Руководство администратора

Жасағаның
دافع عن إبداعاتك
Защити созданное
Defend what you create
Protégez votre univers
Verteidige, was du erschaffen hast
Захисти створене
保护您创建的一切
Proteggi ciò che crei
Защити созданное
Защити созданное
Жасағаныңды қорға
Verteidige, was du erschaffen hast
Proteggi ciò che crei
Захисти створене
Defend what you create
脅威からの保護を提供します
Protégez votre univers
Proteggi ciò che crei
Захисти створене
دافع عن إبداعاتك
脅威からの保護を提供します
Defend what you create
Жасағаныңды қорға
دافع عن إبداعاتك
دافع عن إبداعاتك
Protégez votre univers
保护您创建的一切
Защити созданное
脅威からの保護を提供します
Захисти створене
Verteidige, was du erschaffen hast

Dr.Web Enterprise Security Suite
Версия 10.01.0
Руководство администратора
05.09.2017

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: http://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: Dr.Web Enterprise Security Suite

1.1. Введение

1.1.1. Назначение документа

В документации администратора антивирусной сети Dr.Web Enterprise Security Suite приведены сведения, описывающие как общие принципы, так и детали реализации комплексной антивирусной защиты компьютеров компании с помощью Dr.Web Enterprise Security Suite.

Документация администратора антивирусной сети Dr.Web Enterprise Security Suite состоит из следующих основных частей:

1. **Руководство по установке** (файл **drweb-esuite-10-install-manual-ru.pdf**)
2. **Руководство администратора** (файл **drweb-esuite-10-admin-manual-ru.pdf**)

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

   Администратор антивирусной сети должен обладать полномочиями 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 операционных систем.
3. **Приложения** (файл **drweb-esuite-10-appendices-ru.pdf**)

В документации присутствуют перекрестные ссылки между перечисленными документами. При загрузке документов на локальный компьютер, перекрестные ссылки будут функционировать только в том случае, если документы расположены в одном каталоге и имеют изначальные названия.

В документации администратора не описываются антивирусные пакеты Dr.Web для защищаемых компьютеров. За соответствующими сведениями обращайтесь к **Руководствам пользователя** антивирусного решения Dr.Web для соответствующей операционной системы.

Перед прочтением документов убедитесь, что это последняя версия Руководств. Руководства постоянно обновляются, и последнюю их версию можно найти на официальном веб-сайте компании «Доктор Веб» https://download.drweb.ru/doc/.

1.1.2. Условные обозначения и сокращения

Условные обозначения

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

Таблица 1-1. Условные обозначения

Обозначение	Комментарий
	Важное замечание или указание.
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`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),
- CDN – сеть доставки контента (Content Delivery Network),
- CPU – центральный процессор (Central Processing Unit),
- DFS – распределенная файловая система (Distributed File System),
- DNS – система доменных имен (Domain Name System),
- GUI – графический пользовательский интерфейс (Graphical User Interface), GUI-версия программы – версия, использующая средства GUI,
- NAP – Network Access Protection,
- MTU – максимальный размер полезного блока данных (Maximum Transmission Unit),
- TTL – время жизни пакета (Time To Live),

- UDS – доменный сокет UNIX (UNIX Domain Socket),
- 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.

1.2. О продукте

Dr.Web Enterprise Security Suite предназначен для организации и управления единой и надежной комплексной антивирусной защитой как внутренней сети компании, включая мобильные устройства, так и домашних компьютеров сотрудников.

Совокупность компьютеров и мобильных устройств, на которых установлены взаимодействующие компоненты Dr.Web Enterprise Security Suite, представляет собой единую *антивирусную сеть*.

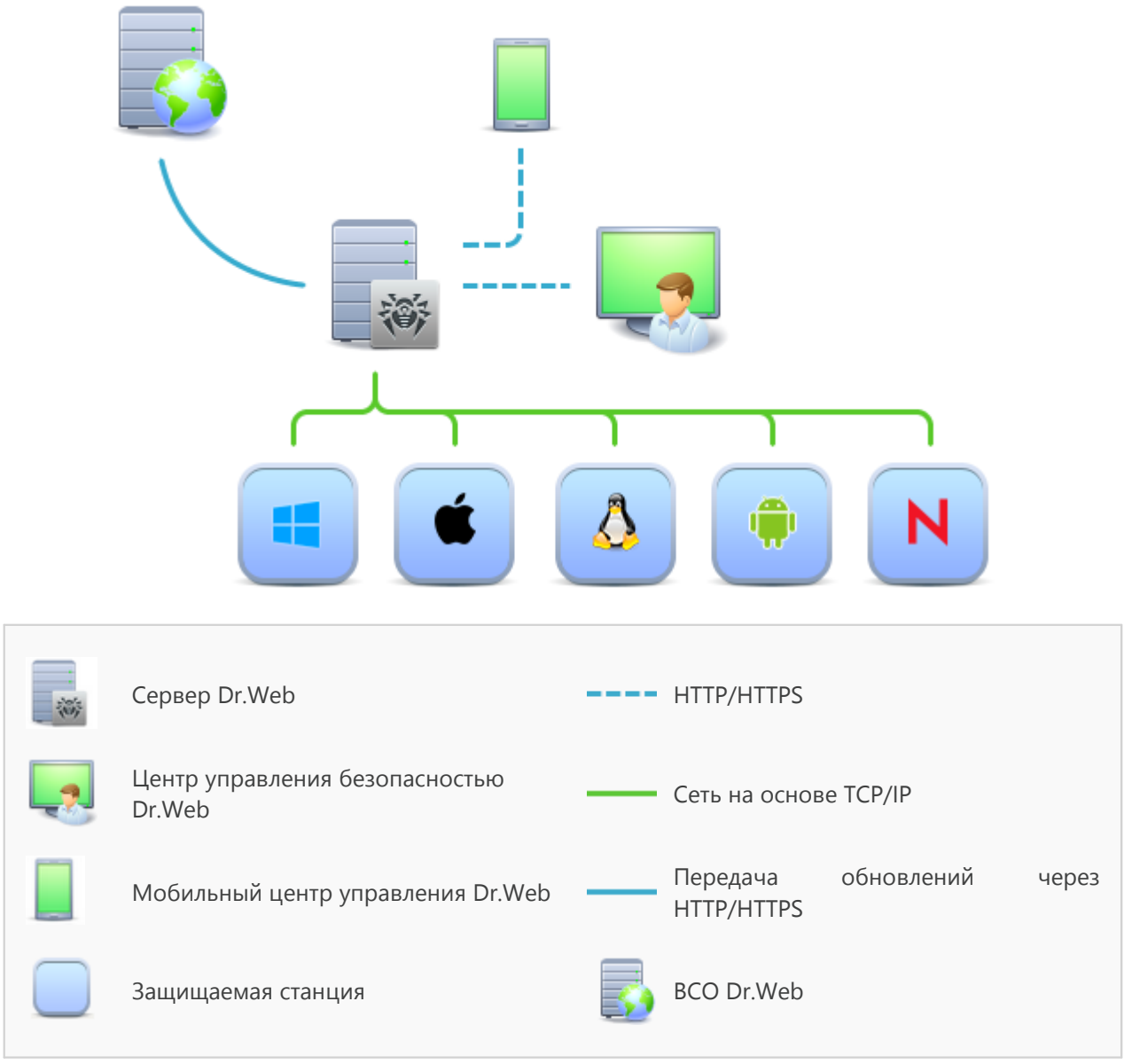


Рисунок 1-1. Логическая структура антивирусной сети

Антивирусная сеть Dr.Web Enterprise Security Suite имеет архитектуру *клиент-сервер*. Ее компоненты устанавливаются на компьютеры и мобильные устройства пользователей и администраторов, а также на компьютеры, выполняющие функции серверов ЛВС. Компоненты антивирусной сети обмениваются информацией, используя сетевые протоколы

TCP/IP. Антивирусное ПО на защищаемые станции возможно устанавливать (и впоследствии управлять ими) как через ЛВС, так и через Интернет.

Сервер централизованной защиты

Сервер централизованной защиты устанавливается на одном из компьютеров антивирусной сети, при этом установка возможна на любом компьютере, а не только на компьютере, выполняющем функции сервера ЛВС. Основные требования к этому компьютеру приведены в п. Системные требования.

Кросс-платформенность серверного программного обеспечения позволяет использовать в качестве Сервера компьютер под управлением следующих операционных систем:

- ОС Windows®,
- ОС семейства UNIX® (Linux®, FreeBSD®, Solaris™).

Сервер централизованной защиты хранит дистрибутивы антивирусных пакетов для различных ОС защищаемых компьютеров, обновления вирусных баз и антивирусных пакетов, лицензионные ключи и настройки антивирусных пакетов защищаемых компьютеров. Сервер получает обновления компонентов антивирусной защиты и вирусных баз через Интернет с серверов Всемирной Системы Обновления и осуществляет распространение обновлений на защищаемые станции.

