Нажмите кнопку **Готово** для завершения работы мастера установки.
10. Перезагрузите компьютер.

Сразу после установки на компьютеры **Агенты** автоматически устанавливают соединение с **Сервером**. Как только **Агент** устанавливает связь с **Сервером**, в окне **Центра Управления** появляется имя соответствующей рабочей станции.

Enterprise Агент можно установить на рабочую станцию удаленно с использованием **Центра Управления**.

2.3.3. Установка Dr.Web Enterprise Agent при помощи Сетевого инсталлятора

Перед первой установкой **Enterprise Агентов** необходимо обязательно обновить репозиторий **Сервера** (см. п. Ручное обновление компонентов Dr.Web Enterprise Security Suite, п. **Проверка наличия обновлений**).

Если сетевой инсталлятор запущен в режиме нормальной инсталляции (т.е. без ключа `-uninstall`) на станции, на которой уже была проведена установка, это не приведет к выполнению каких-либо действий. Инсталлятор завершит работу и отобразит окно со списком допустимых ключей.

Установка при помощи Сетевого инсталлятора возможна в двух основных режимах:

1. В фоновом режиме.
2. В графическом режиме.

Вы также можете установить **Enterprise Агент** на рабочую станцию удаленно, с использованием **Центра Управления**, либо с использованием возможностей службы **Active Directory** (см. п. Удаленная установка Dr.Web Enterprise Agent).

2.3.3.1. Установка Dr.Web Enterprise Agent в фоновом режиме инсталлятора

Чтобы установить Dr.Web Enterprise Agent на рабочую станцию в фоновом режиме инсталлятора:

1. С компьютера, на который будет устанавливаться антивирусное ПО, войдите в сетевой каталог установки **Агента** (при установке **Сервера** это подкаталог `Installer` каталога установки **Сервера**, в дальнейшем его можно переместить) и запустите программу `drwinst`.

   По умолчанию команда `drwinst`, запущенная без параметров, использует режим **Multicast** для сканирования сети на наличие активных **Enterprise Серверов** и осуществляет попытку установки **Агента** с первого найденного **Сервера** в сети.

При использовании режима **Multicast** для поиска активных **Серверов**, установка **Агента** будет производиться с первого найденного **Сервера**. При этом, если имеющийся `pub` ключ не соответствует ключу **Сервера**, установка завершится с ошибкой. В этом случае явно укажите адрес **Сервера** при запуске инсталлятора (см. ниже).

Также команду `drwinst` можно запускать с дополнительными параметрами:

- В случае, когда режим **Multicast** не используется, при установке **Агента** рекомендуется использовать имя **Сервера** (предварительно зарегистрированное в службе DNS):

`drwinst` *<DNS_имя_Сервера>*

Это упростит процесс настройки антивирусной сети, связанный с процедурой переустановки **Enterprise Сервера** на другой компьютер.

- Вы также можете использовать явное указание адреса **Сервера**, например:

```
drwinst 192.168.1.3
```

- Использование ключа `-regagent` позволяет при установке зарегистрировать **Агент** в списке добавления и удаления программ.
- Для запуска инсталлятора в графическом режиме, используйте параметр `-interactive`.

Полный список параметров **Сетевого инсталлятора** приведен в Приложении Н4. Сетевой инсталлятор.

2. После завершения работы инсталлятора, на компьютер будет установлено ПО **Агента** (но не антивирусный пакет).
3. После подтверждения станции на **Сервере** (если этого требуют настройки **Сервера**) антивирусный пакет будет автоматически установлен.
4. Перезагрузите компьютер по требованию **Агента**.

2.3.3.2. Установка Dr.Web Enterprise Agent в графическом режиме инсталлятора

Чтобы установить Dr.Web Enterprise Agent на рабочую станцию в графическом режиме инсталлятора:

1. С компьютера, на который будет устанавливаться антивирусное ПО, войдите в сетевой каталог установки **Агента** (при установке **Сервера** это подкаталог `Installer` каталога установки **Сервера**, в дальнейшем его можно переместить) и запустите программу `drwinst` с параметром `-interactive`.

   Откроется окно мастера установки антивируса **Dr.Web**.

2. Перед началом инсталляции мастер установки попросит подтвердить, что на компьютере не установлены антивирусные программы. Убедитесь, что на компьютере не используется другое антивирусное ПО (в том числе ПО других версий антивирусных программ **Dr.Web**), после чего установите флаг **У меня на компьютере нет**

других антивирусов. Нажмите на кнопку **Далее**.

3. В следующем окне будет предложен выбор варианта установки:
   - **Быстрая (рекомендуется)** - наиболее простой вариант установки. Все параметры задаются автоматически. Далее перейдите к шагу **7**.
   - **Выборочная** - вариант установки, при котором пользователь может выбрать компоненты антивирусного ПО, устанавливаемого на компьютер.
   - **Административная** - наиболее полный вариант установки. Позволяет задать/изменить все параметры инсталляции и устанавливаемого антивирусного ПО.
4. Для вариантов установки **Выборочная** и **Административная**: в следующем окне вам будет предоставлен выбор компонентов антивирусного пакета **Dr.Web**. Установите флаги напротив тех компонентов, которые вы хотите установить на ваш компьютер.

   В разделе **Путь каталога установки** вы можете задать каталог, в который будет установлено антивирусное ПО. По умолчанию - это каталог `Dr.Web Enterprise Suite`, расположенный в каталоге `Program files` на системном диске. Для задания/изменения пути по умолчанию, нажмите на кнопку **Обзор** и укажите требуемый путь.

   Нажмите на кнопку **Далее**.

   Далее для варианта установки **Выборочная** перейдите к шагу **7**.
5. Для варианта установки **Административная**: в следующем окне задайте настройки **Сетевого инсталлятора**:

- В поле **Dr.Web Enterprise Server** задается сетевой адрес **Enterprise Сервера**, с которого будет производиться установка **Агента** и антивирусного пакета. Если при запуске инсталлятора вы задали адрес **Сервера**, то он будет автоматически занесен в данное поле. Если вы заведомо не знаете адрес **Сервера**, нажмите на кнопку **Поиск**. Будет выведено окно для поиска активных **Enterprise Серверов** сети. Задайте необходимые параметры (в формате *<имя_сервера>*@*<IP-адрес>*/*<префикс_сети>*:*<порт>*) и нажмите кнопку **Поиск**. В списке найденных **Серверов** выберите тот, с которого будет устанавливаться антивирусное ПО, и нажмите на кнопку **ОК**.
- В поле **Dr.Web Enterprise Server публичный ключ** задается полный путь к открытому ключу шифрования (`drwcsd.pub`), расположенному на компьютере пользователя (при запуске инсталлятора с **Сервера** по сети, ключ копируется во временные файлы ОС, а после перемещается в каталог установки).
- В разделе **Использовать сжатие при закачке** выберите нужный для вас вариант компрессии трафика: **Да** - использовать сжатие, **Нет** - не использовать, **Возможно** - использование сжатия трафика зависит от настроек на **Сервере**.
- Флаг **Добавить Dr.Web Агент в список исключений Windows Firewall** предписывает добавление портов и интерфейсов, используемых **Агентом**, в список исключений сетевого экрана операционной системы. Рекомендуется установить данный флаг. Это поможет избежать ошибок, например, при автоматическом обновлении компонентов антивируса и вирусных баз.
- При необходимости установите флаг **Зарегистрировать агент в списке установленных программ**.

Данная опция позволяет, в том числе, осуществлять удаление **Агента** и антивирусного пакета штатными средствами ОС Windows (см. п. Удаление компонентов ПО для ОС Windows®).

6. Для варианта установки **Административная**: в следующем окне задайте настройки **Агента**:
   - В разделе **Авторизация** задаются параметры авторизации **Агента** на **Сервере**. При выборе варианта **Автоматически (по умолчанию)** параметры авторизации (идентификатор и пароль) будут автоматически сгенерированы на **Сервере**, при этом режим доступа станции будет определяться на **Сервере** (см. п. Политика подключения станций). При выборе варианта **Ручная** необходимо задать параметры авторизации станции: ее **Идентификатор** на **Сервере** и **Пароль** доступа к нему. При этом станция получит доступ без ручного подтверждения администратором на **Сервере**.
   - В разделах **Сжатие** и **Шифрование** задаются соответствующие режимы для трафика между **Сервером** и **Агентом** (подробнее см. п. Использование шифрования и сжатия трафика).

   Нажмите **Далее**.
7. Начнется установка **Enterprise Агента**. После установки **Агента** нажмите кнопку **Готово** для завершения работы мастера установки.
8. После подтверждения станции на **Сервере** (если этого требуют настройки **Сервера**, см. п. Политика подключения станций и если на шаге **6** при **Административной** установке не был выбран вариант авторизации **Ручная**), антивирусный пакет будет автоматически установлен.
9. Перезагрузите компьютер по требованию **Агента**.

2.4. Удаленная установка Dr.Web Enterprise Agent для ОС Windows®

Dr.Web Enterprise Security Suite предоставляет возможность выявлять компьютеры, на которые еще не установлена антивирусная защита **Dr.Web Enterprise Security Suite**, и в некоторых случаях удаленно устанавливать такую защиту.

Удаленная установка **Enterprise Агентов** возможна только на рабочие станции, работающие под управлением ОС семейства Windows 2000 и старше (см. Приложение А. Полный список поддерживаемых версий ОС), за исключением редакций Starter и Home.

Удаленная установка **Enterprise Агентов** возможна только из **Центра Управления**, запущенного на ОС семейства Windows XP и старше (см. Приложение А. Полный список поддерживаемых версий ОС), за исключением редакций Starter и Home.

Для того чтобы удаленно установить **Enterprise Агент** на рабочие станции, вы должны иметь права администратора соответствующих рабочих станций.

Удаленная установка не требует дополнительной настройки удаленной станции, если она входит в домен и используется доменная учетная запись администратора. В случае, если удаленная машина не входит в домен, или используется локальная учетная запись для установки, то для ряда версий ОС Windows необходима дополнительная настройка удаленной машины.

Дополнительная настройка при удаленной установке на рабочую станцию вне домена или с использованием локальной учетной записи

Указанные настройки могут снизить безопасность удаленной машины. Настоятельно рекомендуется ознакомиться с назначением указанных настроек перед внесением изменений в систему, либо отказаться от использования удаленной установки и установить **Агент** вручную.

При удаленной установке **Агента** на рабочую станцию вне домена, и/или с использованием локальной учетной записи, необходимо на компьютере, на который будет удаленно

устанавливаться **Агент**, выполнить следующие действия:

ОС	Настройка
◆ Windows 2000 ◆ Windows Server 2000	Дополнительная настройка не требуется.
◆ Windows XP	1. Настроить режим доступа к общим файлам: **Панель управления → Свойства папки →** Вкладка **Вид →** снять флаг **Использовать простой общий доступ к файлам (рекомендуется)**. 2. Установить в локальных политиках следующий режим сетевой модели аутентификации: **Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная - локальные пользователи удостоверяются как они сами**.
◆ Windows Server 2003	Дополнительная настройка не требуется.
◆ Windows Vista ◆ Windows 7 ◆ Windows Server 2008	1. Включить опцию **Общий доступ к файлам**: **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Общий доступ и сетевое обнаружение → Общий доступ к файлам → Включить**. 2. Включить встроенную локальную учетную

ОС	Настройка
	запись администратора и установить на нее пароль. При установке использовать эту учетную запись: **Панель управления** → **Система и ее обслуживание** → **Администрирование** → **Управление компьютером** → **Локальные пользователи и группы** → **Пользователи**. Щелчок левой кнопкой по записи **Администратор** → снять флаг **Заблокировать учетную запись** → **ОК**. Щелчок правой кнопкой по записи → **Задать пароль** → задайте пароль.

В случае, если учетная запись на удаленной машине имеет пустой пароль, установить в локальных политиках политику доступа с пустым паролем: **Панель управления** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности** → **Локальные политики** → **Параметры безопасности** → **Учетные записи: ограничить использование пустых паролей только для консольного входа** → **Отключить**.

Необходимо разместить файл инсталлятора **Агента** `drwinst.exe` и открытый ключ шифрования `drwcsd.pub` на разделяемом ресурсе.

2.4.1. Установка Dr.Web Enterprise Agent с использованием Центра Управления Dr.Web

Возможны следующие способы удаленной установки Агентов на рабочие станции сети:

1. Установка через Сканер сети.

   Позволяет осуществить предварительный поиск незащищенных компьютеров сети и установку на них **Enterprise Агентов**.

2. Установка при помощи инструмента Установка по сети.

   Подходит в том случае, если заранее известен адрес станции или группы станций, на которые будут устанавливаться **Агенты**.

3. Установка на станции с заданными ID.

   Позволяет устанавливать на станции и группы станций **Агентов** для выбранных учетных записей (в том числе, для всех имеющихся новых учетных записей) с заданными ID и паролями доступа к **Серверу**.

Для корректной работы **Сканера сети** и инструмента **Установка по сети** под веб-браузером Windows Internet Explorer, IP-адрес и/или DNS-имя машины, на которой установлен **Enterprise Сервер**, должны быть добавлены в доверенные сайты браузера, в котором открывается **Центр Управления** для удаленной установки.

Использование Сканера Сети

В иерархическом списке антивирусной сети **Центра Управления** отображаются компьютеры, уже включенные в состав антивирусной сети. **Dr.Web Enterprise Security Suite** также позволяет обнаруживать компьютеры, не защищенные антивирусным ПО **Dr.Web ESS** и устанавливать антивирусные

компоненты удаленно.

Чтобы быстро осуществить установку ПО **Агента** на рабочие станции, рекомендуется воспользоваться **Сканером сети** (см. п. Сканер сети), который осуществляет поиск компьютеров по IP-адресам.

Для установки Агента с использованием Сканера сети:

1. Откройте Сканер сети. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Сканер Сети**. Откроется одноименное окно с незагруженными данными.
2. Укажите в поле ввода **Сети** перечень сетей в формате:
   - через дефис (например, `10.4.0.1-10.4.0.10`),
   - через запятую и пробел (например, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - с использованием префикса сети (например, `10.4.0.0/24`).

   Подробное описание дополнительных настроек приведено в разделе Сканер сети.
3. Нажмите на кнопку **Запустить сканер**. В окно будет загружен каталог (иерархический список) компьютеров с указанием, на каких из них антивирусное ПО установлено, а на каких — нет.
4. Разверните элементы каталога, соответствующие рабочим группам (доменам). Все элементы каталога, соответствующие рабочим группам и отдельным станциям помечаются различными значками, значение которых приведено ниже.

Таблица 2-1. Возможные виды значков

Знак	Описание
Рабочие группы	
	Рабочие группы, содержащие в числе прочих компьютеры, на которые можно установить антивирус **Dr.Web ESS**.
	Остальные группы, включающие компьютеры с установленным антивирусным ПО или недоступные по сети.
Рабочие станции	
	Обнаруженная станция числится в базе и активна (активные станции с установленным антивирусным ПО).
	Обнаруженная станция числится в базе в таблице удаленных станций.
	Обнаруженная станция не числится в базе (на компьютере нет антивирусного ПО).
	Обнаруженная станция не числится в базе (станция подключена к другому **Серверу**).
	Обнаруженная станция числится в базе, не активна и порт закрыт.

Элементы каталога, соответствующие станциям со значками  или  , можно дополнительно развернуть и ознакомиться с составом установленных компонентов.

При нажатии на значок  компонента станции, подключенной к данному **Серверу**, будет выведено окно настроек данного компонента.

5. В окне **Сканера сети** выберите незащищенный компьютер (или несколько незащищенных компьютеров при помощи кнопок CTRL или SHIFT).
6. Выберите на панели инструментов пункт **Установить Dr.Web Enterprise Agent**.
7. Откроется окно формирования задания на установку **Агента.**
8. В секции **Dr.Web Network Installer** вы можете задать настройки для инсталляции ПО **Агента**.

9. В поле **Компьютеры** указывается IP-адрес компьютера (компьютеров), на которые будет устанавливаться антивирусное ПО.

   - При установке на станции, найденные через **Сканер сети,** в поле **Компьютеры** уже будет указан адрес станции или нескольких станций, на которые будет производиться установка.

   - В противном случае задайте адрес станции или нескольких станций. При установке ПО **Агента** сразу на несколько компьютеров вы можете указать несколько IP-адресов компьютеров в следующем формате:

     - через дефис (например, `10.4.0.1-10.4.0.10`),
     - через запятую и пробел (например, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
     - с использованием префикса сети (например, `10.4.0.0/24`).

Кроме того, вместо IP-адресов вы можете указать доменные имена компьютеров.

Если установка происходит по имени компьютера, которое содержит дефис '-', такое имя необходимо заключать в кавычки, например, "123-456".

10. По умолчанию ПО **Агента** будет установлено в каталог `C:\Program Files\DrWeb Enterprise Suite`. При необходимости укажите другой путь в поле **Каталог установки**.
11. По умолчанию в поле **Сервер** отображается IP-адрес или DNS-имя **Enterprise Сервера**, к которому подключен **Центр Управления**. При необходимости укажите в данном поле адрес **Сервера**, с которого будет устанавливаться антивирусное ПО.
12. В поле **Открытый ключ** указывается путь к открытому ключу, в поле **Исполняемый файл** - полное имя сетевого инсталлятора. При необходимости откорректируйте заданные значения, установите другие необходимые параметры.

Пути к открытому ключу и исполняемому файлу должны быть указаны в формате сетевых адресов.

13. При необходимости введите в поле **Дополнительные параметры** параметры командной строки сетевого инсталлятора (подробнее см. Приложение H4. Сетевой инсталлятор).
14. В выпадающем списке **Детализация протокола** задайте уровень подробности ведения протокола инсталляции.
15. В поле **Тайм-аут установки (сек.)** задайте максимальное время ожидания до завершения установки **Агента** в секундах. Допустимые значения: 1-600. По умолчанию задано значение 180 секунд. При малой пропускной способности канала связи между **Сервером** и **Агентом** рекомендуется увеличить значение данного параметра.
16. При необходимости установите флаг **Зарегистрировать установку в базе данных установленных программ**.
17. В разделе **Установить** выберите компоненты антивирусного пакета, которые будут устанавливаться на станцию. Также задайте параметры сжатия трафика при установке.
18. В разделе **Авторизация** укажите параметры авторизации для доступа к удаленному компьютеру.

    Возможно задание нескольких учетных записей администратора. Для этого:

    a) Нажмите кнопку  , чтобы добавить указанный в разделе **Авторизация** аккаунт в список аккаунтов, используемых при установке.

    b) Для добавления еще одной учетной записи, повторно заполните поля с настройками для авторизации и нажмите кнопку  . Аналогично для каждой новой записи.

    c) В списке используемых учетных записей вы можете исключать или разрешать использовать отключенные ранее записи. Для этого снимите или установите флаги для соответствующих аккаунтов.

При установке **Агента** сначала используется первая учетная запись из списка. Если установка под этой учетной записью завершается с ошибкой, используется следующая учетная запись и т.д.

19. После установки необходимых параметров секции **Dr.Web Network Installer**, нажмите **Далее**.
20. На вкладке **Dr.Web Enterprise Agent для Windows** вы можете указать такие параметры как:
    - В разделе **Авторизация** вы можете указать параметры авторизации **Агента** на **Сервере**. Если флаг **Установить параметры** не установлен и не заполнены соответствующие поля, то параметры авторизации будут заданы автоматически.
    - В разделах **Шифрование** и **Сжатие** вы можете разрешить использование шифрования и сжатия трафика между **Агентом** и **Сервером**.

    В дальнейшем эти параметры можно изменить в настройках Enterprise Агента и свойствах станции.
21. После ввода всех необходимых параметров нажмите **Установить**.

Для запуска установки антивирусного ПО используется встроенная служба.

22. **Enterprise Агент** будет установлен на указанные рабочие станции. После подтверждения станции на **Сервере** (если этого требуют настройки **Enterprise Сервера**, см. также п. Создание простой антивирусной сети), автоматически будет установлен антивирусный пакет.
23. Перезагрузите компьютер по требованию **Агента**.

Использование инструмента Установка по сети

Когда в своей основе антивирусная сеть уже создана и требуется установить ПО **Агента** на определенные компьютеры, рекомендуется воспользоваться **Установкой по сети**.

Для установки по сети:

1. Выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Установка по сети**.
2. Дальнейшие шаги установки аналогичны шагам **8-23** процедуры выше.

Установка для учетных записей с заданными ID

Для удаленной установки Агентов для учетных записей с выбранными ID:

a) При создании новой учетной записи станции:

1. Создайте новую учетную запись или несколько учетных записей рабочих станций (см. п. Создание новой учетной записи).
2. Сразу после создания учетной записи, в правой части главного окна откроется панель с заголовком **Установить Dr.Web Enterprise Agent**. Нажмите кнопку **OK**.
3. Откроется окно **Сканера сети**.
4. Дальнейшие шаги установки аналогичны шагам **2-23** процедуры выше.
5. После завершения установки проверьте, что в иерархическом списке у соответствующих станций изменились значки.

b) При использовании существующей учетной записи станции:

1. В иерархическом списке антивирусной сети выберите новую станцию, группу станций, для которых еще не были установлены **Агенты**, или группу **New** (для установки на все имеющиеся новые учетные записи).
2. На панели инструментов нажмите кнопку **Установить Dr.Web Enterprise Agent**.
3. Откроется окно **Сканера сети**.
4. Дальнейшие шаги установки аналогичны шагам **2-23** процедуры выше.
5. После завершения установки проверьте, что в иерархическом списке у соответствующих станций изменились значки.

Установка **Агента** на станции с выбранными ID доступна также для администратора групп.

При получении ошибок при удаленной установке, обратитесь к разделу Диагностика проблем удаленной установки.

2.4.2. Установка Dr.Web Enterprise Agent с использованием службы Active Directory

Если в защищаемой локальной сети используется служба **Active Directory**, вы можете установить **Enterprise Агент** на рабочие станции дистанционно.

Установка **Агента** через службу Active Directory также возможна при использовании распределенной файловой системы DFS (см. раздел Использование DFS при установке Агента через Active Directory).

Установка Агента

Для установки Агента с использованием службы Active Directory:

1. Загрузите с сайта http://download.drweb.com/esuite/ инсталлятор **Enterprise Агента** для сетей с **Active Directory**.
2. На сервере локальной сети, поддерживающем службу **Active Directory**, выполните административную установку **Enterprise Агента**. Установку можно производить как в режиме в командной строки **(A)**, так и в графическом режиме инсталлятора **(B)**.

При обновлении **Сервера** не является необходимым обновление инсталлятора **Enterprise Агента** для сетей с Active Directory. После обновления ПО **Сервера**, **Агенты** и антивирусное ПО на станциях будут обновлены автоматически после установки.

(A) Настройка параметров установки Dr.Web Enterprise Agent в режиме командной строки

запустите следующую команду со всеми необходимыми параметрами и обязательным параметром отключения графического режима `/qn`:

`msiexec /a <название_пакета>.msi /qn [<параметры>]`

Ключ `/a` запускает развертывание административного пакета.

Название пакета

Название инсталляционного пакета **Enterprise Агента** для сетей с **Active Directory** обычно представлено в следующем формате:

`drweb-es-agent-<версия>-<дата-релиза>-windows-nt-<разрядность>.msi`.

Параметры

`/qn` - параметр отключения графического режима. При использовании этого ключа необходимо задать следующие обязательные параметры:

- `ESSERVERADDRESS=`*<DNS_имя>* - указывает адрес **Enterprise Сервера**, к которому будет подключаться **Агент.** О возможных форматах см. Приложение Е3.
- `ESSERVERPATH=`*<путь_имя_файла>* - указывает полный путь к открытому ключу шифрования **Enterprise Сервера** и имя файла (по умолчанию файл `drwcsd.pub` в подкаталоге `Installer` каталога установки **Enterprise Сервера**).
- `TARGETDIR` - сетевой каталог для образа **Агента** (модифицированного установочного пакета **Агента**), который выбирается через редактор групповых политик для назначенной установки. Данный каталог должен иметь доступ на чтение и запись. Путь к каталогу следует указывать в формате сетевых адресов, даже если он доступен локально; каталог обязательно должен быть доступен с целевых станций.

Перед административной установкой целевой каталог для образа **Агента** (см. параметр `TARGETDIR`) не должен содержать в себе инсталлятор **Enterprise Агента** для сетей с **Active Directory** *(<название_пакета>*`.msi`*)*.

После развертывания административного пакета, в директории:

<целевой_каталог>`\Program Files\DrWeb Enterprise Suite`

должен располагаться только файл `README.txt`.

Примеры:

```
msiexec /a ES_Agent.msi /qn
ESSERVERADDRESS=servername.net ESSERVERPATH=\
\win_serv\drwcs_inst\drwcsd.pub TARGETDIR=\\comp
\share
```

```
msiexec /a ES_Agent.msi /qn
ESSERVERADDRESS=192.168.14.1
ESSERVERPATH="C:\Program Files\DrWeb Enterprise
Server\Installer\drwcsd.pub" TARGETDIR=\\comp
\share
```

Те же параметры можно задать в графическом режиме инсталлятора.

После этого необходимо на сервере локальной сети, где установлено ПО управления Active Directory, назначить установку пакета (см. процедуру ниже).

(B) Настройка параметров установки Dr.Web Enterprise Agent в графическом режиме

Перед административной установкой убедитесь, что целевой каталог для образа **Агента** не содержит в себе инсталлятор **Enterprise Агента** для сетей с **Active Directory** (*<название_пакета>*.msi).

После развертывания административного пакета, в директории:

<целевой_каталог>\Program Files\DrWeb Enterprise Suite

должен располагаться только файл README.txt.

1. Для запуска инсталлятора в графическом режиме выполните команду:

```
msiexec /a <путь_к_инсталлятору>\<название_пакета>.msi
```

2. Откроется окно **InstallShield Wizard**, извещающее об устанавливаемом продукте. Нажмите на кнопку **Далее**.

Установщик **Агента** использует язык, указанный в языковых настройках компьютера.

3. В новом окне укажите DNS-имя или IP-адрес **Enterprise Сервера** (см. Приложение Е3). Укажите местонахождение открытого ключа **Enterprise Сервера** (`drwcsd.pub`). Нажмите на кнопку **Далее**.
4. В следующем окне укажите сетевую папку, в которую будет записан образ **Агента**. Путь к образу следует указывать в формате сетевых адресов, даже если каталог доступен локально; каталог обязательно должен быть доступен с целевых станций. Нажмите на кнопку **Установить**.
5. После завершения инсталляции будет автоматически вызвано окно настройки, с помощью которого вы сможете назначить установку пакетов на компьютеры сети.

Настройка установки пакета на выбранные станции

1. На **Панели управления** (или в меню **Пуск** для ОС Windows 2003/2008 Server, в меню **Пуск** → **Программы** для ОС Windows 2000 Server) выберите **Администрирование** → **Active Directory – пользователи и компьютеры** (в графическом режиме установки **Агента** вызов данного окна настроек осуществляется автоматически).
2. В домене, включающем компьютеры, на которые предполагается установка **Enterprise Агентов**, создайте новое **Подразделение** (для ОС Windows 2000 Server - **Организационное подразделение**) с именем, например, **ESS**. Для этого в контекстном меню домена выберите **Создать** → **Подразделение**. В открывшемся окне введите название нового подразделения и нажмите

ОК. Включите в созданное подразделение компьютеры, на которые предполагается устанавливать **Агент**.

3. Откройте окно редактирования групповых политик. Для этого:
   a) для ОС Windows 2000/2003 Server: в контекстном меню созданного подразделения **ESS** выберите пункт **Свойства**. В открывшемся окне свойств перейдите на вкладку **Групповая политика**.
   b) для ОС Windows 2008 Server: **Пуск** → **Администрирование** → **Управление групповой политикой**.
4. Для созданного подразделения задайте групповую политику. Для этого:
   a) В ОС Windows 2000/2003 Server: нажмите на кнопку **Добавить** и создайте элемент списка с именем политики **ESS**. Дважды щелкните по нему.
   b) В ОС Windows 2008 Server: в контекстном меню созданного подразделения **ESS** выберите пункт **Создать объект GPO в этом домене и связать его**. В открывшемся окне задайте название нового объекта групповой политики и нажмите на кнопку **ОК.** В контекстном меню новой групповой политики выберите пункт **Изменить**.
5. В открывшемся окне **Редактор управления групповыми политиками** внесите настройки для групповой политики, созданной в п. **4**. Для этого:
   a) В ОС Windows 2000/2003 Server: в иерархическом списке выберите элемент **Конфигурация компьютера** → **Конфигурация программ** → **Установка программ**.
   b) В ОС Windows 2008 Server: в иерархическом списке выберите элемент **Конфигурация компьютера** → **Политики** → **Конфигурация программ** → **Установка программ**.
6. В контекстном меню элемента **Установка программ** выберите пункт **Создать** → **Пакет**.

7. Далее задайте установочный пакет **Агента**. Для этого укажите адрес сетевого разделяемого ресурса (созданный при административной установке образ **Агента**). Путь к каталогу с пакетом следует указывать в формате сетевых адресов, даже если каталог доступен локально.
8. Откроется окно **Развертывание программ**. Выберите опцию **Назначенные**. Нажмите **ОК**.
9. В окне редактора управления групповыми политиками появится пункт **Dr.Web Enterprise Agent**. В контекстном меню этого пункта выберите **Свойства**.
10. В открывшемся окне свойств пакета перейдите на вкладку **Развертывание**. Нажмите на кнопку **Дополнительно**.
11. Откроется окно **Дополнительные параметры развертывания**.
    - Установите флаг **Не использовать языковые установки при развертывании**.
    - Если вы планируете установку **Enterprise Агента** при помощи настраиваемого msi-пакета на 64-битные ОС, установите флаг **Сделать доступным это 32-битное приложение для x64 машин**.
12. Нажмите дважды **ОК**.
13. **Enterprise Агент** будет установлен на выбранные компьютеры при ближайшей регистрации их в домене.

Применение политик с учетом предыдущих установок Агента

При назначении политик Active Directory для установки **Агента**, необходимо учесть возможность наличия уже установленного **Агента** на станции. Возможны три варианта:

1. **На станции нет Enterprise Агента**.

   После применения политик, **Агент** будет установлен по общим правилам.

2. **На станции уже установлен Enterprise Агент без использования службы Active Directory**.

После применения политики Active Directory, установленный **Агент** останется на станции.

В данной ситуации **Агент** на станции установлен, но для службы Active Directory **Агент** считается неустановленным. Поэтому, после каждой загрузки станции, будет повторяться неуспешная попытка установки **Агента** через службу Active Directory.

Для установки **Агента** через Active Directory необходимо вручную (или при помощи **Центра Управления**) удалить установленного **Агента** и повторно назначить политики Active Directory для данной станции.

3. **На станции уже установлен Enterprise Агент с использованием службы Active Directory**.

   После применения политики:

   a) Если для станции разрешены права на удаление **Агента**, то он будет удален со станции. Для установки **Агента** через Active Directory необходимо повторно назначить политики Active Directory для данной станции.

В данной ситуации, необходимо повторное назначение политик для установки **Агента**, поскольку, после первого назначения политик, **Агент** на станции будет удален, но для службы Active Directory **Агент** считается установленным.

   b) Если у станции нет прав на удаление **Агента**, назначение политик не приведет к изменению состояния антивирусного ПО на станции. Для дальнейших действий необходимо задать права на удаление **Агента** (см.п.Настройка прав пользователя) и повторно назначить политики Active Directory для данной станции. Далее действия аналогичны п. **a)**.

Повторное назначение политик Active Directory может осуществляться любым удобным для вас способом.

2.5. Установка NAP Validator

Dr.Web NAP Validator служит для проверки работоспособности антивирусного ПО защищаемых рабочих станций.

Данный компонент устанавливается на компьютер с настроенным сервером NAP.

Для установки NAP Validator выполните следующие действия:

1. Запустите файл дистрибутива. Откроется окно выбора языка, на котором будет производиться дальнейшая установка продукта. Выберите **Русский** и нажмите на кнопку **Далее**.
2. Откроется окно **InstallShield Wizard**, извещающее вас об устанавливаемом продукте. Нажмите на кнопку **Далее**.
3. Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора в группе кнопок выбора укажите **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее**.
4. В открывшемся окне в полях **Адрес** и **Порт** задайте соответственно IP-адрес и порт **Enterprise Сервера**. Нажмите на кнопку **Далее**.
5. Нажмите на кнопку **Установить**. Дальнейшие действия программы установки не требуют вмешательства пользователя.
6. После завершения установки нажмите на кнопку **Готово**.

После установки **Dr.Web NAP Validator** необходимо внести **Enterprise Сервер** в группу доверенных серверов NAP. Для этого:

1. Откройте компонент настройки сервера NAP (команда `nps.msc`).
2. В разделе **Группы серверов исправления** нажмите на кнопку **Добавить**.
3. В открывшемся диалоговом окне укажите название для сервера исправления и IP-адрес **Enterprise Сервера**.
4. Для сохранения внесенных изменений нажмите на кнопку **ОК**.

2.6. Установка Прокси-сервера

В состав антивирусной сети может входить один или несколько **Прокси-серверов**.

При выборе компьютера, на который будет устанавливаться **Прокси-сервер**, основным критерием является то, что **Прокси-сервер** должен быть доступен из всех сетей/сегментов сетей, информацию между которыми он будет переадресовывать.

Установка **Прокси-сервера** должна выполняться пользователем с правами администратора данного компьютера.

Ниже описывается установка **Прокси-сервера**. Состав и последовательность шагов могут несколько различаться в зависимости от версии дистрибутива.

Для установки Прокси-сервера на компьютер с ОС Windows:

1. Запустите файл дистрибутива. Откроется окно **InstallShield Wizard**, извещающее вас об устанавливаемом продукте. Нажмите на кнопку **Next**.
2. Откроется окно с текстом лицензионного договора. После

ознакомления с условиями лицензионного договора выберите в нижней части окна пункт **I accept the terms of the license agreement** и нажмите на кнопку **Next**.

3. Откроется окно выбора каталога установки. Если необходимо изменить каталог установки, заданный по умолчанию, нажмите на кнопку **Change** и выберите каталог установки. Нажмите на кнопку **Next**.
4. Откроется окно для настройки параметров **Прокси-сервера**:
   - В поле **Listen to** задайте IP-адрес, "прослушиваемый" **Прокси-сервером**. По умолчанию - `any (0.0.0.0)` – "прослушивать" все интерфейсы.
   - В поле **Port** задайте номер порта, который будет "слушать" **Прокси-сервер**. По умолчанию – это порт **2193** или порт **23** для протокола NetBIOS.
   - В выпадающем списке **Protocol** выберите тип протокола для приема входящих соединений **Прокси-сервером**.
   - Установите флаг **Enable discovery**, для включения режима имитации **Сервера**. Данный режим позволяет **Сканеру сети** обнаруживать **Прокси-сервер** в качестве **Enterprise Сервера**.
   - В поле **Multicast group** задайте IP-адрес многоадресной группы, в которую будет входить **Прокси-сервер**. Указанный интерфейс будет прослушиваться **Прокси-сервером** для взаимодействия с **Сетевыми инсталляторами** при поиске активных **Enterprise Серверов** сети. Если поле оставить пустым, **Прокси-сервер** не будет входить ни в одну из Многоадресных групп.
   - В разделе **Redirect to** задайте адрес или список адресов **Enterprise Серверов**, на один из которых будут перенаправляться соединения, устанавливаемые **Прокси-сервером**.

   После задания настроек **Прокси-сервера**, нажмите **Next**.
5. Откроется окно, извещающее о готовности к установке **Прокси-сервера**. Нажмите на кнопку **Install**.

6. После завершения процесса установки нажмите на кнопку **Finish.**

По окончанию установки вы можете изменить параметры работы **Прокси-сервера**. Для этого служит конфигурационный файл `drwcsd-proxy.xml`, расположенный в каталоге установки **Прокси-сервера**. Настройки конфигурационного файла приведены в Приложении G4.

Для установки Прокси-сервера на компьютер с ОС семейства UNIX:

Выполните следующую команду:

- для ОС **FreeBSD**:
  `pkg_add` *<имя_файла_дистрибутива>*`.tbz`
- для ОС **Solaris**:
  `bzip2 -d` *<имя_файла_дистрибутива>*`.bz2` и затем:
  `pkgadd -d` *<имя_файла_дистрибутива>*
- для ОС **Linux**:
  - для ОС **Debian** и ОС **Ubuntu**:
    `dpkg -i` *<имя_файла_дистрибутива>*`.deb`
  - для **rpm-дистрибутивов**:
    `rpm -i` *<имя_файла_дистрибутива>*`.rpm`

Также существуют так называемые `generic`-пакеты, которые могут быть установлены на любую операционную систему семейства Linux, в том числе не входящую в список официально поддерживаемых. Используйте следующую команду:
`tar -xjf` *<имя_файла_дистрибутива>*`.tar.bz2`

После этого необходимо переместить все содержимое распакованного архива в корневую директорию.

В процессе установки ПО под ОС **FreeBSD** создается `rc`-скрипт `/usr/local/etc/rc.d/0.dwcp-proxy.sh`.

Используйте команды:

- `/usr/local/etc/rc.d/0.dwcp-proxy.sh stop` - для ручной остановки **Прокси-сервера**;
- `/usr/local/etc/rc.d/0.dwcp-proxy.sh start` - для ручного запуска **Прокси-сервера**.

В процессе установки ПО под ОС **Linux** и ОС **Solaris** будет создан `init`-скрипт для запуска и остановки **Прокси-сервера** `/etc/init.d/dwcp-proxy`.

2.7. Удаление отдельных компонентов Dr.Web Enterprise Security Suite

2.7.1. Удаление компонентов ПО для ОС Windows®

Удаление Dr.Web Enterprise Server

Для удаления ПО **Enterprise Сервера** или подключаемого модуля **Dr.Web Browser-Plugin** запустите соответствующий продукту инсталляционный пакет той версии, которая у вас установлена. Инсталлятор автоматически определит программный продукт и предложит удалить его. Для удаления ПО нажмите на кнопку **Удалить**.

Удаление ПО **Enterprise Сервера** и подключаемого модуля **Dr.Web Browser-Plugin** также можно осуществить штатными средствами ОС Windows при помощи элемента **Панель управления** → **Установка и удаление программ**.

Удаление Dr.Web Enterprise Agent и антивирусного пакета по сети

Удаленная установка и деинсталляция ПО **Агента** возможны только в локальной сети и требуют полномочий администратора в этой сети.

Если удаление **Агента** и антивирусного пакета осуществляется при помощи **Центра Управления**, то **Карантин** со станции удален не будет.

Для того чтобы удалить ПО антивирусной станции удаленно (только для ОС семейства Windows):

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**.
2. В открывшемся окне в каталоге антивирусной сети выберите необходимую группу или отдельные антивирусные станции.
3. На панели инструментов каталога антивирусной сети нажмите **Общие** → **Деинсталлировать Dr.Web Enterprise Agent**.
4. ПО **Агента** и антивирусный пакет будут удалены с выбранных вами рабочих станций.

Если команда для запуска процесса удаления задается на тот момент, когда нет связи между **Enterprise Сервером** и антивирусной станцией, удаление ПО **Агента** на выбранной антивирусной станции произойдет, как только такая связь будет восстановлена.

Удаление Dr.Web Enterprise Agent и антивирусного пакета локально

Для возможности локального удаления **Агента** и антивирусного пакета, данная опция должна быть разрешена на **Сервере** в разделе **Права**.

Удаление антивирусного ПО станции (**Агента** и антивирусного пакета) можно осуществить двумя способами:

1. Используя штатные средства ОС Windows.
2. При помощи инсталлятора **Агента**.

Если удаление **Агента** и антивирусного пакета осуществляется при помощи штатных средств ОС Windows или при помощи инсталлятора **Агента**, то пользователю будет выдан запрос на удаление **Карантина**.

Удаление штатными средствами ОС Windows

Данный метод удаления доступен только в том случае, если при установке **Агента** с помощью графического инсталлятора был установлен флаг **Зарегистрировать агент в списке установленных программ**.

Если **Агент** был установлен в фоновом режиме инсталлятора, то удаление антивирусного ПО штатными средствами будет доступно только если при инсталляции был использован ключ `-regagent`.

Для удаления **Агента** и антивирусного пакета штатными средствами ОС Windows воспользуйтесь элементом **Панель управления** → **Установка и удаление программ** (подробная

инструкция приведена в **Руководстве пользователя** для **Агента**).

Удаление при помощи инсталлятора

Для того чтобы удалить ПО **Агента** и антивирусный пакет на станции локально, необходимо выполнить в каталоге установки **Enterprise Агента** (по умолчанию – `C:\Program Files\DrWeb Enterprise Suite`) команду `drwinst` с параметром `-uninstall` (или с параметрами `-uninstall -interactive`, если требуется обеспечить контроль за ходом удаления).

Например:

```
drwinst -uninstall -interactive
```

2.7.2. Удаление Dr.Web Enterprise Agent с использованием службы Active Directory

1. В Панели управления ОС Windows выберите в меню **Администрирование** элемент **Active Directory - пользователи и компьютеры**.
2. В домене выберите созданное вами Организационное подразделение **ESS**. В контекстном меню выберите пункт **Свойства**. Откроется окно **Свойства ESS**.
3. Перейдите на вкладку **Групповая политика**. Выберите элемент списка с именем **Политики ESS**. Дважды щелкните по нему. Откроется окно **Редактор объектов групповой политики**.
4. В иерархическом списке выберите **Конфигурация компьютера → Конфигурация программ → Установка программ → Пакет**. Далее в контекстном меню пакета с дистрибутивом **Агента** выберите **Все задачи → Удалить → ОК**.
5. На вкладке **Групповая политика** нажмите **ОК**.

6. **Enterprise Агент** будет удален с компьютеров при следующей регистрации в домене.

2.7.3. Удаление Dr.Web Enterprise Server для ОС семейства UNIX®

Все действия по удалению необходимо выполнять от имени суперпользователя (**root**).

Чтобы удалить Dr.Web Enterprise Server:

1. Выполните следующую команду:

Для Сервера под		Команда
ОС FreeBSD		`pkg_delete drweb-esuite`
ОС Solaris		1. Остановите **Сервер**: `/etc/init.d/drwcsd stop` 2. Выполните команду: `pkgrm DWEBesuit`
ОС Linux	Debian Ubuntu	`dpkg -r drweb-esuite`
	rpm-пакет	`rpm -e drweb-esuite`
	generic-пакет	`/opt/drwcs/bin/drweb-esuite-uninstall.sh`

Удаление **Сервера** можно прервать в любой момент отправкой процессу любого из следующих сигналов: `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` и `SIGWINCH` (в операционной системе **FreeBSD** изменение размеров окна терминала влечет отправку сигнала `SIGWINCH`). Без необходимости процесс удаления лучше не прерывать, либо следует сделать это как можно раньше.

2. Далее (в случае удаления **Сервера**, установленного под ОС **Solaris**) необходимо подтвердить намерение удалить

ПО, а также согласиться с необходимостью выполнения скриптов удаления от имени администратора.

При удалении **Сервера** (в операционных системах **FreeBSD** и **Linux**) серверные процессы будут автоматически остановлены, база данных, ключевые и конфигурационные файлы будут скопированы под ОС **Linux** в каталог, заданный `${HOME}/drwcs/` (как правило, это `/root/drwcs/`). Под ОС **FreeBSD** предлагается выбрать путь, по умолчанию - в `/var/tmp/drwcs`.

В операционной системе **Solaris** после удаления **Сервера** база данных, ключевые и конфигурационные файлы будут скопированы в каталог `/var/tmp/DrWebES`.

Чтобы удалить модуль Dr.Web Browser-Plugin:

Выполните следующую команду:

- для **deb**-пакетов:
  ```
  dpkg -P drweb-esuite-plugins
  ```
- для **rpm**-пакетов:
  ```
  rpm -e drweb-esuite-plugins
  ```
- для остальных систем (пакеты **tar.bz2** и **tar.gz**):
  ```
  rm -f <директория_модулей>/libnp*.so
  ```
  Например, для браузера Mozilla Firefox:
  ```
  rm -f /usr/lib/mozilla/plugins/libnp*.so
  ```

2.7.4. Удаление Прокси-сервера

Удаление Прокси-сервера для ОС Windows

При удалении **Прокси-сервера** осуществляется удаление конфигурационного файла `drwcsd-proxy.xml`. При необходимости сохраните конфигурационный файл вручную перед удалением **Прокси-сервера**.

Удаление ПО **Прокси-сервера** осуществляется штатными средствами ОС Windows через раздел **Панель управления** → **Установка и удаление программ** (**Программы и компоненты** для ОС Windows 2008).

Удаление Прокси-сервера для ОС семейства UNIX

Для удаления Прокси-сервера выполните:

Для Прокси-сервера под		Команда
ОС FreeBSD		`pkg_delete drweb-esuite-proxy`
ОС Solaris		`pkgrm DWEBespxy`
ОС Linux	deb-пакет	`dpkg -P drweb-esuite-proxy`
	rpm-пакет	`rpm -e drweb-esuite-proxy`
	generic-пакет	Удалите файлы из каталога установки **Прокси-сервера** вручную.

Глава 3. Компоненты антивирусной сети и их интерфейс

3.1. Dr.Web Enterprise Server

Антивирусная сеть должна иметь в своем составе хотя бы один **Enterprise Сервер**.

Для повышения надежности и продуктивности антивирусной сети, а также для распределения нагрузки, **Dr.Web ESS** позволяет создать антивирусную сеть с несколькими **Серверами**. В таком случае, серверное ПО устанавливается на несколько компьютеров одновременно.

Dr.Web Enterprise Сервер - служба, постоянно находящаяся в оперативной памяти. ПО **Enterprise Сервера** разработано для различных ОС (полный список поддерживаемых ОС см. в Приложении А).

Основные функции

Dr.Web Enterprise Server реализует следующие функции:

- инициализация установки антивирусных пакетов на выбранный компьютер или группу компьютеров,
- запрос номера версии антивирусного пакета, а также дат создания и номеров версий вирусных баз на каждом защищаемом компьютере,
- обновление содержимого каталога централизованной установки и каталога обновлений,

- обновление вирусных баз и исполняемых файлов антивирусных пакетов, а также исполняемых файлов компонентов антивирусной сети на защищаемых компьютерах.

Сбор информации о состоянии антивирусной сети

Enterprise Сервер обеспечивает сбор и протоколирование информации о работе антивирусных пакетов, передаваемой ему посредством ПО на защищаемых компьютерах **(Enterprise Агентов,** подробнее см. ниже). Протоколирование производится в общем журнале событий, реализованном в виде базы данных. В сети небольшого размера (не более 200-300 компьютеров) для ведения общего журнала событий может использоваться внутренняя база данных. Для обслуживания больших сетей предусмотрена возможность использования внешних баз данных.

Использование внутренней БД допустимо при подключении к **Серверу** не более 200-300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен **Enterprise Сервер**, и нагрузка по прочим задачам, выполняемым на данном компьютере, возможно подключение до 1000 станций.

В противном случае необходимо использовать внешнюю БД.

При использовании внешней БД и подключении к **Серверу** более 10000 станций рекомендуется выполнение следующих минимальных требований:

- процессор с частотой 3ГГц,
- оперативная память - от 4 Гб для **Enterprise Сервера**, от 8 Гб - для сервера БД,
- ОС семейства UNIX.

Сбору и протоколированию в общем журнале событий подлежит следующая информация:

- информация о версии антивирусных пакетов на защищаемых компьютерах,
- время и дата установки и обновления ПО антивирусной рабочей станции с указанием версии ПО,
- время и дата обновления вирусных баз с указанием их версий,
- информация о версии ОС, установленной на защищаемых компьютерах, типе процессора, расположении системных каталогов ОС и т. п.,
- конфигурация и режимы работы антивирусных пакетов (использование эвристических методов, список проверяемых типов файлов, действия при обнаружении компьютерных вирусов и т. п.),
- информация о вирусных событиях, в том числе название обнаруженного компьютерного вируса, дата обнаружения, предпринятые действия, результат лечения и т. п.

Enterprise Сервер оповещает администратора антивирусной сети о возникновении событий, связанных с работой антивирусной сети по электронной почте или с использованием стандартных широковещательных средств операционных систем Windows. Настройка событий, вызывающих направление сообщения, и прочих параметров оповещения описана в п. Настройка оповещений.

Интерфейс

Enterprise Сервер не имеет встроенного интерфейса. Базовые команды управления **Сервером** приведены в директории Управление Сервером.

Управление **Enterprise Сервером**, как правило, осуществляется при помощи **Центра Управления**, который служит внешним интерфейсом для **Сервера**.

Запуск и останов Dr.Web Enterprise Server

По умолчанию **Enterprise Сервер** запускается автоматически после установки и после каждой перезагрузки операционной системы.

Также вы можете запустить, перезапустить или остановить **Enterprise Сервер** одним из следующих способов:

Для ОС семейства UNIX

- При помощи соответствующей консольной команды (также см. Приложение H5. Dr.Web Enterprise Server):
  - Запуск:
    - для ОС FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh start
      ```
    - для ОС Linux и ОС Solaris:
      ```
      # /etc/init.d/drwcsd start
      ```
  - Перезапуск:
    - для ОС FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh restart
      ```
    - для ОС Linux и ОС Solaris:
      ```
      # /etc/init.d/drwcsd restart
      ```
  - Останов:
    - для ОС FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh stop
      ```
    - Для ОС Linux и ОС Solaris:
      ```
      # /etc/init.d/drwcsd stop
      ```
- Останов и перезапуск через **Центр Управления**:
  - В разделе **Администрирование**: перезапуск при помощи кнопки  , останов при помощи кнопки  (отсутствует под версией для ОС Solaris).

Для ОС Windows

- Общий случай:

- При помощи соответствующей команды, расположенной в меню **Пуск** → **Программы** → **Dr.Web Enterprise Server**.
- При помощи средств управления службами в разделе **Администрирование** на **Панели управления** ОС Windows.

◆ Останов и перезапуск через **Центр Управления**:
- В разделе **Администрирование**: перезапуск при помощи кнопки  , останов при помощи кнопки  .

◆ При помощи консольных команд, выполненных из подкаталога `bin` каталога установки **Сервера** (также см. Приложение H5. Dr.Web Enterprise Server):
- `drwcsd start` — запуск **Сервера**.
- `drwcsd restart` — полный перезапуск службы **Сервера**.
- `drwcsd stop` — нормальное завершение работы **Сервера**.

3.2. Dr.Web Enterprise Agent

Принцип работы

Антивирусная защита рабочих станций осуществляется антивирусными пакетами **Dr.Web**, разработанными для соответствующих ОС.

В составе **Антивируса Dr.Web ESS** эти пакеты работают под управлением **Enterprise Агента**, установленного на защищаемом компьютере и постоянно загруженного в память. При поддержке связи с **Enterprise Сервером**, администратор может централизованно настраивать **Антивирус** на рабочих станциях при помощи **Центра Управления**, задавать расписание антивирусных проверок, просматривать статистику и пр. информацию о работе антивирусных компонентов, запускать и останавливать антивирусное сканирование и т.п.

Enterprise Сервер загружает обновления и распространяет их на подключенные к нему **Агенты**. Таким образом, при помощи **Enterprise Агента** автоматически устанавливается, поддерживается и регулируется оптимальная стратегия защиты от вирусов независимо от уровня квалификации пользователей рабочих станций.

Однако, в случае временного отключения рабочей станции от антивирусной сети, **Enterprise Агент** использует локальную копию настроек, антивирусная защита на рабочей станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление вирусных баз и ПО не производится.

Обновление мобильных **Агентов** описано в п. Обновление мобильных Агентов Dr.Web Enterprise Agent.

Основные функции

Dr.Web Enterprise Agent реализует следующие функции:

- производит установку, обновление и настройку антивирусного пакета **Dr.Web**, запуск сканирования, а также выполнение других заданий, сформированных **Enterprise Сервером**;
- позволяет вызывать компоненты антивирусного пакета **Dr.Web** через специальный интерфейс;
- передает результаты выполнения заданий **Enterprise Серверу**;
- передает **Enterprise Серверу** сообщения о возникновении заранее оговоренных событий в работе антивирусного пакета.

Каждый **Enterprise Агент** подключен к **Enterprise Серверу** и входит в состав одной или нескольких зарегистрированных на этом **Сервере** групп (подробнее см. п. Системные и пользовательские группы). Передача информации между **Агентом** и указанным **Сервером** осуществляется по протоколу, используемому в локальной сети (TCP/IP, IPX или NetBIOS).

В дальнейшем защищаемый компьютер с установленным **Агентом**, в соответствии с его функциями в антивирусной сети, будет именоваться *рабочей станцией* антивирусной сети. Необходимо помнить, что по своим функциям в локальной сети такой компьютер может быть как рабочей станцией, так и сервером локальной сети.

Интерфейс управления в ОС Windows

Запущенный **Enterprise Агент** в среде ОС Windows выводит в область уведомления на панели задач значок  .

Возможные варианты значка **Агента** и соответствующие им состояния компонентов приведены в таблице 3-1.

Таблица 3-1. Возможные виды значка и соответствующие им состояния компонентов

Значок	Описание	Состояние
	Черный рисунок на зеленом фоне.	**Агент** работает нормально и связывается с **Сервером**.
	Красные стрелки на фоне значка.	Отсутствует подключение к **Серверу**.
	Восклицательный знак в желтом треугольнике на фоне значка.	**Агент** запрашивает перезагрузку компьютера, либо отключены компоненты **SelfPROtect** или **Spider Guard**
	Фон значка меняет цвет с зеленого на красный.	Произошла ошибка при обновлении компонентов пакета.
	Фон значка постоянно красного цвета.	**Агент** остановлен или не работает.

Значок	Описание	Состояние
	Фон значка желтого цвета.	**Агент** работает в мобильном режиме. Подробнее см. в п. Обновление мобильных Агентов Dr.Web Enterprise Agent

Некоторые функции управления **Агентом** и антивирусными компонентами на рабочей станцией доступны через контекстное меню значка **Агента**, представленное на рисунке 3-1.

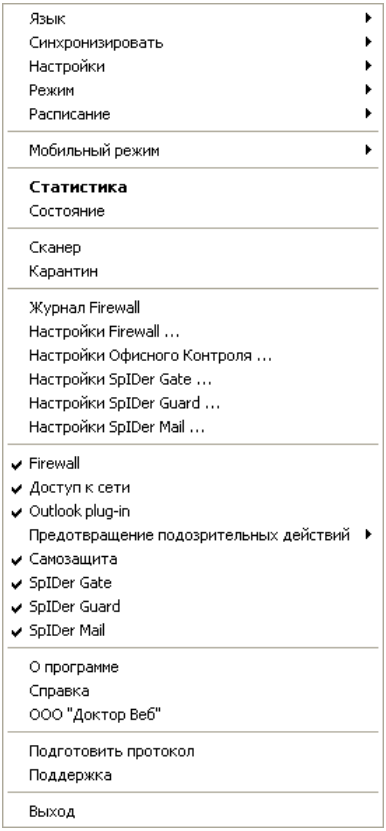


Рисунок 3-1. Контекстное меню Enterprise Агента

Круг настроек, доступных через контекстное меню **Агента**, зависит от конфигурации рабочей станции, заданной на **Enterprise Сервере**, а также прав пользователя на рабочей станции.

Состав параметров **Enterprise Агента**, антивирусного пакета и описание соответствующих им функций для управления рабочей станцией приведены в справке **Enterprise Агента**.

Информация о настройках **Enterprise Агента**, задаваемых через **Enterprise Сервер**, приведена в п. Настройка Dr.Web Enterprise Agent.

Запуск и останов Dr.Web Enterprise Agent под ОС Windows

Команда **Выход** в контекстном меню **Агента** останавливает работу только GUI **Агента** (см. Интерфейс управления в ОС Windows) и удаляет значок из области уведомлений панели задач. **Агент** при этом продолжает работу.

Чтобы остановить работу самого **Агента**, выполните в командной строке:

```
net stop drwagntd
```

Останавливать **Агент** не рекомендуется, так как при этом ПО антивирусного пакета не обновляется, а **Сервер** не получает информацию о состоянии рабочей станции, хотя постоянная защита компьютера при этом не отключается.

Агент автоматически запустится после перезагрузки компьютера. Чтобы запустить **Агент** без перезагрузки компьютера, выполните в командной строке:

```
net start drwagntd
```

3.3. Центр Управления Dr.Web

Для управления антивирусной сетью в целом (включая изменение ее состава и структуры), всеми ее компонентами, а также для настройки **Enterprise Сервера** служит **Центр Управления Dr.Web**.

Для корректной работы **Центра Управления** под веб-браузером Windows Internet Explorer необходимо в настройках веб-браузера добавить адрес **Центра Управления** в доверенную зону: **Tools (Сервис)** → **Internet Options** (**Свойства обозревателя)** → **Security** (**Безопасность**) → **Trusted Sites (Надежные узлы**).

Для корректной работы **Центра Управления** под веб-браузером Chrome необходимо в настройках веб-браузера включить cookies.

Подключение к Dr.Web Enterprise Server

На любом компьютере, имеющем сетевой доступ к **Enterprise Серверу**, **Центр Управления** доступен по адресу:

`http://`*<Адрес_Сервера>*`:9080`

или

`https://`*<Адрес_Сервера>*`:9081`

где в качестве *<Адрес_Сервера>* укажите IP-адрес или доменное имя компьютера, на котором установлен **Enterprise Сервер**.

Номера портов для соединения по http и для защищенного соединения по https различны: 9080 и 9081 соответственно.

В диалоговом окне запроса на авторизацию введите имя и пароль администратора (имя администратора с полными правами по умолчанию – **admin**, пароль – пароль, который вы задавали при установке **Сервера**).

При загрузке по https (защищенное соединение с использованием SSL), браузер запросит подтверждение сертификата, используемого **Сервером**. При этом запрос подтверждения может сопровождаться выражением недоверия к сертификату и информацией о подозрениях на его ошибочность. Данная информация выдается пользователю, поскольку сертификат неизвестен браузеру. Для возможности загрузки **Центра Управления** следует принять предлагаемый сертификат. Иначе загрузка будет невозможна.

В некоторых версиях браузеров, например, **FireFox 3** и выше при загрузке по https будет получена ошибка, и **Центр Управления** не будет загружен. В таком случае на странице об ошибке следует выбрать пункт **Добавить сайт в список исключений** (под сообщением об ошибке). После этого будет разрешен доступ к **Центру Управления**.

Интерфейс Центра Управления Dr.Web

Окно **Центра Управления** (см. рис. 3-2) делится на *заголовок* и *рабочую область*.

Заголовок содержит:

- логотип продукта **Dr.Web Enterprise Security Suite**, при нажатии на который открывается начальное окно **Центра Управления** (соответствует выбору пункта **Антивирусная сеть** главного меню),

- главное меню,
- имя учетной записи администратора, под которой был осуществлен вход в **Центр Управления**,
- кнопку **Выход** для завершения текущего сеанса работы с **Центром Управления**.

Если в **Центре Управления** включена автоматическая авторизации, то при нажатии кнопки **Выход** информация об имени и пароле администратора удаляется.

При следующем входе в **Центр Управления** необходимо повторить стандартную процедуру авторизации с указанием имени и пароля. При этом, в случае включенной автоматической авторизации, указанные имя и пароль запоминаются в данном веб-браузере и авторизация в **Центре Управления** будет проходить автоматически (без ввода имени и пароля) до следующего нажатия кнопки **Выход**.

Рабочая область отвечает за основной функционал **Центра Управления**. Она состоит из двух или трех панелей, в зависимости от осуществляемых действий. При этом реализуется вложенность функционала панелей слева-направо:

- *управляющее меню* всегда расположено в левой части окна,
- в зависимости от пункта, выбранного в управляющем меню, отображается одна или две дополнительные панели. В последнем случае, в правой части выводятся свойства или настройки элементов центральной панели.

Язык интерфейса задается отдельно для каждой учетной записи администратора (см. п. Управление учетными записями администраторов).

Главное Меню

В главном меню **Центра Управления** доступны следующие пункты:

- Администрирование,
- Антивирусная Сеть,
- Настройки,
- Связи,
- Помощь,
- а также Панель поиска.

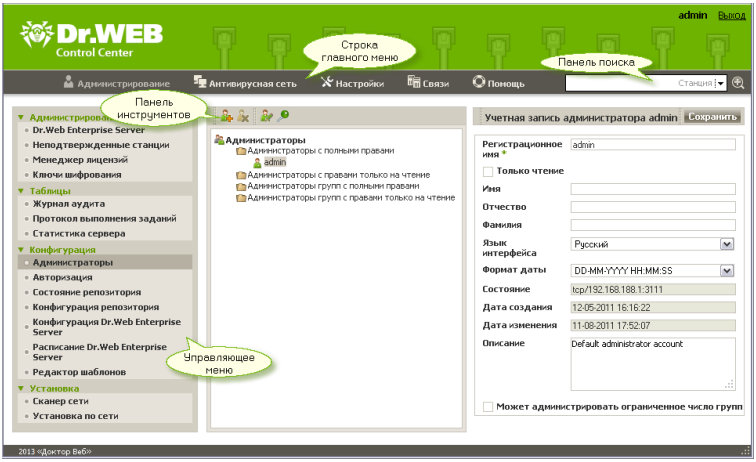


Рисунок 3-2. Окно Центра Управления Dr.Web. Нажмите на пункт главного меню для перехода к описанию

Панель поиска

Для облегчения поиска нужного элемента служит *панель поиска*, расположенная на правой границе главного меню **Центра Управления**. Панель позволяет производить поиск как групп, так и отдельных станций в соответствии с указанными параметрами.

Для поиска станций или групп станций:

1. В выпадающем списке панели поиска выберите критерий поиска:
   - **Станция** - для поиска станций по названию,
   - **Группа** - для поиска групп по названию,
   - **ID** - для поиска групп и станций по уникальным идентификаторам,
   - **Описание** - для поиска групп и станций по их описанию,
   - **IP адрес** - для поиска станций по IP адресу.
2. Введите строку, в соответствии с которой будет производиться поиск. При этом возможно задание:
   - конкретной строки для полного совпадения с параметром поиска,
   - маски искомой строки: допускаются символы * и ?.
3. Нажмите клавишу ENTER для начала поиска.
4. В иерархическом списке будут отображены все найденные элементы, в соответствии с параметрами поиска, при этом:
   - если осуществлялся поиск станции, то будут выведены вхождения станции во все группы,
   - если в результате поиска не найден ни один элемент, будет отображен пустой иерархический список с сообщением **Поиск не дал результатов**.

Также вы можете воспользоваться опцией **Расширенный поиск**.

Для расширенного поиска выполните следующие действия:

1. Нажмите на кнопку  на панели поиска.
2. На открывшейся панели **Поиск групп и станций** укажите следующие параметры:
   - **Название станции** - введите строку, в соответствии с которой будет производится поиск по названиям станций.

- **Название группы** - введите строку, в соответствии с которой будет производится поиск по названиям групп.
- **ID** - введите строку, в соответствии с которой будет производиться поиск по уникальным идентификаторам групп и станций.
- **IP адрес станции** - введите строку, в соответствии с которой будет производится поиск по IP адресам станций.
- **Описание** - задайте строку описания, в соответствии с которым будет производиться поиск элемента.

Вы можете задать значения для одного, нескольких или всех полей расширенного поиска.

Если вы зададите несколько полей, будет производится поиск всех элементов, удовлетворяющих хотя бы одному из введенных значений (объединение значений для поиска по принципу *ИЛИ*).

3. После задания значений необходимых полей поиска, нажмите на кнопку **Найти**.
4. В иерархическом списке будут отображены все найденные элементы или сообщение **Поиск не дал результатов**.

3.3.1. Администрирование

Выберите в главном меню **Центра Управления** пункт **Администрирование**. Для просмотра и редактирования информации в открывшемся окне служит управляющее меню, расположенное в левой части окна.

Управляющее меню содержит следующие пункты:

1. **Администрирование**

- **Dr.Web Enterprise Server** — открывает панель, с помощью которой вы можете просмотреть основную информацию о **Сервере**, а также перезапустить его при помощи кнопки  или остановить при помощи кнопки  (отсутствует под версией для ОС Solaris), расположенных в правой верхней части панели;
- **Неподтвержденные станции** — открывает панель со списком неподтвержденных станций (см. п. Политика подключения станций);
- **Менеджер лицензий** — позволяет управлять лицензионными ключевыми файлами **Сервера** и **Агентов** (см. п. Менеджер лицензий);
- **Ключи шифрования** — позволяет экспортировать (сохранить локально) открытый и закрытый ключи шифрования.

2. **Таблицы**
   - **Журнал аудита** — просмотр журнала событий и изменений, осуществленных при помощи **Центра Управления**;
   - **Протокол выполнения заданий** — содержит список назначенных заданий на **Сервере** с пометкой о выполнении и комментариями;
   - **Статистика сервера** — содержит статистику работы данного **Сервера**.
3. **Конфигурация**
   - **Администраторы** — открывает панель управления учетными записями администраторов антивирусной сети (см. п. Управление учетными записями администраторов);
   - **Авторизация** — открывает панель управления аутентификацией администраторов в **Центре Управления** (см. п. Аутентификация администраторов);
   - **Состояние репозитория** — проверить состояние репозитория: дату последнего обновления компонентов репозитория и их состояние (см. п. Состояние репозитория);

- **Конфигурация репозитория** — открывает окно редактора репозитория (см. п. Редактор конфигурации репозитория);
- **Конфигурация Dr.Web Enterprise Server** — открывает панель основных настроек **Сервера** (см.п. Настройка конфигурации Dr.Web Enterprise Server);
- **Расписание Dr.Web Enterprise Server** — открывает панель настройки расписания заданий **Сервера** (см. п. Настройка расписания Dr.Web Enterprise Server);
- **Редактор шаблонов** — открывает окно редактора шаблонов оповещений (см. п. Настройка оповещений).

4. **Установка**
   - **Сканер сети** — позволяет задавать список сетей и проводить как сканирование сетей на наличие установленного антивирусного программного обеспечения, определяя состояние защиты компьютеров, так и установку последнего (см. п. Сканер сети);
   - **Установка по сети** — позволяет упростить установку ПО **Агента** на конкретные рабочие станции (см. п. Установка Dr.Web Enterprise Agent с использованием Центра Управления Dr.Web).

3.3.2. Антивирусная сеть

Выберите в главном меню **Центра Управления** пункт **Антивирусная сеть**. Для просмотра и редактирования информации в открывшемся окне служит управляющее меню, расположенное в левой части окна.

Иерархический список

В центральной части окна расположен иерархический список антивирусной сети. Иерархический список (каталог) антивирусной сети отображает древовидную структуру элементов антивирусной сети. Узлами данной структуры являются группы и входящие в них станции.

Вы можете выполнять следующие действия над элементами списка:

- нажмите левой кнопкой мыши на название группы или станции для отображения управляющего меню (в левой части окна) соответствующего элемента;
- нажмите левой кнопкой мыши на значок группы для отображения содержимого группы.

Для выбора нескольких станций и групп иерархического списка используйте выделение мышью при нажатых клавишах CTRL или SHIFT.

Вид значка элемента списка зависит от типа или состояния этого элемента (см. таблицу 3-2).

Таблица 3-2. Значки элементов иерархического списка

Знак	Описание	Значение
Группы		
	желтая папка	Группы, всегда отображаемые в иерархическом списке.
	белая папка	Отображение групп в иерархическом списке может быть отключено, если эти группы пустые.
Рабочие станции		
	зеленый значок	Доступная рабочая станции с установленным антивирусным ПО.
	серый значок	Станция недоступна.
	перечеркнутый значок	Антивирусное ПО на станции деинсталлировано.

Если заданы персональные настройки для станции или группы (или в группе есть станции с персональными настройками), то в иерархическом списке на значке этой группы или станции будет отображаться значок . Например, если персональные настройки заданы для доступной рабочей станции с установленным антивирусным ПО, то ее значок будет выглядеть следующим образом: .

Для отображения значков с персональными настройками выберите пункт **Настройки вида дерева** на панели инструментов и установите флаг **Отображать персональные настройки**.

Управление элементами каталога антивирусной сети осуществляется при помощи панели инструментов иерархического списка.

Панель инструментов

Панель инструментов иерархического списка содержит следующие элементы:

Общие. Позволяет управлять общими параметрами иерархического списка. Выберите соответствующий пункт в выпадающем списке:

Удалить отмеченные объекты. Позволяет удалить объекты иерархического списка. Для этого выберите в списке элемент или несколько элементов и нажмите **Удалить отмеченные объекты**.

Редактировать. Открывает панель свойств станции или группы в правой части окна **Центра Управления**.

Установить эту группу первичной. Позволяет установить выбранную в иерархическом списке группу в качестве первичной для всех входящих в нее станций.

Назначить первичную группу. Позволяет назначить для выделенных в списке станций первичную группу. При

этом, если в иерархическом списке выделена группа, то для всех входящих в нее станций будет назначена указанная первичная группа.

 **Объединить станции**. Позволяет объединять станции под единой учетной записью в иерархическом списке. Может использоваться в случае, когда одна и та же станция была зарегистрирована под разными учетными записями (см. п. Объединение станций).

 **Убрать индивидуальные настройки объекта**. Позволяет удалить персональные настройки выбранного в списке объекта. В этом случае, настройки будут унаследованы от первичной группы. Если в иерархическом списке выделена группа, то настройки будут удалены у всех входящих в нее станций.

 **Импорт ключа**. Позволяет задать ключ для станции или группы.

 **Послать сообщение станциям**. Позволяет отправить пользователям сообщение произвольного содержания (см. п. Отправка сообщений пользователю).

 **Деинсталлировать Dr.Web Enterprise Agent**. Удаляет **Агента** и антивирусное ПО с выбранной станции или группы станций.

 **Установить Dr.Web Enterprise Agent**. Открывает Сканер сети для установки **Агента** на выбранные станции. Данный пункт активен только при выборе новых подтвержденных станций или станций с деинсталлированным **Агентом**.

 **Восстановить удаленные станции**. Позволяет восстановить ранее удаленные станции (также см. п. Удаление и восстановление станции). Данный пункт активен только при выборе станций из подгруппы **Deleted** в группе **Status**.