Возможно создание иерархической структуры нескольких Серверов, обслуживающих защищаемые станции антивирусной сети.

Сервер поддерживает функцию резервного копирования критических данных (базы данных, конфигурационных файлов и др.).

Сервер ведет единый журнал событий антивирусной сети.

Единая база данных

Единая база данных подключается к Серверу централизованной защиты и хранит статистические данные по событиям антивирусной сети, настройки самого Сервера, параметры защищаемых станций и антивирусных компонентов, устанавливаемых на защищаемые станции.

Возможно использование следующих типов базы данных:

Встроенная база данных. Предоставляется два варианта базы данных, встроенной непосредственно в Сервер централизованной защиты:

- SQLite2 (InitDB),
- SQLite3.

Внешняя база данных. Предоставляются встроенные драйвера для подключения следующих баз данных:

- Oracle,
- PostgreSQL,
- ODBC-драйвер для подключения других баз данных, таких как Microsoft SQL Server/Microsoft SQL Server Express.

Вы можете использовать любую базу данных, соответствующую вашим запросам. Ваш выбор должен основываться на потребностях, которым должно удовлетворять хранилище данных, таких как: возможность обслуживания антивирусной сети соответствующего размера, особенности обслуживания ПО базы данных, возможности по администрированию, предоставляемые самой базой данных, а также принятые к использованию на вашем предприятии требования и стандарты.

Центр управления централизованной защитой

Центр управления централизованной защитой устанавливается автоматически вместе с Сервером и предоставляет веб-интерфейс для удаленного управления Сервером и антивирусной сетью путем редактирования настроек Сервера, а также настроек защищаемых компьютеров, хранящихся на Сервере и на защищаемых компьютерах.

Центр управления может быть открыт на любом компьютере, имеющем сетевой доступ к Серверу. Возможно использование Центра управления под управлением практически любой операционной системы, с полнофункциональным использованием на следующих веб-браузерах:

- Windows® Internet Explorer®,
- Mozilla® Firefox®,
- Google Chrome®.

Список возможных вариантов использования приведен в п. Системные требования.

Центр управления централизованной защитой предоставляет следующие возможности:

- Удобство установки Антивируса на защищаемые станции, в том числе: удаленная установка на станции под ОС Windows с предварительным обзором сети для поиска компьютеров; создание дистрибутивов с уникальными идентификаторами и параметрами подключения к Серверу для упрощения процесса установки Антивируса администратором или возможности установки Антивируса пользователями на станциях самостоятельно.
- Упрощенное управление рабочими станциями антивирусной сети за счет использования механизма групп (подробную информацию см. в разделе Глава 6: Группы. Комплексное управление рабочими станциями).
- Возможность централизованного управления антивирусными пакетами станций, в том числе: удаление как отдельных компонентов, так и Антивируса в целом на станциях под ОС Windows; настройка параметров работы компонентов антивирусных пакетов; задание прав на настройку и управление антивирусными пакетами защищаемых компьютеров для пользователей данных компьютеров (подробную информацию см. в разделе Глава 7: Управление рабочими станциями).
- Централизованное управление антивирусной проверкой рабочих станций, в том числе: удаленный запуск антивирусной проверки как по заданному расписанию, так и по прямому запросу администратора из Центра управления; централизованная настройка параметров антивирусной проверки, передаваемых на рабочие станции для последующего запуска локальной проверки с данными параметрами (подробную информацию см. в разделе Антивирусная проверка рабочих станций).

- Получение статистической информации о состоянии защищаемых станций, вирусной статистики, состоянии установленного антивирусного ПО, состоянии запущенных антивирусных компонентов, а также списка аппаратно-программного обеспечения защищаемой станции (подробную информацию см. в разделе Просмотр статистики по рабочей станции).
- Гибкая система администрирования Сервера и антивирусной сети за счет возможности разграничения прав для различных администраторов, а также возможность подключения администраторов через внешние системы авторизации такие как Active Directory, LDAP, RADIUS, PAM (подробную информацию см. в разделе Глава 5: Администраторы антивирусной сети).
- Управление лицензированием антивирусной защиты рабочих станций с разветвленной системой назначения лицензий для станций, групп станций, а также передачи лицензий между несколькими Серверами при многосерверной конфигурации антивирусной сети (подробную информацию см. в разделе Менеджер лицензий).
- Обширный набор настроек для задания конфигурации Сервера и отдельных его компонентов, в том числе: задание расписания для обслуживания Сервера; подключение пользовательских процедур; гибкая настройка системы обновления всех компонентов антивирусной сети с ВСО и дальнейшего распространения обновлений на станции; настройка систем оповещения администратора о событиях антивирусной сети с различными методами доставки сообщений; настройка межсерверных связей для конфигурации многосерверной антивирусной сети (подробную информацию см. в разделе Глава 8: Настройка Сервера Dr.Web).

Подробная информация по возможностям установки антивирусной защиты на рабочие станции приведена в **Руководстве по установке**.

Частью Центра управления безопасностью Dr.Web является Веб-сервер, который устанавливается автоматически вместе с Сервером. Основной задачей Веб-сервера является обеспечение работы со страницами Центра управления и клиентскими сетевыми соединениями.

Мобильный центр управления централизованной защитой

В качестве отдельного компонента предоставляется Мобильный центр управления, предназначенный для установки и запуска на мобильных устройствах под управлением iOS и ОС Android. Основные требования к приложению приведены в п. Системные требования.

Подключение Мобильного центра управления к Серверу осуществляется на основе учетных данных администратора антивирусной сети, в том числе по зашифрованному протоколу. Мобильный центр управления поддерживает базовый набор функций Центра управления:

1. Управление репозиторием Сервера Dr.Web:
   - просмотр состояния продуктов в репозитории;
   - запуск обновления репозитория из Всемирной системы обновлений Dr.Web.

2. Управление станциями, на которых обновление антивирусного ПО завершилось с ошибками:
   - отображение сбойных станций;
   - обновление компонентов на сбойных станциях.
3. Отображение статистики о состоянии антивирусной сети:
   - количество станций, зарегистрированных на Сервере Dr.Web, и их текущий статус (в сети/не в сети);
   - статистика заражений защищаемых станций.
4. Управление новыми станциями, ожидающими подключения к Серверу Dr.Web:
   - подтверждение доступа;
   - отклонение станций.
5. Управление антивирусными компонентами, установленными на станциях антивирусной сети:
   - запуск быстрого или полного сканирования для выбранных станций или для всех станций выбранных групп;
   - настройка реакции Сканера Dr.Web на обнаружение вредоносных объектов;
   - просмотр и управление файлами из Карантина на выбранной станции или всех станциях выбранной группы.
6. Управление станциями и группами:
   - просмотр настроек;
   - просмотр и управление составом компонентов антивирусного пакета;
   - удаление;
   - отправка сообщений произвольного содержания на станции;
   - перезагрузка станций под управлением ОС Windows;
   - добавление в список избранного для быстрого доступа.
7. Поиск станций и групп в антивирусной сети по различным параметрам: имя, адрес, ID.
8. Просмотр и управление сообщениями о важных событиях в антивирусной сети посредством интерактивных Push-уведомлений:
   - отображение всех уведомлений на Сервере Dr.Web;
   - задание реакций на события уведомлений;
   - поиск уведомлений по заданным параметрам фильтра;
   - удаление уведомлений;
   - исключение автоматического удаления уведомлений.

Скачать Мобильный центр управления вы можете из Центра управления или напрямую в App Store и Google Play.

Защита станций сети

На защищаемых компьютерах и мобильных устройствах сети осуществляется установка управляющего модуля (Агента) и антивирусного пакета для соответствующей операционной системы.

Кросс-платформенность программного обеспечения позволяет осуществлять антивирусную защиту компьютеров и мобильных устройств под управлением следующих операционных систем:

- ОС Windows®,
- ОС семейства UNIX®,
- OS X®,
- ОС Android,
- ОС Novell® NetWare®.

В качестве защищаемых станций могут выступать как пользовательские компьютеры, так и серверы ЛВС. В частности, поддерживается антивирусная защита почтовой системы Microsoft® Outlook®.

Управляющий модуль производит регулярные обновления антивирусных компонентов и вирусных баз с Сервера, а также отправляет Серверу информацию о вирусных событиях на защищаемом компьютере.

В случае недоступности Сервера централизованной защиты возможно обновление вирусных баз защищаемых станций непосредственно через Интернет из Всемирной Системы Обновления.

В зависимости от операционной системы станции предоставляются соответствующие функции защиты, приведенные далее.

Станции под ОС Windows®

Антивирусная проверка

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления, в том числе на наличие руткитов.

Файловый монитор

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

Почтовый монитор

Проверка всей входящей и исходящей почты при использовании почтовых клиентов.

Также возможно использование спам-фильтра (при условии, что лицензия позволяет использование такой функции).

Веб-монитор

Проверка всех обращений к веб-сайтам по протоколу HTTP. Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Офисный контроль

Управление доступом к локальным и сетевым ресурсам, в частности, контроль доступа к веб-сайтам. Позволяет контролировать целостность важных файлов от случайного изменения или заражения вирусами, и запрещает служащим доступ к нежелательной информации.

Межсетевой экран

Защита компьютеров от несанкционированного доступа извне и предотвращение утечки важных данных по сети Интернет. Контроль подключения и передачи данных по сети Интернет и блокировка подозрительных соединений на уровне пакетов и приложений.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

Самозащита

Защита файлов и каталогов Dr.Web Enterprise Security Suite от несанкционированного или невольного удаления или модификации пользователем, а также вредоносным ПО. При включенной самозащите доступ к файлам и каталогам Dr.Web Enterprise Security Suite разрешен только для процессов Dr.Web.

Превентивная защита

Предотвращение потенциальных угроз безопасности. Контроль доступа к критическим объектам операционной системы, контроль за загрузкой драйверов, автоматическим запуском программ и работой системных служб, а также отслеживание запущенных процессов и их блокировка в случае обнаружения вирусной активности.

Станции под ОС семейства UNIX®

Антивирусная проверка

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

Файловый монитор

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

Веб-монитор

Проверка всех обращений к веб-сайтам по протоколу HTTP. Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

Станции под OS X®

Антивирусная проверка

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

Файловый монитор

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

Веб-монитор

Проверка всех обращений к веб-сайтам по протоколу HTTP. Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

Мобильные устройства под ОС Android

Антивирусная проверка

Сканирование мобильного устройства по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

Файловый монитор

Постоянная проверка файловой системы в режиме реального времени. Сканирование всех файлов при попытке их сохранения в памяти мобильного устройства.

Фильтр звонков и сообщений

Фильтрация SMS-сообщений и телефонных звонков позволяет блокировать нежелательные сообщения и звонки, например, рекламные рассылки, а также звонки и сообщения с неизвестных номеров.

Антивор

Обнаружение местоположения или оперативная блокировка функций мобильного устройства в случае его утери или кражи.

Ограничение доступа к интернет-ресурсам

URL-фильтр позволяет оградить пользователя мобильного устройства от нежелательных интернет-ресурсов.

Межсетевой экран

Защита мобильного устройства от несанкционированного доступа извне и предотвращение утечки важных данных по сети. Контроль подключения и передачи данных по сети Интернет и блокировка подозрительных соединений на уровне пакетов и приложений.

Помощь в решении проблем безопасности

Диагностика и анализ безопасности мобильного устройства и устранение выявленных проблем и уязвимостей.

Контроль запуска приложений

Запрет запуска на мобильном устройстве тех приложений, которые не включены в список разрешенных администратором.

Серверы под ОС Novell® NetWare®

Антивирусная проверка

Сканирование компьютера по запросу пользователя, а также согласно расписанию.

Файловый монитор

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

Обеспечение связи между компонентами антивирусной сети

Для обеспечения стабильной и безопасной связи между компонентами антивирусной сети предоставляются следующие возможности:

Прокси-сервер Dr.Web

Прокси-сервер может опционально включаться в состав антивирусной сети. Основная задача Прокси-сервера – обеспечение связи Сервера и защищаемых станций в случае невозможности организации прямого доступа, например, если Сервер и защищаемые станции 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 защищаемыми станциями.

Сжатие трафика

Предоставляются специальные алгоритмы сжатия при передаче данных между компонентами антивирусной сети, что обеспечивает минимальный сетевой трафик.

Шифрование трафика

Предоставляется возможность шифрования при передаче данных между компонентами антивирусной сети, что обеспечивает дополнительный уровень защиты.

Дополнительные возможности

NAP Validator

NAP Validator поставляется в виде дополнительного компонента и позволяет использовать технологию Microsoft Network Access Protection (NAP) для проверки работоспособности ПО защищаемых рабочих станций. Получаемая безопасность достигается за счет выполнения требований, предъявляемых к работоспособности станций сети.

Загрузчик репозитория

Загрузчик репозитория Dr.Web поставляется в виде дополнительной утилиты и позволяет осуществлять загрузку продуктов Dr.Web Enterprise Security Suite из Всемирной Системы Обновлений. Может использоваться для загрузки обновлений продуктов Dr.Web Enterprise Security Suite для размещения обновлений на Сервере, не подключенном к Интернету.

1.3. Системные требования

Для установки и функционирования Dr.Web Enterprise Security Suite требуется:

- чтобы Сервер Dr.Web был установлен на компьютер, имеющий доступ в Интернет, для автоматического получения обновлений с серверов ВСО (Всемирной системы обновления) Dr.Web;

> Допускается возможность распространения обновлений иным способом на Серверы, не подключенные к Интернету. В частности, при многосерверной конфигурации антивирусной сети возможно получение обновлений с ВСО только одним из Серверов с последующим распространением на другие Серверы, либо использование дополнительной утилиты Загрузчик репозитория Dr.Web для загрузки обновлений с ВСО через Интернет с последующим распространением на Серверы.

- чтобы компьютеры антивирусной сети имели доступ к Серверу Dr.Web либо Прокси-серверу;

- для совместной работы антивирусных компонентов на используемых компьютерах должны быть открыты следующие порты:

Номера портов	Протоколы	Направление соединений	Назначение
2193	TCP	• входящие, исходящие для Сервера и Прокси-сервера • исходящие для Агента	Для связи антивирусных компонентов с Сервером и межсерверных связей. В том числе используется Прокси-сервером для установки соединения с клиентами.
	UDP	входящие, исходящие	Для работы Сканера Сети.
139, 445	TCP	• входящие для Сервера • входящие, исходящие для Агента • исходящие для компьютера, на котором открывается Центр управления	Для работы Сетевого инсталлятора.
	UDP	входящие, исходящие	
9080	HTTP	• входящие для Сервера • исходящие для компьютера, на котором открывается Центр управления	Для работы Центра управления безопасностью Dr.Web.
9081	HTTPS		
10101	TCP		Для работы утилиты дистанционной диагностики Сервера.
80	HTTP	исходящие	Для получения обновлений с ВСО.
443	HTTPS		

Обратите внимание: в Серверах версии 4 использовался порт `2371` для связи антивирусных компонентов с Сервером. В версии 10 данный порт более не поддерживается.

Для работы Сервера Dr.Web требуется:

Компонент	Требования
Процессор и операционная система	Поддерживаются следующие операционные системы, установленные на компьютерах с соответствующими CPU: • CPU с поддержкой инструкций SSE2 и тактовой частотой 1,3 ГГц и выше: ▫ ОС Windows; ▫ ОС Linux; ▫ ОС FreeBSD;

Компонент	Требования
	▫ ОС Solaris x86. • CPU V9 UltraSPARC IIIi и выше: ▫ ОС Solaris Sparc. Полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А.
Оперативная память	• Минимальные требования: 1 ГБ. • Рекомендуемые требования: 2 ГБ и выше.
Место на жестком диске	не менее 12 ГБ: до 8 ГБ для встроенной базы данных (каталог установки), до 4 ГБ в системном временном каталоге (для рабочих файлов). В зависимости от настроек Сервера, может потребоваться дополнительное место для хранения временных файлов, например, для хранения персональных инсталляционных пакетов Агентов (примерно 8,5 МБ каждый) в подкаталоге `var\installers-cache` каталога установки Сервера Dr.Web. ⚠ При установке Сервера необходимо, чтобы на системном диске для ОС Windows или в `/var/tmp` для ОС семейства UNIX (или в другой директории для временных файлов, если она переопределена), вне зависимости от места установки самого Сервера, было не менее 1,2 ГБ для основного дистрибутива и 2,5 ГБ для дополнительного дистрибутива для запуска инсталлятора и распаковки временных файлов.
Прочее	При установке Сервера Dr.Web для ОС семейства UNIX требуется наличие библиотек: `lsb` версии 3 и старше, `glibc` версии 2.7 и старше. Для работы с БД **PostgreSQL** требуется наличие библиотеки `libpq`. Для работы с БД **Oracle** требуется наличие библиотеки `libaio`. Дополнительно под ОС **FreeBSD** требуется наличие библиотеки `compat-8x`.

Для работы Прокси-сервера Dr.Web требуется:

Компонент	Требование
Процессор	Intel® Pentium® III с частотой 667 МГц или выше.
Оперативная память	не менее 1 ГБ.
Место на жестком диске	не менее 1 ГБ.

Компонент	Требование
Операционная система	• Windows; • Linux; • FreeBSD; • Solaris. Полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А.
Прочее	При установке Прокси-сервера для ОС семейства UNIX требуется наличие библиотек: `lsb` версии 3 и старше. Дополнительно под ОС **FreeBSD** требуется наличие библиотеки `compat-8x`.