 **Добавить станцию или группу**. Позволяет создать новый элемент антивирусной сети. Для этого выберите соответствующий пункт в выпадающем списке:

 **Создать станцию**. Позволяет создать новую станцию (см. п. Создание новой учетной записи).

 **Создать группу**. Позволяет создать новую группу (см. п. Создание и удаление групп).

 **Экспортировать данные**. Позволяет записать общие данные о станциях антивирусной сети в файл формата CSV, HTML или XML. Требуемый формат экспорта выбирается в выпадающем списке.

 **Настроить отображение группы**. Позволяет изменять параметры отображения групп. Для этого выберите группу в иерархическом списке и укажите в выпадающем списке один из следующих вариантов (при этом будет изменяться значок группы, см. таблицу 3-2):

 **Скрывать группу** - означает, что отображение группы в иерархическом списке будет всегда отключено.

 **Скрывать, если пустая** - означает, что отображение группы в иерархическом списке будет отключено, если эта группа пустая (не содержит станций).

 **Показывать** - означает, что группа всегда будет отображаться в иерархическом списке.

 **Управление компонентами**. Позволяет управлять антивирусными компонентами на рабочих станциях. Для этого выберите в выпадающем списке один из следующих вариантов:

 **Обновить все компоненты**. Предписывает обновить все установленные компоненты антивируса, например, в ситуации когда **Агент** долгое время не подключался к **Серверу** и т.д. (см. п. Ручное обновление компонентов Dr.Web Enterprise Security Suite);

 **Обновить сбойные компоненты**. Предписывает принудительно синхронизировать компоненты, обновление которых прошло с ошибкой;

 **Прервать запущенные**. Предписывает остановить запущенные на станции сканирования. Подробное описание процедуры прерывания сканирований по типам приведено в п. Прерывание работы запущенных компонентов по типам.

Сканировать. Позволяет провести сканирование станции в одном из режимов, выбираемых в выпадающем списке (см. также п. Запуск сканирования рабочей станции):

Dr.Web Сканер для Windows. Быстрое сканирование. В данном режиме производится сканирование следующих объектов:

- оперативная память,
- загрузочные секторы всех дисков,
- объекты автозапуска,
- корневой каталог загрузочного диска,
- корневой каталог диска установки ОС Windows,
- системный каталог ОС Windows,
- папка `Мои Документы`,
- временный каталог системы,
- временный каталог пользователя.

Dr.Web Сканер для Windows. Полное сканирование. В данном режиме производится полное сканирование всех жестких дисков и сменных носителей (включая загрузочные секторы).

Dr.Web Сканер для Windows. Выборочное сканирование. Данный режим предоставляет возможность выбрать любые папки и файлы для последующего сканирования.

Dr.Web Enterprise Сканер для Windows. В данном режиме осуществляется выборочное сканирование при помощи **Dr.Web Enterprise Сканера**.

Dr.Web Enterprise Сканер для Mac OS X. Для сканирования станций, работающих под ОС семейства Mac OS X, согласно заданным параметрам сканирования.

Dr.Web Enterprise Сканер для Unix. Для сканирования станций, работающих под ОС семейства UNIX, согласно заданным параметрам сканирования.

Настройки вида дерева позволяют изменять внешний вид списка:

- для групп:
  - **Членство во всех группах**. Задает дублирование станции в списке, при вхождении ее в несколько групп одновременно (только для групп, идущих под значком белой папки - см. табл. 3-2). Если флаг поставлен - будут показаны все вхождения станции. Если снят - станция будет отображена в списке единожды.
  - **Показывать скрытые группы**. Отобразить все группы, входящие в антивирусную сеть. При снятии данного флага пустые группы (не содержащие станции) будут скрыты. Это может быть удобно для исключения излишней информации, например, при наличии большого количества пустых групп.
- для станций:
  - **Показывать идентификатор станции**. Задает отображение станций в иерархическом списке по уникальным идентификаторам.
  - **Показывать название станции**. Задает отображение имен (названий) станций, если таковые заданы.
  - **Показывать адрес станции**. Задает отображение станций в иерархическом списке по IP-адресам.
  - **Показывать сервер станции**. Задает отображение имен или адресов антивирусных **Серверов**, к котором подключены станции.
- для всех элементов:
  - **Отображать персональные настройки**. Включает/выключает маркер на значках станций и групп, обозначающий наличие персональных настроек.
  - **Показывать описания**. Включает/выключает отображение описаний групп и станций (описания задаются в свойствах элемента).
  - **Показывать число станций**. Включает/выключает отображение количества станций для всех групп антивирусной сети.

Панель свойств

Панель свойств служит для отображения свойств и настроек рабочих станций и групп.

Для отображения панели свойств:

1. В иерархическом списке выделите станцию или группу и нажмите  **Общие** →  **Редактировать** на панели инструментов.
2. В правой части окна **Центра Управления** откроется панель со свойствами рабочей станции. Данная панель содержит следующие группы настроек: **Общие**, **Конфигурация**, **Группы**, **Расположение**. Подробное описание данных настроек приведено в п. Настройка конфигурации рабочей станции.

3.3.3. Настройки

Выберите в главном меню **Центра Управления** пункт **Настройки**.

Все настройки данного раздела будут действительны только для текущей учетной записи администратора.

Управляющее меню, расположенное в левой части окна, содержит следующие элементы:

- **Моя учетная запись**.
- **Интерфейс**.

Моя учетная запись

При помощи данного раздела осуществляется управление текущей учетной записью администратора антивирусной сети (см. также п. Управление учетными записями администраторов).

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

При необходимости отредактируйте следующие параметры:

- **Регистрационное имя** администратора - логин для доступа к **Центру Управления**.
- Установите флаг **Только чтение** для ограничения прав доступа.
- ФИО администратора.
- **Язык** интерфейса, используемый данным администратором.
- **Формат даты**, используемый данным администратором при редактировании настроек, содержащих даты. Доступны следующие форматы:
  - европейский: `DD-MM-YYYY HH:MM:SS`
  - американский: `MM/DD/YYYY HH:MM:SS`
- **Описание** учетной записи.
- Для учетной записи администратора групп установите флаг **Может администрировать ограниченное число групп** для задания доступных групп.
- Для смены пароля нажмите на кнопку **Новый пароль** на панели инструментов.

Следующие параметры доступны только для чтения:

- Даты создания учетной записи и последнего изменения ее параметров,
- **Состояние** - отображает сетевой адрес последнего подключения под данной учетной записью.

После изменения параметров нажмите на кнопку **Сохранить**.

Для учетных записей с правами только на чтение для редактирования доступны только следующие поля:

- **Язык интерфейса**,
- **Описание**.

Интерфейс

Настройки вида дерева

Параметры данного подраздела позволяют изменять внешний вид списка и аналогичны настройкам, расположенным на панели инструментов пункта  в разделе главного меню **Антивирусная сеть**:

- для групп:
  - **Членство во всех группах**. Задает дублирование станции в списке, при вхождении ее в несколько групп одновременно (только для групп, идущих под значком белой папки - см. табл. 3-2). Если флаг поставлен - будут показаны все вхождения станции. Если снят - станция будет отображена в списке единожды.
  - **Показывать скрытые группы**. Отобразить все группы, входящие в антивирусную сеть. При снятии данного флага пустые группы (не содержащие станции) будут скрыты. Это может быть удобно для исключения излишней информации, например, при наличии большого количества пустых групп.
- для станций:
  - **Показывать идентификатор станции**. Задает отображение станций в иерархическом списке по уникальным идентификаторам.
  - **Показывать название станции**. Задает отображение имен (названий) станций, если таковые заданы.

- **Показывать адрес станции**. Задает отображение станций в иерархическом списке по IP-адресам.
- **Показывать сервер станции**. Задает отображение имен или адресов **Enterprise Серверов**, к котором подключены станции.

◆ для всех элементов:

- **Отображать персональные настройки**. Включает/выключает маркер на значках станций и групп, обозначающий наличие персональных настроек.
- **Показывать описания**. Включает/выключает отображение описаний групп и станций (описания задаются в свойствах элемента).

Сканер сети

Для работы **Сканера сети** необходимо, чтобы был установлен подключаемый модуль Dr.Web Browser-Plugin

Параметры данного подраздела позволяют задать настройки Сканера сети по умолчанию.

Для запуска самого **Сканера сети** выберите в главном меню **Центра Управления** пункт **Администрирование**, в управляющем меню (панель слева) выберите пункт **Сканер сети**.

Задайте следующие параметры **Сканера сети**:

1. В поле ввода **Сети** задайте перечень сетей в формате:
   - через дефис (например, `10.4.0.1-10.4.0.10`),
   - через запятую и пробел (например, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - с использование префикса сети (например, `10.4.0.0/24`).
2. При необходимости измените **Порт** и значение параметра **Тайм-аут**.

3. Для сохранения значений по умолчанию нажмите на кнопку **Сохранить**. В дальнейшем, при использовании Сканера сети данные параметры будут заданы автоматически.

Временной интервал

В данном подразделе задаются настройки временного интервала, в пределах которого отображаются статистические данные (см. п. Просмотр результатов работы и итоговой статистики по рабочей станции):

- В выпадающем списке **Интервал просмотра статистики** задается временной интервал, который будет установлен по умолчанию для всех разделов статистических данных.

  При первом открытии страницы статистика будет отображаться за данный временной интервал. При необходимости можно изменить временной интервал непосредственно в самих разделах статистики.

- Для того чтобы в разделах статистики сохранялся последний заданный для них интервал, установите флаг **Сохранять последний интервал просмотра статистики**.

  Если флаг установлен, то при первом открытии страницы отображается статистика за последний период, который был выбран в Веб-браузере.

  Если флаг снят, то при первом открытии страницы отображается статистика за период, заданный в разделе **Интервал просмотра статистики**.

Авторизация

Установите флаг **Автоматическая авторизация**, чтобы разрешить в текущем веб-браузере автоматическую авторизацию для всех **Центров Управления Dr.Web** с аналогичным именем пользователя и паролем администратора.

После установки данного флага, посредством расширения **Dr.Web Browser-Plugin**, будут сохранены имя и пароль, которые администратор укажет при следующей авторизации в **Центре Управления**.

Для функционирования автоматической авторизации необходимо, чтобы был установлен подключаемый модуль Dr.Web Browser-Plugin.

В дальнейшем, при открытии любого **Центра Управления Dr.Web** в данном веб-браузере, авторизация будет проходить автоматически при наличии на **Сервере** пользователя с такими именем и паролем. Если имя и пароль не совпадают (например, такой пользователь отсутствует или у пользователя с таким именем другой пароль), будет выдано стандартное окно авторизации **Центра Управления**.

При нажатии кнопки **Выход** в заголовке интерфейса **Центра Управления** удаляется информация об имени и пароле администратора.

При следующем входе в **Центр Управления** необходимо повторить стандартную процедуру авторизации с указанием имени и пароля. При этом, в случае включенной автоматической авторизации, указанные имя и пароль запоминаются в данном веб-браузере, и авторизация в **Центре Управления** будет проходить автоматически (без ввода имени и пароля) до следующего нажатия кнопки **Выход**.

3.3.4. Связи

Выберите в главном меню **Центра Управления** пункт **Связи**. Для выбора просматриваемой информации служит управляющее меню, расположенное в левой части окна.

Администрирование

Раздел **Администрирование** управляющего меню содержит пункт **Связи**, который служит для управления связями между **Серверами** в многосерверной антивирусной сети (см. п. Особенности сети с несколькими Серверами).

В иерархическом списке приведены все **Enterprise Серверы**, связанные с данным **Сервером**.

Создание новых межсерверных связей описано в разделе Настройка связей между Серверами.

Таблицы

В разделе **Таблицы** управляющего меню приведена информация о работе антивирусной сети, полученная от других **Серверов** (см. п. Особенности сети с несколькими Серверами).

Для просмотра сводных таблиц с данными по другим **Серверам** нажмите на соответствующий пункт раздела **Таблицы**.

3.3.5. Помощь

Выберите в главном меню **Центра Управления** пункт **Помощь**.

Управляющее меню, расположенное в левой части окна, содержит следующие элементы:

1. **Общие**
   - **Форум** - перейти на форум компании **«Доктор Веб»**.
   - **Задать вопрос** - перейти на страницу **Технической поддержки «Доктор Веб»**.
   - **Прислать вирус** - открыть форму для отправки вируса в лабораторию **«Доктор Веб»**.
   - **wiki** - перейти на страницу Википедии - базы знаний, посвященной продуктам компании **«Доктор Веб»**.

- **Сообщить об ошибке в работе Родительского контроля** - открыть форму для отправки сообщения о ложном срабатывании или пропуске вредных ссылок в модуле **Родительского контроля**.

2. **Документация**
   - **Руководство администратора** - открыть документацию администратора в формате HTML.
   - **Руководство пользователя** - открыть документацию пользователя в формате HTML.
   - **XML Web API** - открыть документацию администратора по XML Web API (см. также Приложение N. Интеграция XML Web API и Dr.Web Enterprise Security Suite) в формате HTML.
   - **Примечания к выпуску** - открыть раздел примечаний к выпуску **Dr.Web Enterprise Security Suite** для установленной у вас версии.

3.4. Компоненты Центра Управления Dr.Web

3.4.1. Сканер сети

В состав **Enterprise Сервера** входит **Сканер сети**.

Не рекомендуется запускать **Сканер сети** под ОС Windows 2000 и младше: обзор сети может быть неполным.

Работа **Сканера сети** гарантируется под ОС семейства UNIX или ОС Windows XP и старше.

Для работы **Сканера сети** необходимо, чтобы был установлен подключаемый модуль Dr.Web Browser-Plugin

Сканер сети реализует следующие функции:

- Сканирование (обзор) сети с целью обнаружения рабочих станций.
- Определение наличия **Enterprise Агента** на станциях.
- Установка **Enterprise Агента** на обнаруженные станции по указанию администратора. Установка **Enterprise Агента** подробно описана в п. Установка Dr.Web Enterprise Agent с использованием Центра Управления Dr.Web.

Для сканирования (обзора) сети выполните следующие действия:

1. Откройте окно **Сканера сети**. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Сканер Сети**. Откроется окно **Сканера сети**.
2. При необходимости установите флаг **Быстрое сканирование** для выполнения сканирования в ускоренном режиме.
3. Укажите в поле ввода **Сети** перечень сетей в формате:
   - через дефис (например, `10.4.0.1-10.4.0.10`),
   - через запятую и пробел (например, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - с использованием префикса сети (например, `10.4.0.0/24`).
4. Укажите порт, по которому следует обращаться к **Агенту**.
5. При необходимости измените значение тайм-аута в секундах, в течение которого будет ожидаться ответ от опрашиваемых станций.
6. Установите флаг **Показывать название станции**, чтобы для найденных компьютеров сети отображался не только их IP-адрес, но и их доменное имя.

   Если станция не зарегистрирована на DNS-сервере, то будет выводится только ее IP-адрес.

7. Установите флаг **Соотносить со списком станций из БД,** чтобы включить синхронизацию результатов поиска

Сканера сети со списком станций, сохраненным в БД **Сервера**. Если данный флаг установлен, то в списке найденных станций сети будут отображаться также те станции, которые числятся в БД **Сервера**, но не были обнаружуены **Сканером сети** при текущем поиске, например, в случае, если на этих станциях установлен firewall, блокирующий передачу пакетов для установки TCP-соединения.

При синхронизации результатов поиска **Сканера сети** с данными БД **Сервера**, приоритет отдается данным из БД **Сервера**. Т.е. при несовпадении статуса станции, полученного в результате поиска, и записанного в БД, будет установлен статус, записанный в БД.

8. Нажмите на кнопку **Запустить сканер**. После этого начнется сканирование сети.
9. В процессе сканирования сети в окно будет загружаться каталог (иерархический список) компьютеров с указанием наличия на них **Enterprise Агента**.

   Разверните элементы каталога, соответствующие рабочим группам (доменам). Все элементы каталога, соответствующие рабочим группам и отдельным станциям помечаются различными значками, значение которых приведено ниже.

Таблица 3-3. Возможные виды значков

Знак	Описание
Рабочие группы	
	Рабочие группы, содержащие в числе прочих компьютеры, на которые можно установить антивирус **Dr.Web ESS**.
	Остальные группы, включающие компьютеры с установленным антивирусным ПО или недоступные по сети.
Рабочие станции	
	Обнаруженная станция числится в базе и активна (активные станции с установленным антивирусным ПО).
	Обнаруженная станция числится в базе в таблице удаленных станций.

Знак	Описание
	Обнаруженная станция не числится в базе (на компьютере нет антивирусного ПО).
	Обнаруженная станция не числится в базе (станция подключена к другому **Серверу**).
	Обнаруженная станция числится в базе, не активна и порт закрыт.

Элементы каталога, соответствующие станциям со значками  или  , можно дополнительно развернуть и ознакомиться с составом установленных компонентов.

При нажатии на значок  компонента станции, подключенной к данному **Серверу**, будет выведено окно настроек данного компонента.

Взаимодействие с Dr.Web Enterprise Agent

Инструмент **Сканер сети** включен в состав **Dr.Web ESS** начиная с версии **4.44**.

Сканер сети способен определить наличие на станции **Агента** только версии **4.44** и старше, но не способен взаимодействовать с **Агентами** более ранних версии.

Установленный на защищаемой станции **Агент** версии **4.44** и старше осуществляют обработку соответствующих запросов **Сканера сети**, поступающих на определенный порт. По умолчанию используется порт `udp/2193`, однако, для совместимости с ПО предыдущих версий, также поддерживается порт `udp/2372`. Соответственно, эти же порты по умолчанию предлагается опрашивать и в **Сканере сети**. **Сканер сети** делает вывод о наличии или отсутствии **Агента** на станции исходя из возможности обмена информацией (запрос-ответ) через вышеуказанный порт.

Если на станции установлен запрет (например, посредством файервола) приема пакетов на `udp/2193`, то **Агент** не может быть обнаружен, а, следовательно, с точки зрения **Сканера сети**, считается, что **Агент** на станции не установлен.

Быстрое сканирование

При включенной опции **Быстрое сканирование** осуществляется следующая последовательность действий:

1. На машины сети рассылаются ping-запросы.
2. Только для машин, ответивших на ping-запросы, осуществляется параллельный опрос с целью обнаружения **Агентов**.
3. Процедура определения наличия **Агента** осуществляется по общим правилам.

Ping-запросы могут блокироваться из-за сетевых политик (например, из-за настроек файервола).

Например:

Если в ОС Windows Vista и старше в настройках сети была задана **Общедоступная сеть**, то ОС будет блокировать все ping-запросы.

При обычном сканировании не рассылаются ping-запросы, а последовательно опрашиваются все станции на наличие **Агента**. Этот метод может использоваться как дополнение к быстрому сканированию в случае, если в сети есть станции, на которых заблокированы ping-запросы.

Быстрое сканирование осуществляется параллельно, обычное - последовательно.

Скорость работы **Сканера сети** значительно отличается. Максимальное время сканирования рассчитывается следующим образом:

- при обычном сканировании: <*N*> * <*timeout*>,
- при быстром сканировании: <*N*>/40 + 2*<*timeout*>,

где: <*N*> - количество станций, <*timeout*> - значение, задаваемое в поле **Тайм-аут**.

3.4.2. Менеджер лицензий

В состав **Enterprise Сервера** входит **Менеджер лицензий**. Данный компонент облегчает управление лицензионными ключевыми файлами **Сервера** и **Агентов**.

Для того чтобы открыть окно **Менеджера лицензий**, выберите в главном меню **Центра Управления** пункт **Администрирование,** в открывшемся окне выберите пункт управляющего меню (панель слева) **Менеджер лицензий**.

Главное окно **Менеджера лицензий** содержит иерархический список, включающий:

- Ключи сервера. Элементами данного пункта являются учетные записи, содержащие лицензионные ключи **Сервера.** При этом только одна из учетных записей активна (используется **Сервером** в данный момент).
- Ключи агента. Элементами данного пункта являются учетные записи, содержащие лицензионные ключи **Агента**. Каждый лицензионный ключ может быть назначен для нескольких групп или станций, которые отображаются в окне **Менеджера лицензий** как вложенные элементы учетной записи ключа.

Для управления лицензионными ключами используются элементы Панели инструментов:

Добавить ключ - позволяет добавить новую запись о ключевом файле. Для этого выберите соответствующий пункт выпадающего меню:

Добавить ключ сервера - для добавления нового ключевого файла **Сервера**.

Добавить ключ агента - для добавления нового ключевого файла **Агентов**.

Удалить ключ - позволяет удалить учетные записи ключевых файлов.

> Нельзя удалить учетную запись **Агентского** ключа, назначенного для группы **Everyone**, и текущую активную запись ключевого файла **Сервера**.

Редактировать - для просмотра информации о лицензии, ее активации (только для **Сервера**) и, при необходимости, замены ключевого файла (только для **Агента**). Данный пункт активен, только если в главном окне выбрана учетная запись ключевого файла для **Сервера** или **Агента**.

Распространить эти настройки на другой объект - позволяет назначить выбранный ключ на заданную группу или станцию, которые указываются в открывающемся списке. Данный пункт активен, только если в главном окне выбрана учетная запись ключевого файла для **Агента**.

Экспортировать ключ - позволяет сохранить локальную копию файла для выбранного в списке ключа.

Пример замены ключей

Если вы хотите полностью заменить (например, обновить закончившиеся лицензии) все лицензионные ключи компонентов антивирусной сети (как **Сервера**, так и **Агента**), выполните следующую последовательность действий в **Менеджере лицензий**:

1. Добавьте новый ключ Сервера.
2. Активируйте новый ключ Сервера.
3. Удалите старый ключ Сервера.
4. Замените лицензионный ключ Агента для группы **Everyone** и, при необходимости, для остальных групп и станций, для которых были назначены лицензионные ключи персонально.

3.4.2.1. Ключи Dr.Web Enterprise Server

При помощи Менеджера лицензий вы можете осуществлять следующие действия над лицензионными ключами Dr.Web Enterprise Server:

1. Просматривать информацию о лицензии.
2. Добавлять новые лицензионные ключи Сервера.
3. Изменять активность лицензии Сервера.
4. Удалять лицензионные ключи Сервера.

Просмотр информации о лицензии

Для того чтобы просмотреть сводную информацию о лицензии, выберите в главном окне **Менеджера лицензий** учетную запись, информацию о которой вы хотите просмотреть, и нажмите на кнопку **Редактировать** на панели инструментов. В открывшейся панели будет выведена такая информация, как:

- пользователь лицензии,

- продавец, у которого была приобретена данная лицензия,
- идентификационный номер лицензии,
- дата истечения срока действия лицензии,
- включает ли данная лицензия поддержку модуля **Антиспам.**

Добавление лицензионного ключа Сервера

Для того чтобы добавить новый лицензионный ключ Сервера:

1. Нажмите на кнопку **Добавить ключ** на панели инструментов и в выпадающем списке выберите пункт **Добавить ключ сервера**.
2. На открывшейся панели нажмите на кнопку **Обзор** и выберите файл с лицензионным ключом **Сервера**.
3. Нажмите на кнопку **Сохранить**.

Допускается задание нескольких учетных записей с ключевыми файлами. При этом, только одна из лицензий **Сервера** будет активна.

Если при смене ключевого файла **Сервера** (при активации нового ключевого файла), параметры `ID1` **Сервера** в старом и новом ключевых файлах будут различаться, тогда расписание **Сервера**, настройки межсерверных связей и статистика заданий **Сервера** будут утеряны.

Для сохранения расписания **Сервера** необходимо выполнить его экспорт перед заменой лицензионного ключа и импорт - после замены.

Изменение активности лицензии Сервера

При наличии нескольких учетных записей с ключевыми файлами, только одна из лицензий **Сервера** является активной (используемой **Сервером** в данный момент).

Для того чтобы изменить активную лицензию Сервера:

1. Выберите учетную запись с той лицензией, которую вы хотите установить для **Сервера**, и нажмите на кнопку **Редактировать** на панели инструментов.
2. В открывшейся панели нажмите на кнопку **Активировать**.
3. После активации нового серверного ключа, для продолжения работы перезагрузите **Сервер**.

Удаление лицензионного ключа Сервера

Нельзя удалить текущую активную запись ключевого файла **Сервера**.

Для того чтобы удалить имеющийся лицензионный ключ Сервера:

1. Выберите в главном окне **Менеджера лицензий** ключ, который вы хотите удалить, и нажмите на кнопку **Удалить ключ** на панели инструментов.
2. В диалоговом окне подтвердите удаление ключа.

3.4.2.2. Ключи Dr.Web Enterprise Agent

При помощи Менеджера лицензий вы можете осуществлять следующие действия над лицензионными ключами для Dr.Web Enterprise Agent:

1. Просматривать информацию о лицензии.
2. Добавлять новые лицензионные ключи Агента.
3. Заменять лицензионные ключи Агента на новые.
4. Заменять лицензионные ключи Агента на ключи, уже входящие в антивирусную сеть.
5. Удалять лицензионные ключи Агента.

Просмотр информации о лицензии

Для того чтобы просмотреть сводную информацию о лицензии, выберите в главном окне **Менеджера лицензий** учетную запись, информацию о которой вы хотите просмотреть, и нажмите на кнопку **Редактировать** на панели инструментов. В открывшейся панели будет выведена такая информация, как:

- пользователь лицензии,
- продавец, у которого была приобретена данная лицензия,
- идентификационный номер лицензии,
- дата истечения срока действия лицензии,
- включает ли данная лицензия поддержку модуля **Антиспам,**
- поддержку каких антивирусных компонентов включает данная лицензия.

Добавление лицензионного ключа Агента

Допускается задание нескольких учетных записей с ключевыми файлами **Агентов**.

Для того чтобы добавить новый лицензионный ключ Агента:

1. Нажмите на кнопку **Добавить ключ** на панели инструментов и в выпадающем списке выберите пункт **Добавить ключ агента**.
2. На открывшейся панели нажмите на кнопку **Обзор** и выберите файл с лицензионным ключом **Агента**.
3. Нажмите на кнопку **Сохранить**.

Замена лицензионного ключа Агента на новый

Для того чтобы заменить текущий лицензионный ключ Агента на новый:

1. Выберите в главном окне **Менеджера лицензий** объект (станцию или группу), для которого назначен ключ, который вы хотите заменить, и нажмите на кнопку **Редактировать** на панели инструментов.
2. В открывшейся панели нажмите на кнопку **Обзор** и выберите файл с лицензионным ключом **Агента**.
3. Нажмите на кнопку **Сохранить**.
4. Если список компонентов, лицензируемых для установки на станции, в новом ключе отличается от списка старого лицензионного ключа,то будет выведен запрос на задание настроек согласно списку компонентов из нового ключа.

   В предлагаемом списке объектов указаны станции и группы, у которых списки в старом и импортируемом ключах различны, а также список отличий (какие компоненты отсутствуют или добавлены в новом ключе). Установите флаги для тех объектов, для которых будут заданы новые настройки списков устанавливаемых компонентов. Для остальных объектов (для которых флаги не установлены) настройки останутся в том виде, в котором они были до замены ключа.

Замена лицензионного ключа Агента на имеющийся

Для того чтобы заменить текущий лицензионный ключ Агента на уже входящий в антивирусную сеть ключ:

1. Выберите в главном окне **Менеджера лицензий** ключ, который вы хотите назначить для объекта (станции или группы), и нажмите на кнопку **Распространить эти настройки на другой объект** на панели инструментов.
2. В открывшемся окне выберите из списка нужную станцию или группу (эта группа должна содержать станции). Для выделения объекта или нескольких объектов достаточно нажать на них левой кнопкой мыши, аналогично для снятия выделения.
3. Нажмите на кнопку **Сохранить**.

> Если для станции или группы уже назначен ключ в персональных настройках, для назначения нового ключа, имеющегося в списке главного окна **Менеджера лицензий**, достаточно переместить данную группу или станцию при помощи мыши (drag and drop) на учетную запись ключа (при этом может наблюдаться небольшая задержка при обновлении списка главного окна).

4. Если список компонентов, лицензируемых для установки на станции, в новом ключе отличается от списка старого лицензионного ключа,то будет выведен запрос на задание настроек согласно списку компонентов из нового ключа.

   В предлагаемом списке объектов указаны станции и группы, у которых списки в старом и импортируемом ключах различны, а также список отличий (какие компоненты отсутствуют или добавлены в новом ключе). Установите флаги для тех объектов, для которых будут заданы новые настройки списков устанавливаемых компонентов. Для остальных объектов (для которых флаги не установлены) настройки останутся в том виде, в котором они были до

замены ключа.

Удаление лицензионного ключа Агента

Нельзя удалить учетную запись **Агентского** ключа, назначенного для группы **Everyone**.

Для того чтобы удалить имеющийся лицензионный ключ Агента:

1. Выберите в главном окне **Менеджера лицензий** ключ, который вы хотите удалить, или объект (станцию или группу), для которого назначен этот ключ, и нажмите на кнопку **Удалить ключ** на панели инструментов.
2. В диалоговом окне подтвердите удаление ключа.
3. Если для объекта, для которого удаляется ключ, были заданы персональные настройки списка устанавливаемых компонентов, то будет выведен запрос на удаление персональных настроек.

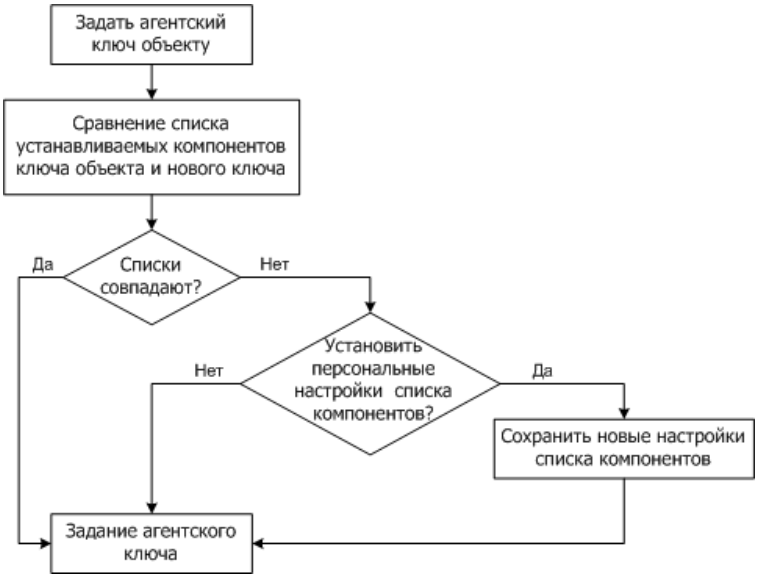
   В предлагаемом списке объектов указаны станции и группы с персональными настройками. Установите флаги для тех объектов, для которых будет задано наследование настроек родительской группы. Для остальных объектов будут сохранены персональные настройки списков устанавливаемых компонентов в том виде, в котором они были до удаления ключа.

Изменение списка устанавливаемых компонентов

Замена или добавление нового лицензионного ключа

Если списки устанавливаемых компонентов в новом и старом ключах отличаются, настройки списков устанавливаемых

компонентов объекта могут либо заменяться на новые, либо сохраняться (см. п. Замена лицензионного ключа Агента).



Процедура при замене или добавлении нового лицензионного ключа Агента

При задании новых настроек:

1. Если в новом ключе содержатся компоненты, которых не было в старом ключе, то для таких компонентов в списке **Устанавливаемые компоненты** будет задано значение **может** (см. п. Настройка конфигурации рабочей станции). В дальнейшем пользователь будет иметь возможность установить данные компоненты на станциях, лицензируемых новым ключом.
2. Если в новый ключ не включены компоненты, которые были включены в старый ключ, то для таких компонентов в списке **Устанавливаемые компоненты** будет выставлено значение **не может**, и они будут удалены со станций, лицензируемых новым ключом.

3. Для всех остальных компонентов, которые были включены в старый и новый ключи, настройки со страницы **Устанавливаемые компоненты** будут сохранены в том виде, в котором они были до замены ключа.

При сохранении настроек:

На странице **Устанавливаемые компоненты** настройки останутся в том виде, в котором они были до замены ключа.

Удаление лицензионного ключа

Настройки списков устанавливаемых компонентов могут либо наследоваться от родительской группы, либо сохраняться (см. п. Удаление лицензионного ключа Агента).

Процедура при удалении лицензионного ключа Агента

При наследовании настроек:

На странице **Устанавливаемые компоненты** будут удалены персональные настройки и задано наследование настроек родительской группы.

При сохранении настроек:

На странице **Устанавливаемые компоненты** останутся настройки в том виде, в котором они были до удаления ключа.

3.5. Схема взаимодействия компонентов антивирусной сети

На рисунке 3-3 представлена общая схема фрагмента антивирусной сети.

Данная схема отображает антивирусную сеть, в состав которой входит только один **Сервер**. В крупных компаниях предпочтительно разворачивать антивирусную сеть с несколькими **Серверами** для распределения нагрузки между ними.

В данном примере антивирусная сеть развернута в пределах одной ЛВС, однако для установки и работы **ESS** и антивирусных пакетов нахождение компьютеров в пределах какой-либо ЛВС необязательно, достаточно доступа в Интернет.

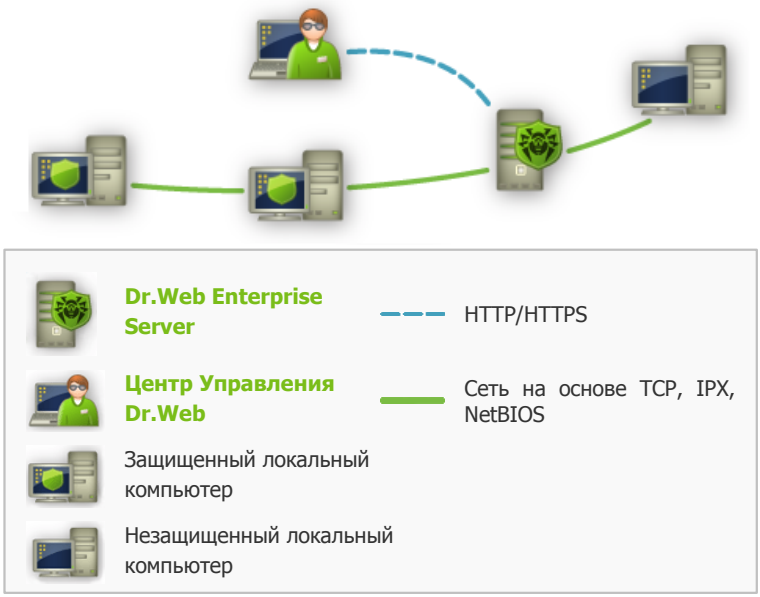


Рисунок 3-3. Структура антивирусной сети

При запуске Dr.Web Enterprise Server выполняется следующая последовательность действий:

1. Загрузка файлов **Enterprise Сервера** из каталога `bin`.
2. Загрузка **Планировщика заданий Сервера**.
3. Загрузка каталога централизованной установки и каталога обновления, инициализация системы сигнального информирования (системы оповещений).
4. Проверка целостности БД **Сервера**.
5. Выполнение заданий **Планировщика заданий Сервера**.
6. Ожидание информации от **Enterprise Агентов** и команд от **Центров Управления**.

Весь поток команд, данных и статистической информации в антивирусной сети в обязательном порядке проходит через **Enterprise Сервер**. **Центр Управления** также обменивается информацией только с **Сервером**; изменения в конфигурации

рабочей станции и передача команд **Enterprise Агенту** осуществляется **Сервером** на основе команд **Центра Управления**.

Таким образом, логическая структура фрагмента антивирусной сети имеет вид, представленный на рисунке 3-4.

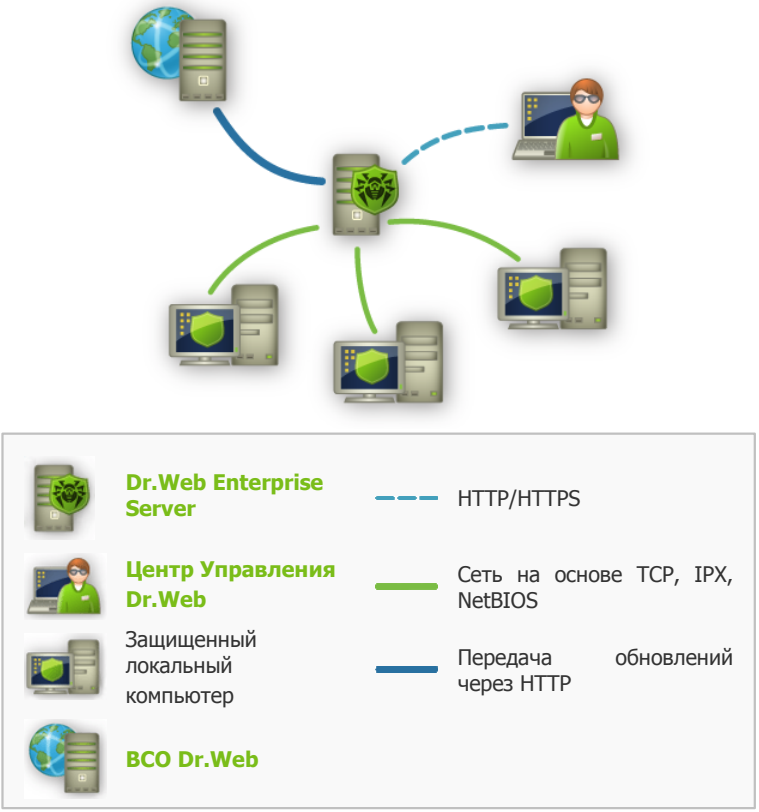


Рисунок 3-4. Логическая структура антивирусной сети

Между **Сервером** и рабочими станциями (сплошная тонкая линия на рисунке 3-4) по одному из поддерживаемых сетевых протоколов (TCP/IP, IPX или NetBIOS) передаются:

- запросы **Агента** на получение централизованного расписания и централизованное расписание данной рабочей станции,
- настройки **Агента** и антивирусного пакета,
- запросы на очередные задания, подлежащие выполнению (сканирование, обновление вирусных баз и т. п.),
- файлы антивирусных пакетов — при получении **Агентом** задания на их установку,
- обновления ПО и вирусных баз — при выполнении задания на обновление,
- сообщения **Агента** о конфигурации рабочей станции,
- статистика работы **Агента** и антивирусных пакетов для включения в централизованный журнал,
- сообщения о вирусных событиях и других подлежащих фиксации событиях.

Объем трафика между рабочими станциями и **Сервером**, в зависимости от настроек рабочих станций и их количества, может быть весьма значительным. Поэтому антивирусная сеть **Dr.Web ESS** предусматривает возможность компрессии трафика. Описание использования этого факультативного режима см. ниже, п. Использование шифрования и сжатия трафика.

Трафик между **Сервером** и рабочей станцией можно зашифровать. Это позволяет избежать разглашения сведений, передаваемых по описываемому каналу, а также подмены ПО, загружаемого на рабочие станции. По умолчанию эта возможность включена. Описание использования этого режима см. ниже, п. Использование шифрования и сжатия трафика.

От веб-сервера обновлений к **Enterprise Серверу** (сплошная толстая линия на рисунке 3-4) передаются, с использованием протокола HTTP, файлы, необходимые для репликации централизованных каталогов установки и обновления, и служебная информация о ходе этого процесса. Целостность передаваемой информации (файлов ПО **Dr.Web ESS** и антивирусных пакетов) обеспечивается использованием механизма контрольных сумм: поврежденный при пересылке или подмененный файл не будет принят **Сервером**.

Между **Сервером** и **Центром Управления** (пунктирная линия на рисунке 3-4) передаются сведения о конфигурации **Сервера** (включая информацию о топологии сети) и настройки рабочих станций. Эта информация визуализируется в **Центре Управления**, и, в случае изменения пользователем (администратором антивирусной сети) каких-либо настроек, информация о внесенных изменениях передается на **Сервер**.

Установление соединения **Центра Управления** с выбранным **Сервером** производится только после аутентификации администратора антивирусной сети посредством ввода его регистрационного имени и пароля на данном **Сервере**.

Глава 4. Начало работы. Общие сведения

4.1. Создание простой антивирусной сети

Перед началом эксплуатации антивирусного ПО рекомендуется изменить настройку каталога резервного копирования критичных данных **Сервера** (см. п. Настройка расписания Dr.Web Enterprise Server). Данный каталог желательно разместить на другом локальном диске, чтобы уменьшить вероятность одновременной потери файлов ПО **Сервера** и резервной копии.

Подключение через Центр Управления Dr.Web

По умолчанию **Enterprise Сервер** запускается автоматически после установки и после каждой перезагрузки системы (см. также п. Dr.Web Enterprise Server).

Для настройки **Сервера** и антивирусного ПО на станциях необходимо подключиться к **Серверу** при помощи **Центра Управления Dr.Web**.

На любом компьютере, имеющем сетевой доступ к **Enterprise Серверу**, **Центр Управления** доступен по адресу:

`http://`*<Адрес_Сервера>*`:9080`

или

`https://`*<Адрес_Сервера>*`:9081`

где в качестве *<Адрес_Сервера>* укажите IP-адрес или доменное имя компьютера, на котором установлен **Enterprise Сервер**.

В диалоговом окне запроса на авторизацию введите имя и пароль администратора (имя администратора по умолчанию – **admin**, пароль – пароль, который был задан при установке **Сервера**, см. п. Установка Dr.Web Enterprise Server).

При успешном подключении к **Серверу** откроется главное окно **Центра Управления**. В этом окне отображается информация об антивирусной сети, управляемой с данного **Сервера** (подробное описание см. в п. Центр Управления Dr.Web).

Управление антивирусной сетью

При помощи **Центра Управления** вы можете управлять **Сервером** и антивирусной сетью:

- создавать антивирусные станции (п. Установка Dr.Web Enterprise Agent с использованием Центра Управления Dr.Web),
- подтверждать станции,
- редактировать, настраивать и удалять антивирусные станции (см. п. Управление рабочими станциями),
- настраивать и редактировать соединения с соседними **Enterprise Серверами** (см. п. Особенности сети с несколькими Серверами),
- просматривать журналы событий данного и соседних **Серверов** и другие данные.

Основные средства управления сосредоточены в главном меню, управляющем меню и на панели инструментов (см. п. Центр Управления Dr.Web).

Подключение Dr.Web Enterprise Agent

После инсталляции **Агента** на рабочую станцию при помощи инсталляционного пакета, **Агент** пытается установить соединение с **Enterprise Сервером**.

При настройках **Enterprise Сервера** по умолчанию администратору необходимо вручную подтвердить новые рабочие станции для их регистрации на **Сервере** (подробнее о политике подключения новых станций см. п. Политика подключения станций). При этом новые рабочие станции не подключаются автоматически, а помещаются **Сервером** в список неподтвержденных станций.

Для того чтобы разрешить подключение новой станции к Dr.Web Enterprise Server:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**.
2. В открывшемся окне выберите пункт управляющего меню **Неподтвержденные станции**.
3. Откроется окно со списком станций, на которых установлен **Агент,** но доступ которых не подтвержден.
4. Выберите станцию в списке (установите напротив нее флаг), после чего на панели инструментов выберите пункт **Разрешить доступ и назначить первичную группу**, чтобы подтвердить доступ для данной рабочей станции. При этом будет предложено выбрать первичную группу для станции.

Подробнее о первичных группах см. п. Наследование элементов конфигурации рабочей станции. Первичные группы.

5. Станция будет подключена к **Серверу**, а изображение значка станции в антивирусной сети изменится.

   При этом рабочая станция помещается в предустановленные группы рабочих станций **Everyone**, **Online**, а также группы, соответствующие протоколу соединения, семейству ОС и конкретной ОС.

Установка антивирусного ПО

Установка на рабочую станцию компонентов антивирусного пакета далее происходит без вмешательства администратора.

На станцию будут установлены компоненты антивирусного пакета, заданные в настройках первичной группы станции (подробнее см. п. Состав антивирусного пакета).

Для завершения установки некоторых компонентов антивирусной рабочей станции может потребоваться перезагрузка компьютера. В этом случае на фоне значка **Enterprise Агента** на **Панели задач** появится восклицательный знак в желтом треугольнике (см. также п. Dr.Web Enterprise Agent).

4.2. Настройка сетевых соединений

Общие сведения

К **Enterprise Серверу** подключаются следующие клиенты:

- **Enterprise Агенты**,
- **Сетевые инсталляторы Enterprise Агентов**,
- другие **Enterprise Серверы**.

Соединение всегда устанавливается по инициативе клиента.

Возможны следующие схемы подключения клиентов к **Серверу**:

1. Посредством прямых соединений (direct connections).

   Данный подход имеет много преимуществ, но не всегда однозначно предпочтителен (также есть ситуации, когда такой подход не следует использовать).

2. При использовании Службы обнаружения Сервера.

По умолчанию (если явно не задано иное) клиенты используют именно эту **Службу**.

Данный подход следует использовать, если необходима перенастройка всей системы, в частности, если требуется перенести **Enterprise Сервер** на другой компьютер или поменять IP-адрес машины, на которой установлен **Сервер**.

При конфигурации антивирусной сети **ESS** на использование прямых соединений **Служба обнаружения Сервера** может быть отключена. Для этого в описании транспортов (**Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт**) поле **Адрес кластера** следует оставить пустым.

Прямые соединения

Настройка Dr.Web Enterprise Server

В настройках **Сервера** должно быть указано, какой адрес (см. Приложение Е. Спецификация сетевого адреса) необходимо "прослушивать" для приема входящих TCP-соединений.

Данный параметр задается в настройках **Сервера** **Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт** → поле **Адрес**.

По умолчанию для "прослушивания" **Сервером** устанавливаются:

- `tcp/0.0.0.0:2371` - поддерживается для обратной совместимости; в частности, для устранения проблем с переходом с версий **4.XX**, в которых используется порт `2371`.
- `tcp/0.0.0.0:2193` - при использовании порта `2193`, зарегистрированного за **Dr.Web Enterprise Security Suite** в IANA.

Обозначение `0.0.0.0` означает "все сетевые интерфейсы", для данной машины, на которой установлен **Сервер**.

Для корректной работы всей системы **ESS** достаточно, чтобы **Сервер** "слушал" хотя бы один TCP-порт, который должен быть известен всем клиентам.

Настройка Dr.Web Enterprise Agent

При установке **Агента** адрес **Сервера** (IP-адрес или сетевое имя машины, на которой запущен **Enterprise Сервер**) может быть явно указан в параметрах установки:

`drwinst` *<Адрес_Сервера>*

При установке **Агента** рекомендуется использовать имя **Сервера**, предварительно зарегистрированное в службе DNS. Это упростит процесс настройки антивирусной сети, связанный с процедурой переустановки **Enterprise Сервера** на другой компьютер.

По умолчанию команда `drwinst`, запущенная без параметров, будет сканировать сеть на наличие **Enterprise Серверов** и попытается установить **Агент** с первого найденного **Сервера** в сети (режим *Multicasting* с использованием Службы обнаружения Сервера).

Таким образом, адрес **Enterprise Сервера** становится известен **Агенту** при установке.

В дальнейшем адрес **Сервера** может быть изменен вручную в настройках **Агента**. Просмотр и редактирование настроек соединения с **Enterprise Сервером** осуществляется при помощи пункта контекстного меню значка **Агента** **Настройки** → **Соединение.**

Служба обнаружения Dr.Web Enterprise Server

При данной схеме подключения клиенту заранее не известен адрес **Сервера**. Перед каждым установлением соединения осуществляется поиск **Сервера** в сети. Для этого клиент посылает в сеть широковещательный запрос и ожидает ответ от **Сервера** с указанием его адреса. После получения отзыва клиент устанавливает соединение с **Сервером**.

Для этого **Сервер** должен "прослушивать" сеть на подобные запросы.

Возможно несколько вариантов настройки подобной схемы. Главное, чтобы метод поиска **Сервера**, заданный для клиентов, был согласован с настройками ответной части **Сервера**.

В **Dr.Web Enterprise Security Suite** по умолчанию используется режим *Multicast over UDP*:

1. **Сервер** регистрируется в мультикаст-группе с адресом `231.0.0.1`.
2. **Агенты**, при поиске **Сервера**, посылают в сеть мультикаст-запросы на групповой адрес `231.0.0.1`.

По умолчанию для "прослушивания" **Сервером** устанавливаются (аналогично прямым соединениям):

- `udp/231.0.0.1:2371`
- `udp/231.0.0.1:2193`

Данный параметр задается в настройках **Сервера** **Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт** → поле **Адрес кластера**.

Настройка сетевого экрана

Для возможности взаимодействия компонентов антивирусной сети необходимо, чтобы все используемые ими порты и интерфейсы были открыты на всех компьютерах, входящих в антивирусную сеть.

При установке **Сервера** инсталлятор позволяет автоматически добавить исключения в настройки сетевого экрана операционной системы Windows (кроме ОС Windows 2000). Для этого достаточно установить флаг **Добавить в исключения брандмауэра порты и интерфейсы сервера**.

При использовании сетевого экрана, помимо встроенного сетевого экрана ОС Windows, администратор антивирусной сети должен произвести соответствующие настройки вручную.

Глава 5. Администраторы антивирусной сети

Рекомендуется назначать администратором антивирусной сети надежного, квалифицированного работника, имеющего опыт администрирования локальной сети и компетентного в вопросах антивирусной защиты. Такой сотрудник должен иметь полный доступ к каталогам установки **Enterprise Сервера**. В зависимости от политики безопасности в организации и кадровой ситуации, администратор антивирусной сети либо должен получать полномочия администратора локальной сети, либо работать в тесном контакте с таким лицом.

Администратору антивирусной сети для текущего управления антивирусной сетью не требуются административные полномочия на компьютерах, включенных в эту антивирусную сеть. Однако удаленная установка и деинсталляция ПО **Агента** возможна только в локальной сети и требует полномочий администратора в этой сети, а отладка **Enterprise Сервера** — полного доступа к каталогу его установки.

5.1. Аутентификация администраторов

Аутентификация администратора для подключения к Enterprise Серверу возможна следующими способами:

1. С хранением данных об администраторах в БД **Сервера**.
2. С помощью Active Directory (в версиях **Сервера** для ОС Windows).
3. С использованием LDAP-протокола.
4. С использованием RADIUS-протокола.

Методы аутентификации используются последовательно согласно следующим принципам:

1. Порядок использования методов аутентификации зависит от порядка их следования в настройках, задаваемых через **Центра Управления**.
2. Первой всегда осуществляется попытка аутентификации администратора из БД **Сервера**.
3. Второй по умолчанию используется аутентификация через LDAP, третьей - через Active Directory, четвертой - через RADIUS.
4. В настройках **Сервера** методы аутентификации через LDAP, Active Directory и RADIUS можно поменять местами, но первой всегда осуществляется попытка аутентификации администратора из БД.
5. Методы аутентификации через LDAP, Active Directory и RADIUS по умолчанию отключены.

Для изменения порядка использования методов авторизации:

1. Выберите пункт **Администрирование** в главном меню **Центра Управления**.
2. В управляющем меню выберите раздел **Авторизация**.
3. В открывшемся окне представлен список типов авторизации в том порядке, в котором они используются. Для изменения порядка следования нажмите на стрелку слева от названия типа авторизации. Соответствующие типы авторизации поменяются местами.

Аутентификация администраторов из БД Сервера

Метод аутентификации с хранением данных об администраторах в БД **Сервера** используется по умолчанию.

Для управления списком администраторов:

1. Выберите пункт **Администрирование** в главном меню **Центра Управления**.
2. В управляющем меню выберите раздел **Администраторы**. Откроется список всех зарегистрированных в БД администраторов.

   Подробнее см. п. Управление учетными записями администраторов.

Аутентификация при использовании Active Directory

Для включения аутентификации через Active Directory:

1. Выберите пункт **Администрирование** в главном меню **Центра Управления**.
2. В управляющем меню выберите раздел **Авторизация**.
3. В открывшемся окне зайдите в раздел **Microsoft Active Directory**.
4. Установите флаг **Использовать авторизацию Microsoft Active Directory**.
5. Нажмите **Сохранить**.

При аутентификации администраторов из Active Directory в **Центре Управления** настраивается только разрешение использования данного метода аутентификации.

Редактирование свойств администраторов Active Directory осуществляется вручную на сервере Active Directory.

Для редактирования администраторов Active Directory:

Следующие операции необходимо выполнять на ПК, где присутствует оснастка для администрирования Active Directory.

1. Для возможности редактирования параметров администраторов необходимо выполнить следующие операции:
   a) Для модификации схемы Active Directory запустите утилиту `drwschema-modify.exe` (входит в дистрибутив **Enterprise Сервера**).
   Модификация схемы Active Directory может занять некоторое время. В зависимости от конфигурации вашего домена, для синхронизации и применения модифицированной схемы может потребоваться до 5 минут и более.
   b) Для регистрации оснастки Active Directory Schema (Схема Active Directory) выполните с административными полномочиями команду `regsvr32 schmmgmt.dll`, после чего запустите `mmc` и добавьте оснастку **Active Directory Schema**.
   c) Используя добавленную оснастку Active Directory Schema, добавьте к классу **User** и (если необходимо) к классу **Group** вспомогательный класс **DrWebEnterpriseUser**.

Если применение модифицированной схемы еще не завершилось, класс **DrWebEnterpriseUser** может быть не найден. В таком случае подождите некоторое время и повторите попытку согласно п. **c)**.

   d) С административными полномочиями запустите файл `drweb-esuite-aduac-600-xxxxxxxxx-windows-nt-xYY.msi` (входит в дистрибутив **Dr.Web Enterprise Security Suite 6.0.4**) и дождитесь окончания установки.
2. Графический интерфейс для редактирования атрибутов

доступен на панели управления **Active Directory Users and Computers** → в разделе **Users** → в окне редактирования свойств выбранного пользователя **Administrator Properties** → на вкладке **Dr.Web Authentication**.

3. Для редактирования доступны следующие параметры (значение каждого атрибута может быть **yes**, **no** или **not set**):

   - **User is administrator** - указывает на то, что пользователь - полноправный администратор.

   - **User is read-only administrator** - указывает на то, что пользователь - администратор с правами только на чтение.

     Если значение **yes** задано только для параметра **User is administrator**, то пользователь - администратор с полными правами.

     Если значение **yes** задано для параметров **User is administrator** и **User is read-only administrator** одновременно, то пользователь - администратор с правами только на чтение.

   - **Inherit permissions from groups** - параметр, разрешающий наследование значений для остальных параметров из групп пользователя. Если какой-либо параметр (или несколько параметров) принимают значение **not set** и для **Inherit permissions from groups** указано значение **yes**, то значения незаданных параметров наследуются от групп, в которые входит данный пользователь.

Алгоритмы принципа работы и разбора атрибутов при авторизации приведены в Приложении О.

Аутентификация при использовании LDAP

Для включения аутентификации через LDAP:

1. Выберите пункт **Администрирование** в главном меню **Центра Управления**.
2. В управляющем меню выберите раздел **Авторизация**.
3. В открывшемся окне зайдите в раздел **LDAP-авторизация.**
4. Установите флаг **Использовать LDAP-авторизацию**.
5. Нажмите **Сохранить**.

Настройка авторизации с использованием LDAP-протокола возможна на любом LDAP-сервере. Также с использованием этого механизма можно настроить **Сервер** под ОС семейства UNIX для авторизации в Active Directory на доменном контроллере.

Настройки LDAP-авторизации сохраняются в файле конфигурации `auth-ldap.xml`.

Описание основных xml-атрибутов авторизации приведено в Приложении О.

В отличие от Active Directory, механизм можно настроить на любую схему LDAP. По умолчанию осуществляется попытка использования атрибутов **Dr.Web Enterprise Security Suite**, как они определены для Active Directory.

Процесс авторизации LDAP сводится к следующему:

1. Адрес LDAP-сервера задается через **Центр Управления** или в конфигурационном xml-файле.
2. Для заданного имени пользователя выполняются следующие действия:
   - Осуществляется трансляция имени в DN (Distinguished Name) с использованием DOS-подобных масок (с использованием символа *), если правила заданы.

- Осуществляется трансляция имени в DN с использованием регулярных выражений, если правила заданы.
- Используется пользовательский скрипт трансляции имен в DN, если он задан в настройках.
- В случае, если не подошло ни одно из правил преобразования, заданное имя используется как есть.

Формат задания имени пользователя никак не определяется и не фиксируется - он может быть таким, как это принято в данной организации, т.е. принудительная модификация схемы LDAP не требуется. Преобразование под данную схему осуществляется с использованием правил трансляции имен в LDAP DN.

3. После трансляции, как и в случае с Active Directory, с помощью полученного DN и введенного пароля осуществляется попытка регистрации данного пользователя на указанном LDAP-сервере.
4. Затем, так же как и в Active Directory, читаются атрибуты LDAP-объекта для полученного DN. Атрибуты и их возможные значения могут быть переопределены в конфигурационном файле.
5. Если остались неопределенные значения атрибутов администратора, то в случае задания наследования (в конфигурационном файле), поиск нужных атрибутов по группам, в которые входит пользователь, ведется также, как в случае с использованием Active Directory.

5.2. Типы администраторов

В данном разделе приводится информация об администраторах, данные об учетных записях которых хранятся в БД **Enterprise Сервера**.

Учетные записи администраторов антивирусной сети делятся на 4 группы:

- администраторы с полными правами,
- администраторы с правами "только для чтения",
- администраторы групп с полными правами,
- администраторы групп с правами "только для чтения".

Администраторы с полными правами

Администраторы с полными правами имеют исключительные права на управление **Enterprise Сервером** и 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 (см. п. Настройка прав пользователей).

Администратор с полными правами может просматривать и редактировать список имеющихся административных учетных записей.

Администраторы с правами "только для чтения"

Администраторы с правами "только для чтения" могут только просматривать настройки сети в целом и отдельных ее элементов, но не менять их.

Администраторы групп с полными правами

Администраторы групп 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 (см. п. Системные и пользовательские группы). 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"

Администраторы групп могут обладать как полными правами для редактирования доступных им групп, так и правами "только для чтения".

Администраторы по умолчанию

После установки **Сервера** автоматически создается учетная запись **admin** - администратор с полными правами. Пароль для входа под данной учетной записью задается при установке **Сервера** (шаг 15 в процедуре установки).

5.3. Управление учетными записями администраторов

В данном разделе приводится информация по управлению администраторами, данные об учетных записях которых хранятся в БД **Enterprise Сервера**.

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.

5.3.1. Создание и удаление администраторов

Добавление администратора

Для добавления новой учетной записи администратора:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Администраторы**.
2. Нажмите на панели инструментов значок **Создать учетную запись**.
3. Откроется окно настроек создаваемой учетной записи. Задайте следующие параметры:
   - В поле **Регистрационное имя** укажите логин администратора, который будет использоваться для доступа к **Центру Управления**.
   - В полях **Пароль** и **Еще раз пароль** задайте пароль для доступа к **Серверу**.

При задании пароля администратора не допускается использование национальных символов.

   - Установите флаг **Только чтение** для ограничения прав доступа.
   - В полях **Фамилия**, **Имя** и **Отчество** можете указать личные данные администратора.

- В выпадающем списке **Язык интерфейса** выберите язык, который будет использоваться создаваемым администратором.
- В выпадающем списке **Формат даты** выберите формат, который будет использоваться данным администратором при редактировании настроек, содержащих даты. Доступны следующие форматы:
  - европейский: `DD-MM-YYYY HH:MM:SS`
  - американский: `MM/DD/YYYY HH:MM:SS`
- В поле **Описание** можете задать произвольное описание учетной записи.
- Для учетной записи администратора групп установите флаг **Может администрировать ограниченное число групп** для задания доступных групп.

При этом станет доступен раздел **Управляемые группы**. В данном разделе выберите пользовательские группы, которыми будет управлять данный администратор. Для этого нажмите на название группы в списке **Известные группы**. Для исключения из списка групп, управляемых данным администратором, нажмите на название группы в списке **Управляемые группы**.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

4. После задания всех необходимых параметров нажмите кнопку **Сохранить** для создания учетной записи администратора.

Удаление администратора

Для удаления учетной записи администратора:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Администраторы**.
2. В списке администраторов выберите учетную запись, которую вы хотите удалить.

3. Нажмите на панели инструментов значок **Удалить учетную запись**.

5.3.2. Редактирование администратора

Для редактирования учетной записи администратора:

1. Откройте раздел настроек учетной записи.

   Для администраторов с полными правами это можно выполнить одним из следующих способов:

   - Выберите пункт **Администрирование** в главном меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Администраторы**. В списке администраторов выберите учетную запись, которую вы хотите отредактировать. На панели инструментов нажмите кнопку **Редактировать**.
   - Выберите пункт **Настройки** главного меню **Центра Управления**, в открывшемся окне выберите пункт **Моя учетная запись**.

   Для администраторов групп и администраторов с правами только для чтения настройки учетной записи открываются только через раздел **Настройки** в главном меню **Центра Управления**.

2. При необходимости вы можете отредактировать параметры, которые были заданы при создании новой учетной записи.

   Значения полей, отмеченных знаком *, должны быть обязательно заданы.

   Для администраторов групп и администраторов с правами "только для чтения" список настроек, доступных для редактирования, ограничен.

3. Следующие параметры доступны только для чтения:

- Даты создания учетной записи и последнего изменения ее параметров,
- **Состояние** - отображает сетевой адрес последнего подключения под данной учетной записью.

4. После изменения параметров нажмите на кнопку **Сохранить**.
5. Для изменения пароля для доступа к учетной записи выберите на панели инструментов значок **Новый пароль**.

Администратор с полными правами может редактировать пароли всех других администраторов.

При задании пароля администратора не допускается использование национальных символов.

Глава 6. Группы. Комплексное управление рабочими станциями

Механизм групп предназначен для облегчения управления рабочими станциями антивирусной сети.

Объединение станций в группы может использоваться для:

- Выполнения групповых операций над всеми станциями, входящими в данные группы.

  Как для отдельной группы, так и для нескольких выбранных групп вы можете запускать, просматривать и прекращать задания на сканирование станций, входящих в данную группу. Точно так же вы можете просматривать статистику (в т.ч. инфекции, вирусы, запуск/завершение, ошибки сканирования и установки и т.п.) и суммарную статистику для всех рабочих станций группы или нескольких групп.

- Задания единых настроек для станций через группу, в которую они входят (см. п. Использование групп для настройки рабочих станций).
- Организации (структурирования) списка рабочих станций.

Также возможно создание вложенных групп.

6.1. Системные и пользовательские группы

Механизм групп предназначен для облегчения управления рабочими станциями антивирусной сети.

Системные группы

При установке **Сервера** создаются так называемые предустановленные (системные) группы.

Изначально **Dr.Web Enterprise Security Suite** содержит набор системных групп. Эти группы создаются в момент инсталляции **Enterprise Сервера** и не могут быть удалены. Однако администратор, при необходимости, может скрыть их отображение.

Каждая системная группа (кроме группы **Everyone**) содержит набор подгрупп, объединенных по определенному признаку.

Everyone

Группа, содержащая в себе все станции, известные **Enterprise Серверу**. Группа **Everyone** содержит настройки по умолчанию.

Operating system

Данная категория подгрупп отображает операционные системы, под управлением которых работают станции в данный момент. Данные группы не виртуальны и могут содержать настройки станций, а также могут являться первичными группами.

- Подгруппы семейства **Android**. Данное семейство включает набор групп, которые соответствуют конкретной версии операционной системы Android для мобильных устройств.
- Подгруппы семейства **Mac OS X**. Данное семейство включает набор групп, которые соответствуют конкретной версии операционной системы Mac OS X.
- Подгруппа **Netware**. Данная подгруппа содержит станции, работающие под операционной системой Novell NetWare.
- Подгруппы семейства **UNIX**. Данное семейство включает набор групп, которые соответствуют операционным системам семейства UNIX, например, Linux, FreeBSD, Solaris и

т.п.

- Подгруппы семейства **Windows**. Данное семейство включает набор групп, которые соответствуют конкретной версии операционной системы Windows.
- Подгруппа **Windows CE**. Данная подгруппа содержит станции, работающие под операционной системой Windows Mobile.

Status

Группа **Status** содержит вложенные группы, отражающие текущее состояние станций: подключены они в данный момент к **Серверу** или нет, а также состояние антивирусного ПО: удалено ПО или закончился период его использования. Данные группы полностью виртуальны и не могут содержать никаких настроек, также они не могут являться первичными группами.

- Группа **Deinstalled**. Как только с рабочей станции удалено ПО **Enterprise Агента**, станция переходит в группу **Deinstalled**.
- Группа **Deleted**. Содержит станции, ранее удаленные администратором с **Сервера**. Возможно восстановление данных станций (см. п. Удаление и восстановление станции).
- Группа **Offline**. Содержит все не подключенные в данный момент станции.
- Группа **Online**. Содержит все подключенные в данный момент станции (реагирующие на запросы **Сервера**).

Transport

Данные подгруппы определяют протокол, по которому станции подключены в данный момент к **Серверу**. Подгруппы полностью виртуальны и не могут содержать никаких настроек, также они не могут являться первичными группами.

- Группа **TCP/IP**. Группа содержит станции, подключенные в данный момент по протоколу TCP/IP.
- Группа **TCP/IP Version 6**. Группа содержит станции,

подключенные в данный момент по протоколу TCP/IP.

- Группа **IPX**. Группа содержит станции, подключенные в данный момент по протоколу IPX.
- Группа **NetBIOS**. Группа содержит станции, подключенные в данный момент по протоколу NetBIOS.

Ungrouped

Данная группа содержит станции, которые не входят ни в одну из пользовательских групп.

Unknown

Данная группа содержит станции, которые были созданы не через **Центр Управления Подписками**.

Пользовательские группы

Это группы, определяемые администратором антивирусной сети для его собственных нужд. Администратор может создавать собственные группы, а также вложенные группы и включать в них рабочие станции. Ни на состав, ни на название данных групп **Dr.Web Enterprise Security Suite** не накладывает никаких ограничений.

Для удобства в таблице ниже сведены все возможные группы и типы групп, а также характерные параметры, которые поддерживаются (+) или не поддерживаются (–) данными группами.

При этом рассматриваются следующие параметры:

- **Автоматическое членство**. Параметр определяет возможность автоматического включения станций в группу (поддержка автоматического членства), а также автоматического изменения состава группы в процессе работы **Сервера**.
- **Управление членством**. Параметр определяет

возможность управления администратором членством в группе: добавлением или удалением станций из группы.

- **Первичная группа**. Параметр определяет, может ли данная группа являться первичной для станции.
- **Содержание настроек**. Параметр определяет, может ли группа содержать настройки антивирусных компонентов (для возможности наследования их станциями).

Таблица 5-1. Группы и поддерживаемые параметры

Группа/тип групп	Параметр			
	Автоматическое членство	Управление членством	Первичная группа	Содержание настроек
Everyone	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Operating System	+	–	+	+
Ungrouped	+	–	–	–
Пользовательские группы	–	+	+	+

Под учетной записью *Администратора группы* пользовательская группа, которой он управляет, будет отображаться в корне иерархического дерева, даже если фактически у нее есть родительская группа. При этом будут доступны все дочерние от управляемой группы.

6.2. Управление группами

6.2.1. Создание и удаление групп

Создание группы

Для создания новой группы:

1. Выберите пункт  **Добавить станцию или группу** на панели инструментов, далее в подменю пункт  **Создать группу**.

   Откроется окно создания группы.

2. Поле ввода **Идентификатор** заполняется автоматически. При необходимости его можно отредактировать в процессе создания. Идентификатор не должен включать пробелов. В дальнейшем идентификатор группы изменять нельзя.
3. Введите в поле **Название** наименование группы.
4. Для вложенных групп в поле **Родительская группа** выберите из выпадающего списка группу, которая будет назначена родительской группой, от которой наследуется конфигурация, если не заданы персональные настройки. Для корневой группы (не имеющей родителя) оставьте это поле пустым, группа будет добавлена в корень иерархического списка. В этом случае настройки будут наследоваться от группы **Everyone**.
5. Введите произвольный комментарий в поле **Описание**.Нажмите на кнопку **Сохранить**.

Созданные вами группы первоначально пусты. Процедура включения рабочих станций в группы описана в разделе Добавление рабочих станций в группу. Удаление рабочих станций из группы.

Удаление группы

Для удаления существующей группы:

1. Выберите пользовательскую группу в иерархическом списке **Центра Управления**.
2. На панели инструментов нажмите **Общие** → **Удалить отмеченные объекты**.

Предустановленные группы удалить невозможно.

6.2.2. Настройки групп

Чтобы задать настройки группы:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке выберите группу.
2. Нажмите пункт **Свойства** в управляющем меню (панель слева).
3. Откроется окно со свойствами группы. Данное окно содержит вкладки **Общие** и **Конфигурация**. Их содержание и настройка описаны ниже.

При открытии свойств группы через пункт **Общие** → **Редактировать** на панели инструментов также будет доступен раздел **Сведения о станциях**, в котором приведена общая информация о станциях, входящих в данную группу.

4. Для сохранения внесенных изменений нажмите на кнопку **Сохранить**.

Общие

В разделе **Общие** приведены следующие поля:

- **Идентификатор** - уникальный идентификатор группы. Не доступен для редактирования.
- **Название** - название группы. При необходимости можете изменить название группы.

Для предустановленных групп поля **Идентификатор** и **Название** не доступны для редактирования.

- **Родительская группа** - родительская группа, в которую входит данная группа и от которой наследует свою конфигурацию, если не заданы персональные настройки. Если родительская группа не назначена, настройки наследуются от группы **Everyone**.
- **Описание** - необязательное поле с описанием группы.

Конфигурация

Для подробной информации о наследовании настроек групп станциями, для которых данная группа является первичной, см. раздел Использование групп для настройки рабочих станций.

В разделе **Конфигурация** приведены настройки группы, включающие:

-  - настройку прав пользователей станций, для которых данная группа является первичной. Настройка прав группы аналогична настройке прав отдельных рабочих станций (см. п. Настройка прав пользователей).
-  - настройку расписания запуска заданий на рабочих станциях, для которых данная группа является первичной. Настройка расписания для группы аналогична настройке

централизованного расписания для станций (см. п. Настройка расписания заданий на рабочей станции).

-  - задание лицензионного ключа для станций, для которых данная группа является первичной.
-  - настройку ограничений при обновлении антивирусного ПО на станциях, для которых данная группа является первичной (см. п. Ограничение обновлений).
-  - список компонентов, устанавливаемых на станциях, для которых данная группа является первичной. Редактирование списка компонентов для групп аналогично редактированию списка компонентов для станций (см. п. Состав антивирусного пакета).
- Настройки компонентов антивирусного пакета: **Dr.Web Сканер для Windows**, **SpIDer Guard G3 для Windows**, **SpIDer Mail для рабочих станций Windows** и др. Для изменения настроек нажмите на кнопку  напротив соответствующего компонента. Настройка компонентов антивирусного пакета для группы аналогична настройке компонентов для станции (см. также п. Настройка конфигурации рабочей станции).

6.3. Добавление рабочих станций в группу. Удаление рабочих станций из группы

Существует несколько способов добавления рабочих станций в пользовательские группы:

1. Изменить настройки станции.
2. Перетащить станцию в иерархическом списке (drag'n'drop).

Чтобы отредактировать список групп, в которые входит станция, через настройки станции:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции.
2. Откройте раздел настроек станции одним из следующих способов:
   - В управляющем меню (панель слева) выберите пункт **Свойства**.
   - Нажмите **Общие** → **Редактировать** на панели инструментов.
3. На открывшейся панели **Свойства станции** перейдите в раздел (на вкладку) **Группы**.

   В списке **Членство в** перечислены группы, в которые рабочая станция уже включена.

   В списке **Известные группы** расположен список всех остальных пользовательских групп.

4. Для добавления станции в пользовательскую группу нажмите на ее название в списке **Известные группы**. Станция будет добавлена в данную группу, а группа - перемещена в список **Членство в**.
5. Для удаления рабочей станции из пользовательской группы нажмите на название группы в списке **Членство в**. Станция будет удалена из данной группы, а группа -

перемещена в список **Известные группы**.

Удаление станций из предустановленных групп невозможно.

6. Для сохранения внесенных изменений нажмите на кнопку **Сохранить**.

Также в разделе свойств станции вы можете задать первичную группу для станции (подробнее см. Наследование элементов конфигурации рабочей станции. Первичные группы).

Чтобы отредактировать список групп, в которые входит станция, через иерархический список:

1. Выберите пункт **Антивирусная сеть** главного меню и разверните иерархический список групп и станций.
2. Чтобы добавить станцию в пользовательскую группу, зажмите клавишу CTRL и перетащите станцию при помощи мыши на нужную группу (drag'n'drop).
3. Чтобы переместить станцию из одной пользовательской группы в другую, перетащите станцию при помощи мыши (drag'n'drop) из пользовательской группы, из которой станция будет удалена, на пользовательскую группу, в которую станция будет добавлена.

При перетаскивании станции из предустановленной группы как по пункту 2, так и по пункту 3, станция будет добавлена в пользовательскую группу и не будет удалена из предустановленной.

Данный метод (drag'n'drop) не работает при использовании Веб-браузера Windows Internet Explorer 7.

Объединение станций

В результате операций с базой данных или при переустановке ПО антивирусных станций, в иерархическом списке антивирусной сети может появиться несколько станций с одинаковым названием (только одно из них будет соотнесено с соответствующей антивирусной станцией).

Для того чтобы убрать повторяющие имена станции:

1. Выделите все повторяющиеся имена одной и той же станции. Для этого используйте клавишу CTRL.
2. На панели инструментов выберите **Общие** → **Объединить станции**.
3. В предложенном списке выберите станцию, которая будет считаться главной. Все остальные станции будут удалены, а их данные будут приписаны выбранной.
4. В предложенном списке выберите станцию, настройки которой будут заданы для выбранной главной станции.
5. Нажмите **Сохранить**.

6.4. Использование групп для настройки рабочих станций

Настройки станций могут быть:

1. Унаследованы от первичной группы.
2. Заданы персонально.

Наследование настроек

При создании новой группы ее настройки наследуются от родительской группы или от группы **Everyone**, если родительская группа не задана.

При создании новой рабочей станции ее настройки наследуются от первичной группы.

Подробнее см. п. Наследование элементов конфигурации рабочей станции. Первичные группы.

При просмотре или редактировании элементов конфигурации рабочей станции, унаследованных от первичной группы, в соответствующих окнах отображается информация о том, что данная настройка унаследована от первичной группы.

Вы можете установить разные конфигурации для разных групп и станций, изменив соответствующие настройки.

Персональные настройки

Для задания персональных настроек станции отредактируйте соответствующий раздел настроек (см. п. Настройка конфигурации рабочей станции). При этом в разделе настроек будет отображаться информация о том, что данная настройка задана персонально для этой станции.

При задании персональных настроек станции настройки первичной группы и любые их изменения не будут влиять на настройки станции.

Вы можете восстановить конфигурацию, унаследованную от первичной группы. Для этого нажмите на кнопку  **Удалить эти настройки** на панели инструментов **Центра Управления** в разделе соответствующих настроек или в разделе свойств станции.

6.4.1. Наследование элементов конфигурации рабочей станции. Первичные группы

Наследование настроек

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**.

Если первичная группа не **Everyone**, и у указанной первичной группы нет персональных настроек, то наследуются настройки группы **Everyone**.

Возможно создание вложенных групп.

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**.

Например:

Структура иерархического списка представляет собой следующее дерево:

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`.

По умолчанию структура сети представлена таким образом, чтобы продемонстрировать вхождения станций во все группы, членом которых она является. Если вы хотите отображать в каталоге сети членство станций только в первичных группах, на панели инструментов **Центра Управления** в пункте **Настройки вида дерева** снимите флаг **Членство во всех группах**.

Задание первичной группы

Существует несколько способов задания первичной группы для рабочей станции и группы рабочих станций.

Чтобы установить первичную группу для рабочей станции:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции.
2. В управляющем меню (панель слева) выберите пункт **Свойства**. В открывшемся окне перейдите на вкладку **Группы**.
3. При необходимости назначить другую первичную группу нажмите на значок группы из списка **Членство в**.

4. Нажмите на кнопку **Сохранить**.

Чтобы установить первичную группу для нескольких рабочих станций:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название нужных станций (можно также выбирать группы — при этом действие будет распространено на все входящие в них станции), для выбора нескольких станций и групп можно воспользоваться выделением мышью при нажатых клавишах CTRL или SHIFT.
2. На панели инструментов нажмите **Общие** → **Назначить первичную группу**. Откроется окно со списком групп, которые могут быть назначены первичными для этих станций.
3. Для указания первичной группы нажмите на название группы.

Вы можете сделать группу первичной для всех входящих в нее рабочих станций. Для этого выберите нужную группу в каталоге, после чего на панели инструментов **Центра Управления** нажмите **Общие** → **Установить эту группу первичной**.

6.4.2. Копирование настроек в другие группы/станции

Настройки конфигурации антивирусных средств, расписаний, прав пользователей и другие настройки группы или рабочей станции могут быть скопированы (распространены) в группу или несколько групп и рабочих станций.

Для копирования настроек:

1. Нажмите на кнопку **Распространить эти настройки на другой объект**:
   - в окне редактирования конфигурации антивирусного компонента,

-  в окне редактирования расписания,
-  в окне настройки ограничений обновления,
-  в окне устанавливаемых компонентов.

Откроется окно каталога сети.

2. Выделите в этом списке группы и станции, на которые вы хотите распространить настройку.
3. Для того чтобы выполнить изменения в конфигурации этих групп, нажмите на кнопку **Сохранить**.

6.5. Сравнение станций и групп

Существует возможность сравнения станций и групп по основным параметрам.

Для сравнения нескольких объектов антивирусной сети:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке выберите объекты, которые вы хотите сравнить. Используйте для этого клавиши CTRL и SHIFT. Возможны следующие варианты:
   - выбор нескольких станций - для сравнения выбранных станций;
   - выбор нескольких групп - для сравнения выбранных групп и всех вложенных групп;
   - выбор нескольких станций и групп - для сравнения всех станций: как выбранных непосредственно в иерархическом списке, так и входящих во все выбранные группы и их вложенные группы.
2. В управляющем меню (панель слева) нажмите пункт **Сравнить**.
3. Откроется сравнительная таблица для выбранных объектов.

- Параметры сравнения для групп:
  - **Станций** - общее количество станций, входящих в данную группу.
  - **Станций в сети** - количество станций, активных на данных момент.
  - **Первичная группа для** - количество станций, для которых выбранная группа является первичной.
  - **Персональные настройки** - список компонентов, для которых назначены персональные настройки, не унаследованные от родительской группы.
- Параметры сравнения для станций:
  - **Дата создания** станции.
  - **Первичная группа** для станции.
  - **Персональные настройки** - список компонентов, для которых назначены персональные настройки, не унаследованные от первичной группы.
  - **Установленные компоненты** - список антивирусных компонентов, установленных на данной станции.

Глава 7. Управление рабочими станциями

Антивирусная сеть, работающая под управлением **Dr.Web Enterprise Security Suite**, позволяет централизованно настраивать антивирусные пакеты на рабочих станциях. **Dr.Web Enterprise Security Suite** позволяет:

- настраивать конфигурационные параметры антивирусных средств,
- настраивать расписание запуска заданий на сканирование,
- запускать отдельные задания на рабочих станциях независимо от настроек расписания,
- запускать процесс обновления рабочих станций, в том числе после ошибки обновления со сбросом состояния ошибки.

При этом администратор антивирусной сети может сохранить за пользователем рабочей станции права на самостоятельную настройку конфигурации и запуск заданий, запретить эти действия или в значительной мере их ограничить.

Изменения в конфигурацию рабочей станции можно вносить даже тогда, когда она временно недоступна для **Сервера**. Эти изменения будут приняты рабочей станцией, как только ее связь с **Сервером** восстановится.

7.1. Управление записями о рабочих станциях

7.1.1. Политика подключения станций

Процедура создания станции через **Центр Управления** описана в п. Создание новой учетной записи.

Возможность управления авторизацией станций на **Enterprise Сервере** зависит от следующих параметров:

1. Если при установке **Агента** на станции был выбран вариант авторизации **Автоматически**, то режим доступа станций к **Серверу** будет определяться в соответствии с настройками, заданными на **Сервере** (используется по умолчанию), см. ниже.
2. Если при установке **Агента** на станции был выбран вариант авторизации **Ручная** и заданы параметры **Идентификатор** и **Пароль**, то при подключении к **Серверу** станция будет авторизована автоматически вне зависимости от настроек **Сервера** (используется по умолчанию при установке **Агента** через инсталляционный пакет *esinst* - см. п. Инсталляционные файлы).

Задание типа авторизации **Агента** при его установке описано в разделе Установка Dr.Web Enterprise Agent в графическом режиме инсталлятора (шаг 6).

Чтобы изменить режим доступа станций к Dr.Web Enterprise Server:

1. Откройте настройки конфигурации **Сервера**. Для этого выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.

2. На вкладке **Общие** в выпадающем списке **Новички** выберите одно из следующих значений:
   - **Ручное подтверждение доступа** (режим устанавливается по умолчанию, если не был изменен при установке **Сервера**),
   - **Автоматически разрешать доступ**,
   - **Всегда отказывать в доступе**.

Ручное подтверждение доступа

В режиме **Ручное подтверждение доступа** новые станции помещаются в список неподтвержденных станций до их непосредственного рассмотрения администратором.

Для доступа к списку неподтвержденных станций:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Неподтвержденные станции**.
2. В открывшемся окне приведена таблица станций с установленными **Агентами**, запрашивающими доступ к **Серверу**, и общая информация о станциях: время получения запроса, сетевое название станции, IP-адрес станции и установленная на станции ОС.
3. Для задания доступа к **Серверу** установите флаги для нужных станций или установите флаг в заголовке таблицы, чтобы отметить все станции. На панели инструментов выберите действие, которое будет применено для выбранных станций:
   -  - разрешить доступ выбранным станциям и назначить первичную группу из предложенного списка,
   -  - отказать в доступе выбранным станциям.

Автоматическое разрешение доступа

В режиме **Автоматически разрешать доступ** все станции, которые запрашивают доступ к **Серверу**, подключаются автоматически без дальнейших запросов администратору. При этом в качестве первичной группы назначается группа **Everyone**.

Отказ в доступе

В режиме **Всегда отказывать в доступе** **Сервер** отказывает в доступе при получении запросов от новых станций. Администратор должен вручную создавать записи о станциях и присваивать им пароли доступа.

7.1.2. Удаление и восстановление станции

Чтобы удалить запись о рабочей станции:

1. Для удаления станции при помощи **Центра Управления**: выберите пункт главного меню **Антивирусная сеть**, в открывшемся окне нажмите на панели инструментов **Общие** → **Удалить отмеченные объекты**.
2. Откроется окно подтверждения удаления станции. Нажмите **ОК**.

После удаления станций из иерархического списка, они помещаются в таблицу удаленных станций, из которой возможно восстановление объектов при помощи **Центра Управления**.

Чтобы восстановить запись о рабочей станции:

1. Выберите пункт главного меню **Антивирусная сеть**, в открывшемся окне в иерархическом списке выберите удаленную станцию или несколько станций, которые вы хотите восстановить.

Все удаленные станции расположены в подгруппе **Deleted** группы **Status**.

2. На панели инструментов выберите пункт **Общие** → **Восстановить удаленные станции**.
3. Откроется раздел восстановления удаленных станций. Вы можете задать следующие параметры станции, которые будут заданы при восстановлении:
   - **Первичная группа** - выберите первичную группу, в которую будет добавлена восстанавливаемая станция. По умолчанию выбрана та первичная группа, которая была задана для станции при ее удалении.

При восстановлении нескольких станций одновременно по умолчанию выбран вариант **Бывшая первичная группа**, означающий, что для каждой из выбранных станций будет задана своя первичная группа, в которой станции числились до удаления. При выборе определенной группы для всех восстанавливаемых станций будет задана одна и та же выбранная группа.

   - В разделе **Членство в** вы можете изменить список групп, в которые будет входить станция. По умолчанию задан список групп, в которые станция входила до удаления. Для добавления станции в пользовательские группы нажмите на название доступных пользовательских групп в разделе **Список групп**. Для исключения пользовательских групп, в которые станция входила до удаления, нажмите на названия соответствующих групп в разделе **Членство в**.
4. Для восстановления станции с заданными параметрами нажмите на кнопку **Восстановить**.

7.2. Настройка конфигурации рабочей станции

Свойства станции

Чтобы просмотреть и отредактировать свойства рабочей станции:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке выделите станцию и нажмите **Общие** → **Редактировать** на панели инструментов.
2. В правой части окна **Центра Управления** откроется окно со свойствами рабочей станции. Данное окно содержит следующие группы настроек: **Общие**, **Конфигурация**, **Группы**, **Безопасность**, **Расположение**. Их содержание и настройка описаны ниже.
3. Для сохранения внесенных изменений нажмите на кнопку **Сохранить**.

Общие

В разделе **Общие** приведены следующие поля, доступные только для чтения:

- **Идентификатор** - уникальный идентификатор станции.
- **Название** - название станции.

Также вы можете задать значения следующих полей:

- В поле **Пароль** задайте пароль для авторизации станции на **Сервере** (необходимо повторить тот же пароль в поле **Еще раз пароль**). При смене пароля, для возможности подключения **Агента**, аналогичную процедуру необходимо произвести в настройках соединения **Агента** на станции.
- В поле **Описание** добавьте дополнительную информацию.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

Конфигурация

В разделе **Конфигурация** вы можете изменить конфигурацию данной станции, включающую:

-  - настройку прав пользователя рабочей станции (см. п. Настройка прав пользователей).
-  - настройку расписания запуска заданий на рабочей станции. Описание настройки централизованного расписания приведено в п. Настройка расписания заданий на рабочей станции.
-  - задание лицензионного ключа для станции.
-  - настройку ограничений при обновлении антивирусного ПО. Описание настройки обновлений приведено в п. Ограничение обновлений рабочих станций.
-  - список устанавливаемых компонентов (см. п. Состав антивирусного пакета).
- Настройки компонентов антивирусного пакета - **Dr.Web Сканер для Windows**, **SpIDer Guard G3 для Windows**, **SpIDer Mail для рабочих станций Windows** и др. Для изменения настроек нажмите на кнопку  напротив соответствующего компонента.

Из **Центра Управления** также доступны кнопки для удаления персональных настроек. Они расположены справа от соответствующих кнопок настройки конфигурации. При удалении персональной конфигурации рабочей станции вновь будет установлена конфигурация, унаследованная от первичной группы.

Состав параметров компонентов и рекомендации по их заданию содержатся в руководстве **Антивирус Dr.Web® для Windows. Руководство пользователя**, а также **Dr.Web® Агент для Windows. Руководство пользователя**.

В то же время, управление настройками через **Центр Управления** имеет некоторые отличия от управления настройками непосредственно через соответствующие компоненты антивируса:

- для того чтобы изменить значения параметров, принимающих значения **Да** или **Нет**, щелкните по соответствующему значению. Поля ввода и выпадающие списки имеют стандартный интерфейс,
- для управления отдельными параметрами используйте кнопки, расположенные справа от соответствующих настроек:

   - восстановить значение, которое параметр имел до редактирования,

   - установить для параметра значение по умолчанию,
- для управления совокупностью параметров используйте кнопки на панели инструментов (верхняя часть большинства окон настроек, например, **Расписание**, **Права, Dr.Web Сканер для Windows**, **SpIDer Guard для Windows** и **SpIDer Mail для рабочих станций Windows**):

   - распространить данные настройки на другие объекты (группу или несколько групп и рабочих станций),

   - восстановить значения, которые все параметры имели до редактирования,

   - установить для всех параметров значения по умолчанию,

   - экспортировать параметры в файл специального формата,

 - импортировать параметры из файла специального формата,

 - удалить специфическую конфигурацию для данной рабочей станции (при этом вновь будет установлена унаследованная от групп конфигурация, см. п. Использование групп для настройки рабочих станций).

- Нажмите на кнопку **Сохранить**, чтобы согласиться с внесенными изменениями.

Группы

В разделе **Группы** настраивается список групп, в которые входит данная рабочая станций (см. п. Добавление рабочих станций в группу. Удаление рабочих станций из группы).

Также в данном разделе можно изменить первичную группу для станции (см. п. Наследование элементов конфигурации рабочей станции. Первичные группы).

Безопасность

В разделе **Безопасность** задаются ограничения на сетевые адреса, с которых разрешен доступ к данной станции.

Чтобы разрешить все соединения, снимите флаг **Использовать этот список доступа**. Для того чтобы задать списки разрешенных или запрещенных адресов, установите этот флаг.

Для того чтобы разрешить доступ с определенного TCP-адреса, включите его в список **TCP: разрешено** или **TCPv6: разрешено**.

Для того чтобы запретить какой-либо TCP-адрес, включите его в список **TCP: запрещено** или **TCPv6: запрещено**.

Для редактирования адресов в списке:

1. Введите сетевой адрес в соответствующее поле и нажмите на кнопку **Сохранить**.

2. Для добавления нового поля адреса, нажмите на кнопку  соответствующего раздела.
3. Для удаления поля нажмите на кнопку  .

   Сетевой адрес задается в виде: <*IP-адрес*>/[<*префикс*>].

Пример использования префикса:

1. Префикс 24 обозначает сети с маской: `255.255.255.0`

   Содержит 254 адреса

   Адреса хостов в этих сетях вида: `195.136.12.*`

2. Префикс 8 обозначает сети с маской `255.0.0.0`

   Содержит до 16387064 адресов (256*256*256)

   Адреса хостов в этих сетях вида: `125.*.*.*`

Кроме того, вы можете удалять адреса из списка и редактировать внесенные в список адреса.

Аналогично настраиваются ограничения для IPX-адресов.

Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлен ли флаг **Приоритетность запрета**: при установленном флаге адреса, не включенные ни в один из списков (или включенные в оба), запрещаются. В противном случае, такие адреса разрешаются.

Расположение

В разделе **Расположение** задаются параметры географического местоположения станции.

Можно создавать различные группы пользователей по признаку, какие права и настройки для них оптимальны. Задание основных параметров работы станций через группы позволит вам сэкономить усилия по редактированию настроек каждой отдельной станции.

Удаление настроек станции

Чтобы удалить персональные настройки станции:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке выберите станцию и нажмите на панели инструментов  **Общие** →  **Убрать индивидуальные настройки объекта**. Откроется список настроек данной станции, персональные будут отмечены флагами.
2. Для настроек, которые необходимо удалить, снимите нужные флаги и нажмите **Сохранить**. Настройки станции, унаследованные от первичной группы, будут восстановлены.

При редактировании конфигурации рабочей станции для компонентов **SpIDer Guard для Windows**, а также **Dr.Web Сканер для Windows** ознакомьтесь с рекомендациями по использованию антивирусных программ для компьютеров под управлением ОС Windows Server 2003, ОС Windows 2000 и ОС Windows XP. Статья, содержащая необходимую информацию, находится по адресу - http://support.microsoft.com/kb/822158/ru. Материал данной статьи призван помочь оптимизировать производительность системы.

При условии, что ваш ключ **Агента** (`agent.key`) разрешает использование спам-фильтра для компонента **SpIDer Mail**, на вкладке **Антиспам** можно произвести настройку фильтра (выберите в контекстном меню любой группы или рабочей станции пункт **SpIDer Mail для рабочих станций Windows**).

Начиная с версии **5.0** в состав антивирусного пакета **Dr.Web Enterprise Security Suite** входят продукты **SpIDer Gate** и **Офисный Контроль**, для возможности использования которых также необходимо, чтобы они были указаны в вашей лицензии (**Антивирус + Антиспам**), которую можно просмотреть в ключе **Агента**.

Описание настроек спам-фильтра, а также компонентов **SpIDer Gate** и **Офисный Контроль** приводится в руководстве **Антивирус Dr.Web® для Windows. Руководство пользователя**.

7.2.1. Настройка прав пользователей

Чтобы настроить права пользователей рабочей станции при помощи Центра Управления Dr.Web:

1. 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.
2. Редактирование прав осуществляется на следующих вкладках:
   - **Компоненты** - настройка прав для управления антивирусными компонентами. По умолчанию за пользователем сохранены права на запуск каждого из компонентов, но ему запрещено редактировать конфигурацию компонентов и останавливать их.
   - **Общие** - настройка прав для управления **Enterprise Агентом** и его функциями:
     - **Мобильный режим и использование BCO Dr.Web** - отключает пункт **Мобильный режим** в контекстном меню **Агента**.
     - **Создание локального расписания** - отключает пункт **Локальное** в группе настроек **Расписание** в контекстном меню **Агента**.

- **Смена режимов работы** - отключает пункт **Режим** и группу настроек **Устанавливаемые компоненты** в контекстном меню **Агента**.
- **Смена установок Dr.Web Enterprise Agent** - отключает в контекстном меню **Агента**, в группе настроек **Настройки** пункт **Синхронизировать время** и группу настроек **Уровень протокола**.
- **Остановка интерфейса Dr.Web Enterprise Agent** - отключает пункт **Выход** в контекстном меню **Агента**, если интерфейс **Агента** запущен под пользователем без административных прав.
- **Запрет доступа в сеть** - отключает пункт **Доступ к сети** в контекстном меню **Агента**.
- **Отключение защиты системы** - отключает группу настроек **Защита системы** в контекстном меню **Агента**.
- **Приостановка самозащиты** - отключает активность пункта **Самозащита** в контекстном меню **Агента**.
- **Деинсталляция Dr.Web Agent** - запрещает удаление **Агента** на станции как при помощи инсталлятора, так и штатными средствами ОС Windows (см. п. Удаление компонентов ПО для ОС Windows®). В этом случае удаление **Агента** можно осуществить только при помощи пункта **Общие** → **Деинсталлировать Dr.Web Enterprise Agent** на панели инструментов **Центра Управления**.

Для того чтобы изменить (предоставить или отнять) какое-либо из этих прав, установите или снимите соответствующий флаг.

При отключении какого-либо из пунктов, отвечающих за изменение настроек **Агента**, будет использоваться значение, которое было задано для данной настройки в последний раз перед отключением.

Описание действий, выполняемых соответствующими пунктами меню, приведено в документации **Dr.Web Агент для Windows. Руководство пользователя**.

3. Для того чтобы отказаться от данной конфигурации прав и вернуться к конфигурации по умолчанию, унаследованной от предустановленных групп, нажмите на кнопку **Удалить эти настройки**.
4. Вы также можете распространить эти настройки на другой объект, нажав на кнопку .
5. Чтобы экспортировать эти настройки в файл, нажмите .
6. Чтобы импортировать эти настройки из файла, нажмите .
7. Для того чтобы принять сделанные изменения прав, нажмите на кнопку **Сохранить**.

Если на момент редактирования настроек рабочей станции она не подключена к **Серверу**, то настройки будут приняты, как только **Агент** восстановит связь с **Сервером**.

7.2.2. Просмотр установленных компонентов антивирусного пакета

Компоненты

Чтобы узнать, какие компоненты антивирусного пакета установлены на рабочей станции:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы.
2. В открывшемся управляющем меню (панель слева) выберите пункт **Установленные компоненты**. Откроется окно со списком установленных компонентов.

Список установленных компонентов зависит от:

- Компонентов, разрешенных для использования в лицензионном ключе.
- ОС рабочей станции.
- Настроек, заданных администратором на **Сервере** антивирусной сети. Администратор может изменять состав компонентов антивирусного пакета на станции как перед установкой **Агента**, так и в любое время после его установки (см. Состав антивирусного пакета).

На сервера, выполняющие важные сетевые функции (домен-контроллеры, сервера раздачи лицензий и т.д.), не рекомендуется устанавливать компоненты **SpIDer Gate**, **SpIDer Mail** и **Dr.Web Firewall** во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса **Dr.Web**.

Вирусные базы

Чтобы узнать, какие вирусные базы установлены на рабочей станции:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции. В открывшемся управляющем меню (панель слева) выберите из подраздела **Таблицы** пункт **Вирусные базы**.
2. Откроется информационное окно с информацией об установленных вирусных базах: название файла, содержащего конкретную вирусную базу; версия вирусной базы; количество записей в вирусной базе; дата создания вирусной базы.

Если отображение пункта **Вирусные базы** отключено, для его включения выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**. На вкладке **Статистические данные** установите флаги **Мониторинг вирусных баз** и **Мониторинг состояния станции**, после чего перезагрузите **Сервер.**

7.2.3. Состав антивирусного пакета

Чтобы настроить список устанавливаемых компонентов антивирусного пакета:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке выберите станцию или группу. В открывшемся управляющем меню (панель слева) выберите пункт **Устанавливаемые компоненты**.
2. Для необходимых компонентов выберите в выпадающем списке один из вариантов:
   - **должен** - задает обязательное наличие компонента на станции. При создании новой станции компонент входит в состав устанавливаемого антивирусного пакета в обязательном порядке. При задании значения **должен** для уже существующей станции компонент будет добавлен в состав имеющегося антивирусного пакета;
   - **может** - определяет возможность установки антивирусного компонента. Решение об установке принимает пользователь;
   - **не может** - запрещает наличие компонента на станции. При создании новой станции компонент не входит в состав устанавливаемого антивирусного пакета. При задании значения **не может** для уже существующей станции компонент будет удален из состава антивирусного пакета.

В таблице 7-1 указано будет ли установлен компонент на станции (+) в зависимости от параметров, заданных пользователем, и настроек, заданных администратором на **Сервере**.

Таблица 7-1.

Параметры, заданные пользователем	Задано на Сервере		
	Должен	Может	Не может
Установить	+	+	
Не устанавливать	+		

3. Нажмите кнопку **Сохранить** для сохранения настроек и соответствующего изменения состава антивирусного пакета на станции.

Компонент **Антиспам VadeRetro** невозможно установить, если не установлен хотя бы один из следующих продуктов:

- **SpIDer Mail**,
- **Dr.Web plug-in для MS Outlook**,
- **Dr.Web для IBM Lotus Domino**,
- **Dr.Web для MS Exchange Server**,
- **Dr.Web для Qbik WinGate plug-in**.

7.3. Настройка Dr.Web Enterprise Agent для ОС Windows®

Чтобы просмотреть или изменить настройки Dr.Web Enterprise Agent на рабочей станции под управлением ОС Windows:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**.
2. В открывшемся окне в иерархическом списке нажмите на название станции или группы.
3. В открывшемся управляющем меню (панель слева) выберите пункт **Dr.Web Enterprise Agent для Windows**.
4. Откроется окно настроек **Агента**.

Внесение изменений в эти настройки, не согласованное с настройками **Сервера** (в частности, изменение режима шифрования и сжатия, а также ключа шифрования), приведет к утрате связи между **Агентом** и **Сервером**.

5. После внесении каких-либо изменений в настройки **Агента** при помощи **Центра Управления**, для принятия этих изменений, нажмите на кнопку **Сохранить**.

Вкладка Общие

На вкладке **Общие** указываются общие параметры **Агента**:

- В поле **Открытый ключ сервера** укажите путь к открытому ключу шифрования **Enterprise Сервера** на компьютере пользователя.
- В поле **Локальный ключевой файл Dr.Web** укажите путь к локальному лицензионному ключевому файлу продукта **Dr.Web**, если хотите, чтобы лицензионный ключевой файл хранился на станции в том числе. В противном случае, ключевой файл будет находиться только на **Сервере**.

- В поле **Периодичность отправки статистики (мин.)** введите значение временного интервала в минутах для отправки **Агентом** на **Сервер** всей статистической информации, собранной на станции.
- В выпадающем списке **Язык** задайте язык интерфейса **Агента** и компонентов **Антивируса Dr.Web** на рабочей станции или на группе рабочих станций под управлением ОС Windows.
- Установите флаг **Microsoft Network Access Protection** для включения поддержки технологии *Microsoft® Network Access Protection*, использующейся для мониторинга состояния станций (подробнее см. п. NAP Validator).
- Установите флаг **Синхронизировать время** для включения синхронизации системного времени на ПК с установленным **Агентом** и времени на ПК, на котором установлен **Dr.Web Enterprise Server**.
- Флаг **Запрещать модификацию системного файла HOSTS** устанавливает запрет на внесение изменения в файл HOSTS, который используется операционной системой для упрощения доступа к сети Интернет: для преобразования текстовых имен некоторых сайтов в соответствующие им IP-адреса. Изменение файла HOSTS может свидетельствовать о действии вредоносных программ.
- Флаг **Запрещать модификацию важных объектов Windows** устанавливает запрет на изменение критически важных объектов операционной системы (реестр и т.п.).

Вкладка Сеть

На вкладке **Сеть** находятся параметры, определяющие настройки взаимодействия с **Сервером**:

- В поле **Сервер** задается адрес **Enterprise Сервера.** Данное поле может оставаться пустым. В этом случае **Агент** будет использовать в качестве адреса **Enterprise Сервера** значение параметра, указанного в настройках на локальной машине пользователя (адрес **Сервера**, с которого производилась установка).

Может быть задан как один адрес **Сервера**, так и несколько адресов различных **Серверов**. Для добавления еще одного адреса **Сервера** нажмите на кнопку  и введите адрес в добавленное поле. Формат задания сетевых адресов **Сервера** описан в Приложении Е. Спецификация сетевого адреса.

Пример задания адреса **Сервера**:

tcp/10.4.0.18:2193
tcp/10.4.0.19
10.4.0.20

При задании нескольких адресов на стороне **Агента**, адреса **Серверов** пишутся через пробел в поле **Сервер** раздела **Настройки** → **Соединение**, вызываемого через контекстное меню значка **Агента**.

Если задать некорректное/неверное значение параметра **Сервер**, то **Агенты** отключатся от **Сервера** и больше не смогут к нему подключиться. В этом случае задание адреса **Сервера** необходимо производить непосредственно на станции.

- В поле **Повторений поиска** задайте параметр, определяющий количество попыток поиска **Dr.Web Enterprise Server** при подключении с использованием режима Mulicasting.
- В поле **Таймаут поиска (сек)** задайте промежуток между попытками поиска **Enterprise Сервера** в секундах при подключении с использованием режима Mulicasting.
- Поля **Режим сжатия** и **Режим шифрования** определяют соответствующие настройки сжатия и шифрования сетевого трафика (также см. п. Использование шифрования и сжатия трафика).

- В поле **Слушать сканирование сети** укажите UDP порт, используемый **Центром Управления** для поиска в сети работающих **Enterprise Агентов**. Чтобы запретить прослушивание портов, введите значение **NONE**.

  Параметр задается в формате сетевого адреса, приведенного в Приложении Е. Спецификация сетевого адреса.

  По умолчанию используется **udp/:2193**, что означает "все интерфейсы, порт 2193".

Вкладка Мобильность

На вкладке **Мобильность** задаются параметры *Мобильного режима* **Агента**:

- В поле **Периодичность обновлений (сек)** укажите временной промежуток между обновлениями антивирусного ПО в секундах.
- Установите флаг **Проверять подключение к Интернет** для включения проверки наличия подключения к сети Интернет перед началом процесса обновления.
- Установите флаг **Использовать прокси-сервер** для использования HTTP прокси-сервера при получении обновлений из сети Интернет. При этом станут активными поля настроек используемого прокси-сервера.

Вкладка Отчет

На вкладке **Отчет** задаются параметры ведения протокола **Агента**:

- В поле **Файл протокола** задается путь к файлу протокола и его название на компьютере пользователя.
- Параметр **Уровень протокола** определяет уровень подробности ведения протокола (см. также п. Ведение серверного протокола).
- Флаги: **Ограничение размера файла отчета**, **Сжимать старые файлы** и поля: **Хранить максимально** <...>

файлов размером <…> определяют такие параметры логирования как: количество и размер файлов протокола, а также необходимость сжатия старых файлов.

- Параметр **Количество файлов протокола обновления** определяет максимальное количество файлов протокола обновления.

Вкладка Интерфейс

На вкладке **Интерфейс** задаются параметры интерфейса **Enterprise Агента**.

В поле **Задержка приветствия** укажите время задержки показа приветственного сообщения после запуска интерфейса **Агента** в минутах. Установите значение этого параметра в **-1** для запрета показа приветственного сообщения. Приветственное сообщение выводится в виде всплывающего окна, содержащего название продукта **Dr.Web**, его версию и информацию об авторских правах.

На вкладке **Интерфейс** вы можете отметить тип сообщений о событиях, которые будет получать пользователь. Для этого установите соответствующий флаг:

- **Критические оповещения -** получать только критические оповещения. К таковым относятся периодические напоминания:
  - об ошибке обновления антивирусного ПО или какого-либо из его компонентов;
  - о необходимости перезагрузки компьютера после обновления.

  Сообщение выводится только в том случае, если пользователь имеет права администратора.
- **Оповещения о вирусах** - получать только оповещения о вирусах. К данному типу оповещений относятся сообщения об обнаружении вируса (вирусов) одним из компонентов антивирусного ПО.
- **Важные оповещения** - получать только важные оповещения. К таковым относятся сообщения:

- об ошибках при запуске какого-либо из компонентов антивирусного ПО;
- об ошибках обновления антивирусного ПО или какого-либо из его компонентов, отображается сразу после ошибочного завершения процедуры обновления;
- о необходимости перезагрузки компьютера после обновления, отображается сразу после обновления;
- о необходимости ожидания сообщения о требовании перезагрузки для окончания установки компонентов.

◆ **Малозначительные оповещения** - получать только малозначительные оповещения. К таковым относятся сообщения:

- о запуске удаленного сканирования;
- о завершении удаленного сканирования;
- о запуске обновления антивирусного ПО или какого-либо из его компонентов;
- об успешном завершении обновления антивирусного ПО или какого-либо из его компонентов (без необходимости перезагрузки).

Если вы хотите, чтобы пользователь получал все группы сообщений, установите все четыре флага. В противном случае будут выводиться только сообщения указанных групп.

Пользователь может управлять получением оповещений, кроме **Критических оповещений**, получение которых настраивает только администратор.

7.4. Настройка расписания заданий на рабочей станции

Расписание - это список действий, выполняемых автоматически в заданное время на станциях. Основное применение расписаний - осуществлять сканирование станций на вирусы в наиболее удобное для пользователей время без необходимости ручного

запуска **Сканера**. Кроме этого, **Enterprise Агент** позволяет выполнять некоторые другие типы действий, описанные ниже.

Расписания бывают двух типов:

- *Централизованное расписание*. Расписание, задаваемое администратором антивирусной сети и подчиняющееся всем правилам наследования конфигураций.
- *Локальное расписание* станции. Расписание, задаваемое пользователем на конкретной станции (при наличии у данной станции прав), хранящееся локально на этой станции; данное расписание не является объектом, управляемым **Enterprise Сервером**.

Централизованное расписание

Редактирование централизованного расписания регулярного выполнения заданий определенной рабочей станции (а также групп) осуществляется при помощи **Центра Управления**.

Для редактирования централизованного расписания выполните следующие действия:

1. Для того чтобы открыть окно редактирования расписания выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите пункт **Расписание**.
2. Вы можете удалять имеющиеся задания, добавлять новые или редактировать имеющиеся. Вы также можете запретить выполнение задания или разрешить выполнение ранее запрещенного задания. Данное действие подробно описывается ниже.

   По умолчанию для станций под управлением ОС Windows и ОС Windows Mobile расписание содержит 2 задания:

   - **Startup scan** - сканирование станции при старте (разрешено),

- **Daily scan** - ежедневное сканирование станции (запрещено).

3. По окончании редактирования расписания нажмите на кнопку **Сохранить**, чтобы принять изменения.

Если в результате редактирования будет создано пустое (не содержащее заданий) расписание, **Центр Управления** предложит вам либо использовать наследуемое от групп расписание, либо использовать пустое расписание. Пустое расписание необходимо задать в том случае, если вы хотите отказаться от расписания, наследуемого от групп.

Чтобы добавить новое задание:

1. Для создания нового задания нажмите на кнопку **Новое задание** на панели инструментов **Центра Управления**.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

2. На вкладке **Общие** задайте следующие параметры:
   - Введите в поле **Название** наименование задания, под которым оно будет отображаться в расписании.
   - Чтобы активировать выполнение задания, установите флаг **Разрешить исполнение**.

   Если флаг не установлен, задание будет присутствовать в списке, но не будет исполняться.
   - Установленный флаг **Критичное задание** дает указание выполнить задание при следующем запуске **Enterprise Агента**, если выполнение данного задания будет пропущено (**Enterprise Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Enterprise Агента** оно выполняется 1 раз.

Если при запуске станции должны выполниться несколько заданий на сканирование при помощи одного и того же сканера (**Сканера для Windows** или **Enterprise Сканера**), то будет выполнено только одно из них - первое, стоящее в очереди.

Например, если разрешено задание **Startup scan** (сканирование станции при старте) и при этом было отложено критичное задание на сканирование при помощи **Enterprise Сканера**, то при запуске станции будет выполняться **Startup scan**, а отложенное критическое сканирование не сможет быть выполнено.

3. На вкладке **Действие** выберите из выпадающего списка **Действие** тип задания. После сделанного выбора нижняя часть окна будет различной для разных альтернатив.
   - Если выбран **Запуск**, введите в поле **Путь** полное имя (с путем) исполняемого файла, который предполагается запускать, а в поле **Аргументы** - параметры командной строки для запускаемой программы.
   - Если выбрано **Dr.Web Сканер для Windows** или **Dr.Web Enterprise Scanner для Windows**, откроется окно настройки сканирования, описанное в п. Запуск и остановка антивирусного сканера на рабочей станции.
   - Если выбрано **Протоколирование**, введите в поле **Строка** текст сообщения, печатаемого в протокол.
4. На вкладке **Время** настройте время запуска задания.

   Для этого в первую очередь выберите в выпадающем списке **Периодичность** один из режимов запуска:

   - Ежедневно,
   - Ежемесячно,
   - Еженедельно,
   - Ежечасно,
   - Каждые X минут,
   - Стартовое.

Описание параметров каждого из режимов приводится в таблице 7-2.

5. По окончании ввода параметров задания нажмите на кнопку **Сохранить**.

Таблица 7-2. Режимы запуска и их параметры

Режим запуска	Параметры и описание
Ежедневно	Необходимо ввести час и минуту — задание будет запускаться ежедневно в указанное время.
Ежемесячно	Необходимо выбрать число (день месяца), ввести час и минуту — задание будет запускаться в заданный день месяца в указанное время.
Еженедельно	Необходимо выбрать день недели, ввести час и минуту — задание будет запускаться в заданный день недели в указанное время.
Ежечасно	Необходимо ввести число от 0 до 59, задающее минуту каждого часа, в которую будет запускаться задание.
Каждые X минут	Необходимо ввести значение **X**. При **X** равном 60 или больше задание будет запускаться каждые **X** минут. При **X** меньше 60 задание будет запускаться в каждую минуту часа, кратную **X**.
Стартовое	Дополнительные параметры не требуются. Задание будет запускаться при старте работы **Агента**.

Чтобы отредактировать имеющееся задание: выберите задание из списка, нажав на него левой кнопкой мыши. Дальнейшие действия аналогичны вводу нового задания (см. выше).

Чтобы удалить какое-либо задание:

1. Установите флаг напротив задания.
2. Нажмите на кнопку **Удалить эти настройки** на панели инструментов **Центра Управления**.

Локальное расписание

Чтобы отредактировать локальное расписание рабочей станции:

1. В контекстном меню **Агента** в пункте **Расписание** выберите вариант **Локальное**.
2. Откроется окно редактирования локального расписания **Enterprise Агента**.

В контекстном меню **Агента** в пункте **Расписание** вариант **Локальное** будет доступен только в том случае, если при редактировании прав антивирусной станции был установлен флаг **Создание локального расписания**.

Используя локальное расписание, пользователь может запускать сканирование с заданием параметров. Варианты задания объектов сканирования, ключи командной строки, задающие параметры программы, а также параметры командной строки для **Сканера** описаны в руководстве **Антивирус Dr.Web® для Windows. Руководство пользователя.**

3. По окончании редактирования нажмите на кнопку **Закрыть**.

При установках рабочей станции по умолчанию, т.е. без всякого вмешательства администратора антивирусной сети, на рабочей станции работает антивирусный монитор, а также периодически запускаются задания на обновление ПО и антивирусное сканирование.

7.5. Антивирусное сканирование рабочей станции

Пользователь рабочей станции может производить антивирусное сканирование станции самостоятельно, используя компонент **Dr.Web Сканер для Windows**. Значок для запуска этого компонента при установке антивирусного ПО размещается на рабочем столе. Запуск и успешная работа **Сканера** возможна даже при неработоспособности **Агента**, в том числе при загрузке ОС Windows в безопасном режиме.

Для каждой станции вы можете:

- Просматривать список всех запущенных в настоящее время антивирусных компонентов.
- Прерывать запущенные антивирусные компоненты по типам.
- Запускать задания на антивирусное сканирование с настройкой параметров сканирования. Сканирования могут быть запущены для:
  - **Dr.Web Сканера для Windows**,
  - **Dr.Web Enterprise Сканера для Windows**,
  - **Dr.Web Enterprise Сканера для Unix**,
  - **Dr.Web Enterprise Сканера для Mac OS X**.

7.5.1. Просмотр и прерывание работы запущенных компонентов

Для просмотра списка и завершения работы запущенных компонентов:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите пункт **Запущенные компоненты**.

   Откроется список всех активных в настоящее время компонентов, как запущенных вручную вами или пользователем, так и запущенных по расписанию.

2. При необходимости прервать какой-либо из компонентов, установите флаг напротив этого компонента, после чего на панели инструментов нажмите на кнопку **Прервать**. Компонент будет остановлен и удален из списка.

7.5.2. Прерывание работы запущенных компонентов по типам

При использовании данной опции буду прерваны текущие сканирования и запущенные мониторы, за исключением **SpIDer Guard**.

Внимание! Запуск мониторов **SpIDer Mail** и **SpIDer Gate** из **Центра Управления** невозможен.

Вы можете прервать компоненты на рабочей станции:

- запущенные вручную вами,
- запущенные пользователем,
- запущенные по расписанию.

Вы также можете прервать сразу все исполняемые компоненты, удовлетворяющие определенному критерию. Это особенно удобно, если такую команду выдают сразу многим станциям.

Чтобы прервать все исполняемые компоненты определенного типа:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке выберите необходимую группу или отдельные антивирусные станции.
2. На панели инструментов каталога антивирусной сети нажмите **Управление компонентами**. В выпадающем списке выберите пункт **Прервать запущенные**. Откроется окно настройки типа прерываемых компонентов.
3. Установите флаги напротив названий тех типов компонентов, которые вы хотите немедленно прервать, либо напротив заголовка области **Прерывание сканирований** - для выбора всех процессов из списка.
4. Нажмите на кнопку **Прервать**.

7.5.3. Запуск сканирования рабочей станции

Чтобы запустить задание на сканирование:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**.
2. В открывшемся окне в иерархическом списке нажмите на название станции или группы.
3. На панели инструментов нажмите на пункт **Сканировать**.
4. В открывшемся списке на панели инструментов выберите один из режимов сканирования:

   Dr.Web Сканер для Windows. Быстрое сканирование. В данном режиме производится сканирование следующих объектов:

   - оперативная память,

- загрузочные секторы всех дисков,
- объекты автозапуска,
- корневой каталог загрузочного диска,
- корневой каталог диска установки ОС Windows,
- системный каталог ОС Windows,
- папка `Мои Документы`,
- временный каталог системы,
- временный каталог пользователя.

При выборе данного пункта начнется проверка на вирусы с параметрами **Сканера**, заданными по умолчанию.

 **Dr.Web Сканер для Windows. Полное сканирование**. В данном режиме производится полное сканирование всех жестких дисков и сменных носителей (включая загрузочные секторы). При выборе данного пункта начнется сканирование с параметрами **Сканера**, заданными по умолчанию.

 **Dr.Web Сканер для Windows. Выборочное сканирование**. Данный режим предоставляет возможность выбрать любые папки и файлы для последующего сканирования. При выборе данного пункта откроется окно настройки **Сканера**. Задайте параметры сканирования и состав проверяемых объектов файловой системы (эти действия подробно описываются ниже) и нажмите кнопку **Проверить на вирусы**.

 **Dr.Web Enterprise Сканер для Windows**. В данном режиме осуществляется выборочное сканирование при помощи **Dr.Web Enterprise Сканера**. При выборе данного пункта откроется окно настройки **Сканера**. Задайте параметры сканирования и состав проверяемых объектов файловой системы (эти действия подробно описываются ниже) и нажмите кнопку **Проверить на вирусы**.

 **Dr.Web Enterprise Сканер для Unix**. Для сканирования станций, работающих под ОС семейства UNIX. Задайте параметры сканирования и состав проверяемых объектов файловой системы и нажмите кнопку **Проверить на вирусы**.

 **Dr.Web Enterprise Сканер для Mac OS X**. Для сканирования станций, работающих под ОС семейства Mac OS X. Задайте параметры сканирования и состав проверяемых объектов файловой системы и нажмите кнопку **Проверить на вирусы**.

7.5.4. Настройка параметров Сканера для ОС Windows®

Для просмотра и редактирования параметров Сканера доступны несколько вариантов:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите пункт **Dr.Web Сканер для Windows**. Откроется окно настроек **Сканера**. Данный список параметров является наиболее полным и включает все группы параметров, описанные ниже.
2. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. На панели инструментов нажмите на пункт  **Сканировать**. В открывшемся списке на панели инструментов выберите пункт  **Dr.Web Сканер для Windows. Выборочное сканирование**. На панели справа откроется окно настроек **Сканера**. Данный список параметров является сокращенным и позволяет настроить только основные параметры, входящие в группы настроек **Общие**, **Действия**, **Отчет** и **Прочее**.

3. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. На панели инструментов нажмите на пункт **Сканировать**. В открывшемся списке на панели инструментов выберите пункт **Dr.Web Enterprise Сканер для Windows**. На панели справа откроется окно настроек **Сканера**. Данный список параметров позволяет задать только основные параметры для **Enterprise Сканера**, входящие в группы настроек **Общие**, **Действия** и **Исключаемые пути**.

Общие

- Флаг **Эвристический анализ** установлен по умолчанию; при этом **Сканер** пытается обнаруживать неизвестные вирусы при помощи эвристического анализатора. В данном режиме возможны ложные срабатывания **Сканера**.
- Флаг **Проверка архивов** установлен по умолчанию. Предписывает **Сканеру** искать вирусы в файлах, упакованных в файловые архивы.
- Флаг **Проверка почтовых файлов** установлен по умолчанию. Предписывает проверять почтовые ящики.
- Флаг **Проверка работающих модулей и процессов (Проверка памяти** для **Enterprise Сканера**) установлен по умолчанию. Предписывает проверять процессы, запущенные в оперативной памяти.
- Флаг **Проверка автоматически запускаемых программ** установлен по умолчанию. Предписывает проверять файлы, автоматически запускаемые при старте операционной системы.
- Флаг **Проверка загрузочных секторов** установлен по умолчанию. Предписывает **Сканеру** проверку загрузочных секторов. Проверяются как загрузочные секторы логических дисков, так и главные загрузочные секторы физических дисков.

- Флаг **Проверка подкаталогов** (отсутствует для **Enterprise Сканера**) установлен по умолчанию. Используется при задании пути на сканирование и предписывает **Сканеру** проверять не только файлы, но и все вложенные подкаталоги по заданному пути.

При задании настроек Сканера через пункт управляющего меню Dr.Web Сканер для Windows доступны следующие параметры:

- Флаг **Проверять файл HOSTS** предписывает проверку состояния системного файла HOSTS, который используется операционной системой для упрощения доступа к сети Интернет: для преобразования текстовых имен некоторых сайтов в соответствующие им IP-адреса. Изменение файла HOSTS может свидетельствовать о действии вредоносных программ.
- Пункт **Сканировать** определяет режим проверки. В выпадающем списке выберите один из вариантов:
  - **Все файлы** - для сканирования всех файлов, независимо от их имени и расширения.
  - **По маске** - для сканирования только тех файлов, имена и расширения которых входят в список, задаваемый в разделе **Список масок**.
  - **Перечисленные типы** - для сканирования только тех файлов, расширения которых входят в список, задаваемый в разделе **Список расширений**.
- Флаг **Подтверждение действий** предписывает получение пользователем сообщений о событиях и запросов на подтверждение действий **Сканера**.
- Флаг **Запрос проверки следующей дискеты** используется при проверке сменных носителей информации (накопителей на магнитных дисках (дискеты), CD/DVD-дисков, flash-накопителей) и предписывает выдачу запроса на подключение (смену текущего) и проверку следующего носителя информации.

При задании настроек Сканера при вызове его из панели инструментов выберите один из двух альтернативных режимов:

1. **Сканировать все диски**.

   для **Enterprise Сканера** в варианте **Сканировать все диски** задайте, какие из дисков системы должны проверяться:

   - установите флаг **Стационарные диски** для проверки стационарных жестких дисков (винчестер и т.п.);
   - установите флаг **Сменные диски** для проверки всех сменных носителей информации, таких как: накопители на магнитных дисках (дискеты), CD/DVD-диски, flash-накопители и т.д.

   В данном режиме также может быть задан список **Исключаемые пути** (способ их задания описывается ниже).

2. **Сканировать указанные пути**.

   В варианте **Сканировать указанные пути** задайте список проверяемых путей (способ их задания описывается ниже).

Для Enterprise Сканера для Windows также доступны следующие флаги:

- Флаг **BurstScan технология** предписывает использовать данную технологию, значительно ускоряющую сканирование на современных системах, оснащенных многоядерными процессорами.
- Установленный по умолчанию флаг **Низкоприоритетная проверка** позволяет снизить нагрузку **Сканера** на имеющиеся вычислительные ресурсы системы. При этом остальные процессы могут обладать более высоким приоритетом при исполнении, чем в случае выключенной настройки. Это достигается путем динамического изменения приоритетов потоков сканирования.
- Флаг **Проверка контейнеров** предписывает **Сканеру** проверять файловые контейнеры различных типов.
- Список **Действия после сканирования** предписывает

автоматическое выполнение заданного действия сразу после окончания процесса сканирования: выключить, перезагрузить, перевести в соответствующий режим, либо не предпринимать никаких действий над компьютером пользователя.

- Флаг **Отключить сеть при сканировании** позволяет отключить компьютер от локальной сети и Интернета на время сканирования.

В разделе **Ограничения** доступны следующие настройки:

- **Максимальное время сканирования** - максимальное время в миллисекундах, в течение которого объект проверяется. По истечении указанного времени проверка объекта будет прекращена.
- **Максимальная глубина вложенности архива** - если уровень вложенности в архив превышает указанный, проверка будет производиться только до указанного уровня вложенности.
- **Максимальный размер архива** - если размер архива превышает указанный, распаковка и проверка производиться не будет.
- **Максимальный уровень сжатия** - если **Сканер** определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка производиться не будет.
- **Максимальный размер распакованного объекта (КБ)** - если **Сканер** определяет, что после распаковки архив будет больше указанного размера в (килобайтах), распаковка и проверка производиться не будет.
- **Порог проверки уровня сжатия** - минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия.

Действия

В группе параметров **Действия** задается реакция **Антивируса** на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов.

Предусмотрены следующие действия над обнаруженными объектами:

- **Лечить** - восстановить состояние инфицированного объекта до заражения. При невозможности лечения применяется настройка, заданная для неизлечимых объектов.

  Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

- **Удалять** - удалить зараженные объекты.
- **В карантин** - переместить зараженные объекты в каталог **Карантина**.
- **Переименовывать** - переименовать зараженные объекты в соответствии с правилом, заданным в поле **Шаблон для переименования**.
- **Информировать** - ограничиться оповещением об обнаружении вируса (о настройке режима оповещений см. в п. Настройка оповещений).
- **Игнорировать** - пропустить объект без выполнения каких-либо действий и не выводить оповещения.

Таблица 7-3. Действия Сканера над обнаруженными вредоносными объектами

Действие	Объект				
	Рекламные программы	Зараженные контейнеры	Заражен-ные	Подозри-тельные	Неизлечи-мые
Лечить			+/*		
Удалять	+	+	+	+	+
В карантин	+	+/*	+	+	+/*
Переимено-вывать	+	+	+	+	+
Информи-ровать	+/*	+	+	+/*	+
Игнориро-вать	+				

Условные обозначения

+	действие разрешено для данного типов объектов
+/*	действие установлено как реакция по умолчанию для данного типов объектов

Для задания действий над обнаруженными вредоносными объектами служат следующие настройки:

- В поле **Шаблон для переименования** указывается маска расширения, которое получают переименованные объекты, если для них было указано действие **Переименовывать** при обнаружении. По умолчанию предлагается вариант `#??`, т.е. первый символ расширения заменяется на символ `#`. Данную маску можно изменять, однако в качестве замены не следует использовать стандартные расширения (`EXE`, `COM`, `BAT`, `DOC`, `PAS`, `BAS` и пр.).
- Выпадающий список **Рекламные программы** задает реакцию **Сканера** на обнаружение данной разновидности нежелательного ПО.

При задании действия **Игнорировать** для рекламных программ не будет произведено никаких действий: пользователю не будет выдано предупреждение, как в случае включенной опции **Информировать** при обнаружении вируса.

- Аналогично действиям над рекламными программами, настраивается реакция **Сканера** при обнаружении прочего нежелательного ПО, такого как:
  - программы дозвона;
  - программы-шутки;
  - потенциально опасные;
  - программы взлома.
- Выпадающий список **Перезагрузка** задает режим перезагрузки компьютера после завершения сканирования.
- Выпадающий список **Зараженные контейнеры** задает реакцию **Сканера** на обнаружение зараженного или подозрительного файла в составе файлового архива или контейнера. Реакция задается для всего архива в целом.
- Выпадающий список **Зараженные** задает реакцию **Сканера** на обнаружение файла, зараженного известным вирусом.
- Выпадающий список **Подозрительные** задает реакцию **Сканера** на обнаружение файла, предположительно зараженного вирусом (срабатывание эвристического анализатора).

При сканировании, включающем каталог установки ОС, рекомендуется выбрать для подозрительных файлов реакцию **Информировать**.

- Выпадающий список **Неизлечимые** задает реакцию **Сканера** на обнаружение файла, зараженного известным неизлечимым вирусом (а также когда предпринятая попытка излечения не принесла успеха).

- Флаг **Разрешить удаление архивов** позволяет удалять обнаруженные зараженные архивы и почтовые файлы. Если данный флаг установлен, то в разделах **Зараженные архивы** и **Зараженные почтовые файлы**, расположенных ниже, будет присутствовать вариант действий **Удалять**. При снятии данного флага, допустимы только действия **В карантин** (по умолчанию для архивов), **Переименовывать** и **Информировать** (по умолчанию для почтовых файлов).

Исключаемые пути и Исключаемые файлы

При редактировании списков исключаемых путей и файлов:

- Введите требуемый путь или файл в строку **Исключаемые пути** или **Исключаемые файлы** соответственно.
- Для того чтобы добавить новую строку в список, нажмите на кнопку  и в открывшуюся строку введите требуемый путь.
- Для того чтобы удалить элемент из списка, нажмите на кнопку  напротив соответствующей строки.

Список исключаемых объектов может содержать элементы следующих видов:

1. Прямой путь в явном виде до исключаемого объекта. При этом:
   - Символ \ или / – исключение из проверки всего диска, на котором находится каталог установки ОС Windows,
   - Путь, заканчивающийся символом \ – данный каталог исключается из проверки,
   - Путь, не заканчивающийся символом \ – любой подкаталог, путь к которому начинается на указанную строку, исключается из проверки.

   Например: `C:\Windows` - не проверять файлы каталога `C:\Windows` и все его подкаталоги.

2. Маски объектов, исключаемых из проверки. Для задания

масок допускается использование знаков ? и *.

Например: C:\Windows**.dll - не проверять все файлы с расширением dll, расположенные во всех подкаталогах каталога C:\Windows.

3. Регулярное выражение. Пути могут задаваться регулярными выражениями. Также любой файл, полное имя которого (с путем) соответствует регулярному выражению, исключается из проверки.

Перед запуском процесса сканирования на вирусы ознакомьтесь с рекомендациями по использованию антивирусных программ для компьютеров под управлением ОС Windows Server 2003, ОС Windows 2000 и ОС Windows XP. Статья, содержащая необходимую информацию, находится по адресу - http://support.microsoft.com/kb/822158/ru. Материал данной статьи призван помочь оптимизировать производительность системы.

Синтаксис регулярных выражений, используемых для записи исключаемых путей, следующий:
qr{выражение}флаги

Наиболее часто в качества флага используется символ i, данный флаг означает "не принимать во внимание различие регистра букв".

Примеры записи исключаемых путей и файлов при помощи регулярных выражений приведены ниже:

- qr{\\pagefile\.sys$}i — не проверять файлы подкачки ОС Windows NT,
- qr{\\notepad\.exe$}i — не проверять файлы notepad.exe,
- qr{^C:}i — не проверять вообще ничего на диске C,
- qr{^.:\\WINNT\\}i — не проверять ничего в каталогах WINNT на всех дисках,
- qr{(^C:)|(^.:\\WINNT\\)}i — объединение двух

предыдущих случаев,

- `qr{^C:\\dir1\\dir2\\file\.ext$}i` — не проверять файл `c:\dir1\dir2\file.ext`,
- `qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i` — не проверять файл `file.ext`, если он в каталоге `c:\dir1\dir2` и его подкаталогах,
- `qr{^C:\\dir1\dir2\\}i` — не проверять каталог `c:\dir1\dir2` и его подкаталоги,
- `qr{dir\\[^\\]+}i` — не проверять подкаталог `dir`, находящийся в любом каталоге, но проверять подкаталоги,
- `qr{dir\\}i` — не проверять подкаталог `dir`, находящийся в любом каталоге, и его подкаталоги.

Использование регулярных выражений кратко описано в Приложении К.

Ссылки на подробные описания синтаксиса регулярных выражений см. в п. Ссылки.

Список расширений (при вызове настроек через управляющее меню)

Раздел **Список расширений** активен только в том случае, когда в разделе **Общие** в пункте **Сканировать** задан вариант **Перечисленные типы**. При этом сканированию подлежат только те файлы, расширения которых входят в данный список.

При изменении списка расширений используйте кнопку  для добавления новых элементов списка, кнопку  - для удаления имеющихся элементов списка.

В элементах списка расширений могут использоваться специальные символы `*` и `?`. По умолчанию хранится список расширений исполняемых и архивных файлов. Для восстановления списка по умолчанию используйте кнопку  .

Список масок (при вызове настроек через управляющее меню)

Раздел **Список масок** активен только в том случае, когда в разделе **Общие** в пункте **Сканировать** задан вариант **По маске**. При этом сканированию подлежат только те файлы, имена и расширения которых входят в данный список.

При изменении списка масок используйте кнопку  для добавления новых элементов списка, кнопку  - для удаления имеющихся элементов списка.

В элементах списка расширений могут использоваться специальные символы `*` и `?`. По умолчанию хранится список исполняемых и архивных файлов. Для восстановления списка по умолчанию используйте кнопку  .

Прочее (кроме Enterprise Сканера)

В разделе **Прочее** указываются дополнительные параметры **Сканера**:

- Флаг **Использовать диск для создания файла подкачки** предписывает использование жесткого диска для создания файла подкачки во избежание нехватки оперативной памяти, используемой **Сканером** при проверке данных больших объемов (крупных архивов и т.п.).
- Флаг **Восстановить дату доступа** предписывает после сканирования восстанавливать дату последнего обращения к файлу (заменять на дату перед началом сканирования).
- Флаг **Сохранять настройки автоматически** предписывает автоматическое сохранение настроек конфигурации **Сканера** после завершения текущего сеанса работы.

- В списке **Приоритет сканирования** задается приоритет потоков процесса сканирования. Выберите один из предложенных вариантов:
  - **простаивающий** - не рекомендуется устанавливать данный уровень приоритета, во избежание замедления работы **Сканера** и, соответственно, значительного увеличения времени сканирования,
  - **низший**,
  - **ниже обычного**,
  - **обычный** - рекомендуемый приоритет сканирования,
  - **выше обычного**,
  - **высший**,
  - **критичный ко времени** - не рекомендуется устанавливать данный уровень приоритета, во избежание сильной загрузки операционной системы **Сканером** во время сканирования.

Отчет

В разделе **Отчет** вы можете назначить ведение файла протокола работы **Сканера**. Для этого установите флаг **Записывать отчет в файл** и задайте необходимые параметры ведения протокола.

Звуки (при вызове настроек через управляющее меню)

В разделе **Звуки** вы можете задать воспроизведение звуковых файлов для событий определенных типов. Для этого установите флаг **Проигрывать звуки** и задайте имена звуковых файлов в полях, соответствующих конкретным событиям.

7.6. Просмотр результатов работы и итоговой статистики по рабочей станции

При помощи управляющего меню раздела **Антивирусная сеть** вы можете просматривать следующую информацию:

- Таблицы - для просмотра табличных данных по статистике работы антивирусных средств на станции, по состоянию рабочих станций и антивирусных средств.
- Графики - для просмотра графиков с информацией о заражениях, обнаруженных на станциях.
- Сводные данные - для просмотра и сохранения отчетов, содержащих все сводные статистические данные или выборочные сводки по заданным типам таблиц.
- Карантин - для просмотра и удаленного редактирования содержимого **Карантина** на рабочей станции.

7.6.1. Таблицы

Для просмотра таблиц:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы.
2. В открывшемся управляющем меню (панель слева) выберите нужный пункт из подраздела **Таблицы**.

Раздел меню **Таблицы** содержит следующие пункты:

- **Сводные данные** - для просмотра и сохранения отчетов, содержащих все сводные статистические данные или выборочные сводки по заданным типам таблиц. Не отображается в меню, если скрыты все остальные пункты меню в разделе **Таблицы** (см. п. Сводные данные).

- **Инфекции** - для просмотра информации об обнаружении вирусов (перечень зараженных объектов, вирус, действия антивируса и т. п.).
- **Ошибки** - для просмотра списка ошибок сканирования на выбранной рабочей станции за определенный период.
- **Статистика** - для получения статистики о работе антивирусных средств на станции (см. п. Статистика).
- **Запуск/Завершение** - для просмотра списка компонентов, запускавшихся на рабочей станции.
- **Вирусы** - для просмотра сведений об обнаружении вирусов на станции, сгруппированных по типам вирусов.
- **Состояние** - для просмотра сведения о необычном и (возможно) требующем вмешательства состоянии рабочих станций за определенный период (см. п. Состояние).
- **Задания** - для просмотра списка заданий, назначенных для рабочей станции в заданный период.
- **Суммарная статистика** - для получения суммарной статистики без разбиения на сеансы.
- **Вирусные базы** - для просмотра информации об установленных вирусных базах: название файла, содержащего конкретную вирусную базу; версия вирусной базы; количество записей в вирусной базе; дата создания вирусной базы. Пункт доступен только при выборе станций.
- **Модули** - для просмотра подробной информации обо всех модулях антивируса **Dr.Web**: описание модуля - его функциональное название; файл, определяющий отдельный модуль продукта; полная версия модуля и т.д. Пункт доступен только при выборе станций.
- **Все сетевые инсталляции** - для просмотра списка установок ПО на рабочую станцию.

Для отображения скрытых пунктов раздела **Таблицы** выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**. На вкладке **Статистические данные** установите соответствующие флаги (см. ниже), после чего нажмите **Сохранить** и перезагрузите **Сервер**.

Таблица 7-4. Соответствие пунктов раздела Таблицы и флагов раздела Статистические данные

Пункты раздела Таблицы	Флаги раздела Статистические данные
Инфекции	Инфекции в БД
Ошибки	Ошибки сканирования в БД
Статистика	Статистика сканирования в БД
Запуск/Завершение	Информация о запуске/завершении компонентов в БД
Вирусы	Инфекции в БД
Состояние	Мониторинг состояния станции
Задания	Протокол выполнения заданий
Суммарная статистика	Статистика сканирования в БД
Вирусные базы	Мониторинг состояния станции Мониторинг вирусных баз Протокол выполнения заданий
Модули	Список модулей станции в БД
Все сетевые инсталляции	Информация об установках агента в БД

Окна просмотра результатов работы различных компонентов и итоговой статистики рабочей станции имеют одинаковый интерфейс, и действия по детализации информации, предоставляемой ими, аналогичны.

Далее рассмотрены некоторые примеры просмотра итоговой статистики при помощи **Центра Управления**.

Статистика

Для получения статистики о работе антивирусных средств на станции:

1. Выберите в списке нужную станцию или группу.

При необходимости просмотра статистики по нескольким станциям или группам, возможен одновременный выбор нужных станций с помощью клавиш SHIFT или CTRL.

2. В управляющем меню (панель слева) в разделе **Таблицы** выберите пункт **Статистика**.
3. Откроется окно статистики. По умолчанию отображается статистика за последние сутки.
4. Для отображения данных за определенный период либо укажите диапазон времени относительно сегодняшнего дня из выпадающего списка, либо задайте произвольный диапазон дат на панели инструментов. Для задания произвольного диапазона введите требуемые даты или нажмите на значки календаря рядом с полями дат. Для того чтобы загрузить данные, нажмите на кнопку **Обновить**. В окно будут загружены таблицы со статистическими данными.
5. В разделе **Общая статистика** приведены суммарные данные:
   - при выборе станций - по выбранным станциям;
   - при выборе групп - по выбранным группам. При выборе нескольких групп будут показаны только группы, содержащие станции;
   - при выборе станций и групп одновременно - отдельно по всем станциям, в том числе, входящим в выбранные не пустые группы.
6. Для того чтобы посмотреть подробную статистику работы конкретных антивирусных средств, нажмите на название станции в таблице. Если были выбраны группы, нажмите на название группы в таблице общей статистики, после чего - на название станции в показанной таблице. Откроется окно (или раздел текущего окна), содержащее таблицу с подробными статистическими данными.
7. Из таблицы со статистикой работы антивирусных средств станции или группы можно открыть окно настройки конкретного антивирусного компонента. Для этого нажмите на соответствующее название компонента в статистической таблице.

8. Чтобы произвести сортировку данных столбца таблицы, нажмите на соответствующую стрелку (сортировка по убыванию или по возрастанию) в заголовке соответствующего столбца.
9. При необходимости сохранить таблицу статистики для распечатки или дальнейшей обработки нажмите на кнопку  **Записать данные в файл в формате CSV**, на кнопку  **Записать данные в файл в формате HTML** или на кнопку  **Записать данные в файл в формате XML**.
10. Для того чтобы получить суммарную статистику без разбиения на сеансы, нажмите на пункт **Суммарная статистика** в управляющем меню. Откроется окно суммарной статистики.
11. Для того чтобы просмотреть статистику по вирусным событиям в форме диаграмм, в управляющем меню (панель слева) выберите пункт **Графики**. Откроется окно просмотра статистических диаграмм (подробное описание см. ниже).

Состояние

Для просмотра сведений о состоянии рабочих станций за определенный период:

1. Выберите в управляющем меню в разделе **Таблицы** пункт **Состояние**.
2. Сведения о состоянии станций отображаются в окне автоматически в соответствии с параметрами, указанными на панели инструментов.
3. Для того чтобы ограничить список сообщений о состоянии только сообщениями определенной серьезности, выберите уровень серьезности в выпадающем списке **Серьезность** на панели инструментов. По умолчанию выбран уровень серьезности **Очень низкая**, что соответствует отображению максимального списка.
4. В список также будут включены станции, не имевшие связи с **Сервером** в течение определенного числа дней. Укажите

это число в поле ввода слева от списка **Серьезность**. При превышении данного значения, ситуация считается критической, и данная информация будет отображаться в окне раздела **Состояние**.

5. Действия по детализации и форматированию информации данной таблицы аналогичны описанным выше для таблицы статистики.

Вы также можете просмотреть результаты работы и статистику нескольких рабочих станций. Для этого необходимо отметить эти станции в каталоге сети.

7.6.2. Графики

Графики заражений

Для просмотра общих графиков с информацией об обнаруженных заражениях:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите в разделе **Общие** пункт **Графики**.
2. Откроется окно, содержащее следующие графические данные:
   - **Десять самых распространенных вирусов** - приводится список из десяти вирусов, инфицировавших наибольшее количество файлов. На графике отображаются численные данные по объектам, которые были заражены указанными вирусами.