Для работы Центра управления безопасностью Dr.Web требуется:

a) Веб-браузер:

Веб-браузер	Поддержка
Windows Internet Explorer 8 и выше	Поддерживается
Mozilla Firefox 25 и выше	
Google Chrome 30 и выше	
Opera® 10 и выше	Использование допускается, однако возможность работы не гарантируется.
Safari® 4 и выше	

При использовании веб-браузера Windows Internet Explorer необходимо учесть следующие особенности:

- Полная работоспособность Центра управления под веб-браузером Windows Internet Explorer с включенным режимом **Enhanced Security Configuration for Windows Internet Explorer** не гарантируется.
- При установке Сервера на компьютер, в названии которого присутствует символ "_" (подчеркивание), работа с Сервером через Центр управления в браузере будет невозможна. В таком случае необходимо использовать другой веб-браузер.
- Для корректной работы Центра управления, IP-адрес и/или DNS-имя машины, на которой установлен Сервер Dr.Web, должны быть добавлены в доверенные сайты веб-браузера, в котором открывается Центр управления.
- Для корректного открытия Центра управления через меню **Пуск** 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**.

b) Для полнофункциональной работы с Центром управления необходима установка расширения Центра управления безопасностью Dr.Web. Расширение поставляется вместе с дистрибутивом Сервера и устанавливается по запросу браузера в процессе работы с элементами Центра управления, требующими подгрузку расширения (для Сканера сети, при удаленной установке антивирусных компонентов).

Установка расширения возможна на следующих веб-браузерах:

Веб-браузер	**Минимальная поддерживаемая версия**	**Максимальная поддерживаемая версия**
Windows Internet Explorer	8	11
Mozilla Firefox	25	50.0.1
Google Chrome	30	44.0.2403

Для работы расширения Центра управления безопасностью Dr.Web на странице Сканера сети как под ОС Windows, так и под ОС семейства GNU/Linux, необходимы права администратора (root).

При использовании веб-браузеров Mozilla Firefox и Google Chrome расширение Центра управления безопасностью Dr.Web доступно только для версий, работающих под ОС Windows и ОС семейства Linux.

c) Рекомендуемое разрешение экрана для работы с Центром управления 1280x1024 px.

Для работы Мобильного центра управления Dr.Web требуется:

Требования различаются в зависимости от операционной системы, на которую устанавливается приложение:

Операционная система	**Требование**	
	Версия операционной системы	**Устройство**
iOS	iOS® 7 и выше	Apple® iPhone® Apple® iPad®
Android	Android 4.0 и выше	–

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 Агента Dr.Web и полного антивирусного пакета требуется:

Требования различаются в зависимости от операционной системы, на которую устанавливается антивирусное решение (полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А. Полный список поддерживаемых версий ОС):

- ОС Windows:

Компонент	Требование
Процессор	CPU с тактовой частотой 1 ГГц и выше.
Свободная оперативная память	Не менее 512 МБ.
Свободное место на жестком диске	1 ГБ для исполняемых файлов + дополнительно для журналов работы и временных файлов.
Прочее	1. Для корректной работы контекстной справки **Агент Dr.Web для Windows** необходимо наличие Windows® Internet Explorer® 6.0 и выше. 2. Для подключаемого модуля Dr.Web для Outlook необходим установленный клиент Microsoft Outlook из состава Microsoft Office: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 SP2; • Outlook 2013; • Outlook 2016.

- ОС семейства Linux:

Компонент	Требование
Процессор	Поддерживаются процессоры с архитектурой и системой команд Intel/AMD: 32-бит (IA-32, x86); 64-бит (x86-64, x64, amd64).
Свободная оперативная память	Не менее 512 МБ.

Компонент	Требование
Свободное место на жестком диске	Не менее 400 Мбайт свободного дискового пространства на томе, на котором размещаются каталоги Антивируса.

- OS X, ОС Android, ОС Novell NetWare: требования к конфигурации совпадают с требованиями для операционной системы.

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 Агентов приведено в руководствах пользователя для соответствующей операционной системы.

1.4. Комплект поставки

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

1. Для ОС семейства UNIX – в виде файлов формата `run`:

Название файла	Компонент
`drweb-esuite-server-10.01.0-<`*сборка*`>-<`*версия_ОС*`>.run`	Основной дистрибутив Сервера Dr.Web
`drweb-esuite-extra-10.01.0-<`*сборка*`>-<`*версия_ОС*`>.run`	Дополнительный дистрибутив Сервера Dr.Web
`drweb-esuite-proxy-10.01.0-<`*сборка*`>-<`*версия_ОС*`>.run`	Прокси-сервер

2. Для ОС Windows – в виде исполняемых файлов:

Название файла	Компонент
`drweb-esuite-server-10.01.0-<`*сборка*`>-<`*версия_ОС*`>.exe`	Основной дистрибутив Сервера Dr.Web
`drweb-esuite-extra-10.01.0-<`*сборка*`>-<`*версия_ОС*`>.exe`	Дополнительный дистрибутив Сервера Dr.Web
`drweb-esuite-proxy-10.01.0-<`*сборка*`>-<`*версия_ОС*`>.msi`	Прокси-сервер
`drweb-esuite-agent-activedirectory-10.01.0-<`*сборка*`>.msi`	Агент Dr.Web для Active Directory

Название файла	Компонент
drweb-esuite-modify-ad-schema-10.01.0-<*сборка*>-<*версия_ОС*>.exe	Утилита для модификации схемы Active Directory
drweb-esuite-aduac-10.01.0-<*сборка*>-<*версия_ОС*>.msi	Утилита для изменения атрибутов у объектов Active Directory
drweb-esuite-napshv-10.01.0-<*сборка*>-<*версия_ОС*>.msi	NAP Validator
drweb-esuite-agent-full-11.00.0-<*версия_сборки*>-windows.exe	Полный инсталлятор Агента Dr.Web. Также входит в состав дополнительного дистрибутива Сервера Dr.Web.

Дистрибутив Сервера Dr.Web состоит из двух пакетов:

1. *Основной дистрибутив* – базовый дистрибутив для установки Сервера Dr.Web. Состав аналогичен составу дистрибутива предыдущих версий Dr.Web Enterprise Security Suite.

   Из основного дистрибутива осуществляется установка самого Сервера Dr.Web, включающего пакеты антивирусной защиты для станции только под ОС Windows.

2. *Дополнительный дистрибутив (extra)* – включает дистрибутивы всех корпоративных продуктов, предоставляемых для установки на защищаемые станции, управляемые всеми поддерживаемыми ОС.

   Устанавливается как дополнение на компьютер с уже установленным основным дистрибутивом Сервера Dr.Web.

   Дополнительный дистрибутив должен устанавливаться из пакета того же типа, что и основной дистрибутив.

В состав основного дистрибутива Сервера Dr.Web входят следующие компоненты:

- ПО Сервера Dr.Web для соответствующей ОС,
- ПО Агентов Dr.Web и антивирусных пакетов для станций под ОС Windows,
- ПО Центра управления безопасностью Dr.Web,
- вирусные базы,
- Расширение Центра управления безопасностью Dr.Web,
- Расширение Dr.Web Server FrontDoor,
- документация, шаблоны и примеры.

  Кроме самого дистрибутива поставляются также серийные номера, после регистрации которых вы получите файлы с лицензионными ключами.

Глава 2: Лицензирование

Для работы антивирусного решения Dr.Web Enterprise Security Suite требуется лицензия.

Состав и стоимость лицензии на использование Dr.Web Enterprise Security Suite зависят от количества защищаемых станций, включая серверы, входящие в состав сети Dr.Web Enterprise Security Suite как защищаемые станции.

Эту информацию необходимо обязательно сообщать продавцу лицензии при покупке решения Dr.Web Enterprise Security Suite. Количество используемых Серверов Dr.Web не влияет на увеличение стоимости лицензии.

Лицензионный ключевой файл

Права на использование Dr.Web Enterprise Security Suite регулируются при помощи лицензионных ключевых файлов.

Формат лицензионного ключевого файла защищен от редактирования при помощи механизма электронной подписи. Редактирование файла делает его недействительным. Чтобы избежать случайной порчи лицензионного ключевого файла, не следует модифицировать и/или сохранять его после просмотра в текстовом редакторе.

Лицензионные ключевые файлы поставляются в виде zip-архива, содержащего один или несколько ключевых файлов для защищаемых станций.

Пользователь может получить лицензионные ключевые файлы одним из следующих способов:

- Лицензионный ключевой файл входит в комплект антивируса Dr.Web Enterprise Security Suite при покупке, если он был включен в состав дистрибутива продукта при его комплектации. Однако, как правило, поставляются только серийные номера.
- Лицензионный ключевой файл высылается пользователям по электронной почте после регистрации серийного номера на веб-сайте компании «Доктор Веб» по адресу 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 электронной почты. Вы также сможете загрузить ключевые файлы непосредственно с указанного сайта.
- Лицензионный ключевой файл может поставляться на отдельном носителе.

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 https://download.drweb.com/demoreq/biz/. Ваш запрос будет рассмотрен в индивидуальном порядке. В случае положительного решения архив с лицензионными ключевыми файлами будет выслан по указанному вами адресу электронной почты.

Использование лицензионных ключевых файлов в процессе установки программы описывается в **Руководстве по установке**, п. Установка Сервера Dr.Web.

Использование лицензионных ключевых файлов для уже развернутой антивирусной сети описывается в п. Менеджер лицензий.

2.1. Особенности лицензирования

1. Сервер Dr.Web не лицензируется.

   UUID Сервера, который в предыдущих версиях Dr.Web Enterprise Security Suite хранился в лицензионном ключе Сервера, теперь хранится в конфигурационном файле Сервера (начиная с версии 10).

   - При установке нового Сервера генерируется новый UUID.
   - При обновлении Сервера с более ранних версий, UUID автоматически берется из ключа Сервера предыдущей версии (файл `enterprise.key` в каталоге `etc` предыдущей установки Сервера) и записывается в конфигурационный файл устанавливаемого Сервера.

   В случае обновления кластера Серверов лицензионный ключ получает Сервер, ответственный за обновление базы данных. Для остальных Серверов необходимо добавлять лицензионные ключи вручную.

2. Лицензионные ключи актуальны только для защищаемых станций. Назначение лицензий возможно как для отдельных станций, так и для групп станций: в этом случае лицензионный ключ действителен для всех станций, которые наследуют его от данной группы. Чтобы задать ключевой файл одновременно для всех станций антивирусной сети, для которых не заданы персональные настройки лицензионного ключа, назначьте лицензионный ключ для группы **Everyone**.
3. Лицензионный ключевой файл может задаваться при установке Сервера Dr.Web (см. **Руководство по установке**, п. Установка Сервера Dr.Web).

   Однако, Сервер также может быть установлен без лицензионного ключа. Лицензия может быть добавлена позднее как локально, так и получена через межсерверную связь.

4. Посредством межсерверной связи возможна передача опционального количества лицензий из ключей, хранящихся на данном Сервере, соседнему Серверу на определенный промежуток времени.
5. Возможно использование нескольких различных лицензий, например, с различным сроком действия или различным набором антивирусных компонентов для защищаемых станций. Каждый лицензионный ключ может быть назначен для нескольких объектов лицензирования (групп и станций) одновременно. Для одного объекта лицензирования может быть назначено несколько лицензионных ключей одновременно.
6. При назначении нескольких ключей на один объект, обратите внимание на следующие особенности:
   a) Если список разрешенных антивирусных компонентов у нескольких ключей одного объекта различается, список разрешенных для станций компонентов будет определяется пересечением множеств компонентов в ключах. Например, если для группы станций назначены ключ с поддержкой Антиспама и ключ без поддержки Антиспама, то для станций установка Антиспама будет запрещена.
   b) Настройки лицензирования для объекта рассчитываются исходя из всех назначенных для этого объекта ключей. Если срок действия лицензионных ключей объекта различается, то по истечении ключа с минимальным сроком действия, вам необходимо заменить или удалить истекший ключ вручную. Если истекший ключ накладывал ограничения на установку антивирусных компонентов, необходимо произвести корректировку настроек объекта лицензирования в разделе **Устанавливаемые компоненты**.
   c) Количество лицензий у объекта рассчитывается из суммы лицензий всех ключей, назначенных для данного объекта. Также следует учитывать возможность передачи лицензий по межсерверной связи соседнему Серверу (см. п. 4). В этом случае из общего количества лицензий вычитаются лицензии, переданные соседнему Серверу.

Управление лицензионными ключами осуществляется через Менеджер лицензий.

При задании лицензионного ключа в Менеджере лицензий, вся информация о данной лицензии сохраняется в базе данных.

2.2. Автоматическое обновление лицензий

Лицензия для Dr.Web Enterprise Security Suite может быть автоматически обновлена.

Автоматическое обновление лицензии подразумевает следующие аспекты:

- При окончании срока действия лицензионного ключа он может быть автоматически заменен программой на заранее приобретенный лицензионный ключ.
- Автоматическое обновление выполняется для конкретного лицензионного ключа, для которого покупалось продление.
- Лицензионный ключ для автоматического обновления располагается на серверах компании «Доктор Веб» до окончания срока действия лицензионного ключа, который должен быть продлен.

- Проверка доступности автоматического обновления (наличие лицензионного ключа на серверах компании «Доктор Веб») и само обновление осуществляются при выполнении задания **Окончание срока действия лицензионного ключа** из расписания Сервера Dr.Web.

  Если задание **Окончание срока действия лицензионного ключа** отключено в расписании Сервера, автоматическое обновление лицензии будет невозможно.

  Для запуска задания необходимо выполнение следующих условий:

  - Заканчивается срок действия текущей лицензии (количество дней до окончания срока действия задается в параметрах задания).
  - Текущая лицензия принадлежит этому Серверу: изначально добавлена вручную или получена через автоматическое обновление. Лицензии, полученные с соседних Серверов через межсерверные связи, не подлежат автоматическому обновлению посредством задания из расписания Сервера.

Автоматическое обновление лицензий по расписанию

Возможны следующие результаты выполнения задания **Окончание срока действия лицензионного ключа**:

1. *Автоматическое обновление для лицензии недоступно.*

   Администратору отправляется оповещение **Окончание срока действия лицензионного ключа**.

2. *Автоматическое обновление для лицензии доступно. Состав лицензируемых компонентов у текущего и нового ключей отличается (в новом ключе нет каких-либо компонентов, которые есть в текущем) или у нового лицензионного ключа меньше лицензий, чем у текущего лицензионного ключа.*

   Новая лицензия скачивается с серверов компании «Доктор Веб», добавляется в Менеджер лицензий и базу данных Сервера, но не распространяется на объекты лицензирования. В такой ситуации лицензионный ключ необходимо распространить вручную.

   Администратору отправляется оповещение **Лицензионный ключ не может быть автоматически обновлен**. Конкретная причина, по которой ключ не может быть автоматически распространен, будет приведена в оповещении.

3. *Автоматическое обновление для лицензии доступно. Состав лицензируемых компонентов у текущего и нового лицензионных ключей совпадает (или в новом ключе лицензировано больше компонентов, чем в текущем, включая все компоненты текущего ключа), количество лицензий у нового лицензионного ключа больше или равно количеству лицензий у текущего лицензионного ключа.*

   Новая лицензия скачивается с серверов компании «Доктор Веб», добавляется в Менеджер лицензий и базу данных Сервера и распространяется на все объекты лицензирования, на которые была распространена предыдущая лицензия, включая соседние Серверы.

   Старая лицензия будет удалена, когда она не будет использоваться ни одним подчиненным Сервером. Таким образом, если в момент автоматического обновления подчинен-

ный Сервер был отключен, старая лицензия будет храниться до тех пор, пока этот подчиненный Сервер не подключится.

Старая лицензия будет храниться, пока ее не удалят вручную, в следующих случаях:

- Если на подчиненный Сервер невозможно распространить лицензию, полученную при автоматическом обновлении (Сервер отключен навсегда).
- Если на подчиненном Сервере используется версия протокола, не поддерживающая функционал автоматических обновлений. При этом лицензии будут переданы на подчиненный Сервер, но не будут распространены.

Администратору отправляется оповещение **Лицензионный ключ автоматически обновлен**. Оповещение об обновлении будет отправлено с каждого Сервера, на который будет распространена новая лицензия.

Все оповещения, отправляемые администратору, настраиваются в разделе **Администрирование** → **Конфигурация оповещений**.

После отправки каждого из оповещений выполняется пользовательская процедура **Автоматическое обновление лицензионного ключа**.

Обновление лицензий вручную

Если вы приобрели лицензионный ключ для автоматического обновления вашего текущего ключа, то добавление нового ключа в Менеджере лицензий вручную не требуется. В зависимости от ситуации (вариант 2 в процедуре выше) может потребоваться только ручное распространение на объекты лицензирования.

Однако, если до выполнения задания **Окончание срока действия лицензионного ключа** вы самостоятельно добавили через Менеджер лицензий новый ключ, подлежащий автоматическому обновлению по варианту 3 (см. процедуру выше), то при выполнении задания будет осуществляться только распространение нового лицензионного ключа. При этом возможны следующие варианты:

a) Новый лицензионный ключ был вручную распространен на все объекты, на которые был распространен предыдущий (обновляемый) ключ. В таком случае, при выполнении задания на обновление никаких изменений не будет внесено.

b) Новый лицензионный ключ был вручную распространен не на все объекты, на которые был распространен предыдущий (обновляемый) ключ. В таком случае, при выполнении задания на обновление новый ключ будет распространен на все оставшиеся объекты предыдущего ключа, которые еще не получили обновление.