- **Посуточная активность вирусов** - заданный временной период разбивается по суткам. На графике отображается общее количество вирусов, найденных в пределах каждых суток для всех выбранных объектов сети (станций и групп). График отображается, если задан временной период, превышающий одни сутки.
- **Классы заражений** - отображаются численные данные по объектам, разделенным в соответствии с классификацией заражения.
- **Количество зараженных машин в группе** - отображаются численные данные по количеству зараженных станций для каждой группы, в которой такие станции присутствуют.
- **Произведенные действия** - отображаются численные данные по инфицированным объектам, над которыми были совершены действия, предусмотренные антивирусным ПО.

3. Для просмотра графических данных за предопределенный период выберите диапазон из выпадающего списка на панели задач: отчет за определенный день или месяц. Либо вы можете выбрать произвольный диапазон дат, для этого введите требуемые даты или нажмите на значки календаря рядом с полями дат. Для просмотра данных нажмите на кнопку **Обновить**.

Графики итоговой статистики

Графические данные приводятся в пункте **Графики** раздела **Общие** и в некоторых пунктах раздела **Таблицы** управляющего меню.

В зависимости от того, какой объект выбран в иерархическом списке (группа или станция), будут отображаться различные наборы графиков. В таблице ниже приведен список возможных графиков и разделы управляющего меню, в которых данные графики отображаются, в зависимости от выбранного в иерархическом списке объекта.

Таблица 7-5. Соответствие графиков выбранным пунктам иерархического списка и разделам управляющего меню

Графики	Для групп	Для станций	Разделы
Десять самых распространенных вирусов	+	+	Инфекции Вирусы Графики
Десять самых зараженных станций	+		Инфекции
Виды инфекций	+	+	Вирусы
Результаты установок			Все сетевые инсталляции
Средняя активность заражения	+		Статистика
По количеству ошибок	+	+	Ошибки
По компонентам	+	+	Ошибки
Результаты выполненных заданий	+	+	Задания
Классы заражений	+	+	Графики
Произведенные действия	+	+	Графики
Посуточная активность вирусов	+	+	Графики
Количество зараженных машин в группе	+		Графики

- **Десять самых зараженных станций** - приводится список из десяти станций, инфицированных наибольшим количеством вредоносных объектов. На графике отображаются численные данные по количеству вредоносных объектов, которые были найдены на указанных станциях.
- **Виды инфекций** - круговая диаграмма, отображающая количество найденных вредоносных объектов по типам этих объектов.
- **Результаты установок** - круговая диаграмма, отображающая количество всех установок, запущенных с

данного **Сервера**, разделенных по результату установки. В случае неуспешной установки - с причиной ошибки. Диаграмма отображается для всех установок с данного **Сервера**, вне зависимости от объекта, выбранного в иерархическом списке.

- **Средняя активность заражения** - отображает среднее значение заражения на станциях выбранной группы. Данное значение высчитывается как сумма количества всех найденных вредоносных объектов, разделенная на количество просканированных объектов на каждой из станций.
- **По количеству ошибок** - приводится список станций, на которых были обнаружены ошибки функционирования антивирусных компонентов, установленных на этих станциях. На графике отображается количество ошибок по станциям.
- **По компонентам** - приводится список антивирусных компонентов, установленных на станциях, в функционировании которых возникали ошибки. На круговой диаграмме отображается общее количество ошибок каждого из компонентов.
- **Результаты выполнения заданий** - приводится список заданий, запускавшихся на выбранных объектах. На графике отображается количество запусков каждого из заданий. В таблице под графиком также приведены результаты выполнения заданий.

7.6.3. Сводные данные

Для просмотра сводных данных:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите в разделе **Таблицы** пункт **Сводные данные**.
2. Откроется окно, содержащее табличные данные отчета. Для того чтобы включить в отчет определенные статистические данные, нажмите на кнопку **Сводные**

данные на панели инструментов и выберите требуемые типы в выпадающем списке: **Статистика**, **Инфекции**, **Задания**, **Запуск/завершение**, **Ошибки**. Статистика, включаемая в данные разделы отчета, соответствует статистике, содержащейся в соответствующих пунктах раздела **Таблицы**. Для просмотра отчета с выбранными таблицами нажмите на кнопку **Обновить**.

3. Для отображения данных за определенный период либо укажите диапазон времени относительно сегодняшнего дня из выпадающего списка, либо задайте произвольный диапазон дат на панели инструментов. Для задания произвольного диапазона введите требуемые даты или нажмите на значки календаря рядом с полями дат. Для просмотра данных нажмите на кнопку **Обновить**.
4. При необходимости сохранить отчет для распечатки или дальнейшей обработки нажмите на кнопку  **Записать данные в файл в формате CSV**, на кнопку  **Записать данные в файл в формате HTML** или на кнопку  **Записать данные в файл в формате XML**.

7.6.4. Карантин

Для возможности управления **Карантином** с **Сервера** необходимо, чтобы станции с установленным модулем **Карантина** работали под ОС, на которые возможна установка **SpIDer Guard G3** (см. п. Системные требования).

В противном случае удаленное управление невозможно. **Карантин** также не сможет управлять файлами из папки `Infected.!!!`, и информация о содержимом **Карантина** не будет отправляться на **Сервер**.

Содержимое Карантина

Файлы в **Карантин** могут быть добавлены:

- одним из антивирусных компонентов, например, **Сканером**,

- вручную пользователем через менеджер **Карантина**.

При попадании в **Карантин** файлы автоматически сканируются повторно. При этом:

- уточняется статус заражения - наличие инфекции и ее тип (поскольку при ручном добавлении в **Карантин** информация о статусе заражения файлов недоступна),
- названия инфекций и их тип приводятся к единому виду.

Также пользователь может сам повторно сканировать файлы, находящиеся в **Карантине**, через **Центра Управления** или через менеджер **Карантина** на станции.

Для просмотра и редактирования содержимого Карантина в Центре Управления:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В управляющем меню (панель слева) выберите в разделе **Общие** пункт **Карантин**.
2. Откроется окно, содержащее табличные данные о текущем состоянии **Карантина**.

   Если была выбрана одна рабочая станция, то будет отображена таблица с объектами, находящимися в **Карантине** на данной станции.

   Если было выбрано несколько станций, группа или несколько групп, то будет отображен набор таблиц, содержащих объекты карантина для каждой станции в отдельности.

3. Для просмотра файлов, помещенных в **Карантин** за определенный промежуток времени, укажите требуемый временной период на панели инструментов и нажмите кнопку **Обновить**.
4. Для управления файлами, находящимися в **Карантине**, установите флаг для соответствующего файла, группы файлов или для всех файлов **Карантина** (в заголовке таблицы). На панели инструментов выберите одно из следующих действий:

- **Восстановить файлы** - для восстановления файлов из **Карантина**.

Используйте данную функцию только если вы уверены, что объект безопасен.

В выпадающем меню выберите один из вариантов:

a) **Восстановить файлы** - восстановить первоначальное местоположение файла на компьютере (восстановить файл в папку, в которой он находился до перемещения в **Карантин**).

b) **Восстановить файлы по указанному пути** - переместить файл в папку, указанную администратором.

- **Удалить файлы** - для удаления выбранных файлов из **Карантина** и из системы.

- **Сканировать файлы** - для повторного сканирования выбранных в **Карантине** файлов.

- **Экспорт** - для копирования и сохранения выбранных в **Карантине** файлов.

  После перемещения подозрительных файлов в локальный **Карантин** на компьютере пользователя, вы можете скопировать эти файлы через **Центр Управления** и сохранить посредством веб-браузера, например, для дальнейшей отправки файлов на анализ в вирусную лабораторию компании **«Доктор Веб»**. Для сохранения установите флаги напротив требуемых файлов и нажмите кнопку **Экспорт**.

- Экспортировать данные о состоянии **Карантина** в файл в одном из следующих форматов:

  - записать данные в файл в формате CSV,

 - записать данные в файл в формате HTML,

 - записать данные в файл в формате XML.

7.7. Настройки некоторых антивирусных компонентов

Состав параметров компонентов и рекомендации по их заданию содержатся в руководстве **Антивирус Dr.Web® для Windows. Руководство пользователя**, а также **Dr.Web® Агент для Windows. Руководство пользователя**.

Далее приведены настройки некоторых антивирусных компонентов, которые отличаются от настроек, доступных на рабочей станции.

7.7.1. Настройка Офисного Контроля для доступа к локальным и сетевым ресурсам под ОС Windows®

Вы можете централизованно ограничить доступ к определенным локальным ресурсам и узлам сети Интернет. Для этого используется компонент **Dr.Web Офисный Контроль**.

Настройка Офисного контроля:

1. Для открытия окна редактирования настроек выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите пункт **Dr.Web Офисный Контроль**.
2. На вкладке **Общие** выберите настройки блокирования и задайте ресурсы (локальные папки и файлы), к которым вы хотите запретить доступ:

- Для активизации блокировки локальных ресурсов и сменных устройств установите флаг **Включить блокировку**.
- Установите флаг **Блокировать сменные носители**, для запрета доступа пользователя к сменным носителям.
- Установите флаг **Защищать каталоги и файлы** для запрета доступа к указанным ресурсам. Пути к блокируемым каталогам и файлам задаются в поле **Список защищаемых папок и файлов**. Для добавления нового пути к ресурсу нажмите на кнопку  , после чего отредактируйте добавленную строку.

Если файл, доступ к которому требуется запретить, указан без пути, то он считается расположенным в папке `%system32%` и в настройках **Офисного контроля** на стороне пользователя будет отображаться с префиксом `c:\windows\system32`.

3. На вкладке **Доступ** установите флаг **Фильтрация WWW**, для того чтобы настроить доступ к доменам сети Интернет. Установите флаг **Блокировать все сайты**, чтобы полностью запретить доступ к Интернету. Внесите в соответствующие списки домены, к которым необходимо разрешить/запретить доступ. Для создания новой записи нажмите на кнопку  и введите значения в открывшееся поле.

   В разделе **Блокировать содержимое** установите флаги напротив категорий сайтов, которые вы хотите заблокировать. Эти флаги активируют встроенный фильтр и заблокируют веб-сайты, соответствующие данным категориям.

4. По окончании настройки нажмите на кнопку **Сохранить**. Настройки вступят в силу после подтверждения новой конфигурации станции.

В настройках Офисного контроля запрещается ставить под защиту следующие папки, включая их корневые каталоги:

- %SYSTEMROOT%,
- %USERPROFILE%,
- %PROGRAMFILES%.

При этом допускается блокировка их подкаталогов.

Офисный контроль не позволяет блокировать сетевые файлы и папки.

Если для станции включено разрешение редактирования конфигурации **Офисного контроля** (см. п. Настройка прав пользователей), пользователь будет иметь возможность самостоятельного ограничения доступа к ресурсам. При этом сохраняется возможность задания настроек на **Сервере**. Настройки, указанные на **Сервере**, будут автоматически обновляться на стороне пользователя.

В случае ошибки администратора при задании настроек **Офисного контроля** на **Сервере** (ошибка в пути к блокируемому ресурсу или задание запрещенной для блокировки папки), настройки обновятся на стороне пользователя, однако запрет не будет действовать. При этом об ошибке администрирования сообщено не будет.

7.7.2. Настройка компонента MailD для защиты почтовых адресов под ОС UNIX® и Mac OS X

При работе **Агента** под ОС семейства UNIX и Mac OS X возможно задание списка защищаемых почтовых адресов. Возможны варианты задания 15, 30 или 50 и более почтовых адресов, которые будут проверяться компонентом **Dr.Web MailD**.

Количество защищаемых почтовых адресов можно посмотреть в ключевом файле **Агента** (`agent.key`).

Для задания списка защищаемых e-mail адресов:

1. Выберите в иерархическом списке **Центра Управления** станцию или группу станций и в управляющем меню (панель слева) нажмите пункт **Почтовые адреса**.
2. В открывшемся окне введите в поле требуемый e-mail адрес.
3. Для добавления нового адреса нажмите кнопку  . Каждый новый адрес необходимо вводит в новую строку.
4. Для удаления адреса нажмите кнопку  напротив соответствующего поля.
5. Для сохранения внесенных изменений нажмите **Сохранить.**

7.8. Отправка сообщений станциям под ОС Windows®

Системный администратор может отправлять пользователям информационные сообщения произвольного содержания, включающие:

- текст сообщения;
- гиперссылки на интернет-ресурсы;
- логотип компании (или любое графическое изображение);
- в заголовке окна также указывается точная дата получения сообщения.

Данные сообщения выводятся на стороне пользователя в виде всплывающих окон (см. рис. 7-1).

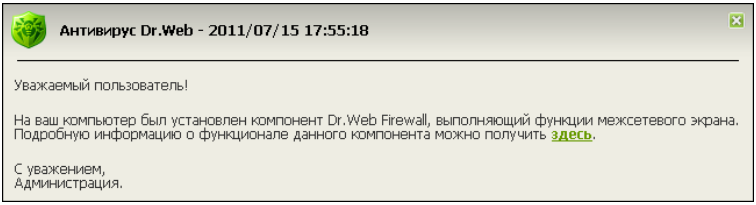


Рисунок 7-1. Окно сообщения на стороне пользователя

Для отправки сообщения пользователю:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**.
2. В открывшемся окне выберите в иерархическом списке станцию или группу и нажмите **Общие** → **Послать сообщение станциям** на панели инструментов.

В открывшемся окне заполните следующие поля:

- **Текст сообщения** - обязательное поле. Содержит непосредственно само сообщение.
- **Показывать логотип компании в сообщении** - установите данный флаг, если хотите, чтобы в заголовке окна сообщения отобразился графический объект. Для загрузки файла логотипа с локального ресурса необходимо нажать на кнопку **Обзор** справа от поля **Файл с логотипом** и выбрать необходимый объект в открывшемся браузере по файловой системе.

  Так же вы можете задать заголовок сообщения или название компании в поле **Название**. Данный текст будет отображен в заголовке окна сообщения (справа от логотипа). Если данное поле останется пустым, то на его месте в окне сообщения будет выведен текст, содержащий информацию об **Агенте**.

  В поле **URL** можно указать ссылку на веб-страницу, которая будет открыта при нажатии на логотип (а также при нажатии на заголовок окна, если он был указан в поле **Название**).

  Если логотип не задан, или размер логотипа превышает максимально допустимый (см. Формат файла логотипа, п. 3),

то на его месте в окне сообщения будет отображен значок **Enterprise Агента**.

При установленном флаге **Показывать логотип компании в сообщении** становится активным флаг **Использовать прозрачность**. Установите этот флаг для использования прозрачности в изображении логотипа (см. Формат файла логотипа, п. 4).

- **Показывать ссылку в сообщении** - установите этот флаг, если хотите, чтобы сообщение пользователю содержало гиперссылки на Веб-ресурсы. Для добавления ссылки необходимо:
  1. В поле **URL** ввести ссылку на интернет-ресурс.
  2. В поле **Текст** указать название ссылки - текст, который будет отображаться на месте ссылки в сообщении.
  3. В поле **Текст сообщения** указать тег `{link}` везде, где необходимо добавить ссылку. В результирующем сообщении на его месте будет вставлена ссылка с указанными параметрами. Количество тегов `{link}` в тексте не ограничено, но все они будут содержать одинаковые параметры (из полей **URL** и **Текст** соответственно).

Например:

Для отправки сообщения, приведенного на рисунке 7-1, были заданы следующие параметры ссылки:

Текст сообщения:

```
Уважаемый пользователь!


На ваш компьютер был установлен компонент Dr.Web Firewall, выполняющий функции межсетевого экрана.
Подробную информацию о функционале данного компонента можно получить {link}.
```

```
С уважением,
Администрация.
```

URL: `http://drweb.com/`

Текст: `здесь`

- **Показать результат доставки** - установите этот флаг, если хотите получить отчет о доставке сообщения пользователю.

Формат файла логотипа

Файл с графическим изображением (логотипом), включаемый в сообщение, должен удовлетворять следующим условиям:

1. Графический формат файла - bmp.
2. Глубина цвета (bit depth) - любая (8 - 24 бит).
3. Максимальный размер видимой части логотипа равен 120x90 px (ширина x высота). Дополнительные 2x2 px - припуск на рамку из пикселей прозрачности (см. п. 4), т.е. полный максимальный размер изображения составляет 122x92 px (см. рис. 7-2).

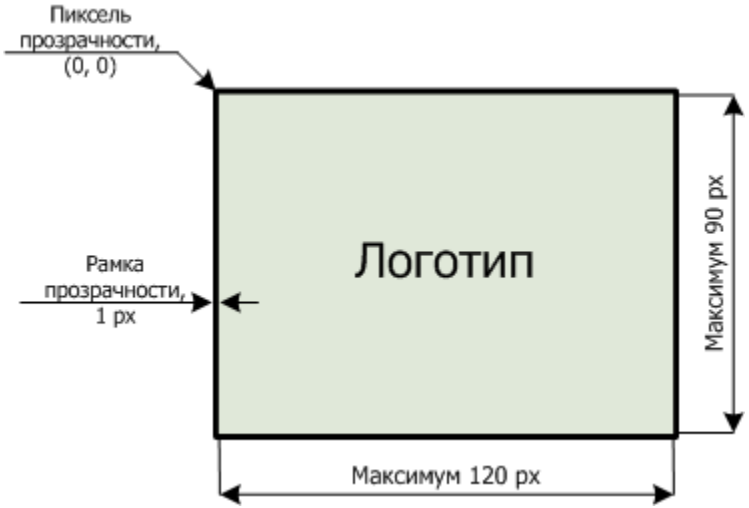


Рисунок 7-2. Формат файла логотипа

4. В случае, если при отправке сообщения была включена опция **Использовать прозрачность**, первый пиксель в позиции (0,0) объявляется *прозрачным*. Все пиксели, имеющие тот же цвет, становятся прозрачными, и на их месте будет отображаться фон окна сообщения.

   Если вы включаете опцию **Использовать прозрачность** для прямоугольного логотипа, рекомендуется сделать прямоугольную рамку во избежание некорректного задания пикселей самого изображения логотипа в качестве "прозрачных".

   Задание опции **Использовать прозрачность** будет полезно в случае нестандартной (непрямоугольной) формы логотипа для исключения нежелательного фона, дополняющего информативную часть изображения до прямоугольного. Например, при использовании в качестве логотипа изображения, приведенного на рисунке 7-3, фиолетовый фон будет исключаться (станет прозрачным).

Рисунок 7-3. Логотип нестандартной формы

Перед отправкой пользовательского сообщения (особенно многоадресного), рекомендуется предварительно отправить его на любой компьютер с установленным **Агентом**, чтобы проверить корректность результата.

Глава 8. Настройка Dr.Web Enterprise Server

8.1. Настройка конфигурации Dr.Web Enterprise Server

Чтобы настроить конфигурационные параметры для Dr.Web Enterprise Server:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.
3. Откроется окно настроек **Сервера**.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

Вкладка Общие

Параметр **Название** определяет имя данного **Сервера**. Если оно не задано, применяется имя компьютера, на котором работает ПО **Enterprise Сервера**.

Параметр **Нитей** определяет количество потоков для обработки данных, поступающих от **Агентов**. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой поддержки.

Параметр **Соединений с БД** задает количество соединений **Сервера** с БД. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой поддержки.

В поле **Очередь авторизации** задается максимальное количество станций в очереди для авторизации на **Сервере**. Допускает ввод любого целого числа.

В выпадающем списке **Трафик обновлений** задается максимальная полоса пропускания сетевого трафика при передаче обновлений между **Сервером** и **Агентами**. При этом:

- Если данный параметр имеет значение **неограниченный**, то обновления для различных **Агентов** передаются без ограничения полосы пропускания сетевого трафика.
- Если для данного параметра установлено значение, отличное от **неограниченный** (конкретное числовое значение), то обновления передаются в пределах заданной полосы пропускания совокупного сетевого трафика обновлений всех **Агентов**.

В выпадающем списке **Новички** задается политика подключения новых рабочих станций (см. п. Политика подключения станций).

Флаг **Переводить неавторизованных в новички** предписывает программе сбрасывать параметры соединения с **Сервером** у станций, не прошедших авторизацию. Данная опция может быть полезна при изменении настроек **Сервера** (таких как открытый ключ) или при смене БД. В подобных случаях станции не смогут подключиться, и потребуется повторное получение новых параметров для доступа к **Серверу**.

В выпадающих списках **Шифрование** и **Сжатие** выбирается политика шифрования и сжатия трафика между **Enterprise Сервером**, **Агентами** и **Центром Управления** (подробнее об этих параметрах см. п. Использование шифрования и сжатия трафика).

Вы также можете изменять состояние следующих флагов:

- **Показывать доменные имена** предписывает программе заносить в файл протокола не IP-адреса рабочих станций, а их доменные имена.
- **Заменять NetBios-имена** предписывает отображать в каталоге антивирусной сети **Центра Управления** не

наименования рабочих станций, а их доменные имена (при невозможности определения доменных имен отображаются IP-адреса).

Оба флага **Показывать доменные имена** и **Заменять NetBios-имена** по умолчанию сняты. При неправильной настройке службы DNS включение этих возможностей может значительно замедлить работу **Сервера**. При включении любого из этих режимов рекомендуется разрешить кэширование имен на DNS-сервере.

Если флаг **Заменять NetBios-имена** установлен, и в антивирусной сети используется **Прокси-сервер**, то для всех станций, подключенных к **Серверу** через **Прокси-сервер**, в **Центре Управления** в качестве названий станций будет отображаться название компьютера, на котором установлен **Прокси-сервер**.

- **Синхронизировать описания станций** - предписывает синхронизацию описания компьютера пользователя с описанием станции в **Центре Управления**. Если описание станции в **Центре Управления** отсутствует, то в данное поле будет записано описание компьютера на стороне пользователя. Если описания различаются, то данные в **Центре Управления** будут заменены на пользовательские.

Вкладка Статистические данные

На вкладке **Статистические данные** задается статистическая информация, которая записывается в журнал протокола и заносится в базу данных **Сервера**.

Для добавления в БД соответствующего типа информации установите следующие флаги:

- **Карантин** - разрешает запись состояния **Карантина** на станциях.
- **Список модулей станций в БД** - разрешает записывать состав модулей **Антивируса** на рабочей станции.

- **Список установленных компонентов в БД** - разрешает записывать, какие компоненты **Антивируса** (**Сканер**, **Мониторы** и т.п.) установлены на рабочей станции.
- **Информация о запуске/завершении компонентов в БД** - разрешает записывать информацию о запуске и завершении работы компонентов **Антивируса** (**Сканер**, **Мониторы** и т.п.) на рабочих станциях.
- **Инфекции в БД** - разрешает запись статистических данных об инфекциях, обнаруженных на рабочих станциях.
- **Ошибки сканирования в БД** - разрешает запись информации обо всех ошибках при сканировании на рабочих станциях.
- **Статистика сканирования в БД** - разрешает запись результатов сканирования на рабочих станциях.
- **Информация об установках агента в БД** - разрешает записывать информацию об инсталляциях **Агентов** на рабочих станциях.
- **Протокол выполнения заданий** - разрешает записывать в БД результат выполнения заданий на станциях.
- **Мониторинг состояния станции** - разрешает вести учет изменений состояния станции и запись информации в БД.
- **Мониторинг вирусных баз** - разрешает вести учет состояния (состава, изменения) вирусных баз на станции и запись информации в БД.

Для просмотра статистической информации:

1. Выберите пункт главного меню **Антивирусная сеть**.
2. В иерархическом списке выберите станцию или группу.
3. Откройте соответствующий раздел управляющего меню (см. таблицу ниже).

Подробное описание статистических данных приведено в разделе Просмотр результатов работы и итоговой статистики по рабочей станции.

В таблице ниже приведено соответствие флагов из раздела **Статистические данные** в настройках **Сервера** и пунктов

управляющего меню на странице **Антивирусная сеть**.

При снятии флагов на вкладке **Статистические данные**, соответствующие им пункты будут скрыты из управляющего меню.

Таблица 8-1. Соответствие настроек Сервера и пунктов управляющего меню

Настройки Сервера	Пункты меню
Карантин	Общие → Карантин
Список модулей станции в БД	Таблицы → Модули
Список установленных компонентов в БД	Общие → Установленные компоненты
Информация о запуске/завершении компонентов в БД	Таблицы → Запуск/ Завершение
Инфекции в БД	Таблицы → Инфекции Таблицы → Вирусы
Ошибки сканирования в БД	Таблицы → Ошибки
Статистика сканирования в БД	Таблицы → Статистика Таблицы → Суммарная статистика
Информация об установках агента в БД	Таблицы → Все сетевые инсталляции
Протокол выполнения заданий	Таблицы → Задания Таблицы → Вирусные базы
Мониторинг состояния станции	Таблицы → Состояние Таблицы → Вирусные базы
Мониторинг вирусных баз	Таблицы → Вирусные базы

Вкладка Статистика

На вкладке **Статистика** настраиваются параметры отправки статистики по вирусным событиям в компанию **«Доктор Веб»**.

Для активации отправки статистики установите флаг **Статистика**. Станут доступны следующие поля:

- **Интервал** - интервал отправки статистики в минутах;
- **Адрес сервера** - IP-адрес или DNS-имя и порт сервера статистики (по умолчанию `stat.drweb.com:80`);
- **URL** - каталог на сервере статистики (по умолчанию `/update`);
- **Идентификатор клиента** - MD5 ключ **Сервера** (находится в ключевом файле **Сервера** `enterprise.key`);
- **Пользователь** - имя пользователя для регистрации статистики. Имя пользователя можно получить в **Службе технической поддержки** компании **«Доктор Веб»**;
- **Пароль** - пароль для регистрации статистики. Пароль можно получить в **Службе технической поддержки** компании **«Доктор Веб»**;
- **Прокси-сервер** - при необходимости можно указать адрес прокси-сервера для отправки статистики;
- **Пользователь прокси** - имя пользователя прокси-сервера (не указывается при анонимной авторизации прокси);
- **Пароль пользователя прокси** - пароль для доступа к прокси-серверу (не указывается при анонимной авторизации прокси).

Обязательными полями являются только **Адрес сервера** статистики и **Интервал** отправки статистики.

Для сохранения внесенных изменений нажмите на кнопку **Сохранить**.

Вкладка Безопасность

На вкладке **Безопасность** задаются ограничения на сетевые адреса, с которых **Агенты**, сетевые инсталляторы и другие ("соседние") **Серверы** смогут получать доступ к данному **Серверу**.

Управление журналом аудита **Сервера** осуществляется при помощи следующих флагов:

- **Аудит операций** разрешает ведение журнала аудита операций администратора с **Центром Управления**, а также запись журнала в БД.
- **Аудит внутренних операций сервера** разрешает ведение журнала аудита внутренних операций **Сервера** и запись журнала в БД.

Журнал аудита можно посмотреть, выбрав в главном меню **Администрирование** пункт **Журнал аудита**.

На вкладке **Безопасность** размещаются дополнительные вкладки **Агенты**, **Инсталляции** и **Соседи**, на которых настраиваются ограничения для соответствующих типов соединений.

Для того чтобы настроить ограничения доступа для какого-либо типа соединения:

1. Перейдите на соответствующую вкладку (**Агенты**, **Инсталляции** или **Соседи**).
2. Чтобы разрешить все соединения, снимите флаг **Использовать этот список доступа**.
3. Для того чтобы задать списки разрешенных или запрещенных адресов, установите флаг **Использовать этот список доступа**.
4. Для того чтобы разрешить доступ с определенного TCP-адреса, включите его в список **TCP: разрешено** или **TCPv6: разрешено**.
5. Для того чтобы запретить какой-либо TCP-адрес, включите его в список **TCP: запрещено** или **TCPv6: запрещено**.

Для редактирования списка адресов:

1. Введите сетевой адрес в соответствующее поле и нажмите на кнопку **Сохранить**.

2. Для добавления нового поля адреса, нажмите на кнопку  соответствующего раздела.
3. Для удаления поля нажмите на кнопку  .

   Сетевой адрес задается в виде: *<IP-адрес>*/[*<префикс>*].

Списки для ввода адресов TCPv6 будут отображены, только если на компьютере установлен интерфейс IPv6.

Пример использования префикса:

1. Префикс 24 обозначает сети с маской: `255.255.255.0`

   Содержит 254 адреса

   Адреса хостов в этих сетях вида: `195.136.12.*`

2. Префикс 8 обозначает сети с маской `255.0.0.0`

   Содержит до 16387064 адресов (256*256*256)

   Адреса хостов в этих сетях вида: `125.*.*.*`

Аналогично настраиваются ограничения для IPX-адресов.

Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлен ли флаг **Приоритетность запрета**: при установленном флаге адреса, не включенные ни в один из списков (или включенные в оба), запрещаются. В противном случае, такие адреса разрешаются.

Вкладка База Данных

На вкладке **База данных** задается выбор СУБД для хранения централизованного журнала антивирусной сети и ее настройки (подробнее об этих параметрах см. п. Настройка режима работы с БД).

Вкладка Оповещения

Параметры на вкладке **Оповещения** позволяют настроить режим оповещения администраторов антивирусной сети и других лиц о вирусных атаках и других событиях, выявленных компонентами **Dr.Web Enterprise Security Suite** (подробнее об этой настройке см. п. Настройка оповещений).

Вкладка Транспорт

На вкладке **Транспорт** настраиваются параметры используемых **Сервером** транспортных протоколов.

Для каждого из протоколов можно указать в поле **Название** имя **Enterprise Сервера**. Если оно не задано, используется имя, заданное на вкладке **Общие** (см. выше, в частности, если на указанной вкладке не задано никакое имя, используется имя компьютера). Если для протокола задано иное имя, чем определенное на вкладке **Общие**, используется имя из описания протокола. Данное имя используется службой обнаружения **Сервера Агентами** и т.д.

В поле **Адрес** необходимо указать адрес интерфейса, прослушиваемого **Сервером** для взаимодействия с **Агентами**, установленными на рабочих станциях.

В поле **Адрес кластера** необходимо указать адрес интерфейса, прослушиваемого **Сервером** для взаимодействия с **Агентами** и **Сетевыми инсталляторами** при поиске активных **Enterprise Серверов** сети. Более подробное описание приведено в разделе Служба обнаружения Сервера.

Данные параметры задаются в формате сетевого адреса, приведенного в Приложении Е. Спецификация сетевого адреса.

Вкладка Модули

На вкладке **Модули** задается режим использования протоколов взаимодействия **Сервера** с другими компонентами **Dr.Web ESS**.

По умолчанию разрешено взаимодействие с:

- **Enterprise Агентами**,
- компонентом **NAP Validator**,
- **Сетевыми инсталляторами Агента**.

Взаимодействие **Enterprise Сервера** с другими **Enterprise Серверами** по умолчанию отключено. При задании многосерверной конфигурации сети (см.п. Особенности сети с несколькими Серверами) включите этот протокол, установив соответствующий флаг.

Вкладка Расположение

На вкладке **Расположение** вы можете указать дополнительную информацию о компьютере, на котором установлено ПО **Enterprise Сервера**.

8.1.1. Использование шифрования и сжатия трафика

Антивирусная сеть **Dr.Web Enterprise Security Suite** позволяет зашифровать трафик между **Сервером** и рабочими станциями **(Enterprise Агентами**), между **Enterprise Серверами** (при многосерверной конфигурации сети), а также между **Сервером** и **Сетевыми инсталляторами**. Этот режим используется, чтобы избежать возможного разглашения пользовательских ключей, а также сведений об оборудовании и пользователях антивирусной сети.

Антивирусная сеть **Dr.Web Enterprise Security Suite** использует криптографически устойчивые средства шифрования и цифровой

электронной подписи, основанные на концепции пар открытых и закрытых ключей.

Политика использования шифрования настраивается раздельно на каждом из компонентов антивирусной сети, при этом настройки остальных компонентов должны быть согласованы с настройками **Сервера**.

Чтобы задать политики сжатия и шифрования для Dr.Web Enterprise Server:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.
3. На вкладке **Общие** выберите в выпадающих списках **Шифрование** и **Сжатие** один из вариантов:
   - **Да** — шифрование (или сжатие) трафика со всеми компонентами обязательно (устанавливается по умолчанию для шифрования, если при установке **Сервера** не было задано другое),
   - **Возможно** — шифрование (или сжатие) будет выполняться для трафика с теми из компонентов, настройки которых этого не запрещают,
   - **Нет** — шифрование (или сжатие) не поддерживается (устанавливается по умолчанию для сжатия, если при установке **Сервера** не было задано другое).

При согласовании настроек политики шифрования на **Сервере** и другом компоненте (**Агенте** или **Сетевом инсталляторе**) следует иметь ввиду, что ряд сочетаний настроек является недопустимым и их выбор приведет к утрате соединения между **Сервером** и компонентом.

В таблице 8-2 собраны сведения о том, при каких установках соединение между **Сервером** и компонентом будет шифрованным (+), при каких — нешифрованным (–), и о том, какие сочетания являются недопустимыми (**Ошибка**).

Таблица 8-2. Совместимость настроек политики шифрования

Настройки Сервера / Настройки компонента	Да	Возможно	Нет
Да	+	+	Ошибка
Возможно	+	+	–
Нет	Ошибка	–	–

Использование шифрования трафика создает заметную вычислительную нагрузку на компьютеры с производительностью, близкой к минимально допустимой для установленных на них компонентов. В тех случаях, когда шифрование трафика не требуется для обеспечения дополнительной безопасности, можно отказаться от этого режима. Шифрование трафика также не рекомендуется в больших сетях (от 2000 клиентов). При этом следует последовательно переключать **Сервер** и компоненты сначала в режим **Возможно**, не допуская создания несовместимых пар **Сетевой инсталлятор-Сервер** и **Агент-Сервер**. Несоблюдение этого правила может привести к потере управляемости компонента и необходимости его переустановки.

По умолчанию **Enterprise Агент** устанавливается с настройками шифрования **Возможно.** Данное сочетание означает, что по умолчанию шифрование будет производиться, но может быть отменено редактированием настроек **Enterprise Сервера**.

Ввиду того, что трафик между компонентами (особенно **Серверами**) может быть весьма значительным, антивирусная сеть позволяет установить сжатие (компрессию) этого трафика. Настройка политики сжатия и совместимость таких настроек на разных компонентах полностью аналогичны описанным выше для шифрования, с тем отличием, что для **Сервера** настройкой

сжатия по умолчанию является **Нет**.

Использование сжатия уменьшает трафик, но значительно увеличивает вычислительную нагрузку на компьютеры, в большей степени, чем шифрование.

8.1.2. Настройка режима работы с БД

Структуру БД **Enterprise Сервера** можно получить на основе sql-скрипта `init.sql`, расположенного в подкаталоге `etc` каталога установки **Enterprise Сервера**.

Для того чтобы настроить параметры работы с базой данных:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.
3. Перейдите на вкладку **База данных** и выберите в выпадающем списке **База данных** тип базы данных:
   - **IntDB** – встроенная БД (компонент **Enterprise Сервера)**,
   - **MS SQL CE** – внешняя БД для **Серверов**, работающих под ОС Windows,

Внешняя БД **MS SQL CE** обладает низкой производительностью и уступает по данному показателю внутренней БД.

При нагрузке более 30 клиентских станций не рекомендуется использование данной БД.

Однако БД **MS SQL CE** может успешно использоваться для создания отчетов через API ADO.NET. Если данная возможность не требуется, то рекомендуется использовать внутреннюю БД или одну из других возможных внешних БД.

- **ODBC** (для **Серверов**, работающих под ОС Windows) или **PostgreSQL** (для **Серверов** под управлением ОС семейства UNIX) – внешняя БД,
- **Oracle** – внешняя БД (для платформ, кроме FreeBSD).

При использовании внешней **СУБД Oracle** необходимо установить последнюю версию **ODBC-драйвера**, поставляемую с данной СУБД. Использование **ODBC-драйвера Oracle**, поставляемого **Microsoft**, категорически не рекомендовано.

Для встроенной БД, при необходимости, введите в поле **Файл** полный путь к файлу с базой данных и задайте размер кэш-памяти и режим записи данных.

Параметры для внешних БД подробно описаны в приложениях (см. Приложение В. Настройки, необходимые для использования СУБД. Параметры драйверов СУБД).

По умолчанию предусмотрено использование встроенной СУБД. Выбор этого режима создает значительную вычислительную нагрузку на **Сервер**. При значительном размере антивирусной сети рекомендуется использовать внешнюю СУБД.

Использование внутренней БД допустимо при подключении к **Серверу** не более 200-300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен **Enterprise Сервер**, и нагрузка по прочим задачам, выполняемым на данном компьютере - возможно подключение до 1000 станций.

В противном случае необходимо использовать внешнюю БД.

При использовании внешней БД и подключении к **Серверу** более 10000 станций рекомендуется выполнение следующих минимальных требований:

- процессор с частотой 3ГГц,
- оперативная память - от 4 Гб для **Enterprise Сервера**, от 8 Гб - для сервера БД,
- ОС семейства UNIX.

Предусмотрена возможность осуществления операций, связанных с очисткой базы данных, используемой **Enterprise Сервером**, а именно: удаление записей о событиях, а также информации о станциях, не посещавших **Сервер** в течение определенного периода. Для очистки базы данных перейдите в раздел расписания Сервера и создайте соответствующее задание.

8.1.3. Настройка оповещений

Для настройки режима отправки оповещений о событиях в антивирусной сети:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.
3. Перейдите на вкладку **Оповещения** и выберите необходимый режим оповещения в выпадающем списке **Оповещения**:
   - **Не включать** – не посылать оповещений (режим по умолчанию),
   - **Электронная почта** – отправлять оповещения по электронной почте,
   - **Сообщения по сети Windows** – отправлять оповещения, используя **Windows Messenger** (только для **Серверов** под ОС Windows).

Оповещения по электронной почте

Для оповещений по электронной почте задайте следующие параметры:

- **Отправитель** – адрес отправителя сообщения.
- **Получатель** – адрес получателя или нескольких получателей сообщения. Для добавления еще одного поля получателя нажмите на кнопку  .
- **SMTP-сервер**, **Порт** – соответственно адрес и порт SMTP-сервера, на который следует отправлять электронную почту.
- **Пользователь**, **Пароль** (**Еще раз пароль**) – при необходимости задайте имя пользователя и пароль для авторизации на SMTP-сервере.

При необходимости установите следующие флаги:

- **Отладочный режим** – для получения детального протокола SMTP-сессии.
- **Использовать TLS/SSL для шифрования трафика** – для использования *TLS/SSL* шифрования трафика при отправке оповещений по электронной почте.
- **Разрешить plain text авторизацию** – для использования *plain text* аутентификации на почтовом сервере.
- **Разрешить CRAM-MD5 авторизацию** – для использования *CRAM-MD5* аутентификации на почтовом сервере.

В разделе **Разрешенные сообщения** установите флаги для тех событий, сообщения о которых будут отправляться по электронной почте.

Сообщения по сети Windows

Система оповещений по сети Windows функционирует только на ОС Windows с поддержкой сервиса Windows Messenger (Net Send).

ОС Windows Vista и старше не поддерживают сервис Windows Messenger.

Для сообщений в сети ОС Windows задайте список имен компьютеров получателей сообщений.

Для добавления нового поля нажмите на кнопку  и введите название компьютера в появившемся поле. Для удаления поля нажмите на кнопку  .

В разделе **Разрешенные сообщения** установите флаги для тех событий, сообщения о которых будут отправляться.

Шаблоны сообщений

Текст сообщения определяется шаблоном сообщения. Шаблоны сообщений хранятся в подкаталоге `var/templates` каталога установки **Сервера**. Чтобы настроить текст сообщения, отправляемого при определенном событии, отредактируйте соответствующий шаблон.

При подготовке сообщения система оповещения заменяет переменные шаблона (в фигурных скобках) на конкретный текст, зависящий от ее текущих настроек. Список доступных переменных указан в приложениях (см. Приложение D. Параметры шаблонов системы оповещения).

Для редактирования шаблонов настоятельно рекомендуется использовать **Редактор шаблонов**. Для этого:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Редактор шаблонов**.
2. Откроется окно редактора шаблонов. Для редактирования какого-либо шаблона выберите его в списке.
   - В поле **Тема** можно отредактировать тему посылаемого сообщения.
   - В поле **Заголовки** задаются, при необходимости, дополнительные заголовки электронного письма.
   - В поле **Сообщение** задается шаблон текста сообщения.

   Для добавления переменных можете использовать выпадающие списки в заголовке сообщения.
3. Для сохранения измененного шаблона нажмите на кнопку **Сохранить**.

В том случае, если вы используете для редактирования шаблонов внешний редактор, сохраняйте файлы шаблонов в кодировке **UTF-8**. Крайне не рекомендуется использовать **Блокнот** и другие редакторы, вставляющие в текст маркер порядка байтов (`BOM`) для определения кодировки **UTF-8**, **UTF-16** или **UTF-32**.

8.2. Ведение серверного протокола

Enterprise Сервер ведет протокол событий, связанных с его работой. Имя файла протокола – `drwcsd.log`.

По умолчанию размещение файла протокола:

- Под ОС **UNIX**:
  - для Linux: `/var/opt/drwcs/log/drwcsd.log`;
  - для FreeBSD и Solaris: `/var/drwcs/log/drwcsd.log`.

- Под ОС **Windows**: в подкаталоге `var` каталога установки **Сервера**.

Файл имеет простой текстовый формат (см. Приложение L. Формат файлов протокола).

Протокол **Сервера** используется для отладки, а также устранения неполадок в случае нештатной работы компонентов антивирусной сети.

8.3. Настройка расписания Dr.Web Enterprise Server

Чтобы настроить расписание выполнения заданий для Dr.Web Enterprise Server:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Расписание Dr.Web Enterprise Server**. Откроется текущий список заданий **Сервера**.
2. Для того чтобы удалить задание из списка, установите напротив него флаг, после чего выберите на панели инструментов пункт **Удалить эти настройки**.
3. Для того чтобы отредактировать параметры задания, выберите его в списке заданий. При этом откроется окно **Редактор заданий**, описываемое ниже.
4. Для того чтобы добавить задание в список, выберите на панели инструментов пункт **Новое задание**. При этом откроется окно **Новое задание**, аналогичное **Редактору заданий**. Укажите необходимые параметры (см. ниже) и нажмите на кнопку **Сохранить**.
5. Вы также можете запретить выполнение задания или разрешить выполнение ранее запрещенного задания.
6. Для того чтобы экспортировать расписание в файл специального формата, нажмите на кнопку панели инструментов.

7. Для того чтобы импортировать параметры из такого файла, нажмите на кнопку  панели инструментов.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

Для редактирования параметров задания:

1. На вкладке **Общие** задайте следующие параметры:
   - Введите в поле **Название** наименование задания, под которым оно будет отображаться в расписании.
   - Чтобы активировать выполнение задания, установите флаг **Разрешить исполнение**.

   Если флаг не установлен, задание будет присутствовать в списке, но не будет исполняться.
   - Установленный флаг **Критичное задание** дает указание выполнить задание при следующем запуске **Enterprise Сервера**, если выполнение данного задания будет пропущено (**Enterprise Сервер** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Enterprise Сервера** оно выполняется 1 раз.
2. На вкладке **Действие** выберите в выпадающем списке **Действие** тип задания. При этом изменится вид нижней части окна, содержащей дополнительные параметры данного типа задания. Введите эти параметры (в таблице 8-3 параметры заданий рассмотрены отдельно по типам).
3. На вкладке **Время** в выпадающем списке **Время** выберите периодичность запуска задания и настройте время в соответствии с выбранной периодичностью (это действие аналогично настройке времени в расписании рабочей станции, см. выше п. Настройка расписания заданий на рабочей станции).
4. Нажмите на кнопку **Сохранить**.

Таблица 8-3. Типы заданий и их параметры

Тип задания	Параметры и описание
Выполнение процедуры	Необходимо указать название выполняемой процедуры в поле **Название.** Название процедуры должно соответствовать названию исполняемого пользовательского lua-скрипта (без расширения), расположенного в каталоге `var/extensions` каталога установки **Сервера** (см. также описание скриптов из каталога `var/extensions`, приведенное в Приложении М).
Завершение	Для завершения работы **Сервера**. Дополнительных параметров не имеет.
Перезапуск	Для перезапуска **Сервера**. Дополнительных параметров не имеет.
Запуск	Необходимо указать в поле **Путь** путь к исполняемому файлу программы, выполняемой в заданное время, в поле **Аргументы —** параметры командной строки для запуска указанной программы. Установите флаг **Выполнять синхронно** для синхронизации с **Сервером** – ожидания завершения выполнения данной программы перед выполнением других заданий типа **Запуск**. Если флаг **Выполнять синхронно** не установлен, то **Сервер** запускает программу и протоколирует только ее запуск. Если флаг **Выполнять синхронно** установлен, то **Сервер** протоколирует ее запуск, код возврата и время завершения программы.
Напоминание об окончании лицензии	Необходимо указать период, до которого будет получено напоминание об окончании срока лицензии на продукт **Dr. Web** (как лицензии **Сервера**, так и **Агента**).
Обновление	О задании см. п. Обновление по расписанию.
Протоколирование	Следует указать текст сообщения, которое заносится в протокол.
Резервное копирование критичных данных сервера	Задания предназначены для создания резервной копии критичных данных **Сервера** (база данных, серверный лицензионный ключевой файл, закрытый ключ шифрования). Следует указать путь к каталогу, в который будут сохранены данные (пустой путь

Тип задания	Параметры и описание
	означает каталог по умолчанию) и максимальное количество резервных копий (значение 0 означает отмену этого ограничения). Подробнее см. Приложение H5.5.
Станция долго не посещала сервер	Необходимо указать период, по истечении которого станция считается долго не посещавшей **Сервер**, о чем будет выдано напоминание.
Удаление неотправленных событий	Необходимо указать период, по истечении которого неотправленные события будут удаляться. Здесь имеются ввиду события, передаваемые подчиненным **Сервером** главному. При неудачной передаче события, оно заносится в список неотправленных. Подчиненный **Сервер** с заданной периодичностью осуществляет попытки передачи. При выполнении задания **Удаление неотправленных событий** осуществляется удаление всех событий, длительность хранения которых достигла и превысила заданный период.
Удаление старых станций	Необходимо указать временной период (по умолчанию 90 дней). Станции, не посещавшие **Сервер** на протяжении указанного периода, признаются старыми и удаляются с **Сервера**.
Удаление старых записей	Необходимо указать количество дней, по истечении которых статистические данные о рабочих станциях (но не сами станции) признаются старыми и удаляются с **Сервера**. Период удаления статистических данных задается для каждого типа записей в отдельности.

Старые данные автоматически удаляются из базы данных с целью экономии дискового пространства. Указываемый по умолчанию период для **Удаления старых записей** и **Удаления старых станций** составляет 90 дней. Уменьшение этого параметра приводит к меньшей репрезентативности накопленной статистики о работе компонентов антивирусной сети.

Увеличение параметра может серьезно увеличить потребность **Сервера** в ресурсах.

8.4. Управление репозиторием Dr.Web Enterprise Server

8.4.1. Введение

Репозиторий **Enterprise Сервера** предназначен для хранения эталонных образцов ПО и обновления их с серверов **ВСО**.

Для этой цели репозиторий оперирует наборами файлов, называемыми *продуктами*. Каждый продукт размещается в отдельном подкаталоге каталога `repository`, расположенного в каталоге `var`, который, при установке по умолчанию, является подкаталогом корневого каталога **Сервера**. Функции репозитория и управление ими осуществляются для каждого продукта независимо.

Для управления обновлением репозиторий использует понятие *ревизии* продукта. Ревизия представляет собой корректное на определенный момент времени состояние файлов продукта (включает имена файлов и контрольные суммы) и характеризуется уникальным номером. Репозиторий производит синхронизацию ревизий продукта в следующих направлениях:

а) на **Enterprise Сервер** с сайта обновления продукта (по протоколу HTTP),

Для версий **Сервера 5.0** и выше, вне зависимости от настроек репозитория для ПО **Сервера**, обновления с серверов **ВСО** не поставляются.

Для обновления **Сервера** используйте инсталлятор необходимой версии и проведите процедуру обновления согласно общим правилам, приведенным в разделах Обновление Dr.Web ESS для ОС Windows® или Обновление Dr.Web ESS для ОС семейства UNIX®.

b) между различными **Enterprise Серверами** в многосерверной конфигурации (в соответствии с заданной политикой обмена),

c) с **Enterprise Сервера** на рабочие станции.

Репозиторий предоставляет Администратору антивирусной сети возможность настраивать следующие параметры:

- перечень сайтов обновления при операциях типа **a)**;
- ограничение состава продуктов, нуждающихся в синхронизации типа **a)** (таким образом, пользователю предоставляется возможность отслеживать только нужные ему изменения отдельных категорий продуктов);
- ограничение частей продукта, нуждающихся в синхронизации типа **c)** (пользователь может выбрать, что именно подлежит установке на рабочие станции);
- контроль перехода на новые ревизии (возможно самостоятельное тестирование продуктов перед внедрением);
- добавление в продукты собственных компонентов;
- самостоятельное создание новых продуктов, для которых также будет выполняться синхронизация.

В настоящее время в поставку входят следующие продукты:

- **Enterprise Сервер**,
- **Enterprise Агент** (ПО **Агента**, антивирусное ПО рабочей станции),
- **Центр Управления Dr.Web**,

- Вирусные базы.

Подробнее о репозитории см. Приложение F. Управление репозиторием.

8.4.2. Состояние репозитория

Чтобы проверить текущее состояние репозитория или обновить компоненты антивирусной сети, выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**.

В открывшемся окне приведен список компонентов антивирусной сети, дата их последнего обновления и их текущее состояние.

Для проверки наличия обновлений и загрузки имеющихся обновлений компонентов с серверов **ВСО** нажмите на кнопку **Проверить обновления**.

8.4.3. Редактор конфигурации репозитория

Редактор конфигурации репозитория позволяет задать общие параметры конфигурации репозитория для всех продуктов.

После изменения настроек репозитория необходимо произвести успешное обновление ПО компонентов антивирусной сети для изменения состояния репозитория в соответствии с выбранными вами настройками.

Чтобы отредактировать конфигурацию репозитория выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Конфигурация репозитория**.

Настройка ВСО Dr.Web

На вкладке **ВСО Dr.Web** осуществляется настройка параметров **Всемирной Системы Обновлений**.

При помощи Центр Управления Dr.Web вы можете:

- Удалить сервер из списка. Для этого выделите один или несколько серверов и на панели инструментов нажмите на кнопку **Удалить сервер из списка**  .

Для выбора нескольких серверов одновременно используйте кнопки CTRL или SHIFT.

- Добавить сервер в список. Для этого на панели инструментов нажмите на кнопку **Создать сервер**  и задайте настройки сервера согласно процедуре, приведенной ниже.
- Задать прокси-сервер. Для этого установите флаг **Использовать прокси-сервер** (настройки прокси аналогичны настройкам серверов обновлений).
- Настроить адрес сервера и параметры авторизации пользователя. Для этого нажмите на значок сервера.

При настройке или добавлении сервера открывается окно настроек сервера.

Для задания настроек сервера обновления:

1. Нажмите на значок соответствующего сервера.
2. В полях ввода **Сервер** укажите соответственно адрес и порт сервера.
3. В полях **Пользователь** и **Пароль** можете задать имя пользователя и пароль на сервере обновлений. Если авторизация на сервере не требуется, оставьте эти поля пустыми.

4. Для сохранения измененных настроек нажмите на кнопку **Сохранить**.

Также вы можете настроить обращение ко всем серверам обновления через прокси-сервер.

Для добавления прокси-сервера:

1. Установите флаг **Использовать прокси сервер**.
2. В открывшемся окне настроек прокси-сервера установите параметры, аналогичные параметрам сервера обновлений.
3. Нажмите на кнопку **Добавить**.
4. Нажмите на кнопку **Сохранить**.

При настройке прокси-сервера особое внимание следует обратить на тип используемой авторизации.

В текущей версии **Dr.Web Enterprise Security Suite** поддерживаются только базовая HTTP-авторизация, Proxy-HTTP-авторизация и RADIUS-авторизация.

Если необходимо отключить сервера обновлений от прокси-сервера, снимите флаг **Использовать прокси сервер**.

Настройка обновлений Dr.Web Enterprise Agent

Конфигурация обновления репозитория для ПО **Агента** и антивирусного пакета настраивается отдельно для различных версий ОС, на которые будет устанавливаться данное ПО:

- На вкладке **Dr.Web Enterprise Agent для Windows** в группе кнопок выбора укажите, требуется ли обновление всех компонентов, устанавливаемых на рабочие станции под ОС Windows, или только вирусных баз.
- На вкладке **Dr.Web Enterprise Agent для Unix** в группе кнопок выбора укажите, для каких ОС семейства UNIX требуется обновление компонентов, устанавливаемых на рабочие станции.

Настройка обновлений Dr.Web Enterprise Server

На вкладке **Dr.Web Enterprise Server** в группе кнопок выбора указывается, для каких ОС требуется обновление файлов **Сервера**: части для ОС Windows, части для ОС UNIX, обеих частей или никаких.

Для версий **Сервера 5.0** и выше, вне зависимости от настроек данного раздела, обновления с серверов **ВСО** не поставляются.

Для обновления **Сервера** используйте инсталлятор необходимой версии и проведите процедуру обновления согласно общим правилам, приведенным в разделах Обновление Dr.Web ESS для ОС Windows® или Обновление Dr.Web ESS для ОС семейства UNIX®.

8.5. Особенности сети с несколькими Серверами Dr.Web Enterprise Server

Dr.Web Enterprise Security Suite позволяет создавать антивирусную сеть с несколькими **Enterprise Серверами**. При этом каждая рабочая станция приписывается к одному определенному **Серверу**, что позволяет распределить нагрузку между ними.

Связи между **Серверами** могут иметь иерархическую структуру, что позволяет оптимальным образом распределить нагрузку на **Серверы**.

При планировании структуры антивирусной сети следует обратить внимание на особенности лицензирования сети с несколькими **Серверами**. Подробнее см. п. Ключевые файлы.

Для обмена информацией между **Серверами** (обновлениями файлов компонентов и сведениями о работе **Серверов** и подключенных к ним станций) используется специальный *протокол межсерверной синхронизации*.

Важнейшей особенностью этого протокола является оперативность передачи обновлений.

При помощи данного протокола:

- обновления передаются немедленно при их получении,
- отпадает необходимость в настройке расписания обновления на **Сервере** (кроме тех **Серверов**, которые получают обновления с серверов **ВСО Dr.Web** с использованием протокола HTTP).

8.5.1. Строение сети с несколькими Серверами Dr.Web Enterprise Server

В антивирусной сети можно установить несколько **Enterprise Серверов**. При этом каждый **Enterprise Агент** присоединяется к одному из **Серверов**. Каждый **Сервер** вместе с присоединенными антивирусными рабочими станциями функционирует как отдельная антивирусная сеть, как описано в предыдущих разделах.

Dr.Web Enterprise Security Suite позволяет связать такие антивирусные сети, организовав передачу информации между **Enterprise Серверами**.

Dr.Web Enterprise Server может передавать другому Серверу Dr.Web Enterprise Server:

- обновления ПО и вирусных баз. При этом получать обновления серверов **ВСО Dr.Web** будет только один из них;

Рекомендуется добавить в расписание подчиненного **Enterprise Сервера** задание на обновление подчиненного **Enterprise Сервера** с серверов **ВСО** на тот случай, если главный **Сервер** будет временно недоступным. Это позволит **Агентам** получать обновление вирусных баз и программных модулей (см. также п. Редактор конфигурации репозитория).

- информацию о вирусных событиях, статистику работы и т. д.

Dr.Web Enterprise Security Suite выделяет два типа связей между Серверами Dr.Web Enterprise Server:

- *связь типа главный-подчиненный*, при которой главный передает подчиненному обновления, и получает обратно информацию о событиях,
- *связь между равноправными*, при которой направления передачи и типы информации настраиваются индивидуально.

На рисунке 8-1 представлен пример структуры сети с несколькими **Серверами**.

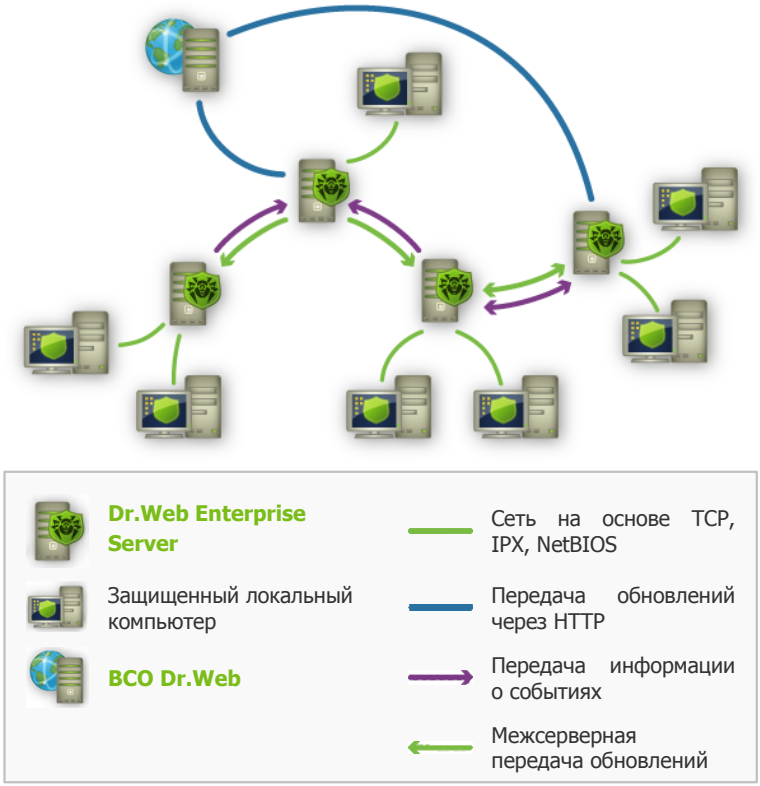


Рисунок 8-1. Сеть с несколькими Серверами

Некоторые из преимуществ антивирусной сети с несколькими Серверами Dr.Web Enterprise Server:

- возможность получения обновлений с серверов **BCO Dr.Web** через один **Enterprise Сервер** с последующей передачей на остальные **Серверы** напрямую или через промежуточные звенья,
- возможность распределения рабочих станций по нескольким **Серверам** с уменьшением нагрузки на каждый из них,

- объединение информации от нескольких **Серверов** на одном; возможность получения ее в сеансе **Центра Управления** на этом **Сервере** в консолидированном виде.

Dr.Web Enterprise Security Suite самостоятельно отслеживает и не допускает возникновения циклических путей передачи информации.

8.5.2. Настройка связей между Серверами Dr.Web Enterprise Server

Для того чтобы воспользоваться возможностями работы с несколькими **Серверами**, необходимо настроить связи между ними.

Рекомендуется предварительно спланировать и нарисовать структуру антивирусной сети, обозначив все предполагаемые потоки информации и приняв решение, какие связи будут типа "между равноправными", а какие — типа "главный-подчиненный". После этого для каждого **Сервера**, входящего в сеть, необходимо настроить связи с "соседними" **Серверами** ("соседние" **Сервера** связывает хотя бы один информационный поток).

Пример настройки соединения главного и подчиненного Серверов Dr.Web Enterprise Server:

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

1. Убедитесь, что оба **Enterprise Сервера** нормально функционируют.
2. Убедитесь, что для каждого из **Enterprise Серверов** используются различные ключи `enterprise.key`.
3. С помощью **Центра Управления** соединитесь с каждым из **Enterprise Серверов** и дайте им «говорящие» имена, так как это поможет не совершить ошибку при

манипуляциях, необходимых для соединения **Enterprise Серверов** и их управления. Сделать это можно в меню **Центра Управления** **Администрирование** → **Конфигурация Dr.Web Enterprise Server** на вкладке **Общие** в поле **Название**. В данном примере назовем главный **Сервер** `MAIN`, а дополнительный (который будет подчиненным) – `AUXILIARY`.

4. На обоих **Enterprise Серверах** включите серверный протокол. Для этого в меню **Центра Управления** **Администрирование** → **Конфигурация Dr.Web Enterprise Server** на вкладке **Модули** установите флаг **Dr.Web Enterprise Server** (см. п. Настройка конфигурации Dr.Web Enterprise Server).

Если серверный протокол не включен, при создании новой связи в **Центре Управления** будет выведено сообщение о необходимости включения данного протокола и дана ссылка на соответствующий раздел **Центра Управления**.

5. Перезапустите оба **Enterprise Сервера**.
6. Подсоедините **Центр Управления** к подчиненному **Серверу** `(AUXILIARY)` и добавьте главный **Сервер** `(MAIN)` в список соседних **Серверов** подчиненного **Сервера**. Для этого выберите пункт **Связи** в главном меню. Откроется окно, содержащее иерархический список **Серверов** антивирусной сети. Для того чтобы добавить **Сервер** в этот список, нажмите на кнопку **Создать связь**  на панели инструментов.

   Откроется окно описания связей между текущим и добавляемым **Сервером** (см. рис. 8-2). Выберите тип **Главный**. В поле **Название** введите название главного **Сервера** `(MAIN)`, в поле **Пароль** введите произвольный пароль для доступа к главному **Серверу**. Справа от поля **Ключ** нажмите на кнопку **Обзор** и укажите ключ `drwcsd.pub`, относящийся к главному **Серверу**, а в поле **Адрес** введите адрес главного **Сервера**.

Возможен поиск списка **Серверов**, доступных в сети. Для этого:

a) Нажмите стрелку справа от поля **Адрес**.

b) В открывшемся окне укажите перечень сетей в формате: через дефис (например, `10.4.0.1-10.4.0.10`), через запятую и пробел (например, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`), с использованием префикса сети (например, `10.4.0.0/24`).

c) Нажмите на кнопку  . Начнется обзор сети на наличие доступных **Серверов**.

d) Выберите **Сервер** списке доступных **Серверов**. Его адрес будет записан в поле **Адрес** для создания связи.

В поле **Адрес административной консоли** можете указать адрес начальной страницы **Центра Управления** для главного **Сервера** (см. п. Центр Управления Dr.Web).

Флаги в разделах **Обновления** и **События** установлены в соответствии с принципом связи *главный-подчиненный* и не подлежат изменению:

- главный **Сервер** посылает обновления на подчиненные **Сервера**;
- главный **Сервер** принимает информацию о событиях с подчиненных **Серверов**.

Нажмите на кнопку **Сохранить**.

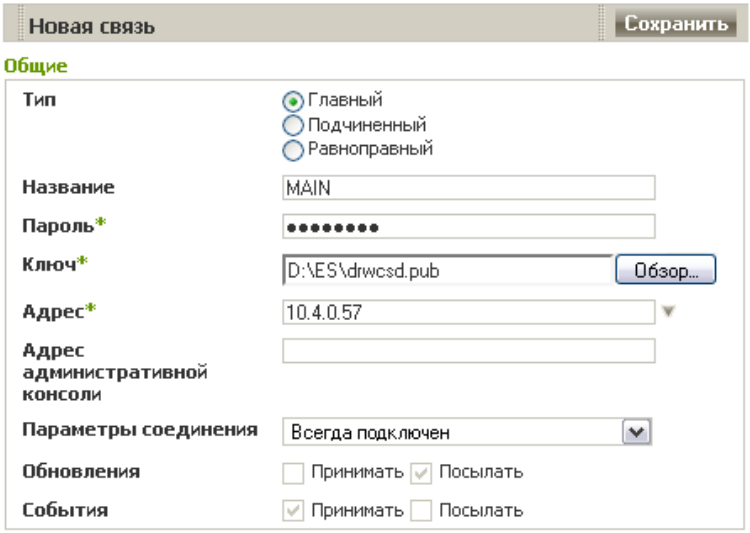


Рисунок 8-2.

В результате главный **Сервер** (MAIN) попадет в папки **Главные** и **Отключенные** (см. рис. 8-3).

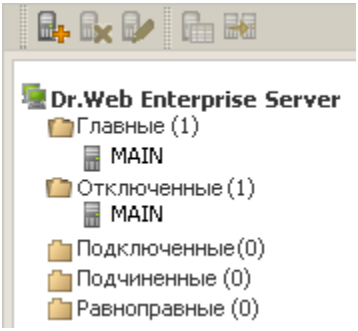


Рисунок 8-3.

7. Подсоедините **Центр Управления** к главному **Серверу** (MAIN) и добавьте подчиненный **Сервер** (AUXILIARY) в список соседних **Серверов** главного **Сервера**. Для этого выберите пункт **Связи** в главном меню. Откроется окно,

содержащее иерархический список **Серверов** антивирусной сети, "соседних" с данным. Для того чтобы добавить **Сервер** в этот список, нажмите на кнопку **Создать связь**  на панели инструментов.

В открывшемся окне (см. рис. 8-4) выберите тип **Подчиненный**. В поле **Название** введите название подчиненного **Сервера** `(AUXILIARY)`, в поле **Пароль** введите тот же пароль, что был указан в п. **6.** Справа от поля **Ключ** нажмите на кнопку **Обзор** и укажите ключ `drwcsd.pub`, относящийся к подчиненному **Серверу**.

В поле **Адрес административной консоли** можете указать адрес начальной страницы **Центра Управления** для подчиненного **Сервера** (см. п. Центр Управления Dr.Web).

Флаги в разделах **Обновления** и **События** установлены в соответствии с принципом связи *главный-подчиненный* и не подлежат изменению:

- подчиненный **Сервер** принимает обновления с главного **Сервера**;
- подчиненный **Сервер** посылает информацию о событиях на главный **Сервер**.

Нажмите на кнопку **Сохранить**.

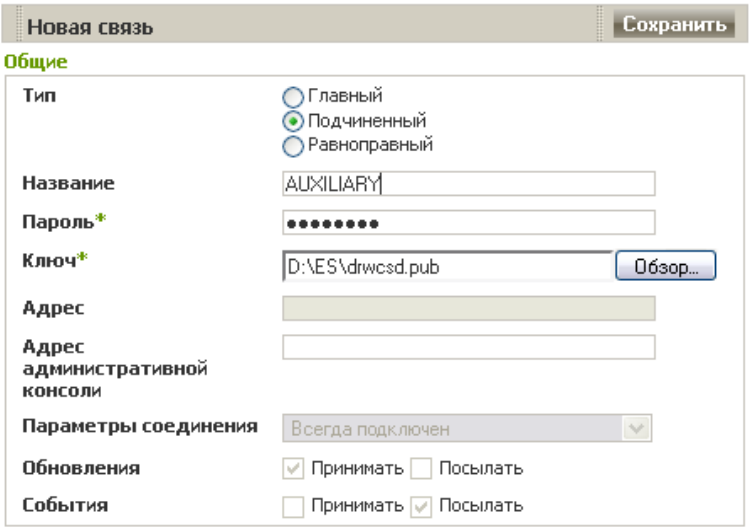


Рисунок 8-4.

В результате подчиненный **Сервер** (AUXILIARY) будет включен в папки **Подчиненные** и **Отключенные** (см. рис. 8-5).

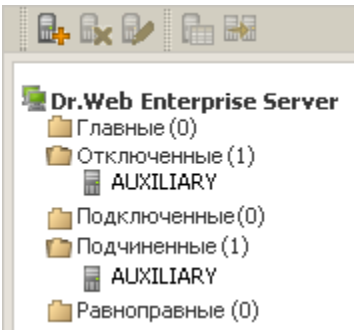


Рисунок 8-5.

8. Дождитесь установления связи между **Серверами** (обычно это занимает не более минуты). Для проверки периодически обновляйте список **Серверов** с помощью клавиши F5. После установления связи подчиненный

Сервер (AUXILIARY) перейдет из папки **Отключенные** в папку **Подключенные** (см. рис. 8-6).

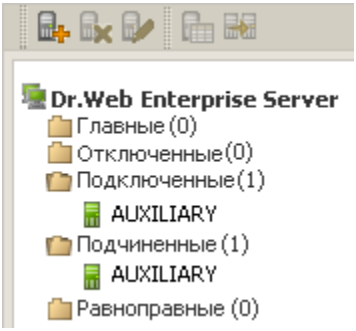


Рисунок 8-6.

9. Подсоедините **Центр Управления** к подчиненному **Серверу** (AUXILIARY) и убедитесь в том, что главный **Сервер** (MAIN) подключен к подчиненному (AUXILIARY) (см. рис. 8-7).

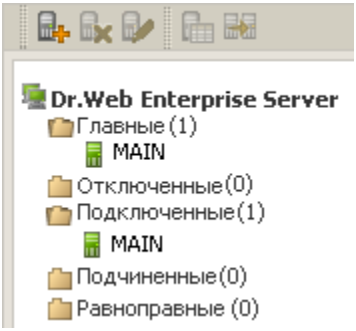


Рисунок 8-7.

Невозможно связать два **Сервера** с одинаковым лицензионным ключом (enterprise.key).

Невозможно связать несколько **Серверов** с одинаковой парой параметров: пароль и открытый ключ шифрования drwcsd.pub.

При создании равноправной связи между **Серверами** рекомендуется указывать адрес подключаемого **Сервера** в настройках только одного из них.

Это не повлияет на взаимодействие между **Серверами**, однако позволит избежать записей типа `Link with the same key id is already activated` в протоколе работы **Серверов**.

Установка соединения между Серверами Dr.Web Enterprise Server невозможна в следующих случаях:

- Проблемы связи по сети.
- При настройке связи задан неверный адрес главного **Сервера**.
- Задан неверный открытый ключ шифрования `drwcsd.pub` на одном из **Серверов**.
- Задан неверный пароль доступа на одном из **Серверов** (заданы несовпадающие пароли на соединяемых **Серверах).**
- Одинаковый лицензионный ключ `enterprise.key` на обоих **Серверах**.
- Лицензионный ключ `enterprise.key` подключаемого подчиненного **Сервера** совпадает с лицензионным ключом подчиненного **Сервера**, уже подключенного к тому же главному **Серверу**.

При создании связей между **Серверами** можно задать ограничение обновлений для связываемых **Серверов**. Для этого, при создании связи, на панели **Ограничение обновлений** нажмите на кнопку . Откроется окно редактирования режимов обновлений, описанное в п. Ограничение обновлений.