   Если новый лицензионный ключ был дополнительно распространен вручную на объекты, которых не было в списке предыдущего ключа, то после выполнения задания новый ключ останется распространен также и на эти объекты. При этом возможны следующие варианты:

   - Количества лицензий хватает на все объекты лицензирования: на те, которые были у предыдущего ключа, и на назначенные новому ключу вручную. Такая ситуация воз-

можна, если новый ключ содержит большее количество лицензий. В таком случае, при выполнении задания на обновление никаких изменений не будет внесено.

- Количества лицензий не хватает для распространения на все объекты лицензирования, которые были у предыдущего ключа, потому что лицензии были назначены вручную на другие объекты. Для объектов, которым не хватило лицензий, обновление не произойдет, однако предыдущий ключ все равно будет удален, и объекты останутся без лицензии. При появлении свободных лицензий все объекты, которым не хватило лицензий, получат новый лицензионный ключ. При этом действия зависят от типа лицензируемых объектов:
  - Если лицензий из нового ключа не хватило станциям данного Сервера, то проверка доступных лицензий будет осуществляться при каждой попытке подключения станции к Серверу. Если в момент подключения станции будет обнаружена освободившаяся лицензия, она будет предоставлена этой станции.
  - Если лицензий из нового ключа не хватило для выдачи соседним Серверам, то проверка доступных лицензий будет осуществляться автоматически примерно раз в минуту. При появлении свободных лицензий, они будут отданы соседним Серверам.

Лицензионный ключевой файл

Обратите внимание на следующие особенности лицензионных ключевых файлов при автоматическом обновлении:

- При выполнении автоматического обновления новая лицензия скачивается с серверов компании «Доктор Веб», информация о ней сохраняется в базе данных Сервера и отображается в Менеджере лицензий. Лицензионный ключевой файл при этом не создается.
- Чтобы получить лицензионный ключевой файл, воспользуйтесь опцией **Администрирование** → **Менеджер лицензий** → **Экспортировать ключ**. Также лицензионный ключевой файл может быть получен при выполнении пользовательской процедуры **Автоматическое обновление лицензионного ключа**.
- При удалении лицензии информация о ней удаляется из Менеджера лицензий и из базы данных Сервера, однако лицензионный ключевой файл остается в каталоге Сервера.

Глава 3: Начало работы

3.1. Создание антивирусной сети

Краткая инструкция по развертыванию антивирусной сети:

1. Составьте план структуры антивирусной сети, включите в него все защищаемые компьютеры и мобильные устройства.

   Выберите компьютер, который будет выполнять функции Сервера Dr.Web. В состав антивирусной сети может входить несколько Серверов Dr.Web. Особенности такой конфигурации описаны в п. Особенности сети с несколькими Серверами Dr.Web.

   > Сервер Dr.Web можно установить на любом компьютере, а не только на компьютере, выполняющем функции сервера ЛВС. Основные требованием к этому компьютеру приведены в п. Системные требования.
   >
   > На все защищаемые станции, включая серверы ЛВС, устанавливается одна и та же версия Агента Dr.Web. Отличие составляет список устанавливаемых антивирусных компонентов, определяемый настройками на Сервере.

   Для установки Сервера Dr.Web и Агента Dr.Web 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 Серверам Dr.Web или рабочим станциям.

2. Согласно составленному плану определите, какие продукты для каких операционных систем потребуется установить на соответствующие узлы сети. Подробная информация по предоставляемым продуктам приведена в разделе Комплект поставки.

   Все требуемые продукты могут быть приобретены в виде коробочного решения Dr.Web Enterprise Security Suite или скачаны на веб-сайте компании «Доктор Веб» https://download.drweb.ru/.

   > Агенты Dr.Web для станции под ОС Android, ОС Linux, OS X также могут быть установлены из пакетов для автономных продуктов и в дальнейшем подключены к централизованному Серверу Dr.Web. Описание соответствующих настроек Агентов приведено в **Руководстве по установке**, п. Установка Агента Dr.Web при помощи персонального инсталляционного пакета.

3. Установите основной дистрибутив Сервера Dr.Web на выбранный компьютер или компьютеры. Описание установки приведено в **Руководстве по установке**, п. Установка Сервера Dr.Web.

   Вместе с Сервером устанавливается Центр управления безопасностью Dr.Web.

   По умолчанию Сервер Dr.Web запускается автоматически после установки и после каждой перезагрузки операционной системы.

4. Если антивирусная сеть будет включать защищаемые станции под ОС Android, ОС Linux, OS X, установите дополнительный дистрибутив Сервера Dr.Web на все компьютеры с установленным основным дистрибутивом Сервера.
5. При необходимости установите и настройте Прокси-сервер. Описание приведено в **Руководстве по установке**, п. Установка Прокси-сервера.
6. Для настройки Сервера и антивирусного ПО на станциях необходимо подключиться к Серверу при помощи Центра управления безопасностью Dr.Web.

   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.

   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 Сервер Dr.Web.

   В диалоговом окне запроса на авторизацию задайте регистрационное имя и пароль администратора.

   Имя администратора по умолчанию – **admin**.

   Пароль:

   - для ОС Windows – пароль, который был задан при установке Сервера.
   - для ОС семейства UNIX – **root**.

   Для Сервера под ОС семейства UNIX измените пароль администратора по умолчанию при первом подключении к Серверу.

   При успешном подключении к Серверу откроется главное окно Центра управления (подробное описание см. в п. Центр управления безопасностью Dr.Web).
7. Произведите начальную настройку Сервера (подробное описание настроек Сервера приведено в Главе 8: Настройка Сервера Dr.Web):
   a. В разделе Менеджер лицензий добавьте один или несколько лицензионных ключей и распространите их на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера не был задан лицензионный ключ.
   b. В разделе Общая конфигурация репозитория задайте, какие компоненты антивирусной сети будут обновляться с ВСО Dr.Web. В разделе Состояние репозитория произведите обновление продуктов в репозитории Сервера. Обновление может занять продолжительное время. Дождитесь окончания процесса обновления перед тем как продолжить дальнейшую настройку.
   c. На странице **Администрирование** → **Сервер Dr.Web** приведена информация о версии Сервера. При наличии новой версии, обновите Сервер как описано в п. Обновление Сервера Dr.Web и восстановление из резервной копии.

d. При необходимости настройте Сетевые соединения для изменения сетевых настроек по умолчанию, используемых для взаимодействия всех компонентов антивирусной сети.

e. При необходимости настройте список администраторов Сервера. Также доступна внешняя аутентификация администраторов. Подробнее см. в Главе 5: Администраторы антивирусной сети.

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

8. Задайте настройки и конфигурацию антивирусного ПО для рабочих станций (подробное описание настройки групп и станций приведено в Главе 6 и Главе 7):

   a. При необходимости создайте пользовательские группы станций.

   b. Задайте настройки группы **Everyone** и созданных пользовательских групп. В частности настройте раздел устанавливаемых компонентов.

9. Установите ПО Агента Dr.Web на рабочие станции.

   В разделе Инсталляционные файлы ознакомьтесь со списком предоставляемых файлов для установки Агента. Выберите подходящий для вас вариант установки, исходя из операционной системы станции, возможности удаленной установки, варианта задания настроек Сервера при установке Агента и т.п. Например:

   - Если пользователи устанавливают антивирус самостоятельно, воспользуйтесь персональными инсталляционными пакетами, которые создаются через Центр управления отдельно для каждой станции. Данный тип пакетов также возможно отправить пользователям на электронную почту непосредственно из Центра управления. После установки подключение станций к Серверу осуществляется автоматически.
   - Для удаленной установки по сети на станцию или несколько станций одновременно (только для станций под ОС Windows) воспользуйтесь сетевым инсталлятором. Установка осуществляется через Центр управления с использованием расширения браузера.
   - Также возможна удаленная установка по сети на станцию или несколько станций одновременно с использованием службы Active Directory. Для этого используется инсталлятор Агента Dr.Web для сетей с Active Directory, поставляемый в комплекте дистрибутива Dr.Web Enterprise Security Suite, но отдельно от инсталлятора Сервера.
   - Если необходимо уменьшить нагрузку на канал связи между Сервером и станциями в процессе установки, можете воспользоваться полным инсталлятором, который осуществляет установку Агента и компонентов защиты единовременно.
   - Установка на станции под ОС Android, ОС Linux, OS X может выполняться локально по общим правилам. Также уже установленный автономный продукт может подключаться к Серверу на основе соответствующей конфигурации.

10. 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):

a. При установке из инсталляционных пакетов, а также при настройке автоматического подтверждения на Сервере рабочие станции автоматически получают регистрацию при первом подключении к Серверу, и дополнительное подтверждение не требуется.

b. При установке из инсталляторов и настройке ручного подтверждения доступа администратору необходимо вручную подтвердить новые рабочие станции для их регистрации на Сервере. При этом новые рабочие станции не подключаются автоматически, а помещаются Сервером в группу новичков.

11. После подключения к Серверу и получения настроек, на станцию устанавливается соответствующий набор компонентов антивирусного пакета, заданный в настройках первичной группы станции.

> Для завершения установки компонентов рабочей станции потребуется перезагрузка компьютера.

12. Настройка станций и антивирусного ПО возможна также после установки (подробное описание приведено в Главе 7).

3.2. Настройка сетевых соединений

Общие сведения

К Серверу Dr.Web подключаются следующие клиенты:

- Агенты Dr.Web,
- Инсталляторы Агентов Dr.Web,
- другие Серверы Dr.Web.

Соединение всегда устанавливается по инициативе клиента.

Возможны следующие схемы подключения клиентов к Серверу:

1. Посредством прямых соединений.

   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 Сервер Dr.Web на другой компьютер или поменять IP-адрес машины, на которой установлен Сервер.

3. Через протокол SRV.

   Данный подход позволяет искать Сервер по имени компьютера и/или службы Сервера на основе SRV-записей на DNS-сервере.

При конфигурации антивирусной сети Dr.Web Enterprise Security Suite на использование прямых соединений Служба обнаружения Сервера может быть отключена. Для этого в опи-

сании транспортов (**Администрирование** → **Конфигурация Сервера Dr.Web** → вкладка **Сеть** → вкладка **Транспорт**) поле **Multicast-группа** следует оставить пустым.

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 автоматически добавляет порты и интерфейсы Сервера в исключения сетевого экрана ОС Windows.

Если на компьютере используется сетевой экран, помимо встроенного сетевого экрана ОС Windows, администратор антивирусной сети должен произвести соответствующие настройки вручную.

3.2.1. Прямые соединения

Настройка Сервера Dr.Web

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

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

По умолчанию для "прослушивания" Сервером устанавливаются:

- **Адрес**: пустое значение – использовать *все сетевые интерфейсы* для данной машины, на которой установлен Сервер.
- **Порт**: `2193` – использовать порт `2193`, зарегистрированный за Dr.Web Enterprise Security Suite в IANA.

> Обратите внимание: в версиях Сервера 4 использовался порт `2371`. В версии 10 данный порт более не поддерживается.

Для корректной работы всей системы Dr.Web Enterprise Security Suite достаточно, чтобы Сервер "слушал" хотя бы один TCP-порт, который должен быть известен всем клиентам.

Настройка Агента Dr.Web

При установке Агента адрес Сервера (IP-адрес или DNS-имя компьютера, на котором запущен Сервер Dr.Web) 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 Сервера Dr.Web на другой компьютер.

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

Таким образом, адрес Сервера Dr.Web становится известен Агенту при установке.

В дальнейшем адрес Сервера может быть изменен вручную в настройках Агента.

3.2.2. Служба обнаружения Сервера Dr.Web

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, заданным в настройках Сервера.
2. Агенты, при поиске Сервера, посылают в сеть мультикаст-запросы на групповой адрес, заданный в п. 1.

По умолчанию для "прослушивания" Сервером устанавливается (аналогично прямым соединениям): `udp/231.0.0.1:2193`.

> Обратите внимание: в Серверах версии 4 использовался порт `2371`. В версии 10 данный порт более не поддерживается.

Данный параметр задается в настройках Центра управления **Администрирование** → **Конфигурация Сервера Dr.Web** → вкладка **Сеть** → вкладка **Транспорт** → поле **Multicast-группа**.

3.2.3. Использование протокола SRV

Клиенты под ОС Windows поддерживают клиентский сетевой протокол *SRV* (описание формата приведено в документе **Приложения**, п. Приложение Е. Спецификация сетевого адреса).

Возможность обращения к Серверу через SRV-записи реализуется следующим образом:

1. При установке Сервера настраивается регистрация в домене Active Directory, инсталлятор вносит соответствующую SRV-запись на DNS-сервер.

   SRV-запись вносится на DNS-сервер в соответствии с RFC2782 (см. http://tools.ietf.org/html/rfc2782).

2. При запросе подключения к Серверу пользователь задает обращение через протокол `srv`.

   Например, запуск инсталлятора Агента:

   - с явным указанием имени сервиса `myservice`:
     `drwinst /server "srv/myservice"`
   - без указания имени сервиса. При этом будет осуществляться поиск в SRV-записях имени по умолчанию – `drwcs`
     `drwinst /server "srv/"`

3. Клиент прозрачно для пользователя использует функционал протокола SRV для обращения к Серверу.

   Если при обращении Сервер явно не указан, по умолчанию в качестве имени сервиса используется `drwcs`.

Глава 4: Компоненты антивирусной сети и их интерфейс

4.1. Сервер Dr.Web

Антивирусная сеть должна иметь в своем составе хотя бы один Сервер Dr.Web.

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

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

Основные функции

Сервер Dr.Web 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

Сервер Dr.Web обеспечивает сбор и протоколирование информации о работе антивирусных пакетов, передаваемой ему посредством ПО на защищаемых компьютерах (Агентами Dr.Web, 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 встроенная база данных. Для обслуживания больших сетей предусмотрена возможность использования внешних баз данных.

Использование встроенной БД допустимо при подключении к Серверу не более 200-300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен Сервер Dr.Web, 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 Сервера Dr.Web, 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.

Сервер Dr.Web 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.

Веб-сервер

Веб-сервер является частью Центра управления безопасностью Dr.Web и выполняет следующие основные функции:

- аутентификация и авторизация администраторов в Центре управления;
- автоматизация работы страниц Центра управления;
- поддержка динамически генерируемых страниц Центра управления;
- поддержка защищённых HTTPS-соединений с клиентами.

4.1.1. Управление Сервером Dr.Web под ОС Windows®

Интерфейс и управление Сервером Dr.Web

Сервер Dr.Web не имеет встроенного интерфейса. Управление Сервером Dr.Web, как правило, осуществляется при помощи Центра управления, который служит внешним интерфейсом для Сервера.

При установке Сервера в главное меню ОС Windows **Программы** размещается каталог **Dr.Web Server**, содержащий следующие элементы, позволяющие осуществлять настройку и базовое управление Сервером:

- Каталог **Управление сервером** – содержит команды запуска, перезапуска и завершения работы Сервера, а также команды настройки протоколирования и другие команды Сервера, подробнее описанные в документе **Приложения**, п. H4. Сервер Dr.Web.
- 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 Сервера Dr.Web имеет следующую структуру:

- `bin` – исполняемые файлы Сервера Dr.Web.
- `etc` – основные конфигурационные файлы компонентов антивирусной сети.
- `Installer` – инсталлятор для установки Антивируса на защищаемый компьютер и открытый ключ шифрования (`drwcsd.pub`).
- `update-db` – скрипты, необходимые для обновления структуры БД Сервера.
- `var` – каталог содержит подкаталоги:
  - `es-dl-cache` – персональные инсталляционные пакеты пользователей в течение двух недель после их создания;
  - `backup` – резервные копий БД и других критичных данных;
  - `extensions` – скрипты пользовательских процедур, предназначенные для автоматизации выполнения определенных заданий;
  - `repository` – каталог репозитория, 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 (как правило, пользователь **LocalSystem**);
  - `templates` – шаблоны отчетов.
- `webmin` – элементы Центра управления безопасностью Dr.Web: документация, значки, модули.

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

Основные конфигурационные файлы

Файл	Описание	Каталог по умолчанию
`agent.key` (имя может отличаться)	лицензионный ключ Агента	`etc`
`certificate.pem`	сертификат для SSL	
`download.conf`	сетевые настройки для формирования инсталляционных пакетов Агента	
`drwcsd.conf` (имя может отличаться)	конфигурационный файл Сервера	
`drwcsd.conf.distr`	шаблон конфигурационного файла Сервера с параметрами по умолчанию	
`drwcsd.pri`	закрытый ключ шифрования	
`enterprise.key` (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 10 отсутствует	
`frontdoor.conf`	конфигурационный файл для утилиты дистанционной диагностики Сервера	
`http-alerter-certs.pem`	сертификаты для верификации хоста apple-notify.drweb.com при отправке push-уведомлений	
`private-key.pem`	закрытый ключ RSA	
`webmin.conf`	конфигурационный файл Центра управления	
`auth-ads.xml`	конфигурационный файл внешней авторизации администраторов через Active Directory	
`auth-ldap.xml`	конфигурационный файл внешней авторизации администраторов через LDAP	
`auth-radius.xml`	конфигурационный файл внешней авторизации администраторов через RADIUS	

Файл	Описание	Каталог по умолчанию
`database.sqlite`	встроенная БД	`var`
`drwcsd.pub`	открытый ключ шифрования	• `Installer` • `webmin\install`

Запуск и останов Сервера Dr.Web

По умолчанию Сервер Dr.Web запускается автоматически после установки и после каждой перезагрузки операционной системы.

Также вы можете запустить, перезапустить или остановить Сервер Dr.Web одним из следующих способов:

- Общий случай:
  - При помощи соответствующей команды, расположенной в меню **Пуск** → **Программы** → **Dr.Web 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. документ **Приложения**, п. H4. Сервер Dr.Web):
  - `drwcsd start` – запуск Сервера.
  - `drwcsd restart` – полный перезапуск службы Сервера.
  - `drwcsd stop` – нормальное завершение работы Сервера.