8.5.3. Использование антивирусной сети с несколькими Серверами Dr.Web Enterprise Server

Особенностью сети с несколькими **Серверами** является получение обновлений с серверов **ВСО Dr.Web** через часть **Enterprise Серверов** (как правило, один или несколько главных **Серверов**). При этом только на этих **Серверах** следует настраивать расписание, содержащее задание на обновление (см. п. Настройка расписания Dr.Web Enterprise Server). Любой **Сервер,** получивший обновления с серверов **ВСО Dr.Web** или от другого **Сервера**, немедленно передает его всем **Серверам**, для которых у него настроена такая возможность (то есть всем связанным подчиненным, а также тем из равноправных, для которых в явном виде указана возможность получать обновления).

Dr.Web Enterprise Security Suite автоматически отслеживает ситуации, когда из-за несовершенного планирования топологии сети и настройки **Серверов** на один и тот же **Сервер** повторно поступает уже принятое из другого источника обновление, и не проводит обновление повторно.

Администратор может также получать сводную информацию о наиболее важных вирусных событиях на сегментах сети, связанных с каким-либо **Сервером** через межсерверные связи (например, в вышеописанной конфигурации "один главный, остальные подчиненные" такая информация консолидируется на главном **Сервере**).

Чтобы просмотреть информацию о вирусных событиях на всех Серверах Dr.Web Enterprise Server, связанных с данным:

1. Выберите пункт **Связи** главного меню **Центра Управления**.

2. В открывшемся окне в разделе управляющего меню **Таблицы** выберите пункт **Суммарный отчет** для просмотра сведений об общем количестве записей о событиях на соседних **Серверах**. В таблице со статистикой по соседним **Серверам** отображаются данные по следующим разделам:
   - **Инфекции** - инфекции, обнаруженные на станциях, подключенных к соседним **Серверам**.
   - **Ошибки** - ошибки сканирования.
   - **Статистика** - статистика по обнаруженным инфекциям.
   - **Запуск/Завершение** - запуск и завершении заданий на сканирование станций.
   - **Состояние** - состояние антивирусного ПО на станциях.
   - **Все сетевые инсталляции** - сетевые инсталляции **Агентов**.
3. Для перехода к странице с подробной табличной информацией о событиях на соседних **Серверах** нажмите на цифру в таблице раздела **Суммарный отчет** с количеством записей по требуемому событию.
4. Также для перехода к табличным данным о событиях на соседних **Серверах** выберите соответствующий пункт (см. шаг 2) раздела **Таблицы** управляющего меню.
5. Для отображения данных за определенный период либо укажите диапазон времени относительно сегодняшнего дня из выпадающего списка, либо задайте произвольный диапазон дат на панели инструментов. Для задания произвольного диапазона введите требуемые даты или нажмите на значки календаря рядом с полями дат. Для просмотра данных нажмите на кнопку **Обновить**.
6. При необходимости сохранить таблицу для распечатки или дальнейшей обработки, нажмите на панели инструментов на кнопку  **Записать данные в файл в формате CSV,** на кнопку  **Записать данные в файл в формате HTML** или на кнопку  **Записать данные в файл в формате XML**.

8.5.4. Работа нескольких Серверов Dr.Web Enterprise Server с одной БД

При создании антивирусной сети с несколькими **Enterprise Серверами** и одной БД необходимо выполнение следующих предписаний:

1. На всех **Серверах** должны быть одинаковые ключи шифрования `drwcsd.pub`, `drwcsd.pri`, сертификаты `certificate.pem`, `private-key.pem` и агентский ключ `agent.key`.
2. В конфигурационном файле **Центра Управления** `webmin.conf` для всех **Серверов** должно быть прописано одинаковое DNS-имя **Сервера** в параметре `ServerName`.
3. На DNS сервере в сети регистрируется общее имя кластера для каждого отдельного **Сервера** и задается метод балансировки нагрузки.
4. Для каждого **Сервера** должен быть свой ключ `enterprise.key` с уникальным идентификатором `ID1`.
5. В конфигурационных файлах **Серверов** `drwcsd.conf` для всех **Серверов** должна быть прописана одна внешняя БД.
6. В серверном расписании задания **Purge Old Data**, **Prepare and send fiscal report periodic job**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge old data**, **Purge unsent IS events** должны быть только на одном из **Серверов** (наиболее производительном, если конфигурации различаются).

Глава 9. Обновление Dr.Web Enterprise Security Suite и его отдельных компонентов

Перед началом обновления **Dr.Web ESS** и его отдельных компонентов настоятельно рекомендуем проверить корректность настроек протокола TCP/IP для возможности доступа в Интернет. В частности, должна быть включена и содержать корректные настройки служба DNS.

Обновление вирусных баз и ПО вы можете производить как вручную, так и с помощью расписания заданий **Сервера** и **Агента.**

Перед обновлением ПО рекомендуется настроить конфигурацию репозитория, в том числе доступ к **ВСО Dr.Web** (см. п. Редактор конфигурации репозитория).

9.1. Обновление Dr.Web Enterprise Security Suite

9.1.1. Обновление Dr.Web Enterprise Server для ОС Windows®

Возможны два варианта обновления ПО **Сервера** до версии **6.0.4:**

1. Автоматическое. Обновление **Сервера** с версий **5.0** и **6.0.0** осуществляется автоматически средствами инсталлятора.

Автоматическое обновление возможно только для **Серверов** с одинаковой разрядностью.

В противном случае необходимо удаление старого **Сервера** и установка нового **Сервера** вручную.

2. Ручное. При обновлении **Сервера** с версий **4.XX**, **6.0.2** и старше необходимо вручную удалить предыдущий **Сервер** и установить новый **Сервер**.

Сохранение файлов конфигурации

При удалении **Сервера** вручную или при обновлении **Сервера** при помощи инсталлятора, автоматически сохраняются следующие файлы:

Файл	Описание	Каталог по умолчанию
`dbinternal.dbs`	внутренняя БД	`var`
`drwcsd.conf` (имя может отличаться)	конфигурационный файл **Сервера**	`etc`
`drwcsd.pri`	закрытый ключ шифрования	
`drwcsd.pub`	открытый ключ шифрования	• `Installer` • `webmin\install`
`enterprise.key` (имя может отличаться)	лицензионный ключ **Сервера**	`etc`
`agent.key` (имя может отличаться)	лицензионный ключ **Агента**	
`certificate.pem`	сертификат для SSL	
`private-key.pem`	закрытый ключ RSA	

При необходимости сохраните другие важные для вас файлы в другом месте, отличном от каталога установки **Сервера**,

например, конфигурационный файл **Центра Управления** `webmin.conf` и шаблоны отчетов, находящиеся в каталоге `\var\templates`.

Сохранение базы данных

Перед обновлением ПО **Dr.Web Enterprise Security Suite** рекомендуется выполнить резервное копирование базы данных.

Для сохранения базы данных:

1. Остановите **Сервер**.
2. Экспортируйте базу данных в файл:

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all exportdb <каталог_резервной_копии>\esbase.es
```

Для **Серверов**, использующих внешнюю базу данных, рекомендуется использовать штатные средства, поставляемые вместе с базой данных.

Убедитесь, что экспорт базы данных **Dr.Web ESS** завершился успешно. Отсутствие резервной копии БД не позволит восстановить **Сервер** в случае непредвиденных обстоятельств.

Важные замечания

Начиная с версии **5.0** в состав антивирусного пакета **Dr.Web Enterprise Security Suite** входят продукты **SpIDer Gate** и **Офисный Контроль**, для возможности использования которых необходимо, чтобы они были указаны в вашей лицензии (**Антивирус+Антиспам**). Если данные продукты не указаны в лицензии, рекомендуется выполнить действия, описанные ниже.

Если на компьютере с **Enterprise Сервером** установлен **Агент** со включенной самозащитой, то в процессе обновления **Сервера** будет выдано сообщение об активности компонента самозащиты **Dr.Web SelfPROtect.** Для продолжения процедуры обновления ПО **Сервера** отключите данный компонент через настройки **Агента**.

Если вы используете в качестве внешней базы данных ODBC для Oracle, то при обновлении (или повторной установке) **Сервера**, в настройках инсталлятора выберите пункт **Выборочная** установка и в следующем окне отмените установку встроенного клиента для СУБД Oracle (в разделе **Database support** - **Oracle database driver**).

В противном случае работа с БД Oracle через ODBC будет невозможна из-за конфликта библиотек.

Автоматическое обновление Dr.Web Enterprise Server с версий 5.0 и 6.0.0

Обновление ПО **Сервера** с версий **5.0** и **6.0.0** до версии **6.0.4** осуществляется автоматически средствами инсталлятора.

Для обновления Dr.Web Enterprise Server запустите инсталлятор и следуйте указаниям мастера по установке:

1. В процессе обновления будет выведено окно **Dr.Web Enterprise Server примечания к обновлению**, извещающее о наличии установленного ПО **Сервера** предыдущей версии. Инсталлятор автоматически определяет папку установки **Сервера**.
2. В последующих шагах мастера установки отображается информация о путях к файлам **Сервера** предыдущей версии (см. выше), которые будут использоваться инсталлятором при установке **Сервера** версии **6.0.4**. При необходимости вы можете изменять пути к файлам, автоматически найденным инсталлятором.

При использовании внешней базы данных **Сервера**, в процессе обновления также выберите вариант **использовать имеющуюся базу данных**. При последующем выборе существующего конфигурационного файла **Сервера** и закрытого ключа шифрования, дальнейшее обновление пройдет автоматически.

3. Для начала процесса удаления **Сервера** предыдущей версии и установки **Сервера** версии **6.0.4** нажмите на кнопку **Установить**.

В процессе обновления ПО **Сервера** осуществляется удаление содержимого репозитория и установка его новой версии.

Если по какой-либо причине при обновлении **Сервера** с версии **5.0** и младше был сохранен репозиторий предыдущей версии, необходимо вручную удалить все содержимое репозитория и произвести его полное обновление.

При многосерверной конфигурации антивирусной сети с главного **Сервера** версии **6.0.4** на подчиненные **Сервера** версии **5.0** и младше будут передаваться только вирусные базы.

Для передачи обновлений всего антивирусного ПО необходимо обновить подчиненный **Сервер** до версии **6.0.4** (для совместимости строения репозиториев).

После обновления Dr.Web Enterprise Server до версии 6.0.4 рекомендуется выполнить следующие действия:

После обновления ПО **Dr.Web Enterprise Server** по общей схеме выполните следующие действия, необходимые для нормального функционирования **Центра Управления**:

1. Очистить кэш веб-браузера, используемого для подключения к **Центру Управления**.
2. Обновить подключаемый модуль **Dr.Web Browser-Plugin**.

Ручное обновление Dr.Web Enterprise Server с версий 4.XX, 6.0.2 и старше

Обновление ПО **Сервера** с версий **4.XX**, **6.0.2** и старше средствами инсталлятора **Enterprise Сервера 6.0.4** не поддерживается. Для перехода на версию **6.0.4** необходимо вручную удалить установленный **Сервер** и установить новый **Сервер**.

В случае обновления с версии **4.xx**, если в вашей лицензии на антивирусное ПО версии **6.0.4** не указаны продукты **SpIDer Gate** и **Офисный Контроль (Антивирус+Антиспам)**, рекомендуется выполнить действия, описанные ниже.

Для обновления Dr.Web Enterprise Server выполните следующие действия:

1. Остановите **Enterprise Сервер** (см. п. Запуск и останов Dr.Web Enterprise Server).
2. Если используется внешняя БД, то сохраните базу данных средствами SQL сервера.
3. Если вы хотите использовать в дальнейшем какие-либо файлы (помимо тех файлов, которые будут автоматически сохранены в процессе удаления **Сервера**), создайте резервные копии этих файлов вручную, например, шаблонов отчетов и т.п.
4. Удалите **Сервер**.
5. Установите новый **Сервер** (см. п. Установка Dr.Web Enterprise Server для ОС Windows®). При установке **Сервера** задайте в параметрах инсталлятора автоматически сохраненные файлы.

   При использовании внешней базы данных укажите создание новой БД.

   При использовании внутренней базы данных укажите сохраненный файл БД `dbinternal.dbs`.

6. Остановите **Сервер** (см. п. Запуск и останов Dr.Web Enterprise Server).
7. Если вы сохраняли какие-либо файлы вручную перед удалением **Сервера**, разместите их в те же директории, где они находились в предыдущей версии **Сервера**.
8. При использовании внешней БД восстановите базу данных на новом **Сервере**, укажите в конфигурационном файле `drwcsd.conf` путь до базы данных.

   Запустите из командной строки файл `drwcsd.exe` с ключом `upgradedb` для обновления базы данных. Полная командная строка будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin
   \drwcsd.exe" upgradedb "C:\Program Files
   \DrWeb Enterprise Server\update-db"
   ```

9. Запустите **Enterprise Сервер** (см. п. Запуск и останов Dr.Web Enterprise Server).

При обновлении Dr.Web Enterprise Server с версии 4.XX до версии 6.0.4 рекомендуется выполнить следующие действия:

1. Перед процессом обновления отключите протоколы **Сетевого Инсталлятора** и **Агента**. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server,** перейдите на вкладку **Модули**. Снимите флаги **Протокол Dr.Web Enterprise Agent** и **Протокол Dr.Web Network Installer** и нажмите **Сохранить**.
2. Проведите обновление **Сервера** до версии **6.0.4** как описано выше (с сохранением файла конфигурации **Сервера**).
3. После обновления **Сервера** настройте список устанавливаемых компонентов на рабочих станциях (см. п. Состав антивирусного пакета), в частности, если у вас нет лицензии на **Антиспам**, должно быть установлено значение **не может** для компонентов **SpIDer Gate** и **Офисный Контроль**.

4. Произведите обновление компонентов **Dr.Web ESS**. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**. Для проверки наличия обновлений на сервере **ВСО** нажмите на кнопку **Проверить обновления**. При необходимости предварительно задайте настройки прокси-серверов для обновления через **ВСО**.
5. При необходимости отредактируйте порты, через которые **Агенты** будут обращаться к **Серверу**. Для этого используйте меню **Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт**.
6. Включите протоколы **Сетевого Инсталлятора** и **Агента**, отключенные на шаге **1**.
7. Обновите ПО на рабочих станциях.

После обновления **Сервера** версии **4.XX** до версии **6.0.4** необходимо, чтобы в конфигурационном файле **Сервера** `drwcsd.conf` был задан параметр `Transport`:

```
Transport "drwcs" "tcp/0.0.0.0:2193" "udp/231.0.0.1:2193"
```

где `drwcs` - имя **Сервера**.

Если данный параметр не задан, добавьте его вручную и перезапустите **Сервер**.

9.1.2. Обновление Dr.Web Enterprise Server для ОС семейства UNIX®

Обновление ПО **Сервера** поверх установленной версии возможно не для всех ОС семейства UNIX. Поэтому под ОС семейства UNIX, в которых не возможно произвести обновление поверх уже установленного пакета, необходимо удалить ПО **Сервера** более ранних версий и установить ПО версии **6.0.4**.

Сохранение файлов конфигурации

При удалении **Сервера** автоматически сохраняются следующие файлы:

Файл	Описание	Каталог по умолчанию
`dbinternal.dbs`	внутренняя БД	• для ОС Linux: /var/opt/drwcs/ • для ОС Solaris и FreeBSD: /var/drwcs/
`drwcsd.conf` (имя может отличаться)	конфигурационный файл **Сервера**	• для ОС Linux: /var/opt/drwcs/etc • для ОС Solaris и FreeBSD: /var/drwcs/etc
`webmin.conf`	конфигурационный файл **Центра управления**	
`common.conf`	конфигурационный файл (для некоторых ОС семейства UNIX)	
`enterprise.key` (имя может отличаться)	лицензионный ключ **Сервера**	
`agent.key` (имя может отличаться)	лицензионный ключ **Агента**	
`certificate.pem`	сертификат для SSL	
`private-key.pem`	закрытый ключ RSA	
`drwcsd.pri`	закрытый ключ шифрования	
`drwcsd.pub`	открытый ключ шифрования	для ОС Linux и ОС Solaris: • /opt/drwcs/Installer/ • /opt/drwcs/webmin/install для ОС FreeBSD:

Файл	Описание	Каталог по умолчанию
		• /usr/local/drwcs/Installer/ • /usr/local/drwcs/webmin/install

Сохранение базы данных

Перед обновлением ПО **Dr.Web Enterprise Security Suite** рекомендуется выполнить резервное копирование базы данных.

Для сохранения базы данных:

1. Остановите **Сервер**.
2. Экспортируйте базу данных в файл:
   - Для ОС FreeBSD:
     ```
     # /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/esbase.es
     ```
   - Для ОС Linux:
     ```
     # /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
     ```
   - Для ОС Solaris:
     ```
     # /etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es
     ```

Для **Серверов**, использующих внешнюю базу данных, рекомендуется использовать штатные средства, поставляемые вместе с базой данных.

Убедитесь, что экспорт базы данных **Dr.Web ESS** завершился успешно. Отсутствие резервной копии БД не позволит восстановить **Сервер** в случае непредвиденных обстоятельств.

Важные замечания

Все действия по обновлению необходимо выполнять от имени администратора **root**.

При обновлении **Сервера** на версию **6.0.4** с версии **5.0** и младше необходимо полное удаление репозитория и установка его новой версии.

При многосерверной конфигурации антивирусной сети с главного **Сервера** версии **6.0.4** на подчиненные **Сервера** версии **5.0** и младше будут передаваться только вирусные базы.

Для передачи обновлений всего антивирусного ПО необходимо обновить подчиненный **Сервер** до версии **6.0.4** (для совместимости строения репозиториев).

Начиная с версии **5.0** в состав антивирусного пакета **Dr.Web Enterprise Security Suite** входят продукты **SpIDer Gate** и **Офисный Контроль**, для возможности использования которых необходимо, чтобы они были указаны в вашей лицензии (**Антивирус+Антиспам**). Если данные продукты не указаны в лицензии, рекомендуется выполнить действия, описанные ниже.

Автоматическое обновление

При обновлении **Сервера** с версии **5.0** и выше до версии **6.0.4** для ОС **Linux**, вместо удаления старой версии и установки новой версии **Сервера**, возможно использование следующих команд для обновления **Сервера**:

- для **rpm**: `rpm -U` <*имя пакета*>
- для **deb**: `dpkg -i` <*имя пакета*>
  при обновлении deb-пакетов каталог `/root/drwcs` должен быть пуст либо отсутствовать.

При этом все автоматически сохраненные файлы будут размещены в требуемых директориях, и ручная замена не требуется.

При обновлении пакета в **rpm**-дистрибутивах для **Сервера** версий **5.0** или **6.0**, если до обновления **Сервера** в конфигурационный файл **Центра Управления** `webmin.conf` были внесены изменения, файл `webmin.conf` сохраняется от старой версии, а новый файл создается с именем `webmin.conf.rpmnew`.

При необходимости использования функционала, за который отвечают измененные параметры конфигурационного файла (в том числе, чтобы инсталлятор **Агента** был доступен по адресу http://<*server_name*>:9080/install, см. Инсталляционные файлы), перенесите все измененные настройки из старого файла в новый файл и переименуйте новый файл `webmin.conf.rpmnew` в `webmin.conf` с заменой старого.

Ручное обновление

Для обновления Dr.Web Enterprise Server в случае использования внутренней базы данных:

1. Остановите **Сервер**.
2. Если вы хотите использовать в дальнейшем какие-либо файлы (помимо тех файлов, которые будут автоматически сохранены в процессе удаления **Сервера** на шаге **4**), создайте резервные копии этих файлов вручную, например, шаблонов отчетов и т.п.
3. Удалите все содержимое репозитория.
4. Удалите ПО **Сервера** (см. п. Удаление Dr.Web Enterprise Server для ОС семейства UNIX®). При этом будет автоматически предложено сохранить резервные копии файлов. Для этого достаточно ввести путь для сохранения или принять путь, предлагаемый по умолчанию.
5. Установите **Enterprise Сервер** версии **6.0.4** согласно штатной процедуре установки (см. п. Установка Dr.Web Enterprise Server для ОС семейства UNIX®).
6. При необходимости замените созданные при установке

файлы автоматически сохраненными в процессе удаления **Сервера** предыдущей версии. Файлы, которые требуется заменить, располагаются в следующих директориях:

Файлы	Путь для ОС		
	Linux	Solaris	FreeBSD
drwcsd.pub	/opt/drwcs/Installer/ /opt/drwcs/webmin/install		/usr/local/drwcs/Installer/ /usr/local/drwcs/webmin/ install
dbinternal.dbs	/var/opt/drwcs/	/var/drwcs/	
drwcsd.conf drwcsd.pri enterprise.key agent.key certificate.pem private-key.pem	/var/opt/drwcs/etc	/var/drwcs/etc	

Конфигурационный файл **Центра Управления** (`webmin.conf`) версий младше **6.0.2** не совместим с ПО версии **6.0.4**. При переустановке **Сервера** с версии младше **6.0.2** данный файл не подлежит замене на автоматически сохраненную копию. Все необходимые настройки, хранящиеся в данном файле, требуется внести вручную.

Если вы сохраняли какие-либо файлы вручную, разместите их в те же директории, где они находились в предыдущей версии **Сервера**.

Для всех сохраненных от предыдущей версии **Сервера** файлов (см. шаг **6**) необходимо установить в качестве владельца файлов пользователя, выбранного при установке новой версии **Сервера** (по умолчанию - **drwcs**).

7. Выполните команды:
   - для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd upgradedb
```

- для ОС **FreeBSD**:

  `/usr/local/etc/rc.d/drwcsd.sh upgradedb`

8. Запустите **Сервер**.
9. Настройте обновление репозитория и обновите его полностью.
10. Перезапустите **Сервер**.

Для обновления Dr.Web Enterprise Server в случае использования внешней базы данных:

1. Остановите **Сервер**.
2. Если вы хотите использовать в дальнейшем какие-либо файлы (помимо тех файлов, которые будут автоматически сохранены в процессе удаления **Сервера** на шаге **4**), создайте резервные копии этих файлов вручную, например, шаблонов отчетов и т.п.
3. Удалите все содержимое репозитория.
4. Удалите ПО **Сервера** (см. п. Удаление Dr.Web Enterprise Server для ОС семейства UNIX®). При этом будет автоматически предложено сохранить резервные копии файлов. Для этого достаточно ввести путь для сохранения или принять путь, предлагаемый по умолчанию.
5. Установите **Enterprise Сервер** версии **6.0.4** согласно штатной процедуре установки (см. п. Установка Dr.Web Enterprise Server для ОС семейства UNIX®).
6. Поместите автоматически сохраненные файлы (см. выше):

   - для ОС **Linux**:

     в директорию `/var/opt/drwcs/etc`, кроме `pub`-ключа, который поместите в `/opt/drwcs/Installer/` и в `/opt/drwcs/webmin/install`

   - для ОС **FreeBSD**:

     в директорию `/var/drwcs/etc`, кроме `pub`-ключа, который поместите в `/usr/local/drwcs/Installer/` и в `/usr/local/drwcs/webmin/install`

   - для ОС **Solaris**:

в директорию `/var/drwcs/etc`, кроме `pub`-ключа, который поместите в `/opt/drwcs/Installer/` и в `/opt/drwcs/webmin/install`

Если вы сохраняли какие-либо файлы вручную, разместите их в те же директории, где они находились в предыдущей версии **Сервера**.

Для всех сохраненных от предыдущей версии **Сервера** файлов (см. шаг **6**) необходимо установить в качестве владельца файлов пользователя, выбранного при установке новой версии **Сервера** (по умолчанию - **drwcs**).

7. Выполните команды:
   - для ОС **Linux** и ОС **Solaris**:
     `/etc/init.d/drwcsd upgradedb`
   - для ОС **FreeBSD**:
     `/usr/local/etc/rc.d/drwcsd.sh upgradedb`
8. Запустите **Сервер**.
9. Настройте обновление репозитория и обновите его полностью.
10. Перезапустите **Сервер**.

При обновлении Dr.Web Enterprise Server с версии 4.XX до версии 6.0.4 рекомендуется выполнить следующие действия:

1. Перед процессом обновления отключите протоколы **Сетевого Инсталлятора** и **Агента**. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Конфигурация Enterprise Server,** перейдите на вкладку **Модули**. Снимите флаги **Протокол Dr.Web Enterprise Agent** и **Протокол Dr.Web Network Installer** и нажмите **Сохранить**.
2. Проведите обновление **Сервера** до версии **6.0.4** как описано выше (с сохранением файла конфигурации **Сервера**).

3. После обновления **Сервера** настройте список устанавливаемых компонентов на рабочих станциях (см. п. Состав антивирусного пакета), в частности, если у вас нет лицензии на **Антиспам**, должно быть установлено значение **не может** для компонентов **SpIDer Gate** и **Офисный Контроль**.
4. Произведите обновление компонентов **Dr.Web ESS**. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**. Для проверки наличия обновлений на сервере **ВСО** нажмите на кнопку **Проверить обновления**. При необходимости предварительно задайте настройки прокси-серверов для обновления через **ВСО**.
5. При необходимости отредактируйте порты, через которые **Агенты** будут обращаться к **Серверу**.
6. Включите протоколы **Сетевого Инсталлятора** и **Агента**, отключенные на шаге **1**.
7. Обновите ПО на рабочих станциях.

После обновления **Сервера** версии **4.XX** до версии **6.0.4** необходимо, чтобы в конфигурационном файле **Сервера** `drwcsd.conf` был задан параметр `Transport`:

```
Transport "drwcs" "tcp/0.0.0.0:2193" "udp/231.0.0.1:2193"
```

где `drwcs` - имя **Сервера**.

Если данный параметр не задан, добавьте его вручную и перезапустите **Сервер**.

9.1.3. Обновление подключаемого модуля Dr.Web Browser-Plugin

Для обновлении подключаемого модуля **Dr.Web Browser-Plugin** (используется **Центром Управления**) необходимо вручную удалить предыдущую версию модуля и установить новый модуль

Dr.Web Browser-Plugin.

Удаление модуля описано в п. Удаление компонентов ПО для ОС Windows® и в п. Удаление Dr.Web Enterprise Server для ОС семейства UNIX®.

Процесс установки описан в п. Установка подключаемого модуля Dr.Web Browser-Plugin.

9.1.4. Обновление Dr.Web Enterprise Agent

После обновления ПО **Сервера** подключенные к нему **Агенты** обновятся автоматически.

Рекомендации по обновлению **Агентов**, установленных на станциях, выполняющих важные функции ЛВС, приведены в разделе Обновление Агентов на серверах ЛВС.

9.1.5. Обновление Прокси-сервера

Обновление Прокси-сервера для ОС Windows

Автоматическое обновление **Прокси-сервера** не поддерживается.

При запуске инсталлятора на компьютере с установленным **Прокси-сервером**:

- Если запускается инсталлятор с той же разрядностью, что и установленный **Прокси-сервер**, будет выдано предупреждение о невозможности установки.

- Если запускается инсталлятор с разрядностью, отличной от разрядности установленного **Прокси-сервера**, будет осуществлена установка **Прокси-сервера** в каталог, отличный от каталога уже установленной версии.

Установка двух **Прокси-серверов** на одном компьютере и настройка их работы через один и тот же порт приведет к неработоспособности обоих **Прокси-серверов**.

Для обновления Прокси-сервера:

1. Если на компьютере с **Прокси-сервером** установлен **Агент** со включенной самозащитой, отключите компонент самозащиты **Dr.Web SelfPROtect** через настройки **Агента.**
2. Удалите **Прокси-сервер** согласно штатной процедуре (см. п. Удаление Прокси-сервера).

При удалении **Прокси-сервера** осуществляется удаление конфигурационного файла `drwcsd-proxy.xml`. При необходимости сохраните конфигурационный файл вручную перед удалением **Прокси-сервера**.

3. Установите новую версию **Прокси-сервера** согласно штатной процедуре (см. п. Установка Прокси-сервера).
4. При необходимости замените конфигурационный файл сохраненным файлом от предыдущей версии.
5. Если на шаге 1 был отключен компонент самозащиты **Dr.Web SelfPROtect**, включите данный компонент через настройки **Агента**.

Обновление Прокси-сервера для ОС семейства UNIX

Для обновления Прокси-сервера необходимо выполнить:

Для Прокси-сервера под		Команда
ОС FreeBSD ОС Solaris		Осуществите удаление и повторную установку согласно штатным процедурам, приведенным в п. Удаление Прокси-сервера и Установка Прокси-сервера
ОС Linux	deb-пакет	`dpkg -i drweb-esuite-proxy`
	rpm-пакет	`rpm -U drweb-esuite-proxy`
	generic-пакет	Распакуйте установочный пакет при помощи следующей команды: `tar -xjf <имя_файла_дистрибутива>.tar.bz2` После этого замените файлы из каталога установки **Прокси-сервера** на файлы из распакованного архива вручную.

9.2. Ручное обновление компонентов Dr.Web Enterprise Security Suite

Перед началом обновления **Dr.Web ESS** и его отдельных компонентов настоятельно рекомендуем проверить корректность настроек протокола TCP/IP для возможности доступа в Интернет. В частности, должна быть включена и содержать корректные настройки служба DNS.

Проверка наличия обновлений

Чтобы проверить наличие обновления продуктов Dr.Web ESS на сервере обновлений:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**.
2. В открывшемся окне отображается информация обо всех компонентах, а также дата их последней ревизии и ее текущее состояние. Для проверки наличия обновлений на сервере **ВСО** нажмите на кнопку **Проверить обновления.**
3. Если проверяемый компонент устарел, то его обновление произойдет автоматически в процессе проверки. Обновление происходит согласно настройкам репозитория (см. п. Управление репозиторием Dr.Web Enterprise Server).
4. После завершения проверки у обновленных компонентов в строке **Последняя ревизия от** будет указана текущая дата.

Запуск процесса обновления ПО станции

Чтобы запустить процесс обновления ПО рабочей станции:

1. Выберите пункт **Антивирусная сеть** главного меню **Центра Управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы.
2. На панели инструментов нажмите на кнопку **Управление компонентами**. В открывшемся подменю выберите пункт:
   - **Обновить сбойные компоненты**, если вы хотите обновить только те компоненты, предыдущее обновление которых сопровождалось ошибкой, и сбросить состояние ошибки,

- **Обновить все компоненты**, если вы хотите запустить принудительное обновление для всех компонентов, в том числе для тех, последняя версия которых уже установлена.

При принудительной синхронизации всех компонентов потребуется две перезагрузки станции. Следуйте указаниям **Агента**.

Вы также можете провести эту операцию с помощью средств управления самого **Enterprise Агента**.

Чтобы запустить процесс обновления ПО рабочей станции при помощи Dr.Web Enterprise Agent

1. Разрешите пользователю данной рабочей станции внесение изменений в настройки **Enterprise Агента** (см. п. Настройка прав пользователей).
2. Выберите в контекстном меню значка **Агента** пункт **Синхронизировать**.
3. В открывшемся подменю выберите пункт:
   - **Только сбойные компоненты**, если вы хотите обновить только те компоненты, предыдущее обновление которых сопровождалось ошибкой, и сбросить состояние ошибки,
   - **Все компоненты**, если вы хотите запустить обновление для сбойных компонентов, как описано выше, и для всех остальных компонентов.

Критическая ошибка обновления

В случае возникновения критической ошибки обновления:

1. Запустите процесс принудительного полного обновления рабочей станции (см. выше).
2. Если ошибка не устранена, установите причину ошибки по файлам протокола **Агента** и модуля обновления на рабочей станции (по умолчанию размещаются в

подкаталоге `logs` каталога установки **Агента**, файлы `drwagntd.log` и `drwupgrade.log`, соответственно).

3. Устраните причину ошибки и снова запустите процесс форсированного обновления рабочей станции.

9.3. Обновление по расписанию

Вы можете настроить расписание выполнения заданий на **Сервере**, для выполнения регулярных обновлений ПО (подробнее о расписании заданий см. п. Настройка расписания Dr.Web Enterprise Server).

Чтобы настроить расписание выполнения задания на обновление на Сервере Dr.Web Enterprise Server:

1. Выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Расписание Dr.Web Enterprise Server**. Откроется текущий список заданий **Сервера**.
2. Для того чтобы добавить задание в список, нажмите на панели инструментов кнопку  **Новое задание**. При этом откроется окно редактирования задания.
3. Введите в поле **Название** наименование задания, под которым оно будет отображаться в расписании.
4. Перейдите на вкладку **Действие** и выберите в выпадающем списке тип задания **Обновление**.
5. В появившемся выпадающем списке выберите обновляемый данным заданием компонент:
   - **Dr.Web Enterprise Agent**
     Dr.Web Enterprise Server
     Dr.Web Enterprise Updater
     Dr.Web для UNIX
     Dr.Web Virus Bases
   - **Все продукты Dr.Web Enterprise**, если вы хотите дать задание на обновление всех компонентов **Dr.Web ESS**.

Для версий **5.0** и выше обновления ПО **Сервера** с серверов **BCO** не поставляются.

Для обновления **Сервера** используйте инсталлятор необходимой версии и проведите процедуру обновления согласно общим правилам, приведенным в разделах Обновление Dr.Web ESS для ОС Windows® или Обновление Dr.Web ESS для ОС семейства UNIX®.

6. Перейдите на вкладку **Время** и укажите в выпадающем списке периодичность запуска задания, после чего настройте время в соответствии с выбранной периодичностью (это действие аналогично настройке времени в расписании рабочей станции, см. п. Настройка расписания заданий на рабочей станции).
7. Для того чтобы сохранить изменения, нажмите на кнопку **Сохранить**.

9.4. Обновление репозитория Dr.Web Enterprise Server, не подключенного к Интернету

Если **Enterprise Сервер** не подключен к Интернету, его репозиторий можно обновить вручную, скопировав репозиторий другого, обновленного, **Enterprise Сервера**.

Данный способ не предназначен для перехода на другую версию.

Для версий **5.0** и выше обновления ПО самого **Сервера** с серверов **BCO** не поставляются.

Для обновления самого **Сервера** используйте инсталлятор необходимой версии и проведите процедуру обновления согласно общим правилам, приведенным в разделах Обновление Dr.Web ESS для ОС Windows® или Обновление Dr.Web ESS для ОС семейства UNIX®.

Для получения обновлений антивирусного ПО рекомендуется следующая последовательность действий:

1. Установите ПО **Enterprise Сервера** на компьютере, имеющем доступ в Интернет, как описано в п. Установка антивирусного Сервера.
2. Остановите оба **Enterprise Сервера**.
3. Для получения обновлений антивирусного ПО запустите **Сервер**, подключенный к Интернету, с ключом `syncrepository`.

   Пример для ОС **Windows**:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin
   \drwcsd.exe" -home="C:\Program Files\DrWeb
   Enterprise Server" syncrepository
   ```

4. Полностью замените содержимое каталога репозитория основного (рабочего) **Сервера** на содержимое аналогичного каталога репозитория **Сервера**, подключенного к Интернету. Обычно это:
   - `var\repository` под ОС **Windows**,
   - `/var/drwcs/repository` под ОС **FreeBSD** и ОС **Solaris**,
   - `/var/opt/drwcs/repository` под ОС **Linux**.

   Если на компьютере с **Enterprise Сервером** установлен **Агент** со включенным компонентом самозащиты **Dr.Web SelfPROtect**, то перед обновлением репозитория необходимо отключить данный компонент через настройки **Агента**.

5. Если основной **Сервер** работает под ОС семейства UNIX, на скопированный репозиторий необходимо установить права пользователя, созданного/выбранного в процессе установки этого **Сервера**.
6. Выполните на основном **Сервере** команду:

```
drwcsd rerepository
```

Под ОС **Windows** команду можно запустить как из *командной строки*:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" rerepository
```

так и из меню `Пуск → Программы → DrWeb Enterprise Server → Управление сервером → Перезагрузить репозиторий`.

7. Запустите основной **Сервер**.

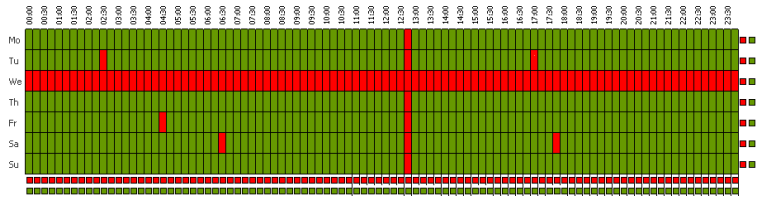
Если при обновлении репозитория был отключен компонент самозащиты **Dr.Web SelfPROtect**, то рекомендуется возобновить работу данного компонента.

9.5. Ограничение обновлений рабочих станций

При помощи **Центра Управления** вы можете задать режим обновлений (разрешено/запрещено) компонентов **Dr.Web Enterprise Security Suite** на защищаемых станциях в определенные промежутки времени. Для этого:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В управляющем меню (панель слева) выберите пункт **Ограничение обновлений**.
2. Откроется таблица, в которой задается режим обновления в следующей цветовой градации:
   - зеленый цвет - обновление разрешено;
   - красный цвет - обновление запрещено.

При этом ограничение задается отдельно на каждые 15 минут каждого дня недели.



3. Для изменения режима обновлений нажмите на соответствующий блок таблицы.

   Для изменения режима целой строки (одного дня полностью), нажмите на маркер соответствующего цвета справа от требуемой строки таблицы.

   Для изменения режима целого столбца (одного 15 минутного интервала для всех дней недели), нажмите на маркер соответствующего цвета под требуемым столбцом таблицы.

4. После завершения редактирования, нажмите на кнопку **Сохранить** для принятия внесенных изменений.

На панели инструментов доступны следующие опции:

Распространить эти настройки на другой объект - для копирования настроек обновлений данной станции или группы в настройки другой станции или группы.

Удалить эти настройки - для сброса настроек обновлений в исходное значение по умолчанию (все обновления разрешены).

Экспортировать настройки в файл - для сохранения настроек обновлений в файл специального формата.

Импортировать настройки из файла - для загрузки настроек обновлений из файла специального формата.

9.6. Обновление мобильных Агентов Dr.Web Enterprise Agent

Если ваш компьютер (или ноутбук) долгое время не будет иметь связи с **Enterprise Сервером**, для своевременного получения обновлений с серверов **ВСО Dr.Web** рекомендуется установить мобильный режим работы **Enterprise Агента**. Для этого в контекстном меню значка **Агента** в области уведомлений **Панели задач** выберите **Мобильный режим → Разрешен**. Цвет значка **Агента** изменится на желтый.

В мобильном режиме **Агент** пытается подключиться к **Серверу**, делает три попытки и, если не удалось, выполняет HTTP-обновление. Попытки найти **Сервер** идут непрерывно с интервалом около минуты.

Вариант **Мобильный режим** будет доступен в контекстном меню при условии, что в правах станции разрешен мобильный режим использования **ВСО Dr.Web** (см. п. Настройка прав пользователей).

Во время функционирования **Агента** в мобильном режиме связь **Агента** с **Enterprise Сервером** прерывается. Все изменения, которые задаются на **Сервере** для такой станции, вступят в силу как только мобильный режим работы **Агента** будет выключен, и связь **Агента** с **Сервером** возобновится.

В мобильном режиме производится обновление только вирусных баз.

Чтобы задать настройки мобильного режима работы выберите **Мобильный режим → Настройки**. В поле **Периодичность** укажите частоту проверки наличия обновлений на **ВСО**. При необходимости установите флаг **Только при соединении с Интернет**.

При использовании прокси-сервера в поле **Прокси** установите флаг **Использовать прокси-сервер** и ниже в полях ввода укажите адрес и порт прокси-сервера, а также параметры авторизации.

Чтобы в мобильном режиме немедленно запустить обновление, выберите **Мобильный режим** → **Запустить обновление**.

Пункт **Запустить обновление** будет недоступен, если есть подключение к **Серверу**.

Чтобы отключить мобильный режим, в контекстном меню значка **Агента** выберите **Мобильный режим** и снимите флаг **Разрешен**. Цвет значка **Агента** изменится с желтого на зеленый, и связь **Агента** с **Сервером** возобновится.

9.7. Обновление серверного ключа и ключа для рабочих станций

Файлы, содержащие серверный ключ и ключ для рабочих станций, устанавливаются вместе с **Enterprise Сервером** (см. п.Установка Dr.Web Enterprise Server). В дальнейшем вы можете получить новые ключи, например, с более продолжительным сроком действия лицензии.

Существует два варианта процедуры замены ключевых файлов в зависимости от того, совпадают ли параметр `ID` **Сервера** в новом ключевом файле и в том, который использовался ранее. Откройте старый и новый ключи `enterprise.key` любым текстовым редактором и в секции `[Enterprise]` посмотрите значение параметра `ID1`.

Ключевой файл имеет формат, защищенный от редактирования при помощи механизма электронной подписи. Редактирование файла делает его недействительным. Чтобы избежать случайной порчи ключевого файла, не следует модифицировать ключевой файл и/или сохранять его при закрытии текстового редактора.

Если на компьютере с **Enterprise Сервером**, установлен **Агент** со включенным компонентом самозащиты **Dr.Web SelfPROtect**, то перед заменой ключевых файлов необходимо отключить данный компонент через настройки **Агента**.

Значения параметров ID1 совпадают

Для установки новых ключевых файлов компонентов антивирусной сети воспользуйтесь Менеджером лицензий.

Чтобы установить новые ключевые файлы компонентов антивирусной сети вручную:

1. Поместите файл с серверным ключом (он должен иметь название `enterprise.key`) в подкаталог `etc` каталога установки **Сервера** вместо имеющегося там одноименного файла.
2. Перезапустите **Сервер**.
3. В каталоге антивирусной сети выберите группу **Everyone**, после чего на панели инструментов нажмите **Общие** → **Импорт ключа**.
4. В открывшемся окне укажите ключевой файл для рабочей станции (`agent.key`) и нажмите **OK**.

Значения параметров ID1 различаются

Чтобы установить новые ключевые файлы компонентов антивирусной сети:

1. Отключите протоколы **Агента** и **Сетевого Инсталлятора.** Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**, перейдите на вкладку **Модули**. Снимите флаги **Протокол Dr.Web Enterprise Agent** и **Протокол Dr.Web Network Installer** и нажмите **Сохранить**. Откроется запрос перезапуска **Сервера**. Нажмите **Да**.
2. Экспортируйте расписание **Enterprise Сервера** в файл. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Расписание Dr.Web Enterprise Server** и на панели инструментов нажмите **Экспортировать настройки в файл**.
3. Для экономии места в базе данных удалите расписание **Enterprise Сервера**. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Расписание Dr.Web Enterprise Server** и на панели инструментов нажмите **Удалить эти настройки**.
4. В случае многосерверной сети:
   a) При необходимости сохранения статистической информации по соседним **Серверам**, экспортируйте статистические таблицы, поскольку после удаления связей эта информация будет утрачена.
   b) Удалите все настроенные межсерверные связи. Это можно сделать через меню **Администрирование**, пункт **Связи**.
5. Установите новые ключевые файлы компонентов антивирусной сети:
   - Воспользуйтесь для этого Менеджером лицензий.

- Для замены ключей вручную воспользуйтесь процедурой, описанной выше.

6. Включите протоколы **Агента** и **Сетевого Инсталлятора**, отключенные в п. **1**.
7. Настройте расписание **Сервера** заново или импортируйте из файла старое расписание, сохраненное в п. **2**.
8. В случае многосерверной сети настройте все необходимые межсерверные связи, удаленные в п. **4**.
9. Перезапустите **Сервер**.

Глава 10. Настройка дополнительных компонентов

10.1. Прокси-сервер

В состав антивирусной сети может входить один или несколько **Прокси-серверов**.

Основная задача **Прокси-сервера** – обеспечение связи **Enterprise Сервера** и **Enterprise Агентов** в случае невозможности организации прямого доступа (например, если **Enterprise Сервер** и **Enterprise Агенты** расположены в различных сетях, между которыми отсутствует маршрутизация пакетов).

Основные функции

Прокси-сервер выполняет следующие функции:

1. Прослушивание сети и прием соединений в соответствии с заданным протоколом и портом.
2. Трансляция протоколов (поддерживаются протоколы TCP/IP, IPv6, IPX и NetBIOS).
3. Пересылка данных между **Enterprise Сервером** и **Enterprise Агентами** в соответствии с настройками **Прокси-сервера.**
4. Кэширование обновлений **Агента** и антивирусного пакета, передаваемых **Сервером**. В случае выдачи обновлений из кэша **Прокси-сервера** обеспечивается:
   - уменьшение сетевого трафика,
   - уменьшение времени получения обновлений **Агентами**.

Возможно создание иерархии **Прокси-серверов**.

Общая схема антивирусной сети при использовании **Прокси-сервера** приведена на рисунке 10-1.

Рисунок 10-1. Схема антивирусной сети при использовании Прокси-сервера

Принцип работы

При использовании Прокси-сервера выполняется следующая последовательность действий:

1. Если на **Агенте** не прописан адрес **Сервера**, то **Агент** отправляет многоадресный запрос в соответствии с протоколом работы сети, в которой он находится.

2. В случае настройки **Прокси-сервера** на трансляцию соединений (параметр `discovery="yes"`), **Агенту** отправляется сообщение о наличии функционирующего **Прокси-сервера**.
3. **Агент** задает полученные параметры **Прокси-сервера** в качестве параметров **Enterprise Сервера**. Дальнейшее взаимодействие осуществляется прозрачно для **Агента**.
4. В соответствии с параметрами конфигурационного файла **Прокси-сервер** прослушивает заданные порты на наличие входящих соединений по указанным протоколам.
5. Для каждого входящего соединения от **Агента Прокси** устанавливает соединение с **Enterprise Сервером**.

Алгоритм переадресации при наличии списка Enterprise Серверов:

1. **Прокси-сервер** загружает в оперативную память список **Enterprise Серверов** из конфигурационного файла `drwcsd-proxy.xml` (см. Приложение G4).
2. К **Прокси-серверу** подключается **Enterprise Агент**.
3. **Прокси-сервер** переадресует **Enterprise Агента** на первый **Enterprise Сервер** из списка в оперативной памяти.
4. **Прокси-сервер** ротирует список, загруженный в оперативную память, и перемещает **Enterprise Сервер** из первого элемента списка в конец списка.

Прокси-сервер не сохраняет измененный порядок **Серверов** в свой файл конфигурации. При перезапуске **Прокси-сервера** список **Enterprise Серверов** загружается в оперативную память в первоначальном виде, в котором он хранится в файле конфигурации.

5. При подключении следующего **Агента** к **Прокси-серверу** процедура повторяется, начиная с шага 2.
6. Если **Enterprise Сервер** отключается от антивирусной сети (например, при выключении или отказе в обслуживании), **Агент** повторно подключается к **Прокси-серверу** и процедура повторяется начиная с шага 2.

Сканер сети, запущенный на машине из внешней по отношению к **Агентам** сети, не сможет обнаружить установленных **Агентов**.

Если флаг **Заменять NetBios-имена** установлен, и в антивирусной сети используется **Прокси-сервер**, то для всех станций, подключенных к **Серверу** через **Прокси-сервер**, в **Центре Управления** в качестве названий станций будет отображаться название компьютера, на котором установлен **Прокси-сервер**.

Шифрование и сжатие трафика

Прокси-сервер поддерживает сжатие трафика. Обработка пересылаемой информации осуществляется вне зависимости от того, сжимается трафик или нет.

Прокси-сервер не поддерживает шифрование. Он анализирует пересылаемую информацию и, если трафик между **Enterprise Сервером** и **Агентом** шифруется, **Прокси-сервер** переходит в прозрачный режим, т.е. пересылает весь трафик между **Сервером** и **Агентом** без какого-либо разбора информации.

В случае включенного режима шифрования трафика между **Агентом** и **Сервером**, кеширование обновлений в **Прокси-сервере** отсутствует.

Кэширование

Прокси-сервер поддерживает кэширование трафика.

Кэширование продуктов осуществляется по ревизиям. Каждая ревизия хранится в отдельном каталоге. В каталоге для каждой следующей ревизии лежат *жесткие ссылки* (*hard links*) на существующие файлы из старых ревизий и оригиналы изменившихся файлов. Таким образом, файлы для каждой версии хранятся на жестком диске в единственном экземпляре, во всех каталогах последующих ревизий приведены только ссылки на

неизменившиеся файлы.

Очистка устаревших ревизий осуществляется раз в час. Хранятся только 3 последние ревизии. Все остальные, более ранние ревизии, считаются устаревшими и удаляются.

Кроме того, каждые 10 минут осуществляется выгрузка неиспользуемых *memory mapped* файлов.

Настройки

Прокси-сервер не имеет графического интерфейса. Задание настроек осуществляется при помощи конфигурационного файла. Формат конфигурационного файла **Прокси-сервера** приведен в Приложении G4.

Управление настройками (редактирование конфигурационного файла) **Прокси-сервера** может осуществлять только пользователь с правами администратора данного компьютера.

Для корректной работы **Прокси-сервера** под ОС семейства Linux после перезагрузки компьютера требуется системная настройка сети без использования Сетевого менеджера.

Запуск и останов

Под ОС Windows запуск и останов **Прокси-сервера** осуществляется штатными средствами при помощи элемента **Панель управления** → **Администрирование** → **Сервисы** → в списке сервисов дважды кликнуть по **drwcsd-proxy** и в открывшемся окне выбрать необходимое действие.

Под ОС семейства UNIX запуск и останов **Прокси-сервера** производится при помощи команд `start` и `stop` применительно скриптов, созданных в процессе установки **Прокси-сервера** (см. п. Установка прокси-сервера).

Также для запуска **Прокси-сервера** под ОС Windows и ОС семейства UNIX вы можете запустить исполняемый файл `drwcsd-proxy` с соответствующими параметрами (см. Приложение Н10. Прокси-сервер).

10.2. NAP Validator

Общие сведения

Microsoft® Network Access Protection (NAP) представляет собой платформу политик, встроенную в операционные системы Windows, которая обеспечивает повышенную безопасность сети. Получаемая безопасность достигается за счет выполнения требований, предъявляемых к работоспособности систем сети.

При использовании технологии NAP возможно создание пользовательских политик работоспособности для оценки состояния компьютера. Полученные оценки анализируются в следующих случаях:

- перед тем, как разрешить доступ или взаимодействие,
- для автоматического обновления соответствующих требованиям компьютеров с целью обеспечения их постоянной совместимости,
- для адаптации не соответствующих требованиям компьютеров таким образом, чтобы они удовлетворяли установленным требованиям.

Подробное описание технологии NAP можно найти по ссылке http://www.microsoft.com/windowsserver2008/en/us/nap-product-home.aspx.

Использование NAP в Dr.Web Enterprise Security Suite

Dr.Web ESS позволяет использовать технологию NAP для проверки работоспособности антивирусного ПО защищаемых

рабочих станций. Для этого служит компонент **Dr.Web NAP Validator**.

При проверке работоспособности используются следующие средства:

- Установленный и настроенный сервер проверки работоспособности NAP.
- **Dr.Web NAP Validator** представляет собой средство оценки работоспособности антивирусного ПО защищаемой системы (System Health Validator - SHV) за счет подключаемых пользовательских политик **Dr.Web**. Устанавливается на компьютер с сервером NAP.
- Агент работоспособности системы (System Health Agent - SHA). Автоматически устанавливается вместе с ПО **Enterprise Агента** на рабочую станцию.
- **Enterprise Сервер** служит в качестве сервера исправлений, обеспечивающего работоспособность антивирусного ПО рабочих станций.

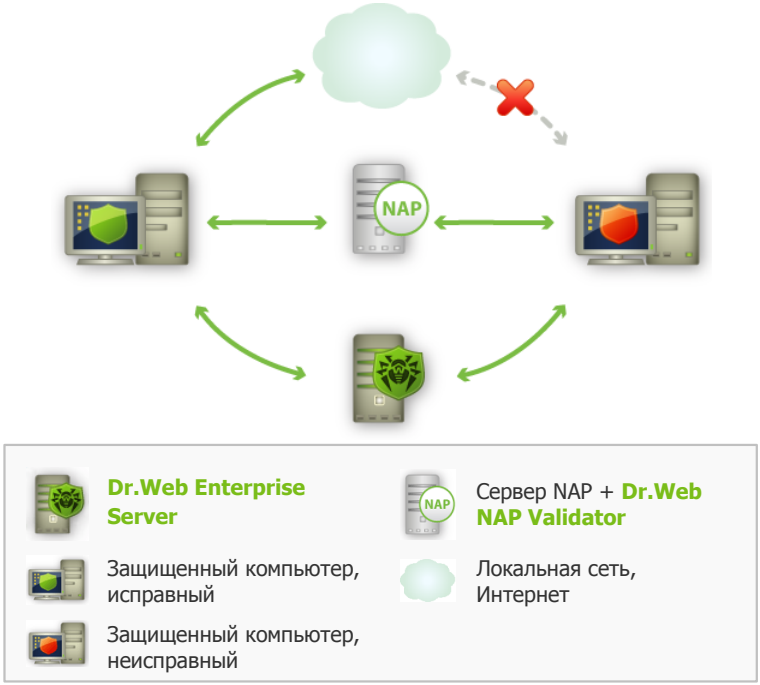


Рисунок 10-2. Схема антивирусной сети при использовании NAP

Процедура проверки осуществляется следующим образом:

1. Активация процесса проверки производится при установке соответствующих настроек **Агента** (см. п. Настройка Dr.Web Enterprise Agent).
2. SHA на рабочей станции связывается с компонентом **Dr.Web NAP Validator**, установленном на сервере NAP.
3. **Dr.Web NAP Validator** осуществляет проверку политик работоспособности (см. ниже). Проверка политик представляет собой процесс, в котором **NAP Validator** выполняет оценку антивирусных средств с точки зрения выполнения заданных им правил, и определяет категорию текущего состояния системы:

- станции, прошедшие проверку на соответствие элементам политики, считаются работоспособными и допускаются к полнофункциональной работе в сети.
- станции, не удовлетворяющие хотя бы одному из элементов политики, признаются неработоспособными. Доступ таких станций разрешен только к **Enterprise Серверу**, от остальной сети они изолируются. Работоспособность станции восстанавливается при помощи **Сервера**, после чего станция проходит повторную процедуру проверки.

Требования к работоспособности:

1. Рабочее состояние агента (запущен и функционирует).
2. Актуальность вирусных баз (базы совпадают с базами на сервере).

Настройка NAP Validator

После инсталляции **Dr.Web NAP Validator** (см. п. Установка NAP Validator) на компьютере с установленным NAP сервером, необходимо выполнить следующие действия:

1. Откройте компонент настройки сервера NAP (команда `nps.msc`).
2. В разделе **Policies** выберите подпункт **Health Policies**.
3. В открывшемся окне откройте свойства элементов:
   - **NAP DHCP Compliant**. В окне настроек установите флаг **Dr.Web System Health Validator**, задающий использование политик компонента **Dr.Web NAP Validator**. В выпадающем списке типа проверок укажите пункт **Client passed all SHV checks**. Согласно данной опции, станция будет объявлена работоспособной, если она соответствует всем элементам заданной политики.

- **NAP DHCP Noncompliant**. В окне настроек установите флаг **Dr.Web System Health Validator**, задающий использование политик компонента **Dr.Web NAP Validator**. В выпадающем списке типа проверок укажите пункт **Client fail one or more SHV checks**. Согласно данной опции, станция будет объявлена неработоспособной, если она не соответствует хотя бы одному из элементов заданной политики.

Приложения

Приложение А. Полный список поддерживаемых версий ОС

Для Dr.Web Enterprise Server:

ОС семейства UNIX:

ALT Linux School Server 5.0
ALT Linux School Server 5.0 x86_64
ASP Linux 12
ASP Linux 14
Debian/GNU Linux Lenny
Debian/GNU Linux Lenny x86_64
Debian/GNU Linux Sid x86_64
Debian/GNU Linux Squeeze
Debian/GNU Linux Squeeze x86_64
FreeBSD 7.3
FreeBSD 7.3 amd64
FreeBSD 7.4
FreeBSD 7.4 amd64
FreeBSD 8.1
FreeBSD 8.1 amd64
FreeBSD 8.2
FreeBSD 8.2 amd64
Linux glibc2.7
Linux glibc2.7 x86_64
Linux glibc2.8
Linux glibc2.8 x86_64

Linux glibc2.9
Linux glibc2.9 x86_64
Linux glibc2.10
Linux glibc2.10 x86_64
Linux glibc2.11
Linux glibc2.11 x86_64
Linux glibc2.12
Linux glibc2.12 x86_64
Linux glibc2.13
Linux glibc2.13 x86_64
Mandriva Linux 2010
Mandriva Linux 2010 x86_64
Mandriva Linux Corporate Server 5.1
Mandriva Linux Corporate Server 5.1 x86_64
openSUSE 11
openSUSE 11 x86_64
RedHat Enterprise Linux 5.3
RedHat Enterprise Linux 5.3 x86_64
RedHat Enterprise Linux 6
RedHat Enterprise Linux 6 x86_64
RedHat Fedora 8
RedHat Fedora 8 x86_64
RedHat Fedora 9
RedHat Fedora 9 x86_64
RedHat Fedora 10
RedHat Fedora 10 x86_64
RedHat Fedora 11
RedHat Fedora 11 x86_64
RedHat Fedora 12
RedHat Fedora 12 x86_64
RedHat Fedora 13
RedHat Fedora 13 x86_64
RedHat Fedora 14

RedHat Fedora 14 x86_64
RedHat Fedora 15
RedHat Fedora 15 x86_64
SUSE Linux Enterprise Server 10
SUSE Linux Enterprise Server 10 x86_64
SUSE Linux Enterprise Server 11
SUSE Linux Enterprise Server 11 x86_64
Sun Solaris 10 x86
Sun Solaris 10 Sparc 32bit (процессор Sparc V9; UltraSparc как минимум)
Sun Solaris 10 Sparc 64bit (процессор Sparc V9; UltraSparc как минимум)
Ubuntu 8.04
Ubuntu 8.04 x86_64
Ubuntu 10.04
Ubuntu 10.04 x86_64
Ubuntu 10.10
Ubuntu 10.10 x86_64
Ubuntu 11.04
Ubuntu 11.04 x86_64
Ubuntu 11.10
Ubuntu 11.10 x86_64

ОС Windows:

- 32 bit:

Windows 2000 Professional (SP4)
Windows 2000 Server (SP4)
Windows XP Professional (SP3)
Windows Server 2003 (SP2)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows 7

Windows 8

- 64 bit:

Windows Server 2003 (SP2)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

Для Dr.Web Enterprise Agent и антивирусного пакета:

ОС семейства UNIX:

Linux glibc 2.7 и выше
FreeBSD 7.3 и выше
Sun Solaris 10 (только для платформы Intel)

ОС Windows:

- 32 bit:

Windows 98
Windows Millennium Edition
Windows NT4 (SP6a)
Windows 2000 Professional (SP4 также с Update Rollup 1)
Windows 2000 Server (SP4 также с Update Rollup 1)
Windows XP Professional (также с SP1 и выше)
Windows XP Home (также с SP1 и выше)
Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)

Windows 7
Windows 8

- 64 bit:

Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

SelfPROtect, SplDer Gate, Офисный Контроль, FireWall

- 32 bit:

Windows 2000 Professional (SP4 также с Update Rollup 1)
Windows 2000 Server (SP4 также с Update Rollup 1)
Windows XP Professional (также с SP1 и выше)
Windows XP Home (также с SP1 и выше)
Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows 7
Windows 8

- 64 bit:

Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

ОС Windows Mobile

Windows Mobile 2003
Windows Mobile 2003 Second Edition
Windows Mobile 5.0
Windows Mobile 6.0
Windows Mobile 6.1
Windows Mobile 6.5

ОС Novell NetWare

Novell NetWare 4.11 SP9
Novell NetWare 4.2
Novell NetWare 5.1
Novell NetWare 6.0
Novell NetWare 6.5

Mac OS X

Mac OS 10.6 (Snow Leopard)
Mac OS 10.6 Server (Snow Leopard Server)
Mac OS 10.7 (Lion)
Mac OS 10.7 Server (Lion Server)
Mac OS 10.8 (Mountain Lion)
Mac OS 10.8 (Mountain Lion Server)

ОС Android

Android 1.6
Android 2.0
Android 2.1
Android 2.2
Android 2.3

Android 3.0
Android 3.1
Android 3.2
Android 4.0.

Приложение В. Настройки для использования СУБД. Параметры драйверов СУБД

Структуру БД **Enterprise Сервера** можно получить на основе sql-скрипта `init.sql`, расположенного в подкаталоге `etc` каталога установки **Enterprise Сервера**.

В качестве базы данных **Enterprise Сервера** может использоваться:

- встроенная СУБД (IntDB);
- внешняя СУБД.

Встроенная СУБД

При настройке обращения к встроенной СУБД для хранения и обработки данных используются параметры, приведенные в таблице В-1.

Таблица В-1. Встроенная СУБД (IntDB)

Имя	Значение по умолчанию	Описание
`DBFILE`	`dbinternal.dbs`	Путь к файлу базы данных
`CACHESIZE`	`2000`	Размер кэша базы данных в страницах
`SYNCHRONOUS`	`FULL`	Режим синхронной записи изменений в базе данных на диск: • `FULL` — полностью синхронная запись на диск, • `NORMAL` — синхронная запись критичных данных,

Имя	Значение по умолчанию	Описание
		• `OFF` — асинхронная запись

Внешняя СУБД

В качестве внешней базы данных **Enterprise Сервера** может использоваться:

- СУБД Oracle. Описание настройки приведено в Приложении В2. Настройка драйвера БД для Oracle.
- СУБД Microsoft SQL Server Compact Edition (SQL CE). Описание настройки приведено в Приложении В3. Настройка драйвера БД для SQL CE.
- СУБД PostgreSQL. Описание настроек, необходимых для СУБД PostgreSQL описано в Приложении В4. Использование СУБД PostgreSQL.
- Microsoft SQL Server/Microsoft SQL Server Express. Для доступа к данным СУБД может использоваться ODBC-драйвер (настройка параметров ODBC-драйвера для ОС Windows приведена в Приложении В1. Настройка ODBC-драйвера).

При использовании Microsoft SQL Server 2005 требуется ODBC-драйвер, поставляемый с данной СУБД.

Поддерживается использование Microsoft SQL Server 2005 (SP4) и выше.

Настоятельно рекомендуется установить последние обновления для используемого сервера БД.

БД Microsoft SQL Server Express не рекомендуется для развертывания антивирусной сети с большим количеством станций (от 100 и выше).

Сравнительные характеристики

Использование внутренней БД допустимо при подключении к **Серверу** не более 200-300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен **Enterprise Сервер**, и нагрузка по прочим задачам, выполняемым на данном компьютере - возможно подключение до 1000 станций.

В противном случае необходимо использовать внешнюю БД.

При использовании внешней БД и подключении к **Серверу** более 10000 станций рекомендуется выполнение следующих минимальных требований:

- процессор с частотой 3ГГц,
- оперативная память - от 4 Гб для **Enterprise Сервера**, от 8 Гб - для сервера БД,
- ОС семейства UNIX.

При выборе между встроенной и внешней базами следует учесть некоторые параметры, присущие каждой из СУБД:

- В больших антивирусных сетях (свыше 200-300 станций) рекомендуется использовать внешнюю БД, более устойчивую к сбоям, чем встроенные БД.
- При использовании встроенной БД не требуется установка компонентов сторонних производителей. Рекомендуется при типичном использовании.
- Встроенная база данных не требует знаний администрирования СУБД и является хорошим выбором для антивирусной сети малого и среднего масштаба.

- Внешнюю базу имеет смысл использовать в том случае, если подразумевается самостоятельная работа с СУБД, требующая прямого доступа к базе. При этом могут использоваться стандартные API для доступа к базам данных, такие как: OLE DB, ADO.NET или ODBC. Однако, стоит учесть, что на данный момент не существует ODBC-драйвера для СУБД Microsoft SQL CE. Но поддержка технологий ADO.NET, а также языка LINQ значительно упрощает работу в приложениях с данной СУБД и позволяет использовать все возможности платформы .NET Framework, в том числе систему создания отчетов CrystalReports.

Приложение В1. Настройка ODBC-драйвера

При настройке обращения к внешней СУБД для хранения и обработки данных используются параметры, приведенные в таблице В-2.

Таблица В-2. ODBC (только в версии для Windows)

Имя	Значение по умолчанию	Описание
DSN	drwcs	Имя набора данных
USER	drwcs	Имя пользователя
PASS	drwcs	Пароль
TRANSACTION	DEFAULT	См. ниже

Возможные значения параметра TRANSACTION:

- SERIALIZABLE
- READ_UNCOMMITTED
- READ_COMMITTED
- REPEATABLE_READ
- DEFAULT

Значение по умолчанию `DEFAULT` означает "использовать умолчание SQL-сервера". Подробнее об уровнях изоляции транзакций смотрите в документации по соответствующей СУБД.

Чтобы исключить проблемы с кодировкой, необходимо отключить следующие параметры ODBC-драйвера:

- **Использовать национальные настройки** - может вызвать ошибки при форматировании числовых параметров.
- **Выполнять перевод символьных данных** - может вызывать некорректное отображение символов в **Центре Управления** для параметров, пришедших из базы данных. Он устанавливает зависимость отображения символов от языкового параметра для программ, не использующих Unicode.

Сама база данных создается предварительно на SQL-сервере с параметрами, указанными выше. **Необходимо также настроить параметры ODBC-драйвера для компьютера**, на который установлен **Enterprise Сервер**. ***Для этого:***

1. На **Панели управления** ОС Windows выберите пункт **Администрирование**, в открывшемся окне дважды щелкните по значку **Источники данных (ODBC)**. Откроется окно **Администратор источников данных ODBC**. Перейдите на вкладку **Системный DSN**.
2. Нажмите на кнопку **Добавить**. Откроется окно выбора драйвера.
3. Выберите в списке пункт, соответствующий ODBC-драйверу для данной БД, и нажмите на кнопку **Готово**. Откроется первое из окон настройки доступа к серверу баз данных.

При использовании внешней СУБД необходимо установить последнюю версию ODBC-драйвера, поставляемую с данной СУБД. Использование ODBC-драйвера, поставляемого вместе с ОС Windows, не рекомендовано. Исключением являются БД, поставляемые Microsoft без ODBC-драйвера.

4. Укажите параметры доступа к источнику данных, совпадающие с заданными в настройках **Enterprise Сервера.** Если сервер БД находится не на том же компьютере, что и **Enterprise Сервер**, укажите в поле ввода **Сервер** его адрес или имя. Нажмите на кнопку **Далее.** Откроется следующее окно настройки.
5. Введите необходимые настройки доступа к БД в этом окне. Нажмите на кнопку **Настройка клиента**. Откроется окно выбора и настройки сетевого протокола.
6. Выберите сетевую библиотеку для протокола **TCP/IP** или **Named pipes** (рекомендуется). Если сервер БД работает не на локальном компьютере, задайте вместо точки в полях ввода **Псевдоним для сервера** и **Имя компьютера** его имя или адрес. Нажмите на кнопку **ОК**. Окно закроется. Вы вернетесь в окно настройки драйвера. Нажмите на кнопку **Далее**. Откроется следующее окно настройки.
7. Убедитесь, что выбрана опция **Только при отключении** и установлены следующие флаги: **Заключенные в кавычки идентификаторы в формате ANSI**, **Значения null**, **Шаблоны и предупреждения в формате ANSI**. Нажмите на кнопку **Далее**. Откроется последнее окно настройки доступа.

Если при настройке ODBC-драйвера имеется возможность изменить язык системных сообщений SQL-сервера, необходимо установить английский язык.

8. По окончании настройки нажмите на кнопку **Готово**. Откроется окно со сводкой заданных вами параметров.
9. Для проверки правильности настроек нажмите на кнопку **Проверить источник данных**. После сообщения об успешности проверки нажмите на кнопку **ОК**.

Приложение В2. Настройка драйвера БД для Oracle

Общее описание

Oracle Database (или Oracle DBMS) — это объектно-реляционная СУБД. Oracle может быть использована в качестве внешней БД для **Dr.Web ESS**.

Enterprise Сервер может использовать СУБД Oracle в качестве внешней базы на всех платформах, кроме FreeBSD (см. п. Установка и поддерживаемые версии).

Для использования СУБД Oracle необходимо:

1. Установить экземпляр БД Oracle с настройками кодировки `AL32UTF8`. Также можно использовать существующий экземпляр БД с указанной кодировкой.
2. Настроить драйвер БД на использование соответствующей внешней базы. Это можно сделать в конфигурационном файле или при помощи **Центра Управления**: меню **Конфигурация Dr.Web Enterprise Server**, вкладка **База данных**.

Если вы планируете использовать в качестве внешней базы данных ODBC для Oracle, то при установке (обновлении) **Сервера**, в настройках инсталлятора выберите пункт **Выборочная** установка и в следующем окне отмените установку встроенного клиента для СУБД Oracle (в разделе **Database support** - **Oracle database driver**).

В противном случае работа с БД Oracle через ODBC будет невозможна из-за конфликта библиотек.

Установка и поддерживаемые версии

Для возможности использования БД Oracle в качестве внешней базы необходимо установить экземпляр БД Oracle и настроить для него кодировку `AL32UTF8` (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`). Это можно сделать следующими способами:

1. При помощи инсталлятора БД Oracle (используйте расширенный режим установки и конфигурирования БД).
2. При помощи SQL команды `CREATE DATABASE`.

Более подробная информация о создании и конфигурации БД приведена в документации к БД Oracle.

В случае использования кодировки, отличной от указанной, национальные символы будут отображаться некорректно.

Клиент для доступа к БД (Oracle Instant Client) входит в состав установочного пакета **Dr.Web ESS**.

Платформы, поддерживаемые СУБД Oracle, приведены на сайте производителя http://www.oracle.com/technology/software/tech/oci/instantclient/index.html.

Dr.Web ESS поддерживает следующие версии СУБД: Oracle9i Database Release 2: 9.2.0.1 - 9.2.0.8 и выше.

Параметры

При настройке обращения к СУБД Oracle используются параметры, описываемые в таблице В-3.

Таблица В-3. Параметры СУБД Oracle

Параметр	Описание
`drworacle`	Имя драйвера
`User`	Имя пользователя БД (обязательный)
`Password`	Пароль пользователя (обязательный)
`ConnectionString`	Строка соединения с базой данных (обязательный)

Формат строки соединения с СУБД Oracle следующий:

//<host>:<port>/<service name>

где:

- *<host>* - IP-адрес либо имя сервера Oracle;
- *<port>* - порт, который "слушает" сервер;
- *<service name>* - имя БД, к которой необходимо подключиться.

Например:

`//myserver111:1521/bjava21`

где:

- `myserver111` - имя сервера Oracle.
- `1521` - порт, который "слушает" сервер.
- `bjava21` - имя БД, к которой необходимо подключиться.

Пример конфигурационного файла drwcsd.conf

При использовании СУБД Oracle необходимо изменить определение и настройки драйвера БД одним из следующих способов:

- в **Центре Управления**: пункт **Администрирование** главного меню → пункт **Конфигурация Dr.Web Enterprise Server** управляющего меню → вкладка **База данных** → выбрать в выпадающем списке **База данных** тип **Oracle**, установить настройки согласно формату, приведенному выше.
- в конфигурационном файле **Сервера**. Фрагмент конфигурационного файла с соответствующими параметрами приведен ниже:

```
...
;Database definition. Mandatory.
;Only one definition is allowed.
database


;DB driver (DLL or shared object name)
drworacle ; Oracle DB, unix & windows


;load library from this path; empty - use default
from ""
using "User=DRWCS Password=root
ConnectionString=//192.168.0.1:1521/ORADB"
```

Приложение В3. Настройка драйвера БД для SQL CE

Рекомендуется использовать встроенную БД вместо БД MS SQL CE, если нет необходимости в самостоятельной работе с БД посредством ADO.NET. Внутренняя база отличается повышенной стабильностью и производительностью по сравнению с MS SQL CE.

Общее описание

Microsoft SQL Server Compact Edition (SQL CE) — это реляционная БД от компании Microsoft. Представляет собой встраиваемую БД для настольных приложений и мобильных устройств. SQL CE может быть использована в качестве внешней БД для **Dr.Web ESS.**

Для использования SQL Server CE необходимо:

1. Установить сервер SQL CE.
2. Настроить драйвер БД на использование соответствующей внешней базы. Это можно сделать в конфигурационном файле или при помощи **Центра Управления**: меню **Конфигурация Dr.Web Enterprise Server**, вкладка **База данных**.

Установка и поддерживаемые платформы

СУБД SQL CE поддерживает операционные системы Windows 2000 и выше (в версиях для x32 и x64).

Dr.Web Enterprise Security Suite поддерживает SQL CE версий 3.5 SP1/SP2 для платформ x64 и x86. Совместимость с последующими версиями БД SQL CE не гарантируется.

Для возможности использования БД SQL Server Compact Edition необходимо скачать исталляционный пакет с сайта производителя http://www.microsoft.com/sqlserver/2005/en/us/compact-downloads.aspx и установить сервер соответствующей версии (см. также см. Системные требования для версии 3.5.).

Не рекомендуется устанавливать более одной версии SQL Server Compact из-за возможных проблем с совместимостью.

БД, созданные под разными версиями SQL Server Compact могут быть несовместимы, поскольку версия 3.1, в отличие от версии 3.5, не поддеживает шифрование. Поэтому, при необходимости смены версии, перенос БД должен осуществляться только при помощи команд **Dr.Web Enterprise Security Suite** `exportdb` и `importdb`.

Клиент для доступа к БД входит в состав установочного пакета **Dr.Web ESS**.

Параметры

При настройке обращения к СУБД SQL CE используются параметры, описываемые в таблице В-4.

Таблица В-4. Параметры СУБД SQL CE

Параметр	Описание
`drwsqlce`	Имя драйвера.
`DBFILE`	Имя БД (по умолчанию `mssqlce.sdf`).
`PASSWORD`	Пароль, используемый для шифрования БД.

Параметр `PASSWORD` является ключом шифрования и не имеет отношения к системе пользователь/пароль.

По умолчанию пароль пустой (база не шифруется).

Пример конфигурационного файла drwcsd.conf

При использовании СУБД SQL CE необходимо изменить определение и настройки БД в конфигурационном файле **Enterprise Сервера**. Фрагмент конфигурационного файла с соответствующими параметрами приведен ниже:

```
...
;Database definition. Mandatory.
;Only one definition is allowed.
database


;DB driver (DLL or shared object name)
drwsqlce  ; sql server compact, windows only


;load library from this path; empty - use default
from ""
;parameters describing database connection
;defaults (DBFILE: varroot/mssqlce.sdf)
;using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
```

Приложение В4. Использование СУБД PostgreSQL

Общее описание

PostgreSQL - объектно-реляционная СУБД. Является свободной альтернативой коммерческой СУБД (таким как Oracle Database, Microsoft SQL Server и др.). В больших антивирусных сетях СУБД PostgreSQL может быть использована в качестве внешней БД для **Dr.Web ESS**.

Для этого необходимо:

1. Установить сервер PostgreSQL.
2. Настроить ODBC-драйвер.
3. Настроить **Enterprise Сервер** на использование соответствующей внешней базы. Это можно сделать в конфигурационном файле или при помощи **Центра Управления**: меню **Конфигурация Dr.Web Enterprise Server**, вкладка **База данных**.

Установка и поддерживаемые версии

Загрузите самую последнюю версию бесплатного продукта PostgreSQL (сервер PostgreSQL и соответствующий ODBC-драйвер) или, по крайней мере, не используйте версию младше чем 8.2.

СУБД PostgreSQL существует в реализациях для следующих платформ: Linux, Solaris/OpenSolaris, Win32, Mac OS X, FreeBSD.

Полезную информацию по установке и использованию PostgreSQL с **Enterprise Сервером** можно найти здесь.

Данная статья подробно описывает создание внешней базы PostgreSQL и установку **Dr.Web Enterprise Security Suite** с

использованием созданной ранее базы. В случае наличия установленной **Dr.Web Enterprise Security Suite**, создание БД PostgreSQL производится аналогично, а переход на внешнюю БД подробно описан в п. Смена типа СУБД Dr.Web Enterprise Suite.

ANSI-версию ODBC-драйвера можно использовать только начиная с версии PostgreSQL 8.2.4. ODBC-драйвер для Unicode работает нормально во всех версиях.

Установка на 64-битные системы

Драйвер psqlODBC для 64-битных ОС официально не поставляется разработчиком. Однако согласно официальному сайту СУБД PostgreSQL, возможна установка предрелизных инсталляционных пакетов, которые можно скачать, например, по следующим ссылкам:

- http://www.enterprisedb.com/products/pgdownload.do#windows
- http://code.google.com/p/visionmap/wiki/psqlODBC
- http://www.geocities.jp/inocchichichi/psqlodbc/index.html

После установки ODBC-драйвера на 64-битную ОС, для возможности доступа к драйверам используйте административную панель управления, расположенную здесь: `C:\WINDOWS\SYSWOW64\odbcad32.exe`.

Параметры

При настройке обращения к БД PostgreSQL используются параметры, описываемые в таблице В-5.

Таблица B-5. PostgreSQL (только в версии для ОС UNIX)

Имя	Значение по умолчанию	Описание
host	*<Локальный UNIX-сокет>*	Хост сервера PostgreSQL
port		Порт сервера PostgreSQL или расширение имени файла сокета
dbname	drwcs	Имя базы данных
user	drwcs	Имя пользователя
password	drwcs	Пароль
options		Опции отладки/трассировки для отправки серверу
tty		Файл или tty для вывода при отладке
requiressl		1 для запроса установки SSL соединения или 0 для отсутствия запроса

Техническую информацию можно также найти по адресу http://www.postgresql.org/docs/manuals/.

Взаимодействие Dr.Web Enterprise Server с БД PosrtgreSQL через UDS

При установке **Enterprise Сервера** и БД PostgreSQL на одной машине возможна настройка их взаимодействия через UDS (доменный сокет UNIX).

Для настройки работы через UDS необходимо:

1. В конфигурационном файле БД PostgreSQL `postgresql.conf` прописать следующую директорию для UDS:

   ```
   unix_socket_directory = '/var/run/postgresql'
   ```

2. Перезапустить PostgreSQL.

Приложение С. Описание параметров системы оповещения

При настройке системы оповещения о событиях, связанных с работой компонентов антивирусной сети, для различных типов драйверов модуля оповещения используются указанные ниже параметры.

Таблица С-1. Оповещения по электронной почте (драйвер drwemail)

Параметр	Значение по умолчанию	Описание
HOST	127.0.0.1	Хост сервера SMTP
PORT	25	Порт сервера SMTP
PASS		Пароль SMTP
USER		SMTP user
DEBUG	NO	Режим отладки
FROM	drwcsd@localhost	Адрес отправителя
TO	root@localhost	Адрес получателя

Таблица С-2. Оповещения с использованием Windows Messenger (драйвер drwwnetm), только в версии для ОС Windows

Параметр	Значение по умолчанию	Описание
TO	Admin	Сетевое имя машины

Система оповещений по сети Windows функционирует только на ОС Windows с поддержкой сервиса Windows Messenger (Net Send).

ОС Windows Vista и старше не поддерживают сервис Windows Messenger.

Приложение D. Параметры шаблонов системы оповещения

Тексты сообщений (по электронной почте или с использованием **Windows Messenger**) генерируются компонентом **Сервера**, именуемым процессором шаблонов, на основе файлов шаблонов.

Система оповещений по сети Windows функционирует только на ОС Windows с поддержкой сервиса Windows Messenger (Net Send).

ОС Windows Vista и старше не поддерживают сервис Windows Messenger.

Файл шаблона состоит из текста и переменных, заключенных в фигурные скобки. При редактировании файлов шаблонов можно использовать перечисленные ниже переменные.

Процессор шаблонов не выполняет рекурсивных подстановок.

Переменные записываются в одной из следующих форм:

- {<*VAR*>} – подставить непосредственно значение переменной <*VAR*>.
- {<*VAR*>:<*N*>} – первые <*N*> символов переменной <*VAR*>.
- {<*VAR*>:<*first*>:<*N*>} – <*N*> символов переменной <*VAR*>, следующих после <*first*> первых (начиная с <*first*>+1-го символа), если остаток меньше – дополняется пробелами справа.
- {<*VAR*>:<*first*>:-<*N*>} – <*N*> символов переменной <*VAR*>, следующих после <*first*> первых (начиная с <*first*>+1-го символа), если остаток меньше – дополняется пробелами слева.

- {*<VAR>*/*<original1>*/*<replace1>*[/*<original2>*/*<replace2>*]} – замена указанных символов переменной *<VAR>* на заданные значения: символы *<original1>* заменяются на символы *<replace1>*, при наличии символы *<original2>* заменяются на символы *<replace2>* и т.д.

  Ограничений для числа пар подстановки не существует.

Таблица D-1. Форма записи переменных

Переменная	Значение	Выражение	Результат
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	°°°35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456°°°
SYS.TIME	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17:456

Условные обозначения

° - пробельный символ.

Системные переменные:

- SYS.TIME — текущее системное время,
- SYS.DATE — текущая системная дата,
- SYS.DATETIME — текущие системная дата и время,
- SYS.VERSION — версия **Сервера**,
- SYS.BUILD — дата сборки **Сервера**,
- SYS.PLATFORM — платформа **Сервера**,
- SYS.PLATFORM.SHORT — краткий вариант SYS.PLATFORM,
- SYS.OS — название операционной системы на компьютере с установленным **Сервером**,
- SYS.BRANCH — версия **Агентов** и **Сервера**,

- SYS.SERVER — название продукта (**Dr.Web Enterprise Server**).

Переменные окружения имеют те же имена, что и переменные, заданные в окружении, с добавлением префикса ENV. (префикс заканчивается на точку).

Общие переменные сообщений, Агент:

- GEN.LoginTime — время подключения станции,
- GEN.StationAddress — адрес станции,
- GEN.StationID — UUID станции,
- GEN.StationName — имя станции.

Общие переменные сообщений, подсистема обновлений Сервера:

- GEN.CurrentRevision — текущий идентификатор версии,
- GEN.NextRevision — идентификатор обновленной версии,
- GEN.Folder — каталог размещения продукта,
- GEN.Product — описание продукта.

Переменные сообщений, по сообщениям (для Агента):

Administrator_Authorization_Failed:

- MSG.Login — регистрационное имя,
- MSG.Address — сетевой адрес **Центра Управления**;

Approved_Newbie:

- MSG.AdminName — имя администратора,
- MSG.AdminAddress — адрес **Центра Управления**;

AutoApproved_Newbie: переменные отсутствуют;

Awaiting_Approval: переменные отсутствуют;

Cannot_Add_Station:

- MSG.ID — UUID станции;

Connection_Terminated_Abnormally:

- MSG.Reason — причина завершения;

Infection:

- MSG.Component — имя компонента,
- MSG.RunBy — пользователь, от имени которого запущен компонент,
- MSG.ServerTime — время получения события, GMT,
- MSG.ObjectName — имя инфицированного объекта,
- MSG.ObjectOwner — владелец инфицированного объекта,
- MSG.InfectionType — тип инфекции,
- MSG.Virus — имя вируса,
- MSG.Action — действие, предпринятое при обнаружении;

Installation_Bad:

- MSG.Error — сообщение об ошибке;

Installation_OK: переменные отсутствуют;

License_Limit — отправляется, когда количество зарегистрированных станций приближается к лицензионному ограничению, а именно: осталось неиспользованным менее 5% лицензионного лимита или менее двух станций:

- MSG.Used — число станций в базе,
- MSG.Licensed — разрешено лицензией;

Low_Var_Free_Space:

- MSG.Path — путь к каталогу с малым объемом памяти,
- MSG.FreeSpace — свободное место в байтах,

- MSG.FreeInodes — число свободных файловых дескрипторов inodes (имеет смысл только для некоторых систем семейства UNIX),
- MSG.RequiredSpace — необходимый для работы объем свободной памяти,
- MSG.RequiredInodes —- необходимое для работы число свободных inodes (имеет смысл только для некоторых систем семейства UNIX);

Near_Max_Stations (отправляется при каждом запуске **Сервера** в том случае, если **Сервер** запущен с ключом, лицензирующим меньшее число станций, чем уже подключено к **Серверу**):

- MSG.Used — число станций в базе,
- MSG.Licensed — разрешено лицензией,
- MSG.Percent — процент свободных лицензий;

Newbie_Not_Allowed: переменные отсутствуют;

Not_Seen_For_A_Long_Time:

- MSG.StationName — название станции,
- MSG.StationID — UUID станции,
- MSG.DaysAgo — количество дней с момента последнего подключения к **Серверу**,
- MSG.LastSeenFrom — адрес, с которого станция в последний раз подключалась к **Серверу**;

Processing_Error:

- MSG.Component — имя компонента,
- MSG.RunBy — пользователь, от имени которого запущен компонент,
- MSG.ServerTime — время получения события, GMT,
- MSG.ObjectName — имя объекта,
- MSG.ObjectOwner — владелец объекта,
- MSG.Error — сообщение об ошибке;

Rejected_Newbie:

- MSG.AdminName — имя администратора,
- MSG.AdminAddress — адрес **Центра Управления**;

Station_Already_Logged_In – отправляется, если станция в настоящее время уже зарегистрирована на этом или другом **Сервере**:

- MSG.ID — UUID станции,
- MSG.StationName — имя станции,
- MSG.Server — ID **Сервера**, на котором станция зарегистрирована,

Station_Authorization_Failed:

- MSG.ID — UUID станции,
- MSG.Rejected — значения rejected — станции отказано в доступе, newbie — сделана попытка перевести станцию в состояние "новичок";

Statistics:

- MSG.Component — имя компонента,
- MSG.ServerTime — время получения события, GMT,
- MSG.Scanned — число просканированных объектов,
- MSG.Infected — число инфицированных объектов,
- MSG.Modifications — число объектов, инфицированных модификациями вирусов,
- MSG.Suspicious — число подозрительных объектов,
- MSG.Cured — число вылеченных объектов,
- MSG.Deleted — число удаленных объектов,
- MSG.Renamed — число переименованных объектов,
- MSG.Moved — число перемещенных объектов,
- MSG.Speed — скорость обработки в Кб/сек;

Too_Many_Stations — отправляется, когда новая станция не может зарегистрироваться на **Сервере** из-за лицензионных

ограничений:

- `MSG.ID` — UUID станции,

`Unknown_Administrator`:

- `MSG.Login` — регистрационное имя,
- `MSG.Address` — сетевой адрес **Центра Управления**.

`Unknown_Station`:

- `MSG.ID` — UUID неизвестной станции,
- `MSG.Rejected` — значения `rejected` — станции отказано в доступе, `newbie` — сделана попытка перевести станцию в состояние "новичок";

`Update_Failed`:

- `MSG.Product` — обновляемый продукт,
- `MSG.ServerTime` — время (местное) получения сообщения **Сервером**;

`Update_Wants_Reboot`:

- `MSG.Product` — обновляемый продукт,
- `MSG.ServerTime` — время (местное) получения сообщения **Сервером**.

Переменные сообщений, по сообщениям (для подсистемы обновлений Сервера):

`Srv_Repository_Cannot_flush`: переменные отсутствуют;

`Srv_Repository_UpToDate`: переменные отсутствуют;

`Srv_Repository_Frozen`: переменные отсутствуют;

`Srv_Repository_Load_failure`:

- `MSG.Reason` — сообщение о причине ошибки;

`Srv_Repository_Update`:

- `MSG.AdddedCount` — количество добавленных файлов,

- MSG.ReplacedCount — количество замененных файлов,
- MSG.DeletedCount — количество удаленных файлов,
- MSG.Added — список добавленных файлов (каждое наименование на отдельной строке),
- MSG.Replaced — список замененных файлов (каждое наименование на отдельной строке),
- MSG.Deleted — список удаленных файлов (каждое наименование на отдельной строке).

Srv_Repository_UpdateFailed:

- MSG.Error — сообщение об ошибке,
- MSG.ExtendedError — подробное описание ошибки.

Переменные последнего шаблона не включают файлы, помеченные как "**игнорируемые при оповещениях**" в конфигурационном файле продукта, см. F1. Синтаксис файла конфигурации .config.

Переменные сообщения Сервера о близком окончании срока действия лицензии:

Key_Expiration:

- MSG.Expiration — дата окончания лицензии,
- MSG.Expired — 1, если срок окончания уже наступил, иначе - 0,
- MSG.ObjId — GUID объекта,
- MSG.ObjName — имя объекта,
- MSG.ObjType — объект, использующий заканчивающийся ключ (server/station/group).

Приложение E. Спецификация сетевого адреса

В данной спецификации приняты следующие обозначения:

- переменные (поля, подлежащие замене на конкретные значения) заключаются в угловые скобки и пишутся курсивом,
- постоянный текст (сохраняющийся после подстановок) пишется моноширинным шрифтом,
- необязательные элементы заключаются в квадратные скобки,
- слева от последовательности символов `::=` располагается определяемое понятие, а справа — определение (как в форме Бэкуса-Наура).

E1. Общий формат адреса

Сетевой адрес имеет следующий вид:
`[`*<protocol>*`/][`*<protocol-specific-part>*`]`

По умолчанию *<protocol>* имеет значение `TCP`. Возможны также `IPX` и `NetBIOS`. Значения по умолчанию *<protocol-specific-part>* определяются приложением.

Адреса семейства IP

- *<interface>*`::=`*<ip-address>*

  <ip-address> может быть именем DNS или IP-адресом, разделенным точками (например, `127.0.0.1`).

- *<socket-address>*`::=`*<interface>*`:`*<port-number>*

  <port-number> должен быть задан десятичным числом.

Адреса семейства IPX

- *<interface>*::=*<ipx-network>*.*<mac-address>*

  <ipx-network> должен содержать 8 шестнадцатеричных цифр, *<mac-address>* должен содержать 12 шестнадцатеричных цифр.

- *<socket-address>*::=*<interface>*:*<socket-number>*

  <socket-number> должен содержать 4 шестнадцатеричные цифры.

Адреса семейства NetBIOS

- Ориентированный на дейтаграмму протокол:

  `nbd/<NAME>[:<PORT>[:<LANA>]]`

- Ориентированный на соединение протокол:

  `nbs/<NAME>[:<PORT>[:<LANA>]]`

  где *<NAME>* — NetBIOS-имя компьютера, *<PORT>* — порт (по умолчанию `23`), *<LANA>* — номер сетевого адаптера (играет роль для NetBEUI).

Примеры:

`1.tcp/127.0.0.1:2193`

означает протокол `TCP`, порт `2193` на интерфейсе `127.0.0.1`.

`2.tcp/[::]:2193`

означает протокол `TCP`, порт `2193` на IPv6-интерфейсе `0:0:0:0:0:0:0:0`

`3.localhost:2193`

то же.

`4.tcp/:9999`

значение для сервера: интерфейс по умолчанию, зависящий от приложения (обычно все доступные интерфейсы), порт `9999`; значение для клиента: связь с хостом по умолчанию, зависящим от приложения (обычно localhost), порт `9999`.

`5.tcp/`

протокол `TCP`, порт по умолчанию.

`6.spx/00000000.000000000001:2193`

означает сокет `SPX loopback 0x2193`.

Адреса семейства UDS

- Ориентированный на соединение протокол:
  `unx/`*<file_name>*
- Ориентированный на дейтаграмму протокол:
  `udx/`*<file_name>*

Примеры:

```
1. unx/tmp/drwcsd:stream
2. unx/tmp/drwcsd:datagram
```

Ориентированный на соединение протокол

<protocol>`/`*<socket-address>*

где *<socket-address>* задает локальный адрес сокета для сервера или удаленный сервер для клиента.

Ориентированный на дейтаграмму протокол

<protocol>`/`*<endpoint-socket-address>*`[-`*<interface>*`]`

Примеры:

1. `udp/231.0.0.1:2193`

   означает использование multicast-группы `231.0.0.1:2193` на зависящем от приложения интерфейсе по умолчанию.

2. `udp/[ff18::231.0.0.1]:2193`

   означает использование multicast-группы `[ff18::231.0.0.1]` на зависящем от приложения интерфейсе по умолчанию.

3. `udp/`

   зависящий от приложения интерфейс и конечная точка.

4. `udp/255.255.255.255:9999-`*<myhost1>*

   использование широковещательных сообщений на порт `9999` на интерфейсе *<myhost1>*.

E2. Адреса Dr.Web Enterprise Server

Прием соединений

<connection-protocol>`/[`*<socket-address>*`]`

По умолчанию, в зависимости от *<connection-protocol>*:

- `tcp/0.0.0.0:2193`

  что означает "все интерфейсы (за исключением тех, которым присвоены IPv6-адреса), порт `2193`";

- `tcp/[::]:2193`

  что означает "все IPv6-интерфейсы, порт `2193`";

- `spx/00000000.000000000001:2193`

  что означает "все интерфейсы, порт `0x2193`";

- `nbs/drwcs:23:0`

  что означает использование протокола NetBIOS stream, порт `23`, компьютер `drwcs`.

Служба обнаружения Dr.Web Enterprise Server

<datagram-protocol> / [*<endpoint-socket-address>* [– *<interface>*]]

По умолчанию, в зависимости от *<datagram-protocol>*:

- `udp/231.0.0.1:2193-0.0.0.0`

  что означает использование multicast-группы `231.0.0.1:2193` на всех интерфейсах;

- `udp/[ff18::231.0.0.1]:2193-[::]:0`

  что означает использование multicast-группы `[ff18::231.0.0.1:2193]` на всех интерфейсах;

- `ipx/00000000.FFFFFFFFFFFF:2193-00000000.000000000000`

  означает прием широковещательных сообщений на сокет `0x2193` на всех интерфейсах;

- `nbd/drwcs:23:0`

  что означает использование протокола NetBIOS datagram, порт `23`, компьютер `drwcs`.

Е3. Адреса Dr.Web Enterprise Agent/ Installer

Прямое соединение с Dr.Web Enterprise Server

[*<connection-protocol>*] / [*<remote-socket-address>*]

По умолчанию, в зависимости от <*connection-protocol*>:

- `tcp/127.0.0.1:2193`

  где `127.0.0.1` - loopback, `2193` - порт;

- `tcp/[::1]:2193`

  где `[::1]` - loopback (IPv6), `2193` - порт;

- `spx/00000000.000000000001:2193`

  где `00000000.000000000001` - loopback, `2193` - порт.

Поиск Сервера <drwcs-name>, использующий указанное семейство протоколов и конечную точку

`[`<*drwcs-name*>`]@`<*datagram-protocol*>`/[`<*endpoint-socket-address*>`[-`<*interface*>`]]`

По умолчанию, в зависимости от <*datagram-protocol*>:

- `drwcs@udp/231.0.0.1:2193-0.0.0.0`

  поиск **Сервера** с именем `drwcs` для TCP-соединения, использующего multicast-группу `231.0.0.1:2193` на всех интерфейсах,

- `drwcs@ipx/00000000.FFFFFFFFFFFF:2193-00000000.000000000000`

  поиск **Сервера** с именем `drwcs` для SPX-соединения, используя широковещательные сообщения на сокет `0x2193` на всех интерфейсах.

Приложение F. Управление репозиторием

Управление функциями репозитория для продуктов осуществляется при помощи следующих расположенных в корне каталога продукта файлов:

- Файл конфигурации `.config`. Задает состав файлов и параметры сервера обновлений. Файл имеет текстовый формат, его структура описывается ниже в Приложениях F1. Синтаксис файла конфигурации .config и F2. Значение инструкций файла .config.
- Файл состояния `.id`. Отображает обобщенное состояние продукта (номер ревизии и шаг выполнения транзакции). Формат описан ниже в Приложении F3. Файлы .id.

При настройке межсерверных связей (см. п. Особенности сети с несколькими Серверами) для зеркалирования продуктов следует иметь в виду, что конфигурационные файлы не являются частью продукта и не обрабатываются системой зеркалирования. Во избежание сбоя в работе системы обновления:

- для равноправных **Серверов** сохраняйте конфигурацию идентичной,
- для подчиненных **Серверов** отключите синхронизацию компонентов по протоколу HTTP или сохраняйте конфигурацию идентичной.

После редактирования файлов конфигурации и состояния требуется перезапуск **Сервера**.

F1. Синтаксис файла конфигурации .config

При описании формата файла конфигурации `.config` используется формальная грамматика, основанная на нотации РБНФ и подразумевающая следующие обозначения:

- `(...)` — группа символов (фрагмент конфигурационного файла);
- `"..."` — терминальный символ;
- `<...>` — нетерминальный символ;
- `|` – символ выбора одного из предложенных элементов;
- `(...)?` – символ (или группа символов в скобках) слева от оператора является необязательной (может встретиться 0 либо 1 раз);
- `(...)*` – символ (или группа символов в скобках) слева от оператора может повторяться произвольное число раз (а также может быть опущен);
- `(...)+` – символ (или группа символов в скобках) слева от оператора может встретиться 1 или более раз;
- `[...]` – любой символ, попадающий в указанный диапазон;
- точка в конце — спецсимвол, указывающий на завершение правила.

Формат файла конфигурации репозитория .config:

```
<строка> := <инструкция>? (<разделитель>+ <комментарий>?)*.

<инструкция> := <название> "{"? <параметр>* "}"?.
<название> := "description" | "sync-with" |
              "sync-delay" |  "sync-only" |
              "sync-ignore" | "state-only" |
              "state-ignore" | "notify-only" |
              "notify-ignore" | "notify-off".
<параметр> := <текст>.
<текст> := <слово> <разделитель>*.
```

```
<слово> := (<символ> | <знак>)+.
<символ> := [a-zA-Z] | [0-9].
<знак> := "" | "/"| "\" | "*" | "^" | "." | "-"| "$".

<разделитель> := \r | \t | \n | \s.

<комментарий> := ";"<текст> | "#"<M1><символ>+<M1> | "'"<M2><текст>+<M2>.
<M1> := <символ>+.
<M2> := <знак>+.
```

Файл конфигурации представляет собой последовательность слов, которые отделяются друг от друга разделителями. *Разделителем* является любая последовательность следующих символов: пробел (`\s`), табуляция (`\t`), возврат каретки (`\r`), перевод строки (`\n`).

Слово, начинающееся с точки с запятой (`;`), обозначает начало комментария, который продолжается до конца строки.

Примеры:

```
ghgh 123 ;это комментарий
123;это; не; комментарий - необходим
      разделитель в начале.
```

Слово, начинающееся со знака числа (`#`), обозначает начало потокового комментария; остаток слова задает маркер конца комментария.

Пример:

```
123 456 #COMM С этого места комментарийCOMM он уже закончился
```

Для включения в слово любых символов используется префикс ' (апостроф) — специальный символ-разделитель для данного слова (т.е., именно этот символ будет считаться разделителем, завершающим данное слово).

Пример:

```
xy123 '*Такое вот слово*УжеДругое
```

Если слово начинается с одного из символов: апостроф, точка с запятой, знак числа (', ;, #), - оно обязательно должно ограничиваться специальными символами-разделителями, как указано выше.

Файл `.config` состоит из комментариев и инструкций. Порядок следования инструкций несущественен.

Формат инструкций конфигурационных файлов предполагает различение верхнего и нижнего регистра букв.

Репозиторий различает регистр букв, независимо от файловой системы и ОС, под управлением которых работает **Сервер**.

Смысл инструкций пояснен в Приложении F2. Значение инструкций файла .config.

F2. Значение инструкций файла .config

Инструкция description

Инструкция `description` задает имя продукта, отображаемое в **Центре Управления**. Если эта инструкция отсутствует, в качестве имени продукта используется имя соответствующего каталога продукта.

Пример:

```
description '"Dr.Web® Enterprise Agent"
```

Инструкция sync-with

Инструкция `sync-with` задает перечень HTTP-серверов и HTTP-прокси-серверов для обновления. Параметр `name` задает доменное имя или IP-адрес. Конструкция `:port` может отсутствовать, в этом случае по умолчанию номером порта считается `80` для HTTP-сервера и `3128` для прокси-сервера.

Серверы в списке запрашиваются последовательно, при успехе обновления процедура опроса завершается.

В текущей версии **Dr.Web Enterprise Security Suite** поддерживаются только базовая HTTP-авторизация, Proxy-HTTP-авторизация и RADIUS-авторизация.

Постоянные HTTP-редиректы (под код 301) кэшируются в памяти до перезагрузки сервера.

Пример:

```
sync-with{
 http{ esuite.msk3.drweb.com /update }
 http{ esuite.msk4.drweb.com /update }
 http{ esuite.msk.drweb.com  /update }
 http{ esuite.us.drweb.com   /update }
 http{ esuite.jp.drweb.com   /update }
}
```

Пример при использовании прокси-сервера

```
sync-with{
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk7.drweb.com /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.jp.drweb.com   /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk5.drweb.com /update  } }
```

```
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.msk6.drweb.com /update   } }
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.msk.drweb.com  /update   } }
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.us1.drweb.com  /update   } }
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.msk3.drweb.com /update   } }
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.msk4.drweb.com /update   } }
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.us.drweb.com   /update   } }
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.fr1.drweb.com  /update   } }
}
```

Где:

- `10.3.0.74` - IP-адрес прокси-сервера;
- `user` - имя пользователя прокси-сервера (может отсутствовать, если прокси не требует аутентификации);
- `pass` - пароль для доступа к прокси-серверу (может отсутствовать, если прокси не требует аутентификации).

Инструкция sync-only

Инструкция `sync-only` явно задает множество имен файлов (заданных как регулярными выражениями в простой форме, как показано в данном разделе, так и в полной форме `qr{}`, как показано в п. Запуск и остановка антивирусного сканера на рабочей станции), подлежащих синхронизации. Если инструкция отсутствует, по умолчанию синхронизации подлежит все содержимое каталога (за исключением файлов, имена которых начинаются с точки).

Пример:

```
sync-only{^common/drw.*vdb$}
```

предписывает обновлять только вирусные базы.

Инструкция sync-ignore

Инструкция `sync-ignore`, напротив, явно задает множество файлов, не подлежащих синхронизации.

Если в продукт локально добавлены файлы (не содержащиеся в оригинале) и инструкция sync-only не используется, добавляемые файлы должны быть перечислены в `sync-ignore`, иначе они будут удалены при синхронизации.

Инструкция sync-delay

Инструкция `sync-delay` задает список файлов, при изменении которых переключение продукта на новую ревизию запрещается. Репозиторий продолжает распространение старой ревизии, синхронизация более не осуществляется (состояние продукта "замораживается"). Если пользователь сочтет принятую ревизию пригодной для распространения, он должен отредактировать файл состояния `.id` и перезапустить **Сервер** (см. Приложение F3. Файлы .id).

Примеры:

- Автоматическое распространение новых ревизий запрещается:

```
sync-delay{ .* }
; никакой автоматики, все тестировать лично
```

- Запрещается автоматическое распространение ревизий, в которых обновлены исполняемые файлы:

```
sync-delay{ .*\.exe$ .*\.dll$ }
```

Инструкции state-only и state-ignore

Инструкции `state-only` и `state-ignore` аналогичным образом задают (ограничивают) список файлов, подлежащих распространению.

Пример:

Для продукта **Enterprise Агент**:

- не требуется получать немецкий, польский и испанский языки интерфейса (остальные - получать),
- не требуется получение компонентов, предназначенных для ОС Windows 98/ОС Windows Me.

```
sync-ignore{
    ; заметим, что если перечисленные файлы уже
    ; присутствуют в репозитории, они по-прежнему
    ; подлежат распространению.
    ; поэтому их надо удалить оттуда или
    ; перечислить в state-ignore{ }, или произвести
    ; полную синхронизацию в данной
    ; конфигурации
;^common/ru-.*\.dwl$ это нам нужно
^common/de-.*\.dwl$
^common/pl-.*\.dwl$
^common/es-.*\.dwl$
^win/de-.*
^win/pl-.*
^win-9x\.*
}
```

Инструкции группы notify

Инструкции группы `notify` позволяют настроить систему оповещения для отдельных продуктов (настройка системы оповещения в целом описана в п. Настройка оповещений).

Репозиторий может генерировать следующие типы оповещений:

- `update` — при успешном обновлении продукта,
- `delay` — при замораживании транзакции,
- `flushfail` — при ошибке записи на диск,
- `loadfail` — при ошибке загрузки.

По умолчанию все типы оповещений разрешены.

Инструкция `notify-off` позволяет запретить конкретные типы оповещений для данного продукта.

Инструкции `notify-ignore` и `notify-only` позволяют ограничить или явно задать список файлов, при изменении которых посылается оповещение типа `update`.

Если в файле одновременно встретятся хотя бы две из числа инструкций `sync-only`, `sync-ignore` или `sync-delay`, используется следующее правило:

- сначала применяется `sync-only`. Файлы, не перечисленные в списке этой инструкции (если она присутствует), не обрабатываются,
- к оставшимся файлам применяется `sync-ignore`,
- только к файлам, оставшимся после двух предыдущих пунктов, применяется `sync-delay`.

Аналогично решается вопрос об очередности применения `state-only` и `state-ignore`.

F3. Файлы .id

Файл состояния продукта — это текстовый файл, в котором **Сервер** хранит номера ревизий продукта. В обычном состоянии файл содержит единственное число (текущий номер ревизии). Синхронизация продукта производится, только если номер ревизии на сервере **ВСО** больше текущего, и происходит в четыре фазы:

1. В файл `.id` записываются 2 числа:

   <новая_ревизия> *<старая_ревизия>*.

   Таким образом помечается, что продукт находится в незавершенной транзакции из

   <старая_ревизия> в *<новая_ревизия>*.

2. По HTTP получаются все изменившиеся файлы и помещаются в соответствующие подкаталоги с именами вида

   <оригинальное имя файла>.*<новая_ревизия>*.

3. В файл `.id` записывается результат транзакции.

   Это может быть обычное состояние, но уже с новым номером, или состояние "заморожен" (`frozen`) в результате срабатывания правила `sync-delay`:

   <новая_ревизия> *<старая_ревизия>* `frozen`.

4. Если состояние не "заморожен", новые файлы замещают оригинальные.

При перезапуске **Сервера** после анализа файла `.id` незавершенная транзакция "откатывается"; в противном случае, выполняется п. **4**.

F4. Примеры управления репозиторием с модификацией файла состояния

Полная синхронизация продукта:

1. Остановите **Сервер**.
2. Удалите все содержимое каталога продукта, кроме `.id` и `.config`.
3. Запишите `0` в файл `.id`.
4. Запустите **Сервер**.
5. Произведите обновление продукта.

Ревизия `0` имеет специальное значение, поскольку при ней запрещается распространение, поэтому "пустое" состояние продукта не тиражируется на **Агенты**.

Запрет распространения:

1. Остановите **Сервер**.
2. Запишите `0` в файл `.id`.
3. Закомментируйте инструкцию `sync-with` в файле `.config`, чтобы запретить синхронизацию.
4. Запустите **Сервер**.
5. Произведите обновление продукта.

Переход из состояния "заморожен" на новую версию:

1. Замените содержимое `.id` с

   <новая_ревизия> *<старая_ревизия>* `frozen`

   на

   <новая_ревизия>.
2. Перезапустите **Сервер**.
3. Произведите обновление продукта.

Откат из состояния "заморожен" на старую версию:

1. Замените содержимое `.id` с

   <новая_ревизия> *<старая_ревизия>* `frozen`

   на

   <новая_ревизия> *<старая_ревизия>*.

2. Перезапустите **Сервер**.
3. Произведите обновление продукта.

При дальнейших попытках синхронизации на *<новую ревизию>*, репозиторий опять перейдет в состояние "заморожен". Сохранение *<старой ревизии>* репозитория с отказом от обновлений может быть оправдано при наличии подходящей ревизии, например, успешно прошедшей испытательный стенд.

Приложение G. Конфигурационные файлы

В данном разделе описывается формат следующих файлов:

- конфигурационный файл **Enterprise Сервера** `drwcsd.conf`;
- конфигурационный файл **Прокси-сервера** `drwcsd-proxy.xml`;
- конфигурационный файл **Центра управления** `webmin.conf`;
- конфигурационный файл `download.conf`.

Если на компьютере с соответствующим компонентом установлен **Агент** со включенной самозащитой, то перед изменением файлов конфигурации необходимо отключить компонент самозащиты **Dr.Web SelfPROtect** через настройки **Агента**.

После сохранения всех внесенных изменений рекомендуется включить компонент **Dr.Web SelfPROtect**.

G1. Конфигурационный файл Dr.Web Enterprise Server

Конфигурационный файл **Enterprise Сервера** `drwcsd.conf` по умолчанию располагается в подкаталоге `etc` корневого каталога **Сервера**. При запуске **Сервера** при помощи параметра командной строки может задаваться нестандартное расположение и наименование конфигурационного файла (подробнее см. Приложение H5. Dr.Web Enterprise Server).

При необходимости ручного редактирования конфигурационного файла Dr.Web Enterprise Server, выполните следующие действия:

1. Остановите **Сервер** (см. п. Запуск и останов Dr.Web Enterprise Server).
2. Отключите самозащиту (в случае наличия на компьютере **Агента** с активной самозащитой - в контекстном меню **Агента**).
3. Внесите необходимые изменения в конфигурационный файл **Сервера**.
4. Запустите **Сервер** (см. п. Запуск и останов Dr.Web Enterprise Server).

Формат конфигурационного файла Dr.Web Enterprise Server

При описании формата файла конфигурации **Сервера** используется формальная грамматика, основанная на нотации РБНФ, подразумевающая следующие обозначения:

- `(...)` — группа символов (фрагмент конфигурационного файла);
- `'...'` — терминальный символ;
- `<...>` — нетерминальный символ;
- `|` – символ выбора одного из предложенных элементов;
- `(...)?` – символ (или группа символов в скобках) слева от оператора является необязательной (может встретиться 0 либо 1 раз);
- `(...)*` – символ (или группа символов в скобках) слева от оператора может повторяться произвольное число раз (а также может быть опущен);
- `(...)+` – символ (или группа символов в скобках) слева от оператора может встретиться 1 или более раз;
- `[...]` – любой символ, попадающий в указанный диапазон;

- точка в конце — спецсимвол, указывающий на завершение правила.

Формат конфигурационного файла Сервера:

```
<инструкция> := (<параметр> '"'<значение>'"')?
(';'<комментарий>)?.
<параметр> := <слово>.
<значение> := (<слово> <разделитель>*)*.
<слово> := ([a-zA-Z] | [0-9] | <спецсимвол>)+.
<спецсимвол> := '&&' | '&r' | '&t' | '&n' | '&v' | '&f' |
'&b' | '&e' | '&l' | '&s'.
<разделитель> := \s | \t | \r | \n | \f.
```

Конфигурационный файл имеет текстовый формат. Основными структурным элементом файла являются слова, разделенные разделителями — пробелами (`\s`), символами табуляции (`\t`), перевода каретки (`\r`), конца строки (`\n`), перевода формата (`\f`). Кроме того, словом считается последовательность символов, заключенная в прямые кавычки `"..."`.

В состав слова могут входить, не разрывая его, специальные последовательности из двух символов, начинающиеся с амперсанда (&). Они интерпретируются следующим образом:

- `&&` — как сам символ `&`,
- `&r` — символ перевода каретки,
- `&t` — табуляция,
- `&n` — символ перевода строки,
- `&v` — вертикальная табуляция,
- `&f` — перевод формата,
- `&b` — возврат на шаг,
- `&e` — знак равенства `(=)`,
- `&l` — вертикальная черта `(|)`,
- `&s` — пробел.

Амперсанд `(&)`, стоящий последним в строке, — то же, что и `&n`.

Таким образом, обычный амперсанд (неиспользуемый для целей задания специальной последовательности) должен удваиваться.

Комментарии начинаются с точки с запятой и продолжаются до конца строки.

Настройки **Сервера** задаются в конфигурационном файле в виде инструкций, каждая из которых представляет собой параметр, состоящий из одного слова, за которым могут следовать его значения (одно или несколько слов).

Ниже описываются возможные инструкции. Порядок следования инструкций в файле несущественен. В угловых скобках — значения параметров, задаваемые пользователем.

- `Name` *<имя>*

  Определяет название (имя) **Сервера**, на которое он будет откликаться при поиске **Сервера Агентом** или **Центром Управления**. Значение по умолчанию — пустая строка ("") означает использование названия компьютера.

- `Threads` *<число>*

  Число нитей **Сервера**, обслуживающих клиентов. По умолчанию — 5. Не следует изменять значение параметра без рекомендации службы поддержки.

- `DBPool` *<число>*

  Число соединений базы данных с **Сервером**. Для **Серверов** ОС Windows и **Серверов** ОС UNIX - по умолчанию 2. Не следует изменять значение параметра без рекомендации службы поддержки.

- `MaximumAuthorizationQueue` *<число>*

  Задает максимальное количество станций в очереди для авторизации на **Сервере**. Не следует изменять значение параметра без рекомендации службы поддержки.

- `Newbie` *<режим>*

Режим доступа новых станций, может принимать значения `Open`, `Close` или `Approval` (по умолчанию `Approval`). Подробнее см. п. Политика подключения новых станций.

- `UnAuthorizedToNewbie` *<режим>*

  Режим может принимать значения либо `Yes` — это означает, что станции, не прошедшие авторизацию (например, в случае разрушения базы данных), будут автоматически переводиться в состояние новичков, либо `No` (по умолчанию), что означает нормальный режим работы.

- `WEBStatistics "Interval=`*<число>*
  `Server=`*<адрес_сервера>*
  `URL=`*<каталог>*
  `ID=`*<идент_клиента>*
  `User=`*<пользователь>*
  `Password=`*<пароль>*
  `Proxy=`*<прокси-сервер>*
  `ProxyUser=`*<польз_прокси>*
  `ProxyPassword=`*<пароль_прокси>*`"`

  Описывается веб-сервер, на котором **Enterprise Сервер** будет публиковать свою статистику по найденным вирусам.

  Интервал публикации задается в минутах, по умолчанию 30.

  Адрес сервера по умолчанию `stat.drweb.com:80`

  `URL` по умолчанию `/update`.

  `ID` — идентификатор клиента (по умолчанию вычисляется из пользовательского серверного ключа `enterprise.key`).

  Поля `User` и `Password` описывают авторизацию на веб-сервере, остальные — прокси-сервер и авторизация на нем. По умолчанию поля пусты (авторизация не требуется).

  Чтобы получить доступ к информации, хранящейся на

сервере статистики, обращайтесь в службу поддержки.

- `Encryption` *<режим>*

  Режим шифрования трафика. Разрешенные значения: `Yes`, `No`, `Possible` (по умолчанию `Yes`). Подробнее см. п. Использование шифрования и сжатия трафика.

- `Compression` *<режим>*

  Режим сжатия трафика. Разрешенные значения: `Yes`, `No`, `Possible` (по умолчанию `No`). Подробнее см. п. Использование шифрования и сжатия трафика.

- `InstallAccess`, `AgentAccess` и `LinksAccess` не отображаются в файле конфигурации, если флаг **Использовать этот список доступа** не установлен (см. п. Настройка конфигурации Dr.Web Enterprise Server). Если флаг установлен, отображаемые значения отключенных параметров "`none`". Для подключенных параметров будут отображены заданные адреса.

- `Database` *<DRIVER>* `from` *<PATH>* `using` *<PARAMETERS>*

  Определение базы данных. *<DRIVER>* — наименование драйвера базы, *<PATH>* — путь, откуда грузить драйвер, *<PARAMETERS>* — параметры установления связи с сервером БД. Подробнее см. п. Настройка режима работы с БД.

Данная инструкция может использоваться в конфигурационном файле только однократно.

- `Alert` *<DRIVER>* `from` *<PATH>* `using` *<PARAMETERS>*

  Определение "оповещателя". *<DRIVER>* — наименование драйвера оповещателя, *<PATH>* — путь, откуда грузить драйвер, *<PARAMETERS>* — параметры оповещателя. Подробнее см. п. Настройка оповещений.

Данная инструкция может использоваться в конфигурационном файле только однократно.

В данной и следующей инструкции параметры в поле `using` разделяются пробелами. Название параметра отделяется от значения знаком равенства `(=)`, который не должен быть окружен пробелами. Если параметр может иметь более одного значения, они отделяются друг от друга вертикальной чертой `(|)`. Если в значении параметра встречаются знак равенства, вертикальная черта или пробел, они заменяются на последовательности `&&e`, `&&l`, `&&s` соответственно.

- `transport` *<NAME> <STREAM> <DATAGRAM>*

  Определение транспортных протоколов и привязка их к сетевым интерфейсам. *<NAME>* — имя **Сервера**, заданное как в инструкции `name` (см. выше), если задана пустая строка, берется из `name`. *<STREAM>* (например, `tcp/`), *<DATAGRAM>* (например, `udp/`) имеют формат, описанный в Приложении Е. Спецификация сетевого адреса

- `Disable Message` *<сообщение>*

  Запретить отправлять сообщения определенного типа, допустимые значения параметра — тип сообщения, полный перечень всех типов сообщений можно найти в каталоге `templates`.

- `Disable Protocol` *<протокол>*

  Запретить использование одного из серверных протоколов, допустимые значения: `AGENT`, `SERVER`, `INSTALL`, `CONSOLE`. В конфигурационном файле по умолчанию имеется инструкция, запрещающая протокол `SERVER`. Подробнее см. п. Настройка конфигурации Dr.Web Enterprise Server.

Запрещение ненужных протоколов экономит ресурсы системы.

- `Disable Plugin` *<модуль>*

  Запретить использование дополнительных модулей **Сервера**, допустимое значение: `WEBMIN`. Подробнее см. п. Настройка конфигурации Dr.Web Enterprise Server.

- `ShowHostNames` *<значение>*

  Разрешить показывать в протоколе доменные имена компьютеров вместо TCP-адреса. Возможные значения: `Yes` или `No`.

- `ReplaceNetBIOSNames` *<значение>*

  Разрешить заменять NetBIOS-имена компьютеров DNS-именем. Возможные значения: `Yes` или `No`.

- Параметры `Organization`, `Department`, `Country`, `Province`, `City`, `Street`, `Floor`, `Room`, `Latitude` и `Longitude` задают дополнительную информацию о географическом и корпоративном расположении станции.

- `TrackAgentJobs` *<значение>*

  Разрешить записывать в БД результат выполнения заданий на станциях. Возможные значения: `Yes` или `No`.

- `TrackAgentStatus` *<значение>*

  Разрешить вести учет изменений состояния станции и запись информации в БД. Возможные значения: `Yes` или `No`.

- `TrackVirusBases` *<значение>*

  Разрешить вести учет состояния (состава, изменения) вирусных баз на станции и запись информации в БД. Возможные значения: `Yes` или `No`.

- `TrackAgentModules` *<значение>*

  Разрешить записывать в БД информацию обо всех программных модулях антивируса **Dr.Web**, установленных на станциях. Возможные значения: `Yes` или `No`.

- `TrackAgentComponents` *<значение>*

Разрешить записывать в БД информацию обо всех антивирусных компонентах, установленных на станциях. Возможные значения: `Yes` или `No`.

- `KeepRunInformation` *<значение>*

  Разрешить записывать в БД информацию о запуске и завершении работы компонентов **Антивируса** (**Сканер**, **Мониторы** и т.п.) на рабочих станциях. Возможные значения: `Yes` или `No`.

- `KeepInfections` *<значение>*

  Разрешить запись в БД статистических данных об инфекциях, обнаруженных на рабочих станциях. Возможные значения: `Yes` или `No`.

- `KeepScanErrors` *<значение>*

  Разрешить запись информации в БД обо всех ошибках при сканировании на рабочих станциях. Возможные значения: `Yes` или `No`.

- `KeepScanStatistics` *<значение>*

  Разрешить запись в БД результатов сканирования на рабочих станциях. Возможные значения: `Yes` или `No`.

- `KeepInstallation` *<значение>*

  Разрешить записывать в БД информацию об инсталляциях **Агентов** на рабочих станциях. Возможные значения: `Yes` или `No`.

- `Quarantine` *<значение>*

  Разрешить запись состояния **Карантина** на станциях. Возможные значения: `Yes` или `No`.

- `UpdatesBandwidth` *<значение>*

  Максимальная ширина полосы пропускания сетевого трафика в КБ при передаче обновлений между **Сервером** и **Агентами**. Значение `0` - полоса пропускания неограничена.

- `Audit` *<значение>*

Разрешить ведение журнала аудита операций администратора с **Центром Управления** и запись журнала в БД. Возможные значения: `Yes` или `No`.

- `AuditInternals` *<значение>*

  Разрешить ведение журнала аудита внутренних операций **Сервера** и запись журнала в БД. Возможные значения: `Yes` или `No`.

G2. Конфигурационный файл Центра Управления Dr.Web

Конфигурационный файл **Центра Управления** `webmin.conf` располагается в подкаталоге `etc` корневого каталога **Сервера**.

При описании формата файла конфигурации **Центра Управления** используется формальная грамматика, основанная на нотации РБНФ, подразумевающая следующие обозначения:

- `(...)` — группа символов (фрагмент конфигурационного файла);
- `'...'` — терминальный символ;
- `<...>` — нетерминальный символ;
- `|` – символ выбора одного из предложенных элементов;
- `(...)?` – символ (или группа символов в скобках) слева от оператора является необязательной (может встретиться 0 либо 1 раз);
- `(...)*` – символ (или группа символов в скобках) слева от оператора может повторяться произвольное число раз (а также может быть опущен);
- `(...)+` – символ (или группа символов в скобках) слева от оператора может встретиться 1 или более раз;
- `[...]` – любой символ, попадающий в указанный диапазон;
- точка в конце — спецсимвол, указывающий на завершение правила.

Формат конфигурационного файла Центра Управления Dr.Web:

```
<инструкция> := <параметр>* (';'<комментарий>)?.

<параметр> := <единичный> | <блок>.
<единичный> := <название> <значение>.
<группа> := <название> '{' (<значение>' ')+ '}'.
<блок> := <префикс>? <название> '{' <единичный>* | <группа>*
| <доступ>? | <авторизация>? '}'.

<префикс> := 'Static' | 'Handler' | 'Scripts' | 'Mixed'.
<доступ> := 'Access {'
            'Secure {'
               'Priority ' <приоритет>?
               ('Allow {' <значение>* '}')?
               ('Deny {' <значение>* '}')?
            '}'
            'InSecure {'
               'Priority ' <приоритет>?
               ('Allow {' <значение>* '}')?
               ('Deny {' <значение>* '}')?
            '}'
          '}'.
<приоритет> := 'deny' | 'allow'.

<авторизация>:= 'Authorization {' <единичный>+ | <группа>+ '}'.

<название> := <слово>.
<значение> := <слово> <разделитель>*.
<слово> := ( [a-zA-Z] | [0-9] | <знак> )+.
<разделитель> := \s | \t | \r | \n | \f.
<знак> := '/' | '*' | ':' | '.' | '-' | '?' | '^'| '[' |
']'.
```

Конфигурационный файл имеет текстовый формат. Основными структурным элементом файла являются слова, между которыми могут быть разделители — пробелы (`\s`), символы табуляции (`\t`), перевода каретки (`\r`), конца строки (`\n`), перевода формата (`\f`).

Комментарии начинаются с точки с запятой и продолжаются до конца строки.

Настройки **Центра Управления** задаются в конфигурационном файле в виде инструкций, каждая из которых представляет собой:

- параметр, состоящий из одного слова (названия параметра), за которым следует его значение (одно или несколько слов),
- блок параметров, состоящий из одного слова (названия блока), за которым в фигурных скобках могут быть определены:
  - простые параметры, представляющих собой одно слово (название параметра), за которым следует значение (одно или несколько слов),
  - группы параметров, представляющих собой одно слово (название параметра), за которым в фигурных скобках следует набор значений (по одному или по несколько слов),
  - группа параметров `Access`, определяющая правила доступа к заданным ресурсам сервера (см. ниже),
  - группа параметров `Authorization`, определяющая параметры авторизации для доступа к заданным ресурсам (см. ниже).

Перед названием блока параметров может задаваться префикс - одно слово, определяющее принцип обработки параметров блока.

Ниже описываются некоторые из возможных инструкций. Порядок следования инструкций в файле несущественен.

Большинство простых (единичных) параметров заданы со значениями по умолчанию и не требуют изменений. Но в процессе работы **Сервера** может потребоваться задание значений для

некоторых из них:

- `ServerName` *<DNS_имя>*:*<номер_порта>* – определяет имя **Сервера** и порт. Используется для подстановки в запросы при обращении к **Серверу**. Необходимо установить соответствующие значения сразу после установки **Сервера** (см. п. Установка Dr.Web Enterprise Server).
- `Listen` *<протокол>* *<интерфейс>*:*<номер_порта>* – задает параметры прослушиваемых интерфейсов. Используется для настройки доступа к **Центру Управления**.

Блоки параметров содержат следующие группы и параметры:

- Префикс (`Static`, `Script`, `Handler` или `Mixed`) задается перед названием блока параметров и определяет принцип обработки соответствующих пользовательских запросов.
  - Префикс `Static` определяет статический метод обработки, подразумевающий передачу пользователю готового значения - запрошенного файла без изменений (например, изображения, хранящегося на **Сервере**).
  - Префикс `Handler` определяет метод обработки, подразумевающий выполнение скрипта, заданного в параметрах блока, при получении пользовательского запроса (корректность путей, указанных в запросе, не важна). При этом в последующем теле блока инструкций необходимо наличие инструкции `Script` *<имя_скрипта>*, определяющего исполняемый скрипт.
  - Префикс `Scripts` определяет метод обработки запросов, подразумевающий исполнение всех файлов из пользовательского запроса как скриптов.
  - Префикс `Mixed` задает смешанный метод обработки, подразумевающий объединение двух методов - `Static` и `Scripts`. При этом в последующем теле блока инструкций необходимо наличие группы параметров `Scripts { `*<расширения_скриптов>*` }`, определяющей

исполняемые скрипты (по расширению). Все остальные файлы, не соответствующие значениям данной группы параметров, будут переданы статически (как есть, без обработки).

- Группа параметров `Access` содержит определение прав доступа к ресурсам **Сервера** при обработке полученных пользовательских запросов.
  - Группа `Secure` задает права доступа для защищенных соединений по протоколу HTTPS.
  - Группа `InSecure` задает права доступа для незащищенных соединений по протоколу HTTP.
    - Параметр `Priority` *<приоритет>* определяет приоритет обработки списков для разрешенных и запрещенных соединений. При задании значения `deny`, все адреса, не входящие в обе группы (`Allow` и `Deny`), будут запрещаться, при задании значения `allow` - разрешаться.
    - Список параметров группы `Allow` задает адреса узлов, доступ с которых к **Серверу** будет разрешен.
    - Список параметров группы `Deny` задает адреса узлов, доступ с которых к **Серверу** будет запрещен.

  Адреса в списках запрещенных/разрешенных узлов задаются в формате:

  для TCP/IP: `tcp/`*<IP-адрес>*`[/`*<префикс>*`]`;

  для SPX: `spx/`*<номер_сети>*`[.`*<адрес_станции>*`]`.
- Группа параметров `Authorization` определяет необходимые параметры авторизации пользователя при обращении к **Серверу** для обработки соответствующего запроса.

G3. Конфигурационный файл download.conf

Назначение файла download.conf:

1. При создании и использовании кластерной системы **Enterprise Серверов** позволяет распределить нагрузку между **Серверами** кластеров при подключении большого количества новых станций.
2. В случае использования на **Enterprise Сервере** нестандартного порта, позволяет задать этот порт при формировании файла инсталляции **Агента**.

Файл `download.conf` используется при формировании файла инсталляции **Агента** для новой станции антивирусной сети. Параметры данного файла позволяют задать адрес **Enterprise Сервера** и порт, используемые для подключения инсталлятора **Агента** к **Серверу** в формате:

```
download = { server = '<Server_Address>'; port = <port_number> }
```

где:

- *<Server_Address>* - IP-адрес или DNS-имя **Сервера**.

  При формировании инсталляционного пакета **Агента** адрес **Сервера** изначально берется из файла `download.conf`. Если в файле `download.conf` адрес **Сервера** не задан, то используется значение параметра `ServerName` из файла `webmin.conf`. Иначе - имя компьютера, возвращаемое операционной системой.

- *<port_number>* - порт для подключения инсталлятора **Агента** к **Серверу**.

  Если в параметрах файла `download.conf` порт не указан, по умолчанию используется порт 2193 (настраивается в **Центре управления** в разделе **Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт**).

По умолчанию параметр `download` в файле `download.conf` закомментирован. Для использования файла `download.conf` необходимо раскомментировать данный параметр, убрав "--" в начале строки, и задать соответствующие значения адреса и порта **Сервера**.

G4. Конфигурационный файл Прокси-сервера

Конфигурационный файл **Прокси-сервера** `drwcsd-proxy.xml` представлен в формате XML и располагается:

- Для ОС Windows: в каталоге установки **Прокси-сервера**.
- Для ОС семейства UNIX: в подкаталоге `etc` каталога установки **Прокси-сервера** или в текущем рабочем каталоге пользователя.

Элемент <cache-root />

Корневой элемент `<drwcsd-proxy />` может содержать необязательный элемент `<cache-root />`, в котором указывается путь к каталогу кэша **Прокси-сервера**. Если элемент `<cache-root />` не задан, то кэшируемые данные будут сохраняться во временном каталоге пользователя ОС.

Элемент <listen />

Корневой элемент `<drwcsd-proxy />` содержит один или несколько обязательных элементов `<listen />`, определяющих основные настройки для приема соединений **Прокси-сервером**. Элемент `<listen />` содержит единственный обязательный атрибут `spec`, свойства которого определяют на каком интерфейсе "слушать" входящие подключения клиентов и запускать ли на этом интерфейсе режим `discovery`. Атрибут `spec` содержит следующие свойства:

- протокол – тип протокола для приема входящих соединений. В качестве параметра указывается адрес, прослушиваемый **Прокси-сервером**.
- порт – номер порта, прослушиваемого **Прокси-сервером**.
- режим имитации – режим имитации **Сервера**. Позволяет **Сканеру сети** обнаруживать **Прокси-сервер** в качестве **Enterprise Сервера**.
- мультикаст-группа – многоадресная группа, в которой располагается **Прокси-сервер**.

Значения свойств атрибута spec и их параметры приведены в таблице G-1.

Таблица G-1. Свойства элемента spec

Свойство	Обязательное	Допустимые значения	Параметры допустимых значений	
			разрешены	по умолчанию
протокол	да	ip, ipx, netbios		0.0.0.0 - -
порт	нет	port		2193
режим имитации	нет	discovery	yes, no	no
мультикаст-группа	нет	multicast		231.0.0.1

Атрибут spec содержит одно обязательное свойство – протокол и три необязательных свойства: порт, режим имитации и мультикаст-группа. В зависимости от значения, принимаемого свойством протокол, список необязательных свойств, указываемых в атрибуте spec, изменяет свой состав.

В таблице G-2 приведен список необязательных свойств, которые могут быть заданы (+) или не могут быть заданы (–) в атрибуте spec в зависимости от значения параметра протокол.

Таблица G-2. Наличие необязательных свойств в зависимости от значения параметра протокол

Протокол	Наличие свойств		
	port	discovery	multicast
ip	+	+	+
ipx	+	+	–
netbios	+	+	–

Элемент <forward />

Настройки, определяющие переадресацию входящих соединений, задает элемент <forward />, являющийся дочерним для элемента <listen />. Элемент <forward /> содержит один или несколько обязательных атрибутов to, в качестве значения которых задаются адреса **Enterprise Серверов**, на один из которых будет перенаправлено соединение. Адрес **Enterprise Сервера** задается в соответствии со спецификацией сетевого адреса, в частности, в формате tcp/*<DNS_name>*:*<port>*.

Элемент <forward /> является обязательным. При этом элемент <listen /> может содержать несколько элементов <forward />.

Алгоритм переадресации при наличии списка Enterprise Серверов:

1. **Прокси-сервер** загружает в оперативную память список **Enterprise Серверов** из конфигурационного файла drwcsd-proxy.xml.
2. К **Прокси-серверу** подключается **Enterprise Агент**.
3. **Прокси-сервер** переадресует **Enterprise Агента** на первый **Enterprise Сервер** из списка в оперативной памяти.
4. **Прокси-сервер** ротирует список, загруженный в оперативную память, и перемещает **Enterprise Сервер** из первого элемента списка в конец списка.

Прокси-сервер не сохраняет измененный порядок **Серверов** в свой файл конфигурации. При перезапуске **Прокси-сервера** список **Enterprise Серверов** загружается в оперативную память в первоначальном виде, в котором он хранится в файле конфигурации.

5. При подключении следующего **Агента** к **Прокси-серверу** процедура повторяется, начиная с шага 2.
6. Если **Enterprise Сервер** отключается от антивирусной сети (например, при выключении или отказе в обслуживании), **Агент** повторно подключается к **Прокси-серверу** и процедура повторяется начиная с шага 2.

Пример конфигурационного файла drwcsd-proxy.xml

```
<?xml version="1.0"?>
<drwcsd-proxy>
  <!-- Specify path to cahe directory, if not specified
will create directory in user temp -->
  <cache-root>C:\Work\es_head\build\a-x86\bin\var</cache-
root>

  <!-- property: ip, ipx, netbios, unx: define protocol
family and address of addapter -->
  <!-- property: port: define port to listen on. Default
2193 or 23 for netbios -->
  <!-- property: name: define discovery name. Default
drwcs -->
  <!-- property: discovery: define should proxy run
discovery server too -->
  <!-- property: multicast: define should proxy enter to
multicast group -->

  <!-- For example -->
  <!-- Listen on IN_ADDR_ANY port 2193, run discovery on
231.0.0.1 -->
  <listen spec="ip(), multicast()">
    <!-- one or more forward tags-->
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>
```

```
  <!-- Listen on ipv6 IN6_ADDR_ANY, port 2194, run
discovery on ff18::231.0.0.1 -->
  <listen spec="ip([]), port(2194), multicast()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on default ipx, port 2194, run simple
discovery -->
  <listen spec="ipx(), discovery()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on default netbios, port 23, lana 0, run
simple discovery -->
  <listen spec="netbios(), discovery()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>
</drwcsd-proxy>
```

Приложение H. Параметры командной строки программ, входящих в состав Dr.Web Enterprise Security Suite

H1. Введение

Параметры командной строки имеют более высокий приоритет, чем настройки по умолчанию или иные постоянные настройки (заданные в конфигурационном файле **Сервера**, реестре ОС Windows и т. п.). В ряде случаев заданные при запуске параметры также переопределяют постоянные настройки. Такие случаи описаны ниже.

Часть параметров командной строки имеют ключевую форму — начинаются с дефиса. Такие параметры также называются ключами.

Многие ключи могут быть представлены в различных эквивалентных формах. Так, ключи, которые подразумевают логическое значение (да/нет, запретить/разрешить), имеют отрицательный вариант, например, ключ `-admin-rights` имеет парный `-no-admin-rights` с противоположным значением. Они же могут даваться с явным указанием значения, например, `-admin-rights=yes` и `-admin-rights=no`.

Синонимами значения `yes` являются значения `on`, `true`, `OK`. Синонимами `no` являются `off`, `false`.

Если значение ключа содержит пробелы или табуляцию, весь параметр нужно заключить в кавычки, например:

```
"-home=c:\Program Files\DrWeb Enterprise Suite"
```

При описании синтаксиса параметров отдельных программ необязательная часть заключается в квадратные скобки `[...]`.

Названия ключей могут быть сокращены (отбрасыванием последних букв), если при этом сокращенное название не совпадает с начальной частью какого-либо другого ключа.

H2. Интерфейсный модуль Dr.Web Enterprise Agent

Интерфейсный модуль **Агента** запускается для каждого пользователя, интерактивно зарегистрированного на компьютере. На компьютерах под управлением ОС Windows NT и старше работает с правами данного пользователя. Для функционирования **Агента** требуется, чтобы оболочкой пользователя был стандартный **Обозреватель Windows** или другая полностью с ним совместимая программа.

Формат команды запуска:

`drwagnui [<ключи>]`

Допустимые ключи:

- `-admin-rights` или `-no-admin-rights` — разрешить или запретить административный режим работы на ОС Windows 98/ОС Windows Me (то есть, считать ли пользователя, работающего на этих версиях, администратором). Администратор может, в частности, менять настройки **Агента**. Для ОС Windows NT и старше это определяется системой прав ОС. По умолчанию подразумевается запрещение.
- `-delay=`*<число>* — через сколько минут показывать приветственное сообщение пользователю после загрузки. По умолчанию 2 минуты, значение `-1` позволяет отключать приветствие.
- `-help` — показать справку по формату команды.
- `-trace` — детально протоколировать место возникновения ошибки, применим и в остальных приложениях.

H3. Dr.Web Enterprise Agent

Настройки **Агента** хранятся в реестре Windows в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\IDAVLab\Enterprise Suite\Dr.Web Enterprise Agent\Settings`, причем для параметров, заданных ключами, наименование параметра совпадает с названием ключа.

Список серверов **ВСО**, к которым может подключаться **Агент**, хранится в файлах `.config`, расположенных в подкаталогах репозитория (для ОС Windows - `DrWeb Enterprise Server \var\repository\`).

При запуске **Агента** с явным указанием каких-либо параметров заданные настройки не только используются в текущем сеансе, но также записываются в реестр и становятся постоянными настройками. Таким образом, если однократно запустить **Enterprise Агент** со всеми нужными параметрами, при последующих запусках параметры можно не указывать.

Настройки **Агента**, задаваемые непосредственно на станции, перезаписываются на настройки, получаемые с **Сервера**.

В случае задания на **Сервере** пустого списка **Серверов**, в которым подключается станция, будет использован список **Серверов**, заданный на станции.

Enterprise Агент запускается системой как служба и управляется через **Панель управления**.

Формат команды запуска:

`drwagntd [<ключи>] [<серверы>]`

Ключи

Допустимые ключи:

- `-compression=<режим>` — режим сжатия трафика с **Сервером**. Допустимые значения `yes`, `no`, `possible` (по умолчанию `possible`).
- `-control=<действие>` — управление состоянием службы **Агента**. Допустимые действия:
  - `install` — установить службу,
  - `uninstall` — удалить службу,
  - `start` — запустить сервис (только ОС Windows NT и старше),
  - `stop` — остановить сервис (только ОС Windows NT и старше),
  - `restart` — перезапустить сервис (только ОС Windows NT и старше).
- `-crypt=<режим>` — режим шифрования трафика с **Сервером**. Допустимые значения `yes`, `no`, `possible` (по умолчанию `yes`).
- `-drweb-key=<лицензионный_ключ>` — лицензионный пользовательский ключ. Данный ключ будет использоваться клиентским ПО при длительном отсутствии связи с **Сервером** и истечении срока действия ключа, полученного с **Сервера**. При наличии связи с **Сервером** данный ключ не нужен. По умолчанию — произвольный действительный ключ в каталоге, заданном параметром `-home`.
- `-help` — выдать справку по формату команды и ее параметрам. Аналогично `-help` интерфейсного модуля, см. Приложение H2. Интерфейсный модуль Агента Dr.Web Enterprise Agent.
- `-home=<каталог>` — каталог, в который установлен **Агент.** Если ключ не задан, подразумевается каталог, в котором находится исполняемый файл **Агента**.
- `-key=<открытый_ключ_сервера>` — файл открытого ключа **Сервера**, по умолчанию `drwcsd.pub` в каталоге,

заданном `-home`.

- `-log=<файл_протокола>` — файл протокола работы **Агента**, по умолчанию он помещается в подкаталог `logs` установочного каталога **Агента**. Для хранения файла протокола удаления **Агента** используется системный каталог временных файлов.
- `-retry=<количество>` — число попыток поиска **Сервера** посредством отправки multicast-запросов (если используется поиск) до сообщения о неуспехе. По умолчанию **3**.
- `-rotate=<N><f>,<M><u>` — режим ротации протокола работы **Агента**, где:
  - <*N*> — общее количество файлов протокола (включая текущий и архивные);
  - <*f*> — формат хранения файлов протокола, возможные значения: `z` (gzip) - компрессировать файлы, используется по умолчанию, или `p` (plain) - не компрессировать файлы;
  - <*M*> — размер файла;
  - <*u*> — единица измерения, возможные значения: `k` (kilo), `m` (mega), `g` (giga).

  По умолчанию `10,10m`, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие. Можно также использовать специальный формат `none` (`-rotate=none`) - это означает "не использовать ротацию, а писать всегда в один и тот же файл неограниченного размера".

  При использовании режима ротации используется следующий формат именования файлов: `file.<N>.log` или `file.<N>.log.dz`, где <*N*> - порядковый номер: 1, 2, и т.д.

  Например, пусть имя файла протокола (см. выше ключ `-log`) задано `file.log`. Тогда:

  - `file.log` — текущий файл (в который идет запись),
  - `file.1.log` — предыдущий,

- `file.2.log` и так далее — чем больше число, тем более старая версия.

- `-save` *<IP-адрес>* — осуществляет проверку корректности значения IP-адреса **Сервера** и сохранение настроек в реестр.
- `-spiderstat=`*<интервал>* — интервал в минутах отсылки на **Сервер** статистики **SpIDer Guard**, по умолчанию **30**. Статистика будет отсылаться на **Сервер** через такие интервалы при условии, что за это время она изменилась.
- `-timeout=`*<время>* — предельное время ожидания для каждого ответа в секундах при поиске **Сервера**. Прием ответных сообщений будет продолжаться, пока время ожидания ответа не превышает значение таймаута. По умолчанию **5**.
- `-trace` — детально протоколировать место возникновения ошибки, применим и в остальных приложениях.
- `-verbosity=`*<уровень_подробности>* — уровень детализации протокола. По умолчанию `INFO`. Допустимые значения: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Значения `ALL` и `DEBUG3` — синонимы (см. также Приложение L. Формат файлов протокола).

Данный ключ определяет степень подробности протоколирования в файл, заданный следующим после него ключом `-log` (см. выше). В одной команде может быть несколько ключей данного типа.

Ключи `-verbosity` и `-log` позиционно-зависимы.

При использовании этих ключей одновременно, ключ `-verbosity` должен идти перед ключом `-log`: ключ `-verbosity` переопределяет уровень детализации протоколов, расположенных по путям, следующим далее в командной строке.

Серверы

<серверы> — список **Серверов**. По умолчанию `drwcs@udp/231.0.0.1:2193`, что означает искать **Сервер** `drwcs`, используя multicast-запросы на группу `231.0.0.1` порт `2193`.

H4. Сетевой инсталлятор

Формат команды запуска:

`drwinst [<ключи>] [<переменные>] [<серверы>]`

Ключи

Допустимые ключи:

- `-compression=<режим>` — режим сжатия трафика с **Сервером**. Допустимые значения `yes`, `no`, `possible` (по умолчанию `no`).
- `-help` — выдать справку. Аналогично интерфейсному модулю **Агента**.
- `-home=<каталог>` — каталог установки. По умолчанию – `"Program Files\DrWeb Enterprise Suite"` на системном диске.
- `-id=<идентификатор_станции>` — задает идентификатор станции, на которую устанавливается **Агент**.
- `-interactive` — запустить инсталлятор в интерактивном режиме.

  Описание установки **Агента** в интерактивном (графическом) режиме инсталлятора приведено в разделе Установка Dr.Web Enterprise Agent.

  Если ключ `-interactive` не задан, установка **Агента** будет производиться в фоновом режиме инсталлятора (см.

раздел Установка Dr.Web Enterprise Agent). При этом интерактивный графический интерфейс инсталлятора может быть отображен в случае возникновения ошибки установки или ошибки запуска установки.

При удаленной инсталляции **Агентов** с использованием **Центра Управления** данный ключ не функционирует.

Ключ `-interactive` не может быть использован совместно с переменными. В случае задания переменных, они будут проигнорированы.

- `-key=`*<открытый_ключ>* — полный путь к файлу открытого ключа **Сервера**. По умолчанию ключ `drwcsd.pub` находится в подкаталоге `Installer` каталога установки **Сервера**.
- `-log=`*<файл_протокола>* — полный путь к файлу протокола установки (указывается при инсталляции **Агента**) или удаления (указывается при деинсталляции **Агента**).

  Для хранения файла протокола установки по умолчанию используется подкаталог `logs` каталога, задаваемого в ключе `-home` при установке.

  Для хранения файла протокола удаления по умолчанию используется пользовательский каталог для хранения временных файлов.

Если ключ `-log` не указан, имена файлов протокола формируются автоматически с использованием GUID и названия компьютера.

- `-platforms=p1,p2,p3...` — порядок загрузки платформ (по умолчанию стандартный, см. Приложение J. Использование скрипта начальной установки для Dr.Web Enterprise Agent).
- `-pwd=`*<пароль>* — указать пароль **Агента** для доступа к **Серверу**.
- `-regagent` — регистрировать **Агент** в списке **Установка**

и удаление программ (**Add or Remove Programs**).

- `-retry=<количество>` — аналогично **Агенту**.
- `-script=<имя_скрипта>` — задает файл с выполняемым скриптом. Используется вместе с ключом `-uninstall` для деинсталляции антивирусного ПО.
- `-timeout=<время>` — аналогично **Агенту**.
- `-trace` — детально протоколировать место возникновения ошибки, применим и в остальных приложениях.
- `-uninstall` — деинсталляция пакета на станции с помощью выполнения скрипта деинсталляции (см. ключ `-script`). Если скрипт не указан явно, будет выполнен внутренний скрипт деинсталляции.

  При отсутствии данного ключа (эквивалентно заданию `-no-uninstall`) производится инсталляция.

- `-verbosity=<уровень_подробности>` — уровень детализации протокола (аналогично **Агенту**, см. H3. Dr.Web Enterprise Agent). По умолчанию `ALL`.

Данный ключ определяет степень подробности протоколирования в файл, заданный следующим после него ключом `-log` (см. выше). В одной команде может быть несколько ключей данного типа.

Ключи `-verbosity` и `-log` позиционно-зависимы.

При использовании этих ключей одновременно, ключ `-verbosity` должен идти перед ключом `-log`: ключ `-verbosity` переопределяет уровень детализации протоколов, расположенных по путям, следующим далее в командной строке.

Переменные

Переменные задаются после ключей в виде списка, формат элементов следующий:

<переменная>=<значение>

Несколько наиболее важных переменных:

- `agent.language="C:\Program Files\DrWeb Enterprise Suite\RU-ESAUI.DWL"` — параметр задает режим отображения контекстного меню **Агента** на русском языке. В качестве значения необходимо использовать полный путь к файлу языковых ресурсов (по умолчанию используется английский язык).
- `spider.install=no` — не устанавливать **SpIDer Guard.** При отсутствии переменной — устанавливать.
- `spiderml.install=no` — аналогично, не устанавливать **SpIDer Mail**.
- `scanner.install=no` — аналогично, не устанавливать **Сканер Dr.Web для Windows**.
- `spidergate.install=no` — аналогично, не устанавливать **SpIDer Gate**.
- `agent.id=`*<идентификатор>*.
- `agent.password=`*<пароль>* — идентификатор и пароль рабочей станции; если эти параметры заданы, станция подключается не как «новичок», а с указанными параметрами.

Серверы

Список **Серверов** полностью аналогичен описанному для **Агента**.

H5. Dr.Web Enterprise Server

Существует несколько вариантов команд запуска **Сервера**, для удобства они описываются отдельно.

Команды, приведенные в пп. H5.1 – H5.5, являются кроссплатформенными: могут быть использованы как под ОС Windows, так и под ОС семейства UNIX, если не указано обратное.

H5.1. Управление Сервером Dr.Web Enterprise Server

`drwcsd [<ключи>]` — задать настройки работы **Сервера** (ключи подробнее описываются ниже).

H5.2. Базовые команды

- `drwcsd start` — запустить **Сервер**.
- `drwcsd restart` — сделать полный перезапуск службы **Сервера** (выполняется как пара `stop` и затем `start`).
- `drwcsd stop` — нормально завершить работу **Сервера**.
- `drwcsd reconfigure` — перечитать конфигурационный файл и перезапуститься (выполняется быстрее — без старта нового процесса).
- `drwcsd retemplate` — перечитать шаблоны оповещений с диска.
- `drwcsd verifyakey` *<путь_к_ключу>* – проверка корректности агентского ключа (`agent.key`).
- `drwcsd verifyekey` *<путь_к_ключу>* – проверка корректности серверного ключа (`enterprise.key`).
- `drwcsd verifyconfig` *<путь_к_файлу>* – проверка синтаксиса конфигурационного файла **Сервера** (`drwcsd.conf`).
- `drwcsd stat` – вывод в файл протокола статистики работы: время CPU, использование памяти и т.п. (под ОС семейства UNIX - аналог команды `send_signal WINCH` или `kill SIGWINCH`).

H5.3. Команды для управления базой данных

Инициализация базы данных

`drwcsd [`*<ключи>*`] initdb` *<ключ_Агента>* `[`*<скрипт_БД>*`]` `[`*<ini_файл>*`]` `[`*<пароль>*`]]` — инициализация базы данных.

- *<ключ_Агента>* — путь к лицензионному ключу **Enterprise Агента** `agent.key` (указывать обязательно).
- *<скрипт_БД>* — скрипт инициализации БД. Специальное значение - (минус) означает не использовать скрипт.
- *<ini_файл>* — предварительно сформированный файл в формате `drweb32.ini`, который будет задавать начальную конфигурацию компонентов ПО **Dr.Web** (для группы **Everyone**). Специальное значение - (минус) означает не использовать такой файл.
- *<пароль>* — начальный пароль администратора **Сервера** (его имя **admin**). По умолчанию **root**.

Знак "минус" может опускаться, если следующие за ним параметры отсутствуют.

Задание параметров инициализции базы данных

При использовании встроенной БД параметры инициализации могут задаваться через внешний файл. Для этого служит команда:

`drwcsd.exe initdbex` *<response-file>*

<response-file> - файл, в котором записаны параметры инициализации БД, построчно, в том же порядке что и параметры initdb.

Формат файла:

```
<путь_к_файлу_ключа>
<путь_к_файлу_initdb.sql>
<путь_к_файлу_drweb32.ini>
<пароль_администратора>
```

При использовании под ОС Windows response-файла возможно использование любых символов в пароле администратора.

Хвостовые строки, следующие за необходимым в конкретном случае параметром, необязательны. Если строка представляет собой "-" (один знак минуса), то используется значение по умолчанию (как в `initdb`).

Обновление базы данных

`drwcsd [`*<ключи>*`] updatedb` *<скрипт>* — произвести какую-либо манипуляцию с базой данных (например, обновление при смене версии), выполнив SQL-операторы из файла *<скрипт>*.

Обновление версии базы данных

`drwcsd upgradedb` *<каталог>* — запустить **Сервер** для обновления структуры базы данных при переходе на новую версию (см. каталог `update-db`).

Экспорт базы данных

`drwcsd exportdb` *<файл>* — экспорт базы данных в указанный файл.

Пример для Windows:

```
C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program Files
\DrWeb Enterprise Server\var" -verbosity=all
exportdb "C:\Program Files\DrWeb Enterprise Server
\esbase.es"
```

Под ОС **UNIX** действие выполняется от имени пользователя `drwcs:drwcs` в каталог `$DRWCS_VAR` (кроме ОС **FreeBSD**, которая по умолчанию сохраняет файл в директорию, из которой запущен скрипт; если указать путь явно, то директория должна быть с правами на запись для *<пользователя>*:*<группы>*, которые были созданы при установке, по умолчанию - `drwcs:drwcs`).

Импорт базы данных

`drwcsd importdb` *<файл>* — импорт базы данных из указанного файла (старое содержимое БД стирается).

Проверка базы данных

`drwcsd verifydb` — запустить **Сервер** для проверки базы данных. По окончании проверки **Сервер** выводит информацию о результатах в файл отчета (по умолчанию `drwcsd.log`).

H5.4. Команды для управления репозиторием

- `drwcsd syncrepository` — произвести синхронизацию репозитория с **ВСО**. Остановите **Сервер** перед запуском этой команды!
- `drwcsd rerepository` — перечитать репозиторий с диска.

H5.5. Резервное копирование критичных данных Сервера Dr.Web Enterprise Server

Резервная копия критичных данных **Сервера** (содержимого базы данных, лицензионного ключевого файла **Сервера**, закрытого ключа шифрования, конфигурационного файла **Сервера** и **Центра Управления**) создается с помощью следующей команды:

`drwcsd -home=<путь> backup [<каталог> [<количество>]]` — критичные данные **Сервера** копируются в указанный каталог. `-home` задает каталог установки **Сервера**. *<количество>* - количество сохраняемых копий одного и того же файла.

Пример для ОС Windows:

```
C:\Program Files\DrWeb Enterprise Server
\bin>drwcsd -home="C:\Program Files\DrWeb
Enterprise Server" backup C:\a
```

Резервные копии сохраняются в формате `.dz`, совместимом с `gzip` и другими архиваторами. После распаковки все файлы, кроме содержимого БД, готовы к использованию. Содержимое БД, сохраненное в резервной копии, можно импортировать в другую БД **Сервера** при помощи ключа `importdb` и таким образом восстановить данные (см. п. Восстановление БД Dr.Web Enterprise Security Suite).

Dr.Web ESS, начиная с версии **4.32**, регулярно сохраняет резервные копии важной информации в `\var\Backup` рабочего каталога **Сервера**. Для этого в расписание **Сервера** включено ежедневное задание, выполняющее эту функцию. Если такое задание в расписании отсутствует, рекомендуется создать его. В частности, задания на резервное копирование критичных данных нет, если изначально установленная версия **Сервера** - **4.32**, а последующие версии устанавливались поверх нее.

H5.6. Команды, доступные только под ОС Windows®

- `drwcsd [<ключи>] install` — установить службу **Сервера** в системе.
- `drwcsd uninstall` — удалить службу **Сервера** из системы.
- `drwcsd kill` — аварийно завершить службу **Сервера** (в случае, если нормально не удалось). Данную команду не рекомендуется использовать без крайней необходимости.
- `drwcsd silent` — запретить вывод сообщений от **Сервера**. Используется в командных файлах, для отключения интерактивности работы **Сервера**.

H5.7. Команды, доступные только под ОС семейства UNIX®

- `drwcsd config` – аналог команды `reconfigure` или `kill SIGHUP` – перезапуск **Сервера**.
- `drwcsd dumpimportdb` – записывать в файл протокола **Сервера** подробную информацию при импорте во внутреннюю или внешнюю базу.
- `drwcsd interactive` – запускает **Сервер**, но не передает управление процессу.
- `drwcsd newkey` – генерация новых ключей шифрования (`drwcsd.pri` и `drwcsd.pub`).
- `drwcsd readtempl` – перечитать шаблоны оповещений с диска.
- `drwcsd readrepo` – перечитать репозиторий с диска.
- `drwcsd selfcert` – генерация нового сертификата SSL и закрытого ключа RSA (`certificate.pem`, `private-key.pem`).
- `drwcsd shell` *<имя_файла>* – запуск бинарного файла.
- `drwcsd showpath` – показать все пути программы,

прописанные в системе.

- `drwcsd status` – показать текущий статус **Сервера** (запущен, остановлен).

H5.8. Описание ключей

Кроссплатформенные ключи

- `-activation-key=<лиц_ключ>` — лицензионный ключ **Сервера**. По умолчанию файл `enterprise.key`, расположенный в подкаталоге `etc` корневого каталога.
- `-bin-root=<каталог_для_исполняемых>` — путь к исполняемым файлам. По умолчанию подкаталог `bin` корневого каталога.
- `-conf=<конф_файл>` — имя и расположение конфигурационного файла **Сервера**. По умолчанию файл `drwcsd.conf` в подкаталоге `etc` корневого каталога.
- `-daemon` — для Windows-платформ означает запуск как службы; для платформ UNIX: "демонизация процесса" (перейти в корневой каталог, отсоединиться от терминала и перейти в фоновый режим).
- `-db-verify=on` — при запуске **Сервера** выполнять проверку целостности БД. Значение по умолчанию. Настоятельно не рекомендуется запускать с явным указанием противоположного значения, за исключением запуска немедленно после проверки БД командой `drwcsd verifydb`, см. выше.
- `-help` — выдать справку. Аналогично описанным выше программам.
- `-hooks` — разрешить выполнение **Сервером** пользовательских скриптов расширения, находящихся в папке:
  - для ОС Windows: `var\extensions`
  - для ОС FreeBSD и ОС Solaris: `/var/drwcs/extensions`
  - для ОС Linux: `/var/opt/drwcs/extensions`

каталога установки **Enterprise Сервера**. Скрипты предназначены для автоматизации работы администратора, упрощая и ускоряя выполнение некоторых заданий. Все скрипты по умолчанию отключены.

- `-home=`*<корень>* — каталог установки **Сервера** (корневой каталог). Структура данного каталога описана в п. Установка Dr.Web Enterprise Server для ОС Windows®. По умолчанию текущий каталог при запуске.
- `-log=`*<протокол>* — имя файла протокола **Сервера**. Вместо имени файла может использоваться "минус" (только для **Сервера** на платформах UNIX), что означает выводить протокол на стандартный вывод. По умолчанию: для Windows-платформ `drwcsd.log` в каталоге, указываемом ключом `-var-root`, для платформ UNIX задается ключом `-syslog=user` (см. ниже).
- `-private-key=`*<закр_ключ>* — закрытый ключ **Сервера**. По умолчанию `drwcsd.pri` в подкаталоге `etc` корневого каталога.
- `-rotate=`*<N><f>*,*<M><u>* - режим ротации протокола работы **Сервера**, где:
  - *<N>* - общее количество файлов протокола (включая текущий и архивные);
  - *<f>* - формат хранения файлов протокола, возможные значения: `z` (gzip) - компрессировать файлы, используется по умолчанию, или `p` (plain) - не компрессировать файлы;
  - *<M>* - размер файла;
  - *<u>* - единица измерения, возможные значения: `k` (kilo), `m` (mega), `g` (giga).

  По умолчанию `10,10m`, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие. Можно также использовать специальный формат `none` (`-rotate=none`) - это означает "не использовать ротацию, а писать всегда в один и тот же файл неограниченного размера".

При использовании режима ротации используется следующий формат именования файлов: `file.<N>.log` или `file.<N>.log.dz`, где <*N*> - порядковый номер: 1, 2, и т.д.

Например, пусть имя файла протокола (см. выше ключ `-log`) задано `file.log`. Тогда:

- `file.log` — текущий файл (в который идет запись),
- `file.1.log` — предыдущий,
- `file.2.log` и так далее — чем больше число, тем более старая версия.

- `-trace` — детально протоколировать место возникновения ошибки.
- `-var-root=`*<каталог_для_изменяемых>* — путь к каталогу, в который **Сервер** имеет право записи и который предназначен для хранения изменяемых файлов (например, протоколов, а также файлов репозитория). По умолчанию подкаталог `var` корневого каталога.
- `-verbosity=`*<уровень_подробности>* — уровень детализации протокола. По умолчанию `WARNING`. Допустимые значения: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Значения `ALL` и `DEBUG3` — синонимы (см. также Приложение L. Формат файлов протокола).

Данный ключ определяет степень подробности протоколирования в файл, заданный следующим после него ключом `-log` (см. выше). В одной команде может быть несколько ключей данного типа.

Ключи `-verbosity` и `-log` позиционно-зависимы.

При использовании этих ключей одновременно, ключ `-verbosity` должен идти перед ключом `-log`: ключ `-verbosity` переопределяет уровень детализации протоколов, расположенных по путям, следующим далее в командной строке.

Ключи, доступные только под ОС Windows

- `-minimized` — (только если запуск не как служба, а интерактивно) — минимизировать окно.
- `-screen-size=`*<размер>* — (только если запуск не как служба, а интерактивно) — размер в строках видимого протокола в окне **Сервера**, по умолчанию 1000.

Ключи, доступные только под ОС семейства UNIX

- `-etc=`*<path>* – путь к директории `etc` (`<var>/etc`).
- `-pid=`*<файл>* — файл, в который **Сервер** записывает идентификатор своего процесса.
- `-syslog=`*<режим>* — протоколирование в системный журнал. Возможные режимы: `auth`, `cron`, `daemon`, `kern`, `lpr`, `mail`, `news`, `syslog`, `user`, `uucp`, `local0` – `local7` и для некоторых платформ — `ftp`, `authpriv` и `console`.

Ключи `-syslog` и `-log` работают совместно. Т.е. при запуске **Сервера** с ключом `-syslog` (например, `service drwcsd start -syslog=user`), **Сервер** запустится с заданным значением для ключа `-syslog` и со значением по умолчанию для ключа `-log`.

- `-user=`*<пользователь>*, `-group=`*<группа>* — доступны только для ОС UNIX, при запуске от имени пользователя **root**; означают изменить пользователя или группу процесса и выполняться с правами указанного пользователя (группы).

H5.9. Переменные, доступные под ОС семейства UNIX®

Для облегчения управления **Сервером** под ОС семейства UNIX администратору предоставляются переменные, располагаемые в файле скрипта `/etc/init.d/drwcsd`.

Соответствие между переменными и ключами командной строки для `drwcsd` приведено в Таблице Н-1.

Таблица Н-1.

Ключ	Переменная	Параметры по умолчанию
-home	DRWCS_HOME	• `/usr/local/drwcs` - для ОС FreeBSD, • `/usr/drwcs` - для всех остальных ОС.
-var-root	DRWCS_VAR	
-etc	DRWCS_ETC	$DRWCS_VAR/etc
-rotate	DRWCS_ROT	10,10m
-verbosity	DRWCS_LEV	trace3
-log	DRWCS_LOG	$DRWCS_VAR/log/drwcsd.log
-conf	DRWCS_CFG	$DRWCS_ETC/drwcsd.conf
-pid	DRWCS_PID	
-user	DRWCS_USER	
-group	DRWCS_GROUP	
-hooks	DRWCS_HOOKS	
-trace	DRWCS_TRACE	

Переменные `DRWCS_HOOKS` и `DRWCS_TRACE` не имеют параметров. При задании переменных соответствующие ключи добавляются при исполнении скрипта. Если переменные не заданы, ключи не будут добавлены.

Прочие переменные приведены в Таблице Н-2.

Таблица Н-2.

Переменная	Параметры по умолчанию	Описание
DRWCS_ADDOPT		
DRWCS_CORE	unlimited	Максимальный размер core-файла.
DRWCS_FILES	8192	Максимальное число файловых дескрипторов, которое сможет открыть **Сервер**.
DRWCS_BIN	$DRWCS_HOME/bin	Директория, из которой будет запускаться `drwcsd`.
DRWCS_LIB	$DRWCS_HOME/lib	Директория с библиотеками **Сервера**.

Значения параметров по умолчанию вступают в силу, если такие переменные не определены в скрипте `/etc/init.d/drwcsd`.

Переменные `DRWCS_HOME`, `DRWCS_VAR`, `DRWCS_ETC`, `DRWCS_USER`, `DRWCS_GROUP`, `DRWCS_HOOKS` уже определены в файле скрипта `/etc/init.d/drwcsd`.

Если существует файл `${TGT_ES_ETC}/common.conf`, то этот файл будет включен в `/etc/init.d/drwcsd`, что может переопределить некоторые переменные, однако, если их не экспортировать (при помощи команды `export`), то они не окажут влияния.

Для задания переменных необходимо:

1. Добавить определение переменной в файле скрипта `/etc/init.d/drwcsd`.
2. Экспортировать переменную при помощи команды `export` (задается там же).
3. При запуске еще одного процесса из этого скрипта, этот процесс считает значения, которые были определены.

Например:

Для изменения уровня детализации протокола **Сервера** на максимальный:

1. В `/etc/init.d/drwcsd` добавить следующие строки:

```
DRWCS_LEV=ALL
export DRWCS_LEV
```

2. Запустить **Сервер**, если он был остановлен:

   `/etc/init.d/drwcsd start` (или `service drwcsd start`)

   Или перезапустить **Сервер**, если он уже был запущен:

   `/etc/init.d/drwcsd restart` (или `service drwcsd restart`)

3. Уровень детализации протокола примет значение `ALL`.

H5.10. Настройка Dr.Web Enterprise Server для ОС семейства UNIX®

Во время установки **Сервера** под ОС семейства UNIX вам будет необходимо произвести настройку некоторых конфигурационных параметров **Сервера**. Процедуру настройки параметров **Сервера** можно инициировать вручную (для этого необходимо, чтобы была установлена среда perl). Для этого достаточно запустить скрипт `configure.pl`, который находится:

- в директории `/usr/local/drwcs/bin/` для ОС **FreeBSD**,
- в директории `/opt/drwcs/bin/` для ОС **Linux** и ОС **Solaris**.

Формат команды запуска:

`configure.pl` *<ключи>*

Допустимые ключи:

- `--proxy server=`*<proxy_server>* – задать адрес прокси-сервера.
  - user=*<proxy_user>* – указать имя пользователя прокси-сервера.
  - password=*<proxy_password>* – указать пароль для пользователя прокси-сервера.
- `--stat server=`*<stat_server>* – задать адрес сервера статистики (по умолчанию `stat.drweb.com:80`).
  - url=*<url_on_server>* – задать URL на сервере статистики (по умолчанию `/update`).
  - interval=*<send_interval>* – задать интервал отправки статистики.
- `--initbase` – инициализировать БД **Сервера**.
- `--upgradebase` – обновить БД на **Сервере**.
- `--interactive` – запустить в интерактивном режиме.
- `--skip proxy=1` – пропустить один из шагов в интерактивном режиме.
  - `stat=1 |`
  - `initbase=1 |`
  - `upgradebase=1`
- `--verbose` – показать подробную информацию.
- `--help | ?` – показать справку по настройкам команды.

Н6. Утилита администрирования встроенной базы данных

Утилита администрирования встроенной БД расположена в следующих директориях:

- для ОС **Linux** и ОС **Solaris**: `/opt/drwcs/bin`
- для ОС **FreeBSD**: `/usr/local/drwcs/bin`
- для ОС семейства **Windows**:

<каталог_установки_Сервера>\bin

(по умолчанию каталог установки **Сервера**: C:\Program Files\DrWeb Enterprise Server).

Формат команды запуска:

drwidbsh *<путь_к_файлу_БД>*

Программа работает в текстовом диалоговом режиме, ожидает ввода пользователем команд программы (команды начинаются с точки).

Для справки по другим командам введите .help. Будет выдан текст справки.

Для дополнительной информации используйте справочные руководства по языку SQL.

H7. Утилита генерации пар ключей и электронной подписи

Имена и расположение файлов ключей шифрования в каталоге установки Сервера:

- \etc\drwcsd.pri - закрытый,
- \Installer\drwcsd.pub - открытый.

Варианты формата команды:

- \bin\drwsign check [-public-key=*<открытый>*] *<файл>* – проверить подпись файла, используя *<открытый>* как открытый ключ персоны, подписавшей данный файл.
- \bin\drwsign extract [-private-key=*<закрытый>*] *<открытый>* – извлекает открытый ключ из файла закрытого ключа комплексного формата (версия **4.33** и позднее).
- \bin\drwsign genkey [*<закрытый>* [*<открытый>*]] – генерация пары открытый-закрытый

ключ и запись их в соответствующие файлы.

Версия утилиты для платформ Windows (в отличие от версии для ОС UNIX) никак не защищает закрытый ключ от копирования.

- `\bin\drwsign help [<команда>]` – краткая справка по программе и формату командной строки.
- `\bin\drwsign join432 [-public-key=<открытый>] [-private-key=<закрытый>] <новый_закрытый>` – объединяет открытый и закрытый ключи формата версии **4.32** в новый комплексный формат закрытого ключа версии **4.33** и выше.
- `\bin\drwsign sign [-private-key=<закрытый>] <файл>` – подписать файл *<файл>*, используя указанный закрытый ключ.

H8. Управление Сервером Dr.Web Enterprise Server под ОС семейства UNIX® при помощи команды kill

Сервер под ОС UNIX управляется сигналами, посылаемыми процессу **Сервера** утилитой `kill`.

Подробная справка об утилите `kill` может быть получена при помощи команды `man kill`.

Ниже приводится перечень сигналов утилиты и производимых ими действий:

- `SIGWINCH` - вывод в файл протокола статистики работы (время CPU, использование памяти и т. п.),
- `SIGUSR1` - перечитывание репозитория с диска,
- `SIGUSR2` - перечитывание шаблонов сообщений с диска,
- `SIGHUP` - перезапуск **Сервера**,
- `SIGTERM` - останов **Сервера**,

- SIGQUIT - останов **Сервера**,
- SIGINT - останов **Сервера**.

Аналогичные действия для **Сервера** под ОС Windows реализуются при помощи ключей команды drwcsd, см. Приложение Н5.3.

Н9. Сканер Dr.Web для ОС Windows®

Данный компонент ПО рабочей станции имеет параметры командной строки, описанные в руководстве пользователя **«Антивирус Dr.Web® для Windows»**. Единственное отличие состоит в том, что при запуске **Сканера Агентом** параметры /go /st передаются **Сканеру** автоматически и в обязательном порядке.

Н10. Прокси-сервер

Для настройки некоторых параметров **Прокси-сервера** запустите с соответствующими ключами исполняемый файл drwcsd-proxy, который находится:

- Для ОС Windows: в каталоге установки **Прокси-сервера**.
- Для ОС семейства UNIX: в подкаталоге bin каталога установки **Прокси-сервера**.

Формат команды запуска:

drwcsd-proxy <*ключи*>

Допустимые ключи:

- --help – вывести справку по ключам для настройки **Прокси-сервера**.
- --daemon – только для ОС семейства UNIX: запустить **Прокси-сервер** в режиме демона.
- --control <*arg*> – только для ОС Windows: задать параметры настройки сервиса.

Допустимые параметры:

- `run` – (по умолчанию) запустить **Прокси-сервер** в фоновом режиме как сервис ОС Windows.
- `install` – установить **Прокси-сервер**.
- `uninstall` – удалить **Прокси-сервер**.

- `--cfg` <*path*> – задать путь к файлу конфигурации **Прокси-сервера**.
- `--pool-size` <*N*> – размер пула для подключений клиентов. По умолчанию 2.
- `--trace` – включить детальное протоколирование обращений к **Прокси-серверу**. Доступно только если сборка **Прокси-сервера** поддерживает детальное протоколирование стека вызовов.
- `--use-console-log` – вести протокол работы **Прокси-сервера** в консоли.
- `--use-file-log` <*file*> – записывать протокол работы **Прокси-сервера** в файл, где <*file*> - путь к файлу протокола.
- `--rotate=`<*N*><*f*>,<*M*><*u*> – режим ротации протокола работы **Прокси-сервера**, где:
  - <*N*> – общее количество файлов протокола (включая текущий и архивные);
  - <*f*> – формат хранения файлов протокола, возможные значения: `z` (gzip) – компрессировать файлы, используется по умолчанию, или `p` (plain) – не компрессировать файлы;
  - <*M*> – размер файла;
  - <*u*> – единица измерения, возможные значения: `k` (kilo), `m` (mega), `g` (giga).

  По умолчанию `10,10m`, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие.

- `--verbosity=<уровень_подробности>` – уровень детализации протокола. По умолчанию `TRACE3`. Допустимые значения: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Значения `ALL` и `DEBUG3` – синонимы.

Все ключи для задания параметров работы **Прокси-сервера** могут быть указаны одновременно.

Вывод протокола работы в файл и в консоль одновременно не поддерживается. При этом:

- Если ни один из ключей не задан, протокол ведется в консоли.
- Если заданы оба ключа, протокол пишется в файл.

Приложение I. Переменные окружения, экспортируемые Сервером Dr.Web Enterprise Server

Для упрощения настройки процессов, запускаемых **Enterprise Сервером** по расписанию, требуется информация о размещении каталогов **Сервера**. С этой целью **Сервер** экспортирует в окружение запускаемых процессов следующие переменные:

- `DRWCSD_HOME` — путь к корневому каталогу (каталогу установки). Значение ключа `-home`, если он был задан при запуске **Сервера**, в противном случае текущий каталог при запуске.
- `DRWCSD_EXE` — путь к каталогу для исполняемых файлов. Значение ключа `-bin-root`, если он был задан при запуске **Сервера**, в противном случае подкаталог `bin` корневого каталога.
- `DRWCSD_VAR` — путь к каталогу, в который **Сервер** имеет право записи и который предназначен для хранения изменяемых файлов (например, протоколов, а также файлов репозитория). Значение ключа `-var-root`, если он был задан при запуске **Сервера**, в противном случае подкаталог `var` корневого каталога.

Приложение J. Использование скрипта начальной установки для Dr.Web Enterprise Agent

Сценарий процесса начальной установки **Агентов** на станции с использованием сетевого инсталлятора (`drwinst.exe`) задается файлом `install.script`. Данные файлы располагаются в корневом каталоге продуктов в репозитории. В стандартной поставке они имеются в каталогах `10-drwupgrade` и `20-drwagntd` и описывают инсталляцию по умолчанию.

При наличии в каталоге файла `.custom.install.script`, используется именно он вместо стандартного сценария.

Файлы с любыми другими именами, начинающимися с точки, не обновляются при обновлениях продукта и не влияют на работу репозитория.

Последовательность действий при начальной установке:

1. Сетевой инсталлятор запрашивает с **Сервера** установку платформ: `win-setup`, `common`, `win`, `win-nt` и `win-9x` — это список стандартных платформ в порядке по умолчанию. Порядок использования платформ может быть изменен при помощи ключа `-platforms=p1,p2,p3...` при вызове `drwinst`. Платформа `win-setup` не входит в стандартную поставку и предназначена для создания, при необходимости, собственных сценариев установки.
2. **Сервер** формирует по списку платформ список файлов, последовательно просматривая все продукты в алфавитном порядке и списки файлов, заданные конструкциями `files { }` для данной платформы в сценарии установки `install.script` (см. ниже). Параллельно строится суммарный скрипт на основе конструкций `scripts{ }`.

3. **Сервер** получает общий список файлов и суммарный скрипт.
4. **Сервер** отсылает файлы и скрипт, который будет выполнен сетевым инсталлятором.

Теперь рассмотрим сам `install.script` на примере каталога `20-drwagntd`.

```
; master part of installation: Agent & its stuff.
; drwscr.dll goes with upgrader, so unlisted here.

platform{   ; win - for all Windows OS
            ; `name: XXX' MUST go first!

   name: win   ; (mandatory stanza)
               ; this platform name

               ; include, scripts{ }, files{ }
               ; can go in any order

   scripts {   ; (optional)
               ; script being merged with all others
win.inst.rexx  ; and executed after transfer all
               ; files for all platforms requested
               ; by installer
               ; Windows installer request order:
               ; - win-setup (optional! for
               ;              customization)
               ;   - common
               ;   - win
               ;   - win-nt OR win-9x
         }

   files {     ; (optional)
               ; this platform files being
               ; transfered to installer
```

```
          win/uninstall.rexx
          win/drwinst.exe
          win/drwagntd.exe
          win/drwagnui.exe
          win/drwhard.dll
        }
}

platform {    ; win-9x - for Windows 95-ME
   name: win-9x
   scripts{ win-9x.inst.rexx }
}

platform {    ; win-nt - for Windows NT-2003
   name: win-nt
   scripts{ win-nt.inst.rexx }
}

platform{        ; common - for any OS including
UNICES
    name: common
    scripts { common.inst.rexx }
}

; include file.name ; (optional)
     ; this stanza tells to include other file.
     ; including file will be searched in the
     ; same directory where current file are
     ; located if `file.name' does not include
     ; directory specificator
```

Скрипт представляет собой список конструкций `platform{ }` и позволяет с помощью конструкции `include` подключать определения из других файлов (`include` допустимо только на верхнем уровне и недопустимо внутри `platform{ }`). Если `file.name` в `include` не содержит пути, а только имя файла,

то он ищется в том же каталоге, что и текущий.

Наличие собственных конструкций `include` в подключаемых файлах допустимо.

Описание платформы начинается с конструкции `name: XXX`. Далее следует пара списков `files{ }` и `scripts{ }`. Порядок появления этих списков не важен; списки могут содержать любое число элементов. Порядок элементов в списке важен, поскольку определяет порядок передачи файлов на станцию и конструкцию формируемого скрипта.

Порядок появления конструкций `platform{ }` также не важен.

Ниже перечислены переменные скриптов инсталляции (значения этим переменным могут быть присвоены из командной строки сетевого инсталлятора) и их значения по умолчанию:

- `spider.install = 'yes'`
- `spiderml.install = 'yes'`
- `scanner.install = 'yes'`
- `install.home` — каталог установки
- `agent.logfile = install.home'\logs \drwagntd.log'`
- `agent.loglevel = 'trace'`
- `agent.logrotate = '10,10m'`
- `agent.servers = install.servers`
- `agent.serverkey = install.home'\drwcsd.pub'`
- `agent.compression = 'possible'`
- `agent.encryption = 'yes'`
- `agent.findretry = '3'`
- `agent.findtimeout = '5'`
- `agent.spiderstatistics = '30'`
- `agent.importantmsg = '2'`
- `agent.discovery = 'udp/:2193'`

- `agent.startmsg = '2'` (или `agent.startmsg = 'NONE'`)

Параметр `agent.importantmsg` определяет, отображать ли пользователю сообщение об ошибке обновления, необходимости перезагрузки и т. д. **0** — не выводить сообщение, **1** — показывать всплывающее информационное сообщение.

Создадим нестандартный сценарий установки, в котором не устанавливается SpIDer Guard и задается максимально подробное протоколирование:

1. Создайте в `20-drwagntd` файл `.win-setup.inst.rexx` и запишите в него:

```
spider.install = 'no'
agent.loglevel = 'all'
```

2. Создайте в `20-drwagntd` файл `.custom.install.script` и запишите в него

```
include install.script

platform{
      name: win-setup
      scripts{ .win-setup.inst.rexx }
}
```

3. Перегрузите **Сервер** или дайте сигнал перезагрузить репозиторий:
   - для ОС **UNIX**: `kill -USR1 cat` `drwcsd.pid`
   - для ОС **Windows**: `drwcsd.exe rerepository`

Приложение K. Использование регулярных выражений в Dr.Web Enterprise Security Suite

Некоторые параметры **Dr.Web ESS** задаются в формате регулярных выражений. Обработка регулярных выражений осуществляется при помощи программной библиотеки PCRE.

Подробное описание синтаксиса библиотеки PCRE доступно на сервере http://www.pcre.org/.

В данном приложении приведено только краткое описание основных моментов использования регулярных выражений.

K1. Опции регулярных выражений

Регулярные выражения применяются как в конфигурационном файле **Сервера**, так и в **Центре Управления** при задании исключаемых из сканирования объектов в настройках **Сканера**.

Регулярные выражения записываются в следующей форме:
`qr{EXP}options`

где `EXP` – собственно выражение, `options` – последовательность опций (строка букв), `qr{}` – литеральные метасимволы. В целом конструкция выглядит, например, так:
`qr{pagefile\.sys}i` – файл подкачки ОС Windows NT

Ниже приведено описание опций и собственно регулярных выражений. Более полное описание см. на http://www.pcre.org/pcre.txt.

- Опция `'a'`, соответствующая `PCRE_ANCHORED`

  С этой настройкой шаблон принудительно "встает на якорь", т.е. ограничивается сопоставлением только с первой искомой

позицией в строке, по которой осуществляется поиск ("строка темы"). Это также можно достигнуть с помощью соответствующих конструкций в самом шаблоне.

- Опция `'i'`, соответствующая `PCRE_CASELESS`

  С этой настройкой буквы в шаблоне сопоставляются как с заглавными, так и со строчными буквами. Данная возможность может быть изменена в шаблоне настройкой опции `(?i)`.

- Опция `'x'`, соответствующая `PCRE_EXTENDED`

  С этой настройкой пробелы между символами в шаблоне игнорируются, за исключением случаев, когда они предваряются управляющими символами или находятся внутри класса символов. Пробел не включает символ `VT` (код 11). Кроме того, символы, находящиеся вне класса символов между символом `#`, не предваренным управляющим символом, и символом новой строки включительно, также игнорируются. Данную опцию можно изменить в шаблоне настройкой опции `(?x)`. Эта настройка дает возможность включать комментарии внутрь сложных шаблонов. Следует обратить внимание, что это применимо только к символам данных. Символы пробела не могут находиться в шаблоне внутри последовательностей специальных символов, например, внутри последовательности `(?(`, которая вводит условный подшаблон.

- Опция `'m'`, соответствующая `PCRE_MULTILINE`

  По умолчанию, PCRE считает, что строка темы состоит из единственной строки с символами (даже если она на самом деле содержит символы перевода строк). Метасимвол *"начала строки"* `"^"` сопоставляется только в начале строки, в то время как метасимвол *"конец строки"* `"$"` сопоставляется только в конце строки или перед заключительным переводом строки (если не установлена опция `PCRE_DOLLAR_ENDONLY`).

  Если установлена опция `PCRE_MULTILINE`, метасимволы *"начало строки"* и *"конец строки"* привязываются к

следующим сразу за ними или перед ними любым переводам строки в строке темы, а также в самом начале и конце строки. Данную опцию можно изменить в шаблоне настройкой опции `(?m)`. Если в тексте нет символов `"\n"` или если в шаблоне не встречается `^` или `$`, опция `PCRE_MULTILINE` не имеет смысла.

- Опция `'u'`, соответствующая `PCRE_UNGREEDY`

  Эта опция отменяет "жадность" квантификаторов, так что они становятся "нежадными" по умолчанию, но восстанавливают "жадность", если за ними следует `"?"`. Это также можно настроить опцией `(?U)` в шаблоне.

- Опция `'d'`, соответствующая `PCRE_DOTALL`

  С этой настройкой метасимвол точки в шаблоне сопоставляется со всеми символами, включая символ новой строки. Без него символы новой строки исключаются. Эту опцию можно изменить в шаблоне установкой новой опции `(?s)`. Отрицательный класс, например, `[^a]`, всегда сопоставляется с символом новой строки, независимо от установок этой опции.

- Опция `'e'`, соответствующая `PCRE_DOLLAR_ENDONLY`

  С этой настройкой символ доллара в шаблоне сопоставляется только в конце строки темы. Без этой опции доллар также сопоставляется в положении непосредственно перед символом перевода строки в конце строки (но не перед любыми другими символами новой строки). Опция `PCRE_DOLLAR_ENDONLY` игнорируется, если установлена опция `PCRE_MULTILINE`.

K2. Особенности регулярных выражений PCRE

Регулярное выражение - это шаблон, сопоставляемый с текстом слева направо. Большинство символов в шаблоне обозначают сами себя и применяются к соответствующим символам в тексте.

Главное преимущество регулярных выражений заключается в возможности включать в шаблон варианты и повторения. Они кодируются с помощью метасимволов, которые не означают сами себя, а наоборот, интерпретируются особым способом.

Существует два различных набора метасимволов: те, которые используются внутри квадратных скобок, и те, которые используются вне квадратных скобок. Рассмотрим их более детально. Вне квадратных скобок используются следующие метасимволы:

- `\` обычный управляющий символ (`escape`), допускающий несколько вариантов применения,
- `^` объявляет начало строки (или текста в многострочном режиме),
- `$` объявляет конец строки (или текста в многострочном режиме),
- `.` соответствует любому символу, кроме символа переноса строки (по умолчанию),
- `[` начало описания класса символов,
- `]` конец описания класса символов,
- `|` начало альтернативной ветви,
- `(` начало подшаблона,
- `)` конец подшаблона,
- `?` расширяет значение `(`,

  также квантификатор 0 или 1,

  также квантификатор-минимизатор;
- `*` 0 или более,
- `+` 1 или более,

  также "притяжательный квантификатор",
- `{` начало минимального/ максимального квантификатора.

Та часть шаблона, которая находится в квадратных скобках, называется "классом символов". В классе символов метасимволами являются:

\ обычный управляющий символ (escape),

^ отрицает класс, но только если в начале класса,

– определяет диапазон символов,

[класс символов POSIX (только если за ним следует синтаксис POSIX),

] закрывает класс символов.

КЗ. Использование метасимволов

Обратная косая черта (\)

Символ обратной косой черты используется в нескольких случаях. Во-первых, если за ним следует небуквенно-цифровой символ, он отнимает у такого символа какое-либо специальное значение. Это употребление обратной косой черты в качестве управляющего символа допустимо как внутри, так и вне класса символов.

Например, если вы хотите задать соответствие символу *, вам необходимо указать в шаблоне *. Независимо от того, интерпретируется ли следующий символ без \ как метасимвол, управляющий символ можно использовать перед небуквенно-цифровым символом «на всякий случай», чтобы указать, что он означает сам себя. В частности, для сопоставления с обратной косой чертой следует писать \\.

Если шаблон задан с опцией PCRE_EXTENDED, пробел в шаблоне (вне класса символов) и символы, находящиеся между # (вне класса символов) и следующим за ним символом перевода строки, игнорируются. Обратная косая черта может использоваться для включения пробела или символа # в качестве части шаблона.

Если вы хотите убрать специальное значение последовательности символов, вы можете сделать это, расположив их между \Q и \E. Последовательность \Q...\E действует как внутри, так и вне класса символов.

Неотображаемые символы

Второе применение обратной косой черты - использование неотображаемых символов в описании шаблона. Ограничений отображения таких символов не существует, за исключением двоичного нуля в конце шаблона. Однако если шаблон составляется в текстовом редакторе, обычно проще использовать управляющую последовательность, чем двоичный символ, который ее представляет:

- \a звонок, т.е. символ BEL (шестнадцатеричный 07),
- \cx "control-x", где x - любой символ,
- \e символ escape (шестнадцатеричный 1B),
- \f перевод страницы (шестнадцатеричный 0C),
- \n перевод строки (шестнадцатеричный 0A),
- \r возврат каретки (шестнадцатеричный 0D),
- \t табуляция (шестнадцатеричный 09),
- \ddd символ с восьмеричным кодом ddd или обратная ссылка,
- \xhh символ с шестнадцатеричным кодом hh.

Эффект применения \cx состоит в следующем: если x выражен строчной буквой, она преобразуется в заглавную. Затем инвертируется 6-й бит символа (шестнадцатеричный 40). Таким образом, \cz становится шестнадцатеричным 1A, но \c { становится шестнадцатеричным 3B, в то время как \c; становится шестнадцатеричным 7B.

После \x читаются от нуля до двух шестнадцатеричных цифр (буквы могут быть заглавными или строчными).

После \0 читаются две следующие восьмеричные цифры. В обоих случаях, если цифр меньше двух, то используются только те, которые имеются.

Таким образом, последовательность \0\x\07 означает два двоичных нуля, за которыми следует символ BEL (значение кода 7). В случае если вы используете представление числа в восьмеричном коде, убедитесь, что за начальным нулем следуют две значащие цифры.

Обработка обратной косой черты, за которой следует цифра, отличная от 0, довольно сложна. Вне класса символов PCRE считывает ее и любые следующие за ней цифры как десятичное число. Если число меньше 10 или если ему в выражении предшествует столько же захватывающих левых скобок, вся последовательность рассматривается как обратная ссылка.

Внутри класса символов или если десятичное число больше 9 и нет такого же количества захватывающих подшаблонов, PCRE еще раз считывает до трех восьмеричных цифр, следующих за обратной косой чертой, и генерирует один байт из самых младших 8 бит значения. Любые другие следующие цифры означают сами себя. Например:

- \040 альтернативный способ записи пробела,
- \40 тоже самое, при условии, что данной записи предшествует менее 40 захватывающих подшаблонов,
- \7 всегда обратная ссылка,
- \11 может быть как обратной ссылкой, так и альтернативной записью символа табуляции,
- \011 всегда обозначает символ табуляции,

- \0113 символ табуляции, за которым следует символ "3",
- \113 может быть обратной ссылкой, иначе - символ с восьмеричным кодом 113,
- \377 может быть обратной ссылкой, иначе - байт, состоящий из единичных битов,
- \81 может быть как обратной ссылкой, так и двоичным нулем, за которым следуют два символа "8" и "1".

Заметьте, что восьмеричные значения 100 или более не следует предварять нулями, так как более трех восьмеричных цифр никогда не считывается.

Все последовательности, определяющие значение единичного символа, могут использоваться как внутри, так и вне класса символов. Кроме того, внутри класса символов последовательность \b интерпретируется как символ возврата (backspace, шестнадцатеричный 08), а последовательность \X как символ "X". Вне класса символов эти последовательности имеют другие значения.

Типы родовых символов

Третий способ применения обратной косой черты - определение типов родовых символов. Следующие типы распознаются всегда:

- \d любая десятичная цифра,
- \D любой символ, кроме десятичной цифры,
- \s любой символ пробела (whitespace),
- \S любой символ, не являющийся символом пробела,
- \w любой алфавитно-цифровой символ и символ подчеркивания,

- \W любой символ, кроме цифр, букв и символов подчеркивания.

Каждая пара таких управляющих последовательностей делит полное множество всех символов на два непересекающихся множества. Любой символ соответствует одному и только одному множеству из пары.

Эти последовательности типов символов могут появляться как внутри, так и вне класса символов. Каждый из них соответствует одному символу определенного типа. Если текущее сопоставление находится в конце текста, поиск заканчивается неудачей, так как нет символа для сопоставления.

\s не соответствует символу VT (код 11). В этом состоит его отличие от класса "пробела" в POSIX. Символами \s являются HT (9), LF (10), FF (12), CR (13) и пробел (32).

Простые утверждения

Четвертое применение обратной косой черты - написание некоторых простых утверждений. Утверждение обозначает условие, которое должно быть соблюдено в определенной позиции при сопоставлении, не затрагивая каких-либо символов из строки темы. Использование подшаблона для более сложных утверждений описывается ниже.

Утверждения, сопровождаемые обратной косой чертой:

- \b сопоставление на границе слова,
- \B сопоставление не на границе слова,
- \A сопоставление на начале текста,
- \Z сопоставление на конце текста или перед символом перевода строки, расположенным в конце,
- \z сопоставление на конце текста,

- \G сопоставление на первой позиции поиска в тексте.

Такие утверждения не могут находиться внутри класса символов (но следует отметить, что \b внутри класса символов имеет иное значение – символ возврата (backspace)).

Диакритический знак (^) и символ доллара ($)

По умолчанию, вне класса символов метасимвол начала строки ^ является утверждением, справедливым только в случае, если текущая позиция поиска находится в начале строки текста. Внутри класса символов диакритический знак имеет совершенно иное значение (см. ниже).

Метасимвол ^ может и не быть первым символом в шаблоне, если используется несколько вариантов, но он должен быть на первом месте в каждом варианте, в котором он появляется, если предполагается, что шаблон должен соответствовать этой ветке. Если все возможные варианты начинаются с диакритического знака, то есть, если шаблон привязан к началу текста, говорят, что шаблон «заякорен». (Существуют и другие способы «заякорить» шаблон).

Символ доллара $ является утверждением, верным только если текущее совпадение находится в конце строки текста или непосредственно перед символом перевода строки, являющимся последним символом в строке (по умолчанию). Не следует употреблять знак доллара в качестве последнего символа в шаблоне, если используется несколько альтернативных вариантов, но его следует поместить в конец каждой ветки, в которой он появляется. В классе символов у доллара нет специального значения.

Значения диакритического знака ^ и знака доллара $ изменяются, если установлена опция PCRE_MULTILINE. В этом случае, помимо сопоставления в начале и конце строки темы, они сопоставляются сразу после или непосредственно перед

внутренним символом перевода строки соответственно. Например, в многострочном представлении шаблон `/^abc$/` соответствует строке "`def\nabc`" (где `\n`– символ перевода строки), и не иначе. Следовательно, шаблоны, которые привязаны к концу или началу в однострочном представлении из-за того, что все ветви начинаются с `^`, не являются привязанными в многострочном представлении, и сопоставление с диакритическим знаком возможно при ненулевом начальном смещении аргумента функции `pcre_exec()`.

Точка

Вне класса символов точка в шаблоне соответствует любому символу в теме, включая неотображаемые символы, кроме (по умолчанию) символа перевода строки. Обработка точки совершенно не зависит от обработки диакритического знака `^` и символа доллара `$`, единственная связь между ними состоит в использовании символов перевода строки. У точки нет особого значения в классе символов.

Квадратные скобки и классы символов

Открывающая квадратная скобка вводит класс символов, завершаемый закрывающей квадратной скобкой. Закрывающая квадратная скобка сама по себе не имеет специального значения. Если закрывающая квадратная скобка требуется в качестве члена класса, она должна быть первым символом в классе (после начального диакритического знака, если таковой имеется) или экранироваться обратной косой чертой. Класс символов соответствует единственному символу в тексте.

Класс символов соответствует одиночному символу в теме. Искомый символ должен находиться в наборе символов, определенных классом, за исключением случая, когда первым символом в определении класса является диакритический знак, в таком случае символ темы не должен входить в набор, определенный классом. Если необходимо использовать диакритический знак в качестве члена класса, убедитесь, что он

не является первым символом, или экранируйте его обратной косой чертой.

Например, класс символов `[aeiou]` соответствует любой прописной гласной, тогда как `[^aeiou]` соответствует любому символу, который не является прописной гласной.

Обратите внимание, что диакритический знак всего лишь служит для указания тех символов, которые не входят в класс, тем самым упрощая обозначение тех символов, которые в него входят. Класс, начинающийся с диакритического знака, не является утверждением: ему все равно требуется один символ из текста, и если текущий указатель поиска находится в конце строки, то сопоставления шаблону не происходит.

При сопоставлении без учета регистра все буквы в классе представляют свои как заглавные, так и строчные версии.

Символ минуса (дефис) можно использовать для обозначения диапазона символов в классе символов. Например, `[d-m]` соответствует любой букве от `d` до `m` включительно. Если в классе требуется символ минуса, он должен быть предварен обратной косой чертой или стоять в позиции, где он не может быть интерпретирован как обозначение диапазона (как правило, первым или последним в классе).

Буквенный символ "`]`" не может быть конечным символом диапазона. Шаблон вида `[W-]46]` будет интерпретирован как класс, состоящий из двух символов ("`W`" и "`-`"), за которым следует буквенная строка "`46]`", и, таким образом, будет соответствовать "`W46]`" или "`46]`". Однако, если "`]`" предварить символом обратной косой черты, он будет интерпретирован как конец диапазона, таким образом, `[W-\]46]` будет интерпретирован как класс, содержащий диапазон, за которым следуют два символа. Восьмеричные или десятеричные представления "`]`" также могут использоваться в качестве конца диапазона.

Типы символов `\d`, `\D`, `\p`, `\P`, `\s`, `\S`, `\w` и `\W` могут также появляться в классе символов, добавляя в класс символы, которым они соответствуют.

Единственные метасимволы, которые распознаются в классах символов, это обратная косая черта, дефис (только там, где его можно интерпретировать как определитель диапазона), диакритический знак (только в начале), открывающая квадратная скобка (только там, где ее можно интерпретировать как ввод имени класса POSIX, - см. следующий раздел) и закрывающая квадратная скобка. Однако экранирование обратной косой чертой любых других неалфавитно-цифровых символов также не повредит.

Классы символов POSIX

PCRE поддерживает условные обозначения POSIX для классов символов. Например,

```
[01[:alpha:]%]
```

соответствует "0", "1", любому алфавитному символу или "%". Поддерживаемые имена классов

- `alnum` буквы и цифры,
- `alpha` буквы,
- `ascii` коды символов `0 – 127`,
- `blank` только пробел или знак табуляции,
- `cntrl` управляющие символы,
- `digit` десятичные цифры (тоже самое, что и `\d`),
- `graph` печатные символы, кроме пробела,
- `lower` строчные буквы,
- `print` печатные символы, включая пробел,
- `punct` печатные символы, кроме букв и цифр,
- `space` символ пробела (не совсем тоже самое, что и `\s`),
- `upper` заглавные буквы,
- `word` алфавитно-цифровые символы (тоже, что и `\w`),
- `xdigit` десятеричные цифры.

Вертикальная черта (|)

Символ вертикальной черты используется для разделения альтернативных шаблонов. Например, шаблон

```
gilbert|sullivan
```

соответствует либо "gilbert", либо "sullivan". Допускается любое количество вариантов, в том числе и пустой (соответствующий пустой строке). В процессе подбора соответствия каждый вариант проверяется по очереди, слева направо, и используется первый найденный. Если варианты находятся внутри подшаблона (см. ниже), "найденный" означает соответствие как остальной части основного шаблона, так и варианту в подшаблоне.

Установка внутренних опций

Установки опций PCRE_CASELESS, PCRE_MULTILINE и PCRE_EXTENDED можно локально изменить в шаблоне с помощью последовательности букв-опций Perl, заключенных между "(?" и ")".

Буквы-опции:

- i для PCRE_CASELESS
- m для PCRE_MULTILINE
- x для PCRE_EXTENDED

Например, (?im) определяет многострочный поиск совпадения без учета регистра. Также возможно отключить эти опции, предварив их дефисом, можно комбинировать установку и отмену опций, например, (?im-x) устанавливает PCRE_CASELESS и PCRE_MULTILINE и отменяет PCRE_EXTENDED. Если перед дефисом или после него появляется буква, опция отменяется.

Подшаблоны

Подшаблоны заключаются в круглые скобки, которые могут быть вложенными. Превращение части шаблона в подшаблон служит двум целям:

1. Локализирует набор вариантов. Например, шаблон

   ```
   cat(aract|erpillar|)
   ```

   соответствует одному из слов: "cat", "cataract" или "caterpillar". Без скобок он бы соответствовал "cataract", "erpillar" или пустой строке.

2. Указывает на необходимость захвата подстроки. Открывающие скобки нумеруются слева направо (начиная с 1) и их порядковые номера используются для нумерации соответствующих подстрок в результате.

   Например, если строка "the red king" сопоставляется с шаблоном

   ```
   the ((red|white) (king|queen))
   ```

   будут захвачены подстроки "red king", "red" и "king" и пронумерованы соответственно 1, 2 и 3.

То, что простые круглые скобки выполняют две функции, не всегда удобно. Бывают случаи, когда необходима группировка вариантов без захвата строки. В случае, когда после открывающей круглой скобки следует "?:", захват строки не происходит и текущий подшаблон не нумеруется. Например, если строка "the white queen" сопоставляется с шаблоном

```
((?:red|white) (king|queen))
```

будут захвачены подстроки "white queen" и "queen" и пронумерованы 1 и 2. Максимальное количество захватывающих подшаблонов 65535, а максимальная глубина вложенности всех подшаблонов, как захватывающих, так и незахватывающих, 200.

В случае, если в незахватывающем подшаблоне необходимо указать дополнительные опции, можно воспользоваться удобным сокращением: поместить символ, обозначающий устанавливаемую опцию, между "?" и ":". Таким образом, следующие два шаблона

```
(?i:saturday|sunday)
(?:(?i)saturday|sunday)
```

соответствуют одному и тому же набору строк. Так как альтернативные ветви проверяются слева направо, и установленные опции сохраняют свое действие до конца подшаблона, опция, установленная в одной ветке, также действует во всех последующих ветках. Таким образом, вышеприведенные шаблоны соответствуют как "SUNDAY", так и "Saturday".

Повторение

Повторение задается квантификаторами, следующими за любым из указанных ниже элементов:

- буквенный символ данных,
- метасимвол . (точка),
- управляющая последовательность \C,
- управляющая последовательность, соответствующая одному символу, например, \d,
- класс символов,
- обратная ссылка (см. следующий раздел),
- подшаблон, заключенный в круглые скобки (если он не является утверждением).

Обычный квантификатор повторения обозначает минимальное и максимальное число допустимых сопоставлений путем заключения в фигурные скобки двух чисел, разделенных запятой. Числа должны быть меньше 65536, а первое из них должно быть меньше или равным второму. Например:

```
z{2,4}
```

соответствует "zz", "zzz" или "zzzz". Закрывающая фигурная скобка сама по себе не является специальным символом. Если второе число опущено, но запятая присутствует, верхнего ограничения не существует. Если пропущены и второе число, и запятая, квантификатор определяет точное число требуемых соответствий, например,

```
[aeiou]{3,}
```

соответствует, по крайней мере, 3 (и более) следующим друг за другом гласным, в то время как

```
\d{8}
```

сопоставляется точно 8 цифрам. Открывающая фигурная скобка, появляющаяся в позиции, где квантификатор не допускается, или в позиции, не соответствующей синтаксису квантификатора, рассматривается как буквенный символ. Например, `{,6}` является не квантификатором, а буквенной строкой, состоящей из 4 символов.

Квантификатор `{0}` допускается. Причем выражение ведет себя так, будто предыдущий элемент и квантификатор не существуют.

Для удобства (и обратной совместимости) три наиболее распространенных квантификатора имеют односимвольные сокращения:

- `*` эквивалентен `{0,}`
- `+` эквивалентен `{1,}`
- `?` эквивалентен `{0,1}`

Можно конструировать бесконечные циклы, введя после подшаблона, который не совпадает ни с одним символом, квантификатор, не имеющий верхнего предела, например:

```
(a?)*
```

По умолчанию, квантификаторы являются "жадными", что означает, что они совпадают максимально возможное количество раз (до максимально допустимого количества раз), не вызывая неудачи выполнения остальной части шаблона. Классическим примером, когда это создает проблемы, является поиск

соответствия в комментариях в программах C. Комментарии могут находиться между символами /* и */, а внутри комментария могут появляться отдельные символы * и /. Попытка найти совпадение с комментариями C путем применения шаблона

```
/\*.*\*/
```

к строке

```
/* первый комментария */ не комментарий
/* второй комментарий */
```

потерпит неудачу, потому что происходит совпадение со всей строкой из-за жадности элемента *.

Однако, если за квантификатором следует знак вопроса, он перестает быть жадным и совпадает минимально возможное количество раз. Тогда шаблон

```
/\*.*?\*/
```

правильно обрабатывает комментарий C. Значение других квантификаторов при этом не изменяется, они обеспечивают необходимое число совпадений. Не следует путать это употребление знака вопроса с использованием его в качестве квантификатора как такового. Поскольку он может использоваться двояко, иногда его можно дублировать, как в

```
\d??\d
```

что в первую очередь соответствует одной цифре, но может соответствовать и двум, если это единственный способ совпадения с оставшейся частью шаблона.

Если установлена опция PCRE_UNGREEDY, квантификатор утрачивает жадность по умолчанию, отдельные квантификаторы могут наделяться жадностью, если за ними следует знак вопроса. Другими словами, им возвращается их поведение по умолчанию.

Если подшаблон в круглых скобках квантифицируется с минимальным числом повторений, которое больше 1, или имеет ограничение максимума, для скомпилированного шаблона потребуется больше памяти, пропорционально размеру минимума

или максимума.

Поэлементное группирование и притяжательные квантификаторы

И при максимальном, и при минимальном количестве повторений отсутствие совпадения обычно заставляет произвести повторное сопоставление повторяемого выражения, чтобы проверить, позволяет ли иное число повторений добиться совпадения с оставшейся частью шаблона. Бывают случаи, когда необходимо изменить описанную логику работы для реализации специфического сопоставления или сокращения попыток сопоставления (если автор уверен, что нет смысла продолжать поиск).

Рассмотрим для примера шаблон `\d+foo` применительно к тексту:

```
123456bar
```

После совпадения всех 6 цифр и констатации отсутствия совпадения с "`foo`", поисковой механизм сделает еще одну попытку найти совпадение для элемента `\d+`, но уже из 5 цифр, после очередной неудачи будет сопоставлено 4 цифры и так далее.

С помощью *«поэлементного группирования»* (*atomic grouping*, термин взят из книги Jeffrey Friedl) указывается, что если одна часть шаблона была сопоставлена, ее не следует анализировать повторно.

Если мы воспользуемся группированием на предыдущем примере, поисковый механизм немедленно прекратит поиск, констатировав несовпадение с "`foo`" с первого раза. Записываются однократные шаблоны при помощи круглых скобок следующим образом: `(?>`. Например:

```
(?>\d+)foo
```

Такой вид скобок "блокирует" содержащуюся в них часть шаблона при первом же обнаружении совпадения, а при обнаружении

несоответствия с остальной частью шаблона предотвращает повторный анализ заблокированной части. Однако это не мешает повторно анализировать любые другие элементы, в том числе предшествующие группе.

Другими словами, можно сказать, что подшаблон такого типа соответствует строке символов, которой бы соответствовал идентичный отдельный шаблон, если бы он был привязан к («заякорен на») текущей позиции текста.

Подшаблоны поэлементного группирования не являются захватывающими. Простые примеры, подобные приведенному выше, можно охарактеризовать как безусловный захват максимального количества повторений. Таким образом, в то время как `\d+` и `\d+?` применяются для регулирования количества цифр, которые должны совпасть, чтобы совпала остальная часть шаблона, `(?>\d+)` может совпадать только со всей последовательностью цифр.

Поэлементные группы могут, конечно, содержать произвольные сложные подшаблоны и могут быть вложенными. Однако, когда подшаблон для группирования является единичным повторяемым элементом, как в примере выше, можно использовать более простое обозначение, которое называется «притяжательным квантификатором». Притяжательный квантификатор указывается с помощью дополнительного символа плюс + после квантификатора. Используя это обозначение, предыдущий пример можно переписать как

```
\d++foo
```

Притяжательные квантификаторы всегда жадные; установка опции `PCRE_UNGREEDY` игнорируется. Они являются удобным обозначением для простых форм поэлементного группирования. Однако разницы в значении или обработке притяжательного квантификатора и соответствующей поэлементной группы нет.

Если шаблон содержит неограниченное повторение внутри подшаблона, который сам по себе может быть повторен неограниченное число раз, использование поэлементного группирования является единственным способом избежать ложных совпадений, которые занимают много времени. Шаблон

```
(\D+|<\d+>)*[!?]
```

соответствует неограниченному количеству подстрок, которые либо состоят из не цифр, либо цифры в них заключены в угловые скобки <>, за которыми следует либо восклицательный знак !, либо вопросительный ?. При обнаружении совпадения процесс происходит быстро. Однако применительно к

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

уйдет много времени, пока будет сделано заключение о несоответствии. Происходит это в силу того, что строка может быть разделена многими различными способами между внутренним повторением \D+ и внешним повторением *, и они все должны быть перебраны. (В примере использовано [!?], что предпочтительнее, чем единичный символ в конце, потому что в PCRE есть оптимизация, которая допускает быстрое обнаружение несовпадения при использовании единичного символа. Запоминается последний единичный символ, необходимый в соответствии, и если символ не присутствует в строке, быстро возвращается результат с несовпадением.) При изменении шаблона с использованием поэлементного группирования, например:

```
((?>\D+)|<\d+>)*[!?]
```

последовательность нецифровых символов не может быть разорвана, и вывод о несоответствии делается быстро.

Обратные ссылки

Вне класса символов обратная косая черта, за которой следует цифра больше 0 (и, возможно, последующие цифры), интерпретируется как обратная ссылка на предшествующий захватывающий подшаблон при условии, что имеется соответствующее количество предшествующих открывающих круглых скобок.

Обратная косая черта всегда рассматривается как обратная ссылка, если десятичное число после нее меньше 10, и приводит к ошибке, если нет соответствующего числа открывающих скобок. Другими словами, для чисел меньше 10 скобки, на которые идет

ссылка, необязательно должны быть слева от ссылки. Обработка цифр после обратной косой черты подробно рассмотрена выше в подразделе "Неотображаемые символы".

Обратная ссылка сопоставляется с частью строки, захваченной соответствующим подшаблоном, но не с самим подшаблоном.

Таким образом, шаблон

```
(sens|respons)e and \1ibility
```

совпадает с "`sense and sensibility`" и "`response and responsibility`", но не с "`sense and responsibility`". В случае если обратная ссылка обнаружена во время регистрозависимого поиска, то при сопоставлении обратной ссылки регистр также учитывается. Например,

```
((?i)rah)\s+\1
```

совпадает с "`rah rah`" и "`RAH RAH`", но не "`RAH rah`", хотя основной захватывающий подшаблон сопоставляется без учета регистра.

Обратные ссылки к названным подшаблонам используют синтаксис Python `(?P=name)`. Пример, приведенный выше, можно переписать следующим образом:

```
(?(?i)rah)\s+(?P=p1)
```

К одному и тому же подшаблону может быть больше одной обратной ссылки. Если подшаблон фактически не использован в каком-либо сопоставлении, любая обратная ссылка к нему всегда приводит к неудаче. Например, шаблон

```
(a|(bc))\2
```

всегда терпит неудачу, если находит соответствие с "`a`" раньше, чем с "`bc`". Поскольку в шаблоне может присутствовать множество захватывающих скобок, все цифры, следующие за обратной косой чертой, рассматриваются как часть потенциальной обратной ссылки.

Если за ссылкой должна следовать цифра, необходимо использовать ограничитель обратной ссылки. Если установлена

опция PCRE_EXTENDED, этим ограничителем может быть символ пробела. В противном случае можно использовать пустой комментарий.

Ссылка на подшаблон, внутри которого она расположена, всегда терпит неудачу, если это первое сопоставление текущего подшаблона. Например, (a\1) не будет ничему соответствовать. Однако такие ссылки могут быть полезны внутри повторяющихся подшаблонов. Например, шаблон

```
(a|b\1)+
```

соответствует любому количеству "a" и "aba", "ababbaa" и т.д. При каждой итерации шаблона обратная ссылка соответствует той части строки, которая была захвачена при предыдущей итерации. Чтобы это работало, шаблон должен быть построен так, чтобы при первой итерации сопоставления с обратной ссылкой не проводилось. Этого можно достичь использованием чередования, как в предыдущем примере, или квантификатора с минимумом, равным нулю.

Утверждения

Утверждение это проверка символов, идущих до или после текущей позиции сопоставления, которая не затрагивает каких-либо символов из строки темы. Простые утверждения \b, \B, \A, \G, \Z, \z, ^ и $ описаны выше.

Более сложные утверждения программируются как подшаблоны двух видов: те, которые анализируют текст, предшествующий текущей позиции (утверждения с просмотром вперед), и те, которые анализируют текст, идущий после нее (утверждения с просмотром назад). Подшаблоны утверждения сопоставляются обычным способом, за исключением того, что они не вызывают изменения текущей позиции поиска.

Подшаблоны утверждения не являются захватывающими и не могут повторяться, так как не имеет смысла несколько раз утверждать одно и то же. Если захватывающие подшаблоны содержатся в каком-либо утверждении, они подсчитываются для

нумерации захватывающих подшаблонов во всем шаблоне. Вместе с тем, захват подстрок производится только для положительных утверждений, так как это не имеет смысла для отрицательных утверждений.

Утверждения с просмотром вперед

Утверждения с просмотром вперед начинаются с `(?=` для положительных утверждений и с `(?!` для отрицательных утверждений. Например,

```
\w+(?=;)
```

соответствует слову, за которым идет точка с запятой, но не включает точку с запятой в соответствие, а

```
foo(?!bar)
```

соответствует любому найденному "`foo`", за которым не следует "`bar`". Следует учесть, что явно схожий шаблон

```
(?!foo)bar
```

не будет искать вхождение "`bar`", перед которым стоит не "`foo`", а просто будет искать любое "`bar`", так как утверждение `(?!foo)` всегда верно, если следующие три символа "`bar`". Для достижения обратного эффекта необходимо утверждение с просмотром назад.

Если необходимо вызвать остановку поиска в какой-то точке шаблона, удобнее всего использовать `(?!)`, потому что пустая строка всегда сопоставляется и, таким образом, утверждение, требующее, чтобы пустой строки не было, всегда терпит неудачу.

Утверждения с просмотром назад

Утверждения с просмотром назад начинаются с `(?<=` для положительных утверждений и с `(?<!` для отрицательных утверждений. Например,

```
(?<!foo)bar
```

не находит вхождение "bar", перед которым не следует "foo". Содержимое утверждений с просмотром назад ограничено таким образом, что все строки, которым они соответствуют, должны иметь фиксированную длину. Однако, если существует несколько вариантов, им необязательно быть одной и той же фиксированной длины, таким образом,

```
(?<=bullock|donkey)
```

допускается, но

```
(?<!dogs?|cats?)
```

приводит к ошибке. Ветви, совпадающие со строками разной длины, допускаются только на верхнем уровне утверждения с просмотром назад. Утверждение

```
(?<=ab(c|de))
```

не допускается, так как его единственная верхнего уровня может соответствовать двум различным длинам, но допускается, если его переписать таким образом, чтобы использовались две ветви верхнего уровня:

```
(?<=abc|abde)
```

Утверждения с просмотром назад реализованы так, что для каждого варианта текущая позиция временно переносится назад, на фиксированную ширину, после чего выполняется поиск соответствия условию. Если перед текущей позицией недостаточно символов, совпадений обнаружено не будет.

В PCRE не допускается экранирование последовательностью \C в утверждениях с просмотром назад, потому что невозможно высчитать длину просмотра назад. Экранирование последовательностью \X, которая может соответствовать различному количеству байтов, также не допускается.

Поэлементные группы могут использоваться совместно с утверждениями с просмотром назад для обозначения эффективных сопоставлений в конце строки темы. Рассмотрим простой шаблон

```
abcd$
```

в применении к длинной строке, не соответствующей указанной маске. Так как процесс поиска соответствия осуществляется слева направо, PCRE просмотрит каждое "a" в теме и только потом будет анализировать следующие записи в шаблоне. Если шаблон задан как

```
^.*abcd$
```

сначала .* сопоставляется со всей строкой, но когда это сопоставление терпит неудачу (так как далее не следует никакого "a"), производится сопоставление со всеми символами, кроме последнего, затем кроме последних двух и т.д. В конечном итоге поиск "a" захватывает всю строку, справа налево, что ничем не лучше предыдущего поиска. Однако, если шаблон записать в виде

```
^(?>.*)(?<=abcd)
```

или, что то же самое, с использованием синтаксиса притяжательного квантификатора

```
^.*+(?<=abcd)
```

повторное сопоставление для символа .* не выполняется; он может соответствовать только всей строке целиком. Последующее утверждение с просмотром назад только однократно проверяет последние четыре символа. Если проверка терпит неудачу, сразу же терпит неудачу и все сопоставление. При анализе длинных строк разница по времени значительна.

Использование многочисленных утверждений

Количество следующих друг за другом утверждений (любого порядка) не ограничено. Например,

```
(?<=\d{3})(?<!999)foo
```

соответствует "foo", перед которым находятся три цифры, но не "999". Заметьте, что каждое из утверждений применяется самостоятельно в одной и той же позиции в строке темы. Сначала проводится проверка того, являются ли три предыдущие символа цифрами, а затем проверяется, не являются ли эти три цифры

"999". Этот шаблон не сопоставляется с "foo", перед которым расположены 6 символов, первые из которых являются цифрами, а последние три не являются "999". Например, он не сопоставляется с "123abc-foo". Для этого требуется следующий шаблон

```
(?<=\d{3}...)(?<!999)foo
```

Здесь первое утверждение просматривает предыдущие шесть символов, проверяя, являются ли первые три цифрами, а затем второе утверждение проверяет, не являются ли предшествующие три цифры "999".

Утверждения могут быть вложены в любой комбинации. Например,

```
(?<=(?<!foo)bar)baz
```

сопоставляет вхождение "baz", перед которым находится "bar", перед которым, в свою очередь, не стоит "foo", тогда как

```
(?<=\d{3}(?!999)...)foo
```

это другой шаблон, который соответствует "foo", перед которым находятся три цифры и любые три символа, не являющиеся "999".

Условные подшаблоны

Процесс поиска соответствия можно подчинить условию или выбрать из двух альтернативных подшаблонов в зависимости от результата утверждения или успеха сопоставления с предыдущим захватывающим подшаблоном. Существует две возможные формы условных шаблонов

```
(?(condition)yes-pattern)
(?(condition)yes-pattern|no-pattern)
```

Если условие удовлетворено, используется yes-шаблон, в противном случае no-шаблон (при наличии). Если в подшаблоне более двух вариантов, происходит ошибка во время компиляции.

Существует три типа условий. Если текст, заключенный в круглые скобки, состоит из последовательности цифр, условие будет удовлетворено, если захватывающему подшаблону под этим номером было ранее найдено соответствие. Число должно быть больше нуля. Рассмотрим следующий шаблон, который содержит не имеющие значения пробелы для простоты чтения (предположим, что установлена опция PCRE_EXTENDED) и разделения его на три части, чтобы упростить обсуждение:

```
( \( )?     [^()]+     (?(1) \) )
```

Первая часть соответствует факультативной открывающей круглой скобке и, если этот символ присутствует, устанавливает его как первую захваченную подстроку. Вторая часть соответствует одному или нескольким символам, не являющимся круглыми скобками. Третья часть является условным подшаблоном, который проверяет, был ли сопоставлен первый набор скобок или нет. В случае обнаружения совпадения, т.е., если текст начинался открывающей скобкой, условие будет интерпретировано как истинное, а следовательно, применяется yes-шаблон и требуется закрывающая скобка. В противном случае, так как нет no-шаблона, шаблон ничему не сопоставляется. Другими словами, этот шаблон совпадает с последовательностью не-скобок, факультативно заключенной в скобки.

Если условием является строка (R), условие считается соблюденным, если производится рекурсивный запрос к шаблону или подшаблону. В "верхнем уровне" условие ложно.

Если условием является не последовательность цифр или (R), оно должно быть утверждением. Это может быть положительное или отрицательное утверждение с просмотром вперед или с просмотром назад. Рассмотрим шаблон, в котором снова содержатся не имеющие значения пробелы с двумя вариантами во второй строке:

```
(?(?=[^a-z]*[a-z])
\d{2}-[a-z]{3}-\d{2}  |  \d{2}-\d{2}-\d{2} )
```

Условие является положительным утверждением с просмотром вперед, соответствующим необязательной последовательности

небуквенных символов, за которыми следует буква. Другими словами, происходит проверка, есть ли, по крайней мере, одна буква в теме. Если буква найдена, тема проверяется на соответствие первому варианту; в противном случае второму. Этот шаблон соответствует строкам в одной из двух форм: `dd-aaa-dd` или `dd-dd-dd`, где `aaa` буквы и `dd` цифры.

Приложение L. Формат файлов протокола

Файлы протокола **Сервера** (см. п. Ведение серверного протокола) и **Агента** ведутся в текстовом формате, где каждая строка представляет собой отдельное сообщение.

Формат строки сообщения следующий:

<год><месяц><число>
.<час><минута><секунда>.<сотые_секунды>
<тип_сообщения> [*<id_процесса>*] *<имя_потока>*
[*<источник_сообщения>*] *<сообщение>*

где:

- *<год><месяц><число>*
  .<час><минута><секунда>.<сотые_секунды> – точная дата записи сообщения в файл протокола.
- <*тип_сообщения*> – уровень протокола:
  - **ftl** (fatal error – фатальная ошибка) – сообщения о критических ошибках функционирования;
  - **err** (error – ошибка) – сообщения об ошибках функционирования;
  - **wrn** (warning – предупреждение) – предупреждения об ошибках;
  - **ntc** (notice – замечание) – важные информационные сообщения;
  - **inf** (info – информация) – информационные сообщения;
  - **tr0..3** (trace0..3 – трассировка) – трассировка происходящих действий с разной степенью детализации (**Трассировка3** – максимальный уровень детализации);
  - **db0..3** (debug0..3 – отладка) – отладочные сообщения с разной степенью детализации (**Отладка3** – максимальный уровень детализации).

Сообщения с уровнем протокола **tr0..3** (трассировка) и **db0..3** (отладка) ведутся только для разработчиков ПО **Dr. Web ESS**.

- `[<id_процесса>]` – уникальный числовой идентификатор процесса, в рамках которого выполнялся поток, записавший сообщение в файл протокола. Под некоторыми ОС `[<id_процесса>]` может быть представлен в виде `[<id_процесса> <id_потока>]`.
- *<имя_потока>* – символьное обозначение потока, в рамках которого производилась запись сообщения в файл протокола.
- `[<источник_сообщения>]` – обозначение системы, являющейся инициатором записи сообщения в файл протокола. Источник присутствует не всегда.
- *<сообщение>* – текстовое описание действий в соответствии с уровнем протокола. Может включать в себя как формальное описание сообщения, так и значения некоторых важных для конкретного случая переменных.

Например:

1) `20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS events" said OK`

где:

- `20081023` – *<год><месяц><число>*,
- `171700` – *<час><минута><секунда>*,
- `74` – *<сотые_секунды>*,
- `inf` – *<тип_сообщения>* - информационное сообщение,
- `[001316]` – [*<id_процесса>*],
- `mth:12` – *<имя_потока>*,
- `[Sch]` – [*<источник_сообщения>*] - планировщик,
- `Job "Purge unsent IS events" said OK` – *<сообщение>* о корректном выполнении задания **Удаление неотправленных событий**.

2) `20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193`

где:

- `20081028` – *<год><месяц><число>*,
- `135755` – *<час><минута><секунда>*,
- `61` – *<сотые_секунды>*,
- `inf` – *<тип_сообщения>* - информационное,
- `[001556]` – [*<id_процесса>*],
- `srv:0` – *<имя_потока>*,
- `tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193` – *<сообщение>* об установлении нового соединения через указанный сокет.

Приложение М. Описание пользовательских процедур

Для упрощения и автоматизации выполнения определенных заданий **Enterprise Сервера** возможно использование пользовательских процедур, реализованных в виде lua-скриптов. Данные скрипты должны располагаться в каталоге:

- для ОС Windows: `var\extensions`
- для ОС FreeBSD и ОС Solaris: `/var/drwcs/extensions`
- для ОС Linux: `/var/opt/drwcs/extensions`

каталога установки **Сервера**. После инсталляции **Сервера** в данном каталоге размещаются предустановленные процедуры, которые могут использоваться в процессе работы. Для возможности их исполнения **Сервер** должен быть запущен с ключом `-hooks`.

Все скрипты по умолчанию отключены. Для включения скриптов необходимо в файле скрипта удалить начальный параметр `disabled` или весь комментарий полностью (оставить пустую строку).

Каталог `extensions` содержит следующие скрипты:

- `access_check.ds` – вызывается перед проверкой доступа согласно соответствующих ACL (Access Control List - списки контроля доступа);
- `access_denied.ds` – вызывается при запрете доступа согласно настройкам ACL или результату выполнения процедуры `access_check`;
- `admin_logged.ds` – вызывается при успешной авторизации администратора в **Центре Управления**;
- `admin_noauth.ds` – вызывается при ошибке авторизации администратора в **Центре Управления**;
- `agent_status.ds` – вызывается при сообщении **Агентом** его локальных политик;

- backup.ds – вызывается после завершения резервного копирования файлов (backup), но перед удалением файлов предыдущего резервного копирования;
- bad_connection.ds – вызывается при невозможности установления соединения с клиентом;
- connection_denied.ds – вызывается при запрете нового соединения согласно ограничениям в лицензионном соглашении;
- database_load.ds – вызывается после завершения процесса загрузки драйвера базы данных;
- database_verify.ds – вызывается после завершения верификации базы данных;
- deinstallation.ds – вызывается после завершения удаления **Агента**;
- disconnected.ds – вызывается после завершения соединения с клиентом;
- group_changed.ds – вызывается при изменении настроек группы;
- group_created.ds – вызывается при создании новой группы;
- group_deleted.ds – вызывается при удалении группы;
- install.ds – вызывается при получении события installation;
- installed_components.ds – вызывается при сообщении **Агентом** списка установленных на станции компонентов;
- jobexecuted.ds – вызывается при получении от **Агента** события job executed;
- license_error.ds – вызывается в случае невозможности установления соединения с клиентом согласно ограничениям в лицензионном соглашении;
- load_plugin.ds – вызывается после загрузки подключаемого модуля (plugin-а);
- load_protocol.ds – вызывается после загрузки модуля протокола;

- neighbor_connected.ds – вызывается при соединении с **Сервером**;
- neighbor_install.ds – вызывается при получении события installation от соседнего **Сервера**;
- neighbor_noauth.ds – вызывается после отказа соединения с **Сервером** вследствие ошибки авторизации;
- neighbor_run_begin.ds – вызывается при получении события component started от соседнего **Сервера**;
- neighbor_run_end.ds – вызывается при получении события component completed от соседнего **Сервера**;
- neighbor_scan_error.ds – вызывается при получении события scan error от соседнего **Сервера**;
- neighbor_scan_statistics.ds – вызывается при получении события scan statistics от соседнего **Сервера**;
- neighbor_station_status.ds – вызывается при получении от соседнего **Сервера** локальных политик/настроек станции;
- neighbor_virus.ds – вызывается при получении события virus detected от соседнего **Сервера**;
- newbie_accepted.ds – вызывается при предоставлении доступа новичку, успешной его авторизации и создании станции в базе данных;
- newbie_came.ds – вызывается при подключении новичка;
- newbie_registered.ds – вызывается после предоставления доступа новичку, но перед занесением соответствующей информации в базу данных;
- pong.ds – вызывается при получении PONG от клиента;
- run_begin.ds – вызывается при получении события component started от **Агента**;
- run_end.ds – вызывается при получении события component completed от **Агента**;
- scan_error.ds – вызывается при получении события scan error от **Агента**;

- scan_statistics.ds – вызывается при получении события scan statistics от **Агента**;
- server_jobexecuted.ds – вызывается после выполнения задания на **Сервере**;
- server_load.ds – вызывается после загрузки бинарного файла **Сервера** для исполнения некоторых служебных функций (**Сервер** не будет обслуживать клиентов);
- server_start.ds – вызывается при запуске **Сервера** и его готовности обслуживать клиентов;
- server_terminate.ds – вызывается после завершения обслуживания клиентов **Сервером**;
- server_unload.ds – вызывается после завершения исполнения некоторых служебных функций **Сервером** (**Сервер** не обслужил клиентов);
- station_connected.ds – вызывается при удачном соединении с **Агентом**;
- station_create.ds – вызывается при завершении создания станции;
- station_date.ds – вызывается при обнаружении некорректных времени/даты у станции;
- station_deleted.ds – вызывается при удалении станции;
- station_noauth.ds – вызывается после отказа соединения с **Агентом** вследствие ошибки авторизации;
- station_update_failed.ds - вызывается после получения сообщения от **Агента** об ошибке обновления станции;
- station_update_reboot.ds - вызывается после получения сообщения от **Агента** о необходимости перезагрузки станции после обновления;
- unload_plugin.ds – вызывается при выгрузке подключаемого модуля (plugin-а);
- unload_protocol.ds – вызывается при выгрузке модуля протокола;
- virus.ds – вызывается при получении события virus detected от **Агента**;

- `virusbases.ds` – вызывается при отправке **Агентом** информации о вирусной базе данных.

Приложение N. Интеграция XML Web API и Dr.Web Enterprise Security Suite

Описание **XML Web API** приводится в руководстве **XML API для Dr.Web® Enterprise Security Suite** (см. также п. Помощь).

Применение

При интеграции **XML Web API** и **Dr.Web Enterprise Security Suite** предоставляются функции для операций с учетными записями и автоматизации процесса администрирования пользователей сервиса. Вы можете использовать его, например, при создании динамических страниц для получения от пользователя запроса и выдачи ему установочного файла.

Аутентификация

Для взаимодействия с **Enterprise Сервером** используется протокол HTTP(S). XML API принимает RESET запросы и возвращает XML. Для доступа к XML API используется Basic HTTP-аутентификация (согласно стандарту RFC 2617). При несоблюдении стандарта RFC 2617, HTTP(S) сервер не будет запрашивать учетные данные клиента (регистрационное имя и пароль администратора **Dr.Web ESS**).

Приложение О. Процедуры аутентификации администраторов

Базовая информация по аутентификации администраторов на **Enterprise Сервере** приведена в разделе Аутентификация администраторов.

Аутентификация при использовании Active Directory

Конфигурируется только разрешение использования и порядок в списке аутентификаторов: тэги `<enabled/>` и `<order/>` в `auth-ads.xml`.

Принцип работы:

1. Администратор задает имя пользователя и пароль в одном из следующих форматов:
   - `username`,
   - `domain\username`,
   - `username@domain`,
   - LDAP DN пользователя.
2. Сервер регистрируется с этим именем и паролем на доменном контроллере по умолчанию (или доменном контроллере для домена, указанного в имени пользователя).
3. Если не удалось зарегистрироваться, осуществляется переход к следующему механизму аутентификации.
4. Определяется LDAP DN зарегистрированного пользователя.
5. У объекта с вычисленным DN читается атрибут `DrWeb_Admin`. Если он установлен в `FALSE` - неуспех и переход к следующему механизму аутентификации.
6. Читается атрибут `DrWeb_AdminReadOnly`. Если он установлен в `TRUE`, администратор имеет права только на

чтение.

7. Читается атрибут `DrWeb_AdminGroupOnly`. Если он установлен в `TRUE`, администратор имеет права только на управление определенными группами.
8. Читается атрибут `DrWeb_AdminGroup`, который должен содержать список групп для управления данным администратором.
9. Если на этом этапе какие-либо атрибуты не определены, их поиск осуществляется в группах, в которые входит данный пользователь. Для каждой группы просматриваются ее родительские группы (стратегия поиска - вглубь).

В случае любой ошибки осуществляется переход к следующему механизму аутентификации.

Утилита `drwschema-modify.exe` (входит в дистрибутив **Сервера**, располагается в каталоге `bin` каталога установки **Сервера**) создает новый класс объектов `DrWebEnterpriseUser` для Active Directory и описывает новые атрибуты для данного класса.

Атрибуты имеют следующие OID в **Enterprise** пространстве:

```
#define DrWeb_enterprise_OID      "1.3.6.1.4.1"
              // iso.org.dod.internet.private.enterprise
#define DrWeb_DrWeb_OID           DrWeb_enterprise_OID
  ".29690"      // DrWeb
#define DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID
  ".1"          // EnterpriseSuite
#define DrWeb_Alerts_OID
DrWeb_EnterpriseSuite_OID ".1"          // Alerts
#define DrWeb_Vars_OID
DrWeb_EnterpriseSuite_OID ".2"          // Vars
#define DrWeb_AdminAttrs_OID
DrWeb_EnterpriseSuite_OID ".3"          // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSu
ite.AdminAttrs.Admin)

#define DrWeb_Admin_OID           DrWeb_AdminAttrs_OID
  ".1"          // R/W admin
```

```
#define DrWeb_AdminReadOnly_OID   DrWeb_AdminAttrs_OID
  ".2"          // R/O admin
#define DrWeb_AdminGroupOnly_OID  DrWeb_AdminAttrs_OID
  ".3"          // Group admin
#define DrWeb_AdminGroup_OID      DrWeb_AdminAttrs_OID
  ".4"          // Admin's group
#define DrWeb_Admin_AttrName              "DrWebAdmin"
#define DrWeb_AdminReadOnly_AttrName
"DrWebAdminReadOnly"
#define DrWeb_AdminGroupOnly_AttrName
"DrWebAdminGroupOnly"
#define DrWeb_AdminGroup_AttrName         "DrWebAdminGroup"
```

Редактирование свойств пользователей Active Directory осуществляется вручную на сервере Active Directory (см. п. Аутентификация администраторов).

Алгоритм разбора атрибутов при авторизации:

1. Читаются атрибуты пользователя.
2. Если атрибут `DrWebAdmin` установлен в `TRUE`, то:
   2.1. Если не хватает части атрибутов и атрибут `DrWebInheritPermissions` установлен в `TRUE`, то недостающие атрибуты считываются из групп. Как только все атрибуты заданы - процедура обхода групп завершается. Таким образом, чем раньше были считаны атрибуты, тем больше у них приоритет. Доступ администратору разрешается.
   2.2. Если не хватает части атрибутов и атрибут `DrWebInheritPermissions` установлен в `FALSE` (или не определен), доступ администратору разрешается.
   2.3. Если все атрибуты заданы, доступ администратору разрешается.
3. Если атрибут `DrWebAdmin` установлен в `FALSE`, доступ администратору запрещается.
4. Если атрибут `DrWebAdmin` не задан, то:
   4.1. Если атрибут `DrWebInheritPermissions` принимает значение `TRUE`, то считываются атрибуты из групп. Далее аналогично шагу 2.

4.2. Если атрибут `DrWebInheritPermissions` принимает значение `FALSE` (или не задан) аналогично шагу 3.

Аутентификация при использовании LDAP

Настройки приводятся в файле конфигурации `auth-ldap.xml`.

Основные теги конфигурационного файла:

- `<enabled/>` и `<order/>` - аналогично варианту для Active Directory.
- `<server/>` задает адрес LDAP-сервера.
- `<user-dn/>` определяет правила трансляции имен в DN с использованием DOS-подобных масок.

  В теге `<user-dn/>` допускается использование символов подстановки:

  - `*` заменяет последовательность любых символов кроме `.` `,` `=` `@` `\` и пробелов;
  - `#` заменяет последовательность любых символов.
- `<user-dn-expr/>` определяет правила трансляции имен в DN с использованием регулярных выражений.

  Например, одно и то же правило в разных вариантах:

```
<user-dn          user="*@example.com"          dn="CN=\1,DC=example,DC=com"/>
<user-dn-expr     user="(.*)@example.com"       dn="CN=\1,DC=example,DC=com"/>
```

  `\1` .. `\9` определяют место подстановки в шаблоне значений *, # или выражений в скобках.

  Исходя из данного принципа: если указано имя пользователя в виде `login@example.com`, то после трансляции получится DN: "`CN=login,DC=example,DC=com`".

- `<user-dn-extension-enabled/>` разрешает выполнение Lua-скрипта `ldap-user-dn-translate.ds` (из каталога `extensions`) для выполнения трансляции имени

пользователя в DN. Данный скрипт выполняется после попыток применения всех правил `user-dn`, `user-dn-expr` в случае, если не найдено ни одно подходящее правило. У скрипта один параметр - введенное имя пользователя. Скрипт возвращает строку, содержащую либо DN, либо ничего. В случае, если не подошло ни одно правило и скрипт не разрешен или не вернул ничего, то введенное имя пользователя используется как есть.

- Атрибуты LDAP-объекта для DN, полученного в результате трансляции, и их возможные значения могут быть переопределены тэгами (указаны значения по умолчанию):

```
  <!-- DrWebAdmin attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.1) -->
  <admin-attribute-name value="DrWebAdmin" true-
value="^TRUE$" false-value="^FALSE$"/>

  <!-- DrWebAdminGroupOnly attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.2) -->
  <readonly-admin-attribute-name
value="DrWebAdminReadOnly"  true-value="^TRUE$" false-
value="^FALSE$"/>

  <!-- DrWebAdminGroupOnly attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.3) -->
  <grouponly-admin-attribute-name
value="DrWebAdminGroupOnly" true-value="^TRUE$" false-
value="^FALSE$"/>

  <!-- DrWebAdminGroup attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.4) -->
  <groups-admin-attribute-name
value="DrWebAdminGroup"/>
```

В качестве значений параметров `true-value`/`false-value` задаются регулярные выражения.

- Если остались неопределенные значения атрибутов администратора, то в случае задания в конфигурационном файле тэга `<group-reference-attribute-name value="memberOf"/>`, значение атрибута memberOf рассматривается как список DN групп, в которые входит данный администратор, и поиск нужных атрибутов по этим группам ведется также, как в случае с использованием Active Directory.

Приложение Р. Лицензии

В данном разделе приведен список сторонних программных библиотек, которые используются ПО **Dr.Web ESS**, информация по их лицензированию и адреса проектов разработки.

Сторонняя библиотека	Лицензия	URL проекта
boost	http://www.boost.org/users/license.html*	http://www.boost.org/
c-ares	MIT License*	http://c-ares.haxx.se/
Gecko SDK	Mozilla Public License* GNU Lesser General Public License* GNU General Public License*	https://developer.mozilla.org/ru/docs/Gecko_SDK
jQuery	MIT License* GNU General Public License*	http://jquery.com/
libcurl	http://curl.haxx.se/docs/copyright.html*	http://curl.haxx.se/libcurl/
libradius	© Juniper Networks, Inc.*	http://www.freebsd.org
libxml2	MIT License*	http://www.xmlsoft.org/
lua	MIT License*	http://www.lua.org/
lua-xmlreader	MIT License*	http://asbradbury.org/projects/lua-xmlreader/
md5 implementation	© WIDE Project*	–
Net-snmp	http://www.net-snmp.org/about/license.html*	http://www.net-snmp.org/
OpenLDAP	http://www.openldap.org/software/release/license.html*	http://www.openldap.org
OpenSSL	http://www.openssl.org/source/license.html*	http://www.openssl.org/

Сторонняя библиотека	Лицензия	URL проекта
Oracle Instant Client	http://www.oracle.com/technetwork/licenses/instant-client-lic-152016.html*	http://www.oracle.com
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
Prototype JavaScript framework	MIT License*	http://prototypejs.org/assets/2009/8/31/prototype.js
Regina Rexx Interpreter	GNU Lesser General Public License*	http://regina-rexx.sourceforge.net/
sha2 implementation	© Dr. Brian Gladman, Worcester, UK*	–
SQLite	Public Domain (http://www.sqlite.org/copyright.html)	http://www.sqlite.org/
wtl	Common Public License (http://opensource.org/licenses/cpl1.0.php)*	http://sourceforge.net/projects/wtl/
XML/SWF Charts	Bulk License (http://maani.us/xml_charts/index.php?menu=Buy)	http://www.maani.us/xml_charts/index.php?menu=Introduction
zlib	http://www.zlib.net/zlib_license.html*	http://www.zlib.net/

* - тексты лицензий приведены далее.

P1. Boost

```
Boost Software License - Version 1.0 - August 17th, 2003


Permission is hereby granted, free of charge, to any
person or organization obtaining a copy of the software
and accompanying documentation covered by this license
```

(the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

P2. Curl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

P3. Libradius

Copyright 1998 Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3 2012/04/21 18:30:48 melifaro Exp $

P4. MD5 implementation

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,

```
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.
```

P5. Net-snmp

```
Various copyrights apply to this package, listed in
various separate parts below. Please make sure that you
read all the parts.


---- Part 1: CMU/UCD copyright notice: (BSD like) -----


          Copyright 1989, 1991, 1992 by Carnegie Mellon
University


       Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University
of California


       All Rights Reserved


Permission to use, copy, modify and distribute this
software and its documentation for any purpose and
without fee is hereby granted, provided that the above
copyright notice appears in all copies and that both
that copyright notice and this permission notice appear
in supporting documentation, and that the name of CMU
and The Regents of the University of California not be
used in advertising or publicity pertaining to
distribution of the software without specific written
permission.
```

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND

CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above

copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

```
*   Redistributions in binary form must reproduce the
above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other
materials provided with the distribution.


*   Neither the name of ScienceLogic, LLC nor the names
of its contributors may be used to endorse or promote
products derived from this software without specific
prior written permission.


THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL
THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT,   STRICT   LIABILITY,   OR   TORT   (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.
```

P6. OpenLDAP

```
The OpenLDAP Public License

  Version 2.8, 17 August 2003


Redistribution and use of this software and associated
documentation     ("Software"),     with     or     without
modification, are permitted provided that the following
conditions are met:


1. Redistributions in source form must retain copyright
statements and notices,
```

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following

disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR (S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

```
OpenLDAP is a registered trademark of the OpenLDAP
Foundation.


Copyright 1999-2003 The OpenLDAP Foundation, Redwood
City,

California, USA.  All Rights Reserved.  Permission to
copy and

distribute verbatim copies of this document is granted.
```

P7. OpenSSL

```
LICENSE ISSUES

  ==============


  The OpenSSL toolkit stays under a dual license, i.e.
both the conditions of the OpenSSL License and the
original SSLeay license apply to the toolkit.

  See below for the actual license texts. Actually both
licenses are BSD-style Open Source licenses. In case of
any license issues related to OpenSSL please contact
openssl-core@openssl.org.


  OpenSSL License

  ---------------


 ================================================

  Copyright (c) 1998-2011 The OpenSSL Project.  All
rights reserved.


  Redistribution and use in source and binary forms,
with or without modification, are permitted provided
that the following conditions are met:
```

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young

(eay@cryptsoft.com). This product includes software written by Tim

Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

```
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.


  The licence and distribution terms for any publically
available version or derivative of this code cannot be
changed.  i.e. this code cannot simply be copied and put
under another distribution licence

  [including the GNU Public Licence.]
```

P8. Oracle Instant Client

```
Export Controls on the Programs

Selecting the "Accept License Agreement" button is a
confirmation of your agreement that you comply, now and
during the trial term, with each of the following
statements:


-You are not a citizen, national, or resident of, and
are not under control of, the government of Cuba, Iran,
Sudan, Libya, North Korea, Syria, nor any country to
which the United States has prohibited export.

-You will not download or otherwise export or re-export
the Programs, directly or indirectly, to the above
mentioned countries nor to citizens, nationals or
residents of those countries.

-You are not listed on the United States Department of
Treasury lists of Specially Designated Nationals,
Specially Designated Terrorists, and Specially
Designated Narcotic Traffickers, nor are you listed on
the United States Department of Commerce Table of Denial
Orders.


You will not download or otherwise export or re-export
the Programs, directly or indirectly, to persons on the
above mentioned lists.


You will not use the Programs for, and will not allow
```

the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle®'s Global Trade Compliance web site (http://www.oracle.com/products/export).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the

Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at http://www.oracle.com/technetwork/indexes/documentation/index.html.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights

in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:

-use the Programs for any purpose other than as provided above;

-charge your end users for use of the Programs;

-remove or modify any Program markings or any notice of our proprietary rights;

-assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;

-cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;

-disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at http://www.oracle.com/products/export/index.html. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply

with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/ licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 01/24/08

Should you have any questions concerning this License Agreement, or if you desire to contact Oracle for any reason, please write:

Oracle America, Inc.

500 Oracle Parkway,

Redwood City, CA 94065

Oracle may contact you to ask if you had a satisfactory experience installing and using this OTN software download.

P9. PCRE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are

```
both optional features that can be omitted when the
library is built.


THE BASIC LIBRARY FUNCTIONS

---------------------------


Written by:       Philip Hazel

Email local part: ph10

Email domain:     cam.ac.uk


University of Cambridge Computing Service,

Cambridge, England.


Copyright (c) 1997-2013 University of Cambridge

All rights reserved.


PCRE JUST-IN-TIME COMPILATION SUPPORT

-------------------------------------


Written by:       Zoltan Herczeg

Email local part: hzmester

Emain domain:     freemail.hu


Copyright(c) 2010-2013 Zoltan Herczeg

All rights reserved.


STACK-LESS JUST-IN-TIME COMPILER

--------------------------------
```

```
Written by:       Zoltan Herczeg

Email local part: hzmester

Emain domain:     freemail.hu


Copyright(c) 2009-2013 Zoltan Herczeg

All rights reserved.


THE C++ WRAPPER FUNCTIONS

-------------------------


Contributed by:   Google Inc.


Copyright (c) 2007-2012, Google Inc.

All rights reserved.


THE "BSD" LICENCE

-----------------


Redistribution and use in source and binary forms, with
or without modification, are permitted provided that the
following conditions are met:


     * Redistributions of source code must retain the
above copyright notice, this list of conditions and the
following disclaimer.


    * Redistributions in binary form must reproduce the
above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other
materials provided with the distribution.
```

```
     * Neither the name of the University of Cambridge
nor the name of Google Inc. nor the names of their
contributors may be used to endorse or promote products
derived from this software without specific prior
written permission.


THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.
```

P10. Sha2 implementation

```
        Copyright (c) 2001, Dr Brian Gladman
<brg@gladman.me.uk>, Worcester, UK.

   All rights reserved.


   TERMS


    Redistribution and use in source and binary forms,
with or without modification, are permitted subject to
the following conditions:


    1. Redistributions of source code must retain the
above copyright notice, this list of conditions and the
following disclaimer.
```

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission.

This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

This is a byte oriented version of SHA256 that operates on arrays of bytes stored in memory. The operation uses a type 'sha256_ctx' to hold details of the current hash state and uses the following three calls:

void sha256_begin(sha256_ctx ctx[])

void sha256_hash(const unsigned char data[], unsigned long len, sha256_ctx ctx[])

void sha256_end(unsigned char hval[], sha256_ctx ctx[])

The first subroutine initialises a hash computation by setting up the context in the sha256_ctx context.

The second subroutine hashes 8-bit bytes from array data[] into the hash state withinh sha256_ctx context, the number of bytes to be hashed being given by the the unsigned long integer len.

The third subroutine completes the hash calculation and places the resulting digest value in the array of 8-bit bytes hval[]

```
    This implementation of SHA256 also supports SHA384
and SHA512 but these hash functions depend on the use of
64-bit long integers and are not very efficient on 32-
bit machines. This code is NOT recommended for these
hash functions.


     My thanks to Erik Andersen <andersen@codepoet-
consulting.com> for testing this code on big-endian
systems and for his assistance with corrections
```

P11. Wtl

```
Common Public License Version 1.0


THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF
THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE,
REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES
RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.


1. DEFINITIONS


"Contribution" means:


a) in the case of the initial Contributor, the initial
code and documentation distributed under this Agreement,
and


b) in the case of each subsequent Contributor:


i) changes to the Program, and


ii) additions to the Program;
```

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive,

worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form.

This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably

allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those

damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent (s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the

intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

P12. Zlib

zlib.h -- interface of the 'zlib' general purpose compression library

version 1.2.8, April 28th, 2013

Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

P13. MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

P14. GNU General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if

you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To

prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code

form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf,

under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are

being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if

neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a

statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for

the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the

conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be

used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an

absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

P15. GNU Lesser General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a

class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a

reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of

this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

P16. Mozilla Public License

Version 2.0

1. Definitions

1.1. “Contributor”

means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. “Contributor Version”

means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor’s Contribution.

1.3. “Contribution”

means Covered Software of a particular Contributor.

1.4. “Covered Software”

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. “Incompatible With Secondary Licenses”

means

that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. “Executable Form”

means any form of the work other than Source Code Form.

1.7. “Larger Work”

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. “License”

means this document.

1.9. “Licensable”

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. “Modifications”

means any of the following:

any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

any new file in Source Code Form that contains any Covered Software.

1.11. “Patent Claims” of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made,

import, or transfer of either its Contributions or its Contributor Version.

1.12. “Secondary License”

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. “Source Code Form”

means the form of the work preferred for making modifications.

1.14. “You” (or “Your”)

means an individual or a legal entity exercising rights under this License. For legal entities, “You” includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

for any code that a Contributor has removed from Covered Software; or

for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for,

warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence

to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party’s ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - “Incompatible With Secondary Licenses” Notice

This Source Code Form is “Incompatible With Secondary Licenses”, as defined by the Mozilla Public License, v. 2.0.

Часто задаваемые вопросы

Перенос Сервера Dr.Web Enterprise Server на другой компьютер (для ОС Windows®)

Для переноса Сервера Dr.Web Enterprise Server (при установке аналогичной версии Dr.Web Enterprise Server) под ОС Windows:

1. Остановите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server).
2. Запустите из командной строки файл `drwcsd.exe` с ключом `exportdb` для экспорта содержимого базы данных в файл. Полная командная строка для экспорта в версии под ОС Windows будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin
   \drwcsd.exe" exportdb <путь_к_файлу>
   ```

3. Сохраните содержимое директории `C:\Program Files\DrWeb Enterprise Server\etc`, а также ключ `drwcsd.pub` из `C:\Program Files\DrWeb Enterprise Server\Installer`.
4. Удалите **Сервер**.
5. Установите новый **Сервер** (пустой, с новой базой) на нужном компьютере. Остановите службу **Dr.Web Enterprise Server** с помощью средств управления службами ОС Windows или с помощью **Центра Управления**.
6. Скопируйте содержимое сохраненного ранее каталога `etc` в `C:\Program Files\DrWeb Enterprise Server\etc`, а также ключ `drwcsd.pub` в `C:\Program Files\DrWeb Enterprise Server\Installer`.
7. Запустите из командной строки файл `drwcsd.exe` с

ключом importdb для импорта содержимого базы данных из файла. Полная командная строка для импорта в версии под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" importdb <путь_к_файлу>
```

8. Запустите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server).

При использовании внутренней базы данных можно не производить экспорт и импорт БД, а просто сохранить файл внутренней базы dbinternal.dbs и заменить новый файл БД на установленном **Сервере** старым файлом, сохраненным от предыдущего **Сервера**.

Для переноса Сервера Dr.Web Enterprise Server (при установке другой версии Dr.Web Enterprise Server) под ОС Windows:

1. Остановите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server).
2. Сохраните базу данных средствами SQL сервера (если используется внутренняя БД, то просто сохраните файл dbinternal.dbs).
3. Сохраните содержимое директории C:\Program Files\DrWeb Enterprise Server\etc, а также ключ drwcsd.pub из C:\Program Files\DrWeb Enterprise Server\Installer.
4. Удалите **Сервер**.
5. Установите новый **Сервер** (пустой, с новой базой) на нужном компьютере. Остановите службу **Dr.Web Enterprise Server** с помощью средств управления службами ОС Windows или с помощью **Центра Управления**.
6. Скопируйте содержимое сохраненного ранее каталога etc в C:\Program Files\DrWeb Enterprise Server\etc, а также ключ drwcsd.pub в C:\Program Files\DrWeb Enterprise Server\Installer.

7. Восстановите базу данных на новом **Сервере**, укажите в конфигурационном файле `drwcsd.conf` путь до базы данных.
8. Запустите из командной строки файл `drwcsd.exe` с ключом `upgradedb` для обновления базы данных. Полная командная строка для импорта в версии под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" upgradedb "C:\Program Files
\DrWeb Enterprise Server\update-db"
```

9. Запустите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server).

В случае смены IP-адреса Сервера при переносе:

1. Осуществите перенос **Сервера** согласно соответствующей процедуре, описанной выше.
2. У всех **Агентов**, которых обслуживал переносимый **Сервер**, задайте в настройках адрес нового **Сервера** (см. п. Подключение Агента Dr.Web Enterprise Agent к другому Серверу Dr.Web Enterprise Server).
3. Для возможности перехода **Агентов**, для которых адрес нового **Сервера** указывался через **Центр Управления**, а не в настройках самого **Агента** на станции, оставьте включенными оба **Сервера** (на обоих **Серверах** в настройках **Агента** должен быть указан адрес нового **Сервера**) до тех пор, пока все **Агенты** не подключатся к старому **Серверу** для получения нового IP-адреса и не перейдут на новый **Сервер**.

Подключение Агента Dr.Web Enterprise Agent к другому Серверу Dr.Web Enterprise Server

При подключении **Агента** к другому **Серверу** все действия на станции необходимо выполнять с правами администратора ОС.

Для переключения Dr.Web Enterprise Agent на другой Dr.Web Enterprise Server необходимо:

1. Если открытый ключ шифрования `drwcsd.pub` с нового **Сервера** не совпадает с ключом шифрования старого **Сервера**, необходимо заменить данный ключ на **Агенте**:
   1.1. Если на компьютере с **Агентом** включена самозащита, то необходимо отключить компонент **SelfPROtect** через настройки **Агента** (для этого необходимы права администратора на станции и права на отключение самозащиты, устанавливаемые на **Сервере**).
   1.2. Скопировать в каталог установки **Агента** открытый ключ шифрования `drwcsd.pub` с нового **Сервера**.
2. Изменить адрес **Сервера** в настройках **Агента**:
   - Через **Центр Управления** (у старого **Сервера**): пункт **Антивирусная сеть** главного меню → пункт **Dr.Web Enterprise Agent для Windows** управляющего меню → вкладка **Сеть** → поле **Сервер**.
   - Непосредственно на станции: при помощи пункта контекстного меню **Агента** **Настройки** → **Соединение** → поле **Сервер**.
3. Перевести станцию в новички (сбросить параметры соединения с **Сервером**):

- Через **Центр Управления** (у нового **Сервера**): пункт **Администрирование** главного меню → пункт **Конфигурация Dr.Web Enterprise Server** управляющего меню → вкладка **Общие** → установить флаг **Переводить неавторизованных в новички**.
- Непосредственно на станции: при помощи пункта контекстного меню **Агента** **Настройки** → **Соединение** → кнопка **Новичок**.

4. Перезапустить **Агента** (см. п. Dr.Web Enterprise Agent).

В случае, если для станции не установлены права на изменение настроек Dr.Web Enterprise Agent, используйте следующую процедуру:

1. Если открытый ключ шифрования `drwcsd.pub` с нового **Сервера** не совпадает с ключом шифрования старого **Сервера**, необходимо заменить данный ключ на **Агенте**:
   1.1. Если на компьютере с **Агентом** включена самозащита, то необходимо отключить компонент **SelfPROtect** через настройки **Агента** (для этого необходимы права администратора на станции и права на отключение самозащиты, устанавливаемые на **Сервере**).
   1.2. Скопировать в каталог установки **Агента** открытый ключ шифрования `drwcsd.pub` с нового **Сервера**.
2. Задать настройки **Агента** при помощи следующей команды:

   ```
   drwagntd -save <new_server_ip>
   ```

   где *<new_server_ip>* - адрес нового **Сервера**, к которому должен подключиться **Агент**. Адрес задается в формате сетевых адресов.
3. Перезапустить **Агента** (см. п. Dr.Web Enterprise Agent).

Смена типа СУБД Dr.Web Enterprise Security Suite

Для ОС Windows

1. Остановите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server).
2. Запустите файл `drwcsd.exe` с ключом `exportdb` для экспорта содержимого базы данных в файл. Полная командная строка для экспорта в версии под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all exportdb D:\esbase.es
```

   В данном примере подразумевается, что **Dr.Web Enterprise Server** установлен в каталоге `C:\Program Files\DrWeb Enterprise Server`, а экспорт базы производится в некий файл `esbase.es` в корне диска `D`. Скопируйте эту строчку (это одна строка) через буфер обмена в `cmd`-файл и выполните его.

   Если в пути к файлу присутствуют пробелы и/или национальные символы (или имя файла содержит пробелы и/или национальные символы), то путь нужно заключить в кавычки: `"D:\<`*длинное имя*`>\esbase.es"`.

3. Запустите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server), подключите к нему **Центр Управления** и перенастройте **Сервер** на использование другой СУБД. Откажитесь от предложения перезапустить **Сервер**.
4. Остановите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server).

5. Запустите файл `drwcsd.exe` с ключом `initdb` для инициализации новой базы данных. Строка инициализации базы данных для версии **Сервера** под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all initdb D:\Keys\agent.key - -
<пароль>
```

   Подразумевается, что **Сервер** установлен в каталоге `"C:\Program Files\DrWeb Enterprise Server"`, а агентский ключ `agent.key` лежит в `D:\Keys`. Скопируйте эту строчку (это одна строка) через буфер обмена в `cmd`-файл и выполните его.

   Если в пути к файлу присутствуют пробелы и/или национальные символы (или имя файла содержит пробелы и/или национальные символы), то путь к ключу нужно заключить в кавычки: `"D:\`*<длинное имя>*`\agent.key"`.

6. Запустите файл `drwcsd.exe` с ключом `importdb` для импорта содержимого базы данных из файла. Полная командная строка для импорта в версии под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all importdb D:\esbase.es"
```

   Скопируйте эту строчку (это одна строка) через буфер обмена в cmd-файл и выполните его.

7. Запустите службу **Dr.Web Enterprise Server** (см. п. Запуск и останов Dr.Web Enterprise Server).

Для ОС семейства UNIX

1. Остановите службу **Dr.Web Enterprise Server** с помощью скрипта:
   - для ОС **Linux** и ОС **Solaris**:

     ```
     /etc/init.d/drwcsd stop
     ```

   - для ОС **FreeBSD**:

     ```
     /usr/local/etc/rc.d/drwcsd.sh stop
     ```

   или с помощью **Центра Управления** (кроме ОС Solaris).

2. Запустите **Сервер** с ключом `exportdb` для экспорта содержимого базы данных в файл. Командная строка из каталога установки **Сервера** будет выглядеть примерно так:
   - для ОС **Linux**:

     ```
     "/etc/init.d/drwcsd exportdb /var/opt/
     drwcs/esbase.es"
     ```

   - для ОС **Solaris**:

     ```
     "/etc/init.d/drwcsd exportdb /var/drwcs/
     etc/esbase.es"
     ```

   - для ОС **FreeBSD**:

     ```
     "/usr/local/etc/rc.d/drwcsd.sh exportdb /
     var/drwcs/esbase.es"
     ```

   В данном примере подразумевается, что экспорт базы производится в файл `esbase.es`, расположенный в каталоге пользователя.

3. Запустите службу **Dr.Web Enterprise Server** с помощью скрипта:
   - для ОС **Linux** и ОС **Solaris**:

     ```
     /etc/init.d/drwcsd start
     ```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh start
```

подключите к нему **Центр Управления** и перенастройте **Сервер** на использование другой СУБД: в меню **Администрирование** → пункт **Конфигурация Dr.Web Enterprise Server** → вкладка **База данных**.

Перенастройку **Сервера** на использование другой СУБД также можно осуществить, отредактировав напрямую конфигурационный файл **Сервера** `drwcsd.conf`. Для этого следует закомментировать/удалить запись о текущей БД и прописать новую базу (подробнее см. Приложение G1. Конфигурационный файл Dr.Web Enterprise Server).

Откажитесь от предложения перезапустить **Сервер**.

4. Остановите **Dr.Web Enterprise Server** (см. шаг **1**).
5. Запустите файл `drwcsd` с ключом `initdb` для инициализации новой базы данных. Строка инициализации будет выглядеть примерно так:
   - для ОС **Linux** и ОС **Solaris**:

     ```
     /etc/init.d/drwcsd initdb
     ```

   - для ОС **FreeBSD**:

     ```
     /usr/local/etc/rc.d/drwcsd.sh initdb
     ```

6. Запустите файл `drwcsd` с ключом `importdb` для импорта содержимого базы данных из файла. Командная строка для импорта будет выглядеть примерно так:
   - для ОС **Linux**:

     ```
     "/etc/init.d/drwcsd importdb /var/opt/
     drwcs/esbase.es"
     ```

   - для ОС **Solaris**:

     ```
     "/etc/init.d/drwcsd importdb /var/drwcs/
     etc/esbase.es"
     ```

   - для ОС **FreeBSD**:

```
"/usr/local/etc/rc.d/drwcsd.sh importdb /
var/drwcs/esbase.es"
```

7. Запустите **Dr.Web Enterprise Server** (см. шаг **3**).

Если при запуске скрипта **Сервера** требуется задать параметры (например, указать каталог установки **Сервера**, изменить уровень подробности лога и т.п.), изменение соответствующих значений производится в стартовом скрипте:

- для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh
```

- для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd
```

Восстановление БД Dr.Web Enterprise Security Suite

В процессе работы **Enterprise Сервер** регулярно выполняет резервное копирование ценной информации (содержимого базы данных, лицензионного ключевого файла **Сервера**, закрытого ключа шифрования, конфигурационного файла **Сервера** и **Центра Управления**). Резервные копии сохраняются в следующих каталогах относительно рабочего каталога **Сервера**:

- для ОС **Windows**: `\var\Backup`
- для ОС **Linux**: `/var/opt/drwcs/backup`
- для ОС **FreeBSD** и **Solaris**: `/var/drwcs/backup`

Для этого в расписание **Сервера** включено ежедевное задание, выполняющее эту фунцию. Если такое задание в расписании отсутствует, рекомендуется создать его.

Резервные копии сохраняются в формате `.dz`, совместимом с `gzip` и другими архиваторами. После распаковки все файлы, кроме содержимого БД, готовы к использованию. Содержимое БД, сохраненное в резервной копии, можно импортировать в рабочую БД **Сервера** при помощи ключа `importdb` и таким образом восстановить данные.

Восстановление БД для различных версий Dr.Web Enterprise Server

Восстановить БД можно только из резервной копии, созданной при помощи **Сервера** с той же мажорной версией, что и версия **Сервера**, на котором происходит восстановление.

Например:

- БД из резервной копии, созданной при помощи **Сервера** версии **5.0**, можно восстановить, используя **Сервер** только версии **5.0**.

- БД из резервной копии, созданной при помощи **Сервера** версии **6.0**, можно восстановить, используя **Сервер** только версии **6.0**.
- БД из резервной копии, созданной при помощи **Сервера** версии **5.0** или **4.XX**, нельзя восстановить, используя **Сервер** версии **6.0**.

Если во время обновления Сервера на версию 6.0 с более ранних версий по каким-либо причинам была повреждена БД, выполните следующее:

1. Удалите **Сервер** версии **6.0**. При этом будут автоматически сохранены резервные копии файлов, используемых **Сервером**.
2. Установите **Сервер** той версии, которая стояла до обновления и при помощи которой создавалась резервная копия.

   При этом, согласно штатной процедуре обновления, следует использовать все сохраненные файлы **Сервера** кроме файла БД.

   В процессе установки **Сервера** создайте новую БД.
3. Восстановите БД из резервной копии по общим правилам (см. ниже).
4. В настройках **Сервера** отключите протоколы **Агента**, **Сервера** и **Сетевого инсталлятора**. Для этого выберите пункт **Администрирование** главного меню **Центра Управления**, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**, перейдите на вкладку **Модули** и снимите соответствующие флаги.
5. Обновите **Сервер** до версии **6.0** по общим правилам (см. п. Обновление Dr.Web Enterprise Security Suite и его отдельных компонентов).
6. Включите протоколы **Агента**, **Сервера** и **Сетевого инсталлятора**, отключенные на шаге 4.

Для ОС Windows

Для восстановления БД из резервной копии:

1. Остановите службу **Enterprise Сервера** (если она запущена, см. п. Запуск и останов Dr.Web Enterprise Server).
2. Импортируйте из соответствующего файла резервной копии содержимое базы данных. Строка импорта выглядит примерно так:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin
   \drwcsd.exe" -home="C:\Program Files\DrWeb
   Enterprise Server" -var-root="C:\Program
   Files\DrWeb Enterprise Server\var" -
   verbosity=all importdb "<диск:>
   \<путь_к_бэкап_файлу>\database.dz"
   ```

   Данная команда тоже должна быть набрана в одну строку. В примере подразумевается, что **Сервер** установлен в каталоге `C:\Program Files\DrWeb Enterprise Server`.

3. Запустите службу **Enterprise Сервера** (см. п. Запуск и останов Dr.Web Enterprise Server).

Для восстановления БД из резервной копии при смене версии Enterprise Сервера (в пределах одной мажорной версии) или порче текущей версии БД:

1. Остановите службу **Enterprise Сервера** (если она запущена, см. п. Запуск и останов Dr.Web Enterprise Server).
2. Удалите содержимое текущей БД. Для этого:

   2.1.При использовании внутренней БД:

   a) Удалите файл базы данных `dbinternal.dbs`.

   b) Произведите инициализацию новой базы данных. Строка инициализации базы данных в версии **Сервера** под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Enterprise Server
\bin\drwcsd.exe" -home="C:\Program Files
\DrWeb Enterprise Server" -var-
root="C:\Program Files\DrWeb Enterprise
Server\var" -verbosity=all initdb D:\Keys
\agent.key - - <пароль>
```

Данная команда должна быть набрана в одну строку (см. также формат команды `drwcsd` с ключом `initdb` в Прил. H5.3). В примере подразумевается, что **Сервер** установлен в каталоге `C:\Program Files\DrWeb Enterprise Server`, а агентский ключ `agent.key` лежит в каталоге `D:\Keys`.

c) После выполнения этой команды в папке `var` каталога установки **Enterprise Сервера** должен появиться новый файл базы `dbinternal.dbs` размером около 200 KB.

2.2. При использовании внешней БД: произведите очистку БД при помощи скрипта `clean.sql`, расположенного в каталоге `etc` каталога установки **Сервера**.

3. Импортируйте из соответствующего файла резервной копии содержимое базы данных. Строка импорта выглядит примерно так:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all importdb "<диск:>
\<путь_к_бэкап_файлу>\database.dz"
```

Данная команда тоже должна быть набрана в одну строку. В примере подразумевается, что **Сервер** установлен в каталоге `C:\Program Files\DrWeb Enterprise Server`.

4. Запустите службу **Enterprise Сервера** (см. п. Запуск и останов Dr.Web Enterprise Server).

Для ОС семейства UNIX

1. Остановите **Enterprise Сервер** (если он запущен):
   - для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd stop
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh stop
```

   - для **остальных** поддерживаемых версий:

```
/bin/drwcs.sh stop
```

2. Удалите файл базы данных `dbinternal.dbs` из следующей директории каталога установки **Enterprise Сервера**:
   - для ОС **Linux**: `/var/opt/drwcs/`
   - для ОС **FreeBSD** и ОС **Solaris**: `/var/drwcs/`

При использовании внешней БД ее очистка осуществляется с помощью скрипта `clean.sql`, расположенного в каталоге:
   - для ОС **Linux**: `/var/opt/drwcs/etc`
   - для ОС **Solaris** и ОС **FreeBSD**: `/var/drwcs/etc`

3. Инициализируйте базу данных **Сервера**. Для этого служит следующая команда:
   - для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd initdb
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh initdb
```

   - для **остальных** поддерживаемых версий:

```
su drwcs -c "bin/drwcsd -var-root=./var -verbosity=all -log=./var/server.log initdb
```

```
etc/agent.key - - <пароль>"
```

4. После выполнения этой команды в папке `var` каталога установки **Enterprise Сервера** должен появиться новый файл базы `dbinternal.dbs` размером около 200 KB.
5. Импортируйте из соответствующего файла резервной копии содержимое базы данных. Строка импорта выглядит примерно так:
   - для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd importdb "/
<путь_к_бэкап_файлу>/database.dz"
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh importdb "/
<путь_к_бэкап_файлу>/database.dz"
```

   - для **остальных** поддерживаемых версий:

```
bin/drwcsd -var-root=./var -verbosity=all -
log=logfile.log importdb "/
<путь_к_бэкап_файлу>/database.dz"
```

6. Запустите **Enterprise Сервер**.
   - для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd start
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh start
```

   - для **остальных** поддерживаемых версий:

```
/bin/drwcs.sh start
```

Если при запуске скрипта **Сервера** требуется задать параметры (например, указать каталог установки **Сервера**, изменить уровень подробности лога и т.п.), изменение соответствующих значений производится в стартовом скрипте:

- для ОС **FreeBSD**: `/usr/local/etc/rc.d/drwcsd.sh`

- для ОС **Linux** и ОС **Solaris**: `/etc/init.d/drwcsd`

Если какие-либо **Агенты** были установлены после создания последней резервной копии и выпали из базы данных после восстановления, то рекомендуется включить опцию **Переводить неавторизованных в новички**. Для этого в **Центре Управления** в меню **Администрирование** выберите пункт **Конфигурация Dr.Web Enterprise Server**. На вкладке **Общие** установите соответствующий флаг.

После восстановления базы рекомендуется подключиться к **Серверу** посредством **Центра Управления**, открыть в меню **Администрирование** пункт **Расписание Dr.Web Enterprise Server** и проверить в нем наличие задания **Резервное копирование критичных данных сервера.** Если такое задание отсутствует, рекомендуется его создать.

Восстановление Dr.Web Enterprise Server из резервной копии данных

Dr.Web Enterprise Security Suite регулярно сохраняет резервные копии важной информации **Сервера**: лицензионного ключа **Сервера**, содержимого базы данных, ключа шифрования, конфигурации **Сервера** и **Центра Управления**. Резервные копии сохраняются в следующих каталогах относительно рабочего каталога **Сервера**:

- для ОС **Windows**: `\var\Backup`
- для ОС **Linux**: `/var/opt/drwcs/backup`
- для ОС **FreeBSD** и **Solaris**: `/var/drwcs/backup`

Для выполнения этой функции в расписание **Сервера** включено ежедевное задание. Если такое задание в расписании отсутствует, рекомендуется создать его.

Резервные копии сохраняются в формате `.dz`, совместимом с `gzip` и другими распаковщиками. После распаковки все файлы, кроме содержимого БД, готовы к использованию. Содержимое БД, сохраненное в резервной копии, можно импортировать в другую БД **Сервера** при помощи ключа `importdb` и таким образом восстановить данные (см. п. Восстановление БД Dr.Web Enterprise Security Suite).

Также рекомендуется хранить на другом ПК копии следующих файлов: ключей шифрования `drwcsd.pri` и `drwcsd.pub`, лицензионных ключей `enterprise.key` и `agent.key`, сертификата для SSL `certificate.pem`, закрытого ключа RSA `private-key.pem` и периодически сохранять там же резервные копии содержимого базы данных **Сервера** `database.dz`, конфигурационного файла **Сервера** `drwcsd.conf` и **Центра Управления** `webmin.conf`. Таким образом, вы сможете избежать потери данных при повреждении ПК, на котором установлен **Enterprise Сервер**, и полностью восстановить данные и функциональность **Сервера**. В случае утраты лицензионных ключей их можно запросить заново, как указано в

п. Ключевые файлы.

Для восстановления Dr.Web Enterprise Server под ОС Windows

На рабочем ПК установите ПО **Enterprise Сервера** той же версии, что была утрачена (см. п. Установка Dr.Web Enterprise Server для ОС Windows®). При этом:

- Если сохранилась копия БД (внутренней или внешней) на другом компьютере и она не повреждена, укажите ее в соответствующем диалоговом окне инсталлятора, а также сохраненные файлы лицензионного ключа **Сервера**, закрытого ключа шифрования и конфигурации **Сервера**.
- Если БД **Сервера** (внутренняя или внешняя) была утрачена, но сохранилась резервная копия ее содержимого `database.dz`, то при установке в соответствующих диалоговых окнах выберите создание новой базы данных, укажите сохраненные файлы лицензионного ключа **Сервера** и **Агента**, закрытого ключа шифрования и конфигурации **Сервера**. После установки импортируйте содержимое БД из резервной копии (см. Восстановление БД Dr.Web Enterprise Security Suite).

Для восстановления Dr.Web Enterprise Server под ОС семейства UNIX

1. На рабочем ПК установите ПО **Enterprise Сервера** той же версии, что была утрачена (см. п. Установка Dr.Web Enterprise Server для ОС семейства UNIX®).
2. Поместите сохраненные файлы
   - для ОС **Linux**: в директорию `/var/opt/drwcs/etc`, кроме `pub`-ключа, который поместите в `/opt/drwcs/Installer/`
   - для ОС **FreeBSD**: в директорию `/var/drwcs/etc`, кроме `pub`-ключа, который поместите в `/usr/local/drwcs/Installer/`

- для ОС **Solaris**: в директорию `/var/drwcs/etc`, кроме `pub`-ключа, который поместите в `/opt/drwcs/Installer/`

На все замененные файлы **Сервера** необходимо установить те же системные права, что были выбраны при предыдущей (утраченной) установке **Сервера**.

3. Сгенерируйте новый сертификат SSL:
   - для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd selfcert
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh selfcert
```

   - для **остальных** поддерживаемых версий:

```
/opt/drwcs/bin/drwcsd  -var-root=/var/drwcs
-log=/var/drwcs/log/drwcsd.log selfcert
```

4. Дальнейшие действия зависят от наличия базы данных **Сервера**:

   a) При наличии внешней БД дальнейших действий по восстановлению не требуется, при условии, что сохранен конфигурационный файл и билд **Сервера** совпадает со старым. В противном случае необходимо прописать базу данных в конфигурационном файле **Сервера** и/или обновить структуру базы данных при помощи ключа `upgradedb` (см. вариант **c)** ниже).

   b) При наличии бэкапа БД `database.dz`, как внутренней, так и внешней, запустите **Сервер**, удалите созданную при установке внутреннюю БД, проинициализируйте создание новой и импортируйте содержимое старой БД из резервной копии (см. п. Восстановление БД Dr.Web Enterprise Security Suite).

   c) При наличии сохраненного файла внутренней БД замените им новый файл:

      - для ОС **Linux**:

`/var/opt/drwcs/dbinternal.dbs`

- для ОС **FreeBSD** и ОС **Solaris**:

`/var/drwcs/dbinternal.dbs`

На все замененные файлы **Сервера** необходимо установить те же системные права, что были выбраны при предыдущей (утраченной) установке **Сервера**.

Выполните команды:

- для ОС **Linux** и ОС **Solaris**:

```
/etc/init.d/drwcsd upgradedb
```

- для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh upgradedb
```

- для **остальных** поддерживаемых версий:

```
/opt/drwcs/bin/drwcsd -var-root=/var/drwcs
-log=/var/drwcs/log/drwcsd.log upgradedb
update-db
```

5. Запустите **Сервер**.

Если какие-либо **Агенты** были установлены после создания последней резервной копии и выпали из базы данных после восстановления, то их можно дистанционно перевести в режим "**Новичок**". Для этого нужно подключить **Центр Управления** к **Серверу**, открыть меню **Администрирование** → пункт **Конфигурация Dr.Web Enterprise Server** → вкладка **Общие** и включить режим **Переводить неавторизованных в новички**.

Обновление Агентов на серверах ЛВС

При обновлении **Агентов**, установленных на серверах ЛВС, могут быть нежелательны перезагрузки станций или остановы сетевого ПО, работающего на таких станциях.

Во избежание функционального простоя станций, выполняющих важные функции ЛВС, предлагается следующий режим обновления **Агентов** и антивирусного ПО:

1. В расписании **Сервера** изменить стандартные задания для обновления всех компонентов на обновление только вирусных баз.
2. Создать новое задание на обновление всех компонентов в удобное время, когда это не скажется критически на работе серверов ЛВС.

   Создание и редактирование заданий в расписании **Сервера** приведено в разделе Настройка расписания Dr.Web Enterprise Server.

На сервера, выполняющие важные сетевые функции (домен-контроллеры, сервера раздачи лицензий и т.д.), не рекомендуется устанавливать компоненты **SpIDer Gate**, **SpIDer Mail** и **Dr.Web Firewall** во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса **Dr.Web**.

Восстановление пароля администратора Dr.Web Enterprise Security Suite

В случае, если пароль администратора для доступа к **Enterprise Серверу** был утерян, существует возможность его просмотра или изменения с использованием прямого доступа к базе данных **Сервера**:

a) При использовании внутренней базы для просмотра и смены пароля администратора используется утилита `drwidbsh`, входящая в дистрибутив **Сервера**.

b) Для внешней БД используйте соответствующий sql-клиент.

Параметры учетных записей администраторов хранятся в таблице `admins`.

Примеры использования утилиты drwidbsh

1. Запустите утилиту с указанием пути до файла БД:
   - Для внутренней БД под ОС Linux:

```
/opt/drwcs/bin/drwidbsh     /var/opt/drwcs/
dbinternal.dbs
```

   - Для внутренней БД под ОС Windows:

```
"C:\Program Files\DrWeb Enterprise Server
\bin\drwidbsh" "C:\Program Files\DrWeb
Enterprise Server\var\dbinternal.dbs"
```

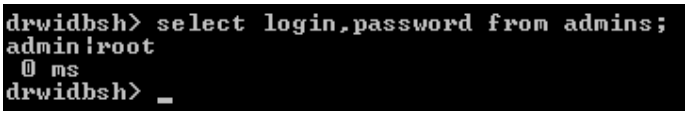
2. Для просмотра всех данных, хранящихся в таблице `admins`, выполните команду:

```
select * from admins;
```

3. Для просмотра имен и паролей для всех учетных записей администраторов выполните команду:

```
select login,password from admins;
```

4. Результат для варианта, когда существует только одна учетная запись с именем `admin` и у нее пароль `root`, приведена на скриншоте:



5. Для изменения пароля используйте команду `update`. Пример команды, изменяющей пароль от учетной записи `admin` на `qwerty`:

```
update admins set password='qwerty' where login='admin';
```

6. Для выхода из утилиты выполните команду:

```
.exit
```

Описание работы утилиты `drwidbsh` приведено в приложении Н6. Утилита администрирования встроенной базы данных.

Использование DFS при установке Агента через Active Directory

При установке **Enterprise Агента** через Active Directory возможно использование службы распределенной файловой системы (DFS).

Данный подход может быть удобен, например, при наличии в ЛВС нескольких контроллеров домена.

При установке в сети с несколькими контроллерами домена:

1. На каждом из контроллеров домена создать по каталогу с одинаковым именем.
2. При помощи DSF объединить созданные каталоги в один корневой целевой каталог.
3. Осуществить административную установку пакета `*.msi` в созданный целевой каталог.
4. Полученный целевой каталог использовать при назначении пакета в редакторе объектов групповой политики.

   При этом использовать сетевое имя вида: `\\<domain>\<folder>`

   где: *<domain>* - имя домена, *<folder>* - название целевого каталога.

Диагностика проблем удаленной установки

Принцип установки:

1. Браузер (модуль **Dr.Web Browser-Plugin**) подключается к ресурсу `ADMIN$` на удаленной машине (`\\<удаленная_машина>\ADMIN$`) и копирует файлы инсталлятора (`drwinst.exe`, `drwcsd.pub`), пути к которым указаны в **Центре Управления**, в папку `\\<удаленная_машина>\ADMIN$\Temp`.
2. Плагин запускает файл `drwinst.exe` на исполнение на удаленной машине с ключами, соответствующими настройкам в **Центре Управления**.

Для успешной установки необходимо, чтобы на машине, с которой происходит установка:

1. Был доступен ресурс `ADMIN$` на удаленной машине.

   Доступность можно проверить следующим образом:

   Введите в адресную строку приложения `Windows Explorer`:

   `\\<удаленная_машина>\ADMIN$`

   Должно появиться приглашение на ввод пользователя и пароля для доступа к этому ресурсу. Введите учетные данные, которые были указаны на странице инсталляции.

   Ресурс `ADMIN$` может быть недоступен по следующим причинам:

   a) учетная запись не имеет прав администратора;
   b) машина отключена или межсетевой экран блокирует доступ к порту 445;

c) ограничения удаленного доступа к ресурсу ADMIN$ на ОС Windows Vista и выше в случае, если они не входят в домен.

2. Был доступ к файлам drwinst.exe и drwcsd.pub.

В **Центре Управления** отображается расширенная информация (этап и код ошибки), помогающая диагностировать причину ошибки.

Список часто встречающихся ошибок

Этап	Код ошибки	Причина
Проверка корректности адресов удаленных машин (1)	Этот хост неизвестен (11001)	Не удалось преобразовать DNS-имя машины в адрес. Такого DNS-имени не существует, либо неправильно настроен сервер имен.
Проверка доступности сетевых ресурсов на удаленной машине (2)	Произошла ошибка операции на сокете, т.к. конечный хост выключен (10064)	Не доступен 445 TCP-порт на удаленной машине, возможные причины: ◆ машина отключена; ◆ межсетевой экран блокирует указанный порт; ◆ на удаленной машине установлена ОС, отличная от ОС Windows.
Соединение с административным ресурсом ADMIN$ (1001)	На этом этапе происходит соединение с административным ресурсом ADMIN$ на удаленной машине.	

Этап	Код ошибки	Причина
	Системой обнаружена попытка нарушения безопасности. Проверьте наличие доступа к серверу, через который был выполнен вход (1265).	◆ Не настроена модель совместного доступа и безопасности для локальных учетных записей. ◆ Не доступен сервер авторизации (контроллер домена)
	Вход в систему не произведен: имя пользователя или пароль не опознаны (1326).	Неизвестный пользователь или неверный пароль.
	Синтаксическая ошибка в имени файла, имени папки или метке тома (123).	Не существует ресурс `ADMIN$` на удаленной машине.
Проверка статуса завершения работы инсталлятора (1009)	На этом этапе происходит проверка результата работы инсталлятора.	
	Неизвестная ошибка (2).	Обратитесь в службу технической поддержки компании **Доктор Веб**.
	Агент уже установлен, инсталляция не требуется (4).	На данной машине **Агент** уже установлен, либо был некорректно удален (в этом случае воспользуйтесь утилитой **drwebremover**).
	Нарушение протокола (6).	Инсталлятор (`drwinst.exe`) не соответствует версии **Сервера**. Убедитесь, что инсталлятор получен из пакета установки **Сервера**.

Этап	Код ошибки	Причина
	Ошибка инициализации REXX (7).	Системная ошибка. Обратитесь в службу технической поддержки компании **Доктор Веб**.
	Тайм-аут соединения с **Сервером** (8).	**Enterprise Сервер** недоступен с удаленной машины.
	Необходимо перезагрузить систему, чтобы завершить предыдущую деинсталляцию (9).	Перезагрузите машину для завершения процесса предыдущей деинсталляции.

Предметный Указатель

Предметный Указатель

Б

Предметный Указатель

Предметный Указатель

Предметный Указатель

P

C

Предметный Указатель

Т

У

Ф

Предметный Указатель

© «Доктор Веб», 2004-2013