> Обратите внимание, чтобы Сервер считал переменные окружения, необходимо выполнить перезапуск сервиса при помощи средств управления службами или при помощи консольной команды.

4.1.2. Управление Сервером Dr.Web под ОС семейства UNIX®

Интерфейс и управление Сервером Dr.Web

Сервер Dr.Web не имеет встроенного интерфейса. Управление Сервером Dr.Web, как правило, осуществляется при помощи Центра управления, который служит внешним интерфейсом для Сервера.

Каталог установки Сервера Dr.Web имеет следующую структуру:

`/opt/drwcs/` для ОС Linux, ОС Solaris и `/usr/local/drwcs` для ОС FreeBSD:

- `bin` – исполняемые файлы Сервера Dr.Web.
- `doc` – файлы лицензионных соглашений.
- `ds-modules`
- `fonts` – шрифты для интерфейса Центра управления.
- `Installer` – сетевой инсталлятор и открытый ключ шифрования для установки Антивируса на защищаемые компьютеры.
- `lib` – набор библиотек для работы Сервера.
- `update-db` – скрипты, необходимые для обновления структуры баз данных Сервера.
- `webmin` – все элементы Центра управления безопасностью Dr.Web.

`/var/opt/drwcs/` для ОС Linux, ОС Solaris и `/var/drwcs` для ОС FreeBSD:

- `backup` – резервные копии БД и других критичных данных.
- `bases` – распакованные вирусные базы для обратной совместимости с предыдущими версиями Агентов Dr.Web.
- `coredump` – дампы падений Сервера.
- `database.sqlite` – встроенная база данных Сервера.
- `etc` – файлы основных настроек компонентов антивирусной сети.
- `extensions` – пользовательские скрипты, предназначенные для автоматизации выполнения определенных заданий.
- `installers-cache` – кэш инсталляторов Агента. Служит для хранения инсталляционных пакетов Агента при создании станций в Центре управления.
- `log` – файлы журнала Сервера.
- `object` – кэш объектов Центра управления.
- `reports` – временный каталог для генерации и хранения отчетов.
- `repository` – 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 (как правило, пользователь **drwcs**).
- `run` – PID процесса Сервера.
- `sessions` – сессии Центра управления.
- `upload` – директория для загрузки временных файлов, которые задаются через Центр управления (ключи и т.д.).

/etc/opt/drweb.com/ для ОС Linux (только при установке из generic-пакетов *.tar.gz.run) и /usr/local/etc/opt/ для ОС FreeBSD:

- software/drweb-esuite.remove – скрипт для удаления Сервера.
- + возможно дополнительные файлы и каталоги.

/usr/local/etc/rc.d/ для ОС FreeBSD:

- drwcsd.sh – скрипт для запуска и останова Сервера.

/var/tmp/drwcs – резервная копия после удаления Сервера.

Основные конфигурационные файлы

Файл	Описание	Каталог по умолчанию
agent.key (имя может отличаться)	лицензионный ключ Агента	• для ОС Linux и ОС Solaris: /var/opt/drwcs/etc • для ОС FreeBSD: /var/drwcs/etc
certificate.pem	сертификат для SSL	
common.conf	конфигурационный файл (для некоторых ОС семейства UNIX)	
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента	
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера	
drwcsd.conf.distr	шаблон конфигурационного файла Сервера с параметрами по умолчанию	
drwcsd.pri	закрытый ключ шифрования	
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 10 отсутствует	
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера	
http-alerter-certs.pem	сертификаты для верификации хоста apple-notify.drweb.com при отправке push-уведомлений	
private-key.pem	закрытый ключ RSA	
webmin.conf	конфигурационный файл Центра управления	

Файл	Описание	Каталог по умолчанию
`auth-ldap.xml`	конфигурационный файл внешней авторизации администраторов через LDAP	
`auth-pam.xml`	конфигурационный файл внешней авторизации администраторов через PAM	
`auth-radius.xml`	конфигурационный файл внешней авторизации администраторов через RADIUS	
`database.sqlite`	встроенная БД	• для ОС Linux и ОС Solaris: `/var/opt/drwcs` • для ОС FreeBSD: `/var/drwcs`
`drwcsd.pub`	открытый ключ шифрования	• для ОС Linux и ОС Solaris: `/opt/drwcs/Installer` `/opt/drwcs/webmin/install` • для ОС FreeBSD: `/usr/local/drwcs/Installer` `/usr/local/drwcs/webmin/install`

Запуск и останов Сервера Dr.Web

По умолчанию Сервер Dr.Web запускается автоматически после установки и после каждой перезагрузки операционной системы.

Также вы можете запустить, перезапустить или остановить Сервер Dr.Web одним из следующих способов:

- Останов и перезапуск через Центр управления:

  В разделе **Администрирование**: перезапуск при помощи кнопки, останов при помощи кнопки (отсутствует под версией для ОС Solaris).

- При помощи соответствующей консольной команды (также см. документ Приложения, п. H4. Сервер Dr.Web):
  - 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
    ```

Обратите внимание, чтобы Сервер считал переменные окружения, необходимо выполнить перезапуск сервиса при помощи консольной команды.

4.2. Защита рабочих станций

Детальное описание настроек антивирусных компонентов, задаваемых через Центр управления, приведено в **Руководствах администратора** по управлению станциями для соответствующей операционной системы.

Защищаемый компьютер с установленным антивирусным пакетом, в соответствии с его функциями в антивирусной сети, именуется *рабочей станцией* антивирусной сети. Необходимо помнить, что по своим функциям в локальной сети такой компьютер может быть как рабочей станцией или мобильным устройством, так и сервером локальной сети.

Защита рабочих станций осуществляется антивирусными пакетами Dr.Web, разработанными для соответствующих операционных систем.

Антивирусные пакеты устанавливаются на защищаемых станциях и подключаются к Серверу Dr.Web. Каждая станция входит в состав одной или нескольких групп, зарегистрированных на этом Сервере (подробнее см. п. Системные и пользовательские группы). Передача информации между станцией и Сервером осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

Установка

Антивирусный пакет может быть установлен на рабочую станцию одним из следующих способов:

1. Локально. Локальная установка осуществляется на компьютере или мобильном устройстве пользователя непосредственно. Может производится как администратором, так и пользователем.
2. Удаленно. Удаленная установка доступна только для станций под ОС Windows и осуществляется в Центре управления через ЛВС. Производится администратором антивирусной сети. При этом вмешательство пользователя не требуется.

Подробное описание процедур установки антивирусных пакетов на рабочие станции приведено в **Руководстве по установке**.

Управление

При поддержке связи с Сервером Dr.Web администратору доступны следующие функции, реализуемые антивирусным пакетом на станции:

- Централизованная настройка Антивируса на рабочих станциях при помощи Центра управления.

  При этом администратор может как запретить, так и оставить возможность пользователю самостоятельно изменять настройки Антивируса на станции.
- Настройка расписания антивирусных проверок и других заданий, выполняемых на станции.
- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии станции.
- Запуск и останов антивирусного сканирования и т.п.

Удаленный запуск Сканера возможен только на станциях, работающих под ОС Windows, ОС семейства UNIX и OS X.

Обновление

Сервер Dr.Web загружает обновления и распространяет их на подключенные к нему станции. Таким образом автоматически устанавливается, поддерживается и регулируется оптимальная стратегия защиты от угроз независимо от уровня квалификации пользователей рабочих станций.

В случае временного отключения рабочей станции от антивирусной сети, Антивирус на станции использует локальную копию настроек, антивирусная защита на рабочей станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление ПО не производится. Если для станции разрешено функционирование в *Мобильном режиме*, при потере связи с Сервером будет доступно обновление вирусных баз непосредственно с серверов ВСО.

Принцип работы станций в мобильном режиме описан в п. Обновление мобильных Агентов Dr.Web.

4.3. Центр управления безопасностью Dr.Web

Для управления антивирусной сетью в целом (включая изменение ее состава и структуры), всеми ее компонентами, а также для настройки Сервера Dr.Web служит Центр управления безопасностью 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: **Сервис** → **Свойства обозревателя** → **Безопасность** → **Надежные узлы**.

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

Подключение к Серверу Dr.Web

На любом компьютере, имеющем сетевой доступ к Серверу Dr.Web, 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 Сервер Dr.Web.

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 безопасностью Dr.Web

Окно Центра управления (см. рис. 4-1) делится на *заголовок главного меню* и *рабочую область*.

Рабочая область

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:

- раздел Администрирование,
- раздел Антивирусная Сеть,
- раздел Связи,
- Панель поиска,
- имя учетной записи администратора, под которой был осуществлен вход в Центр управления. Также может быть доступно меню межсерверных связей,
- раздел События,
- раздел Настройки,
- раздел Помощь,
- кнопка **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**.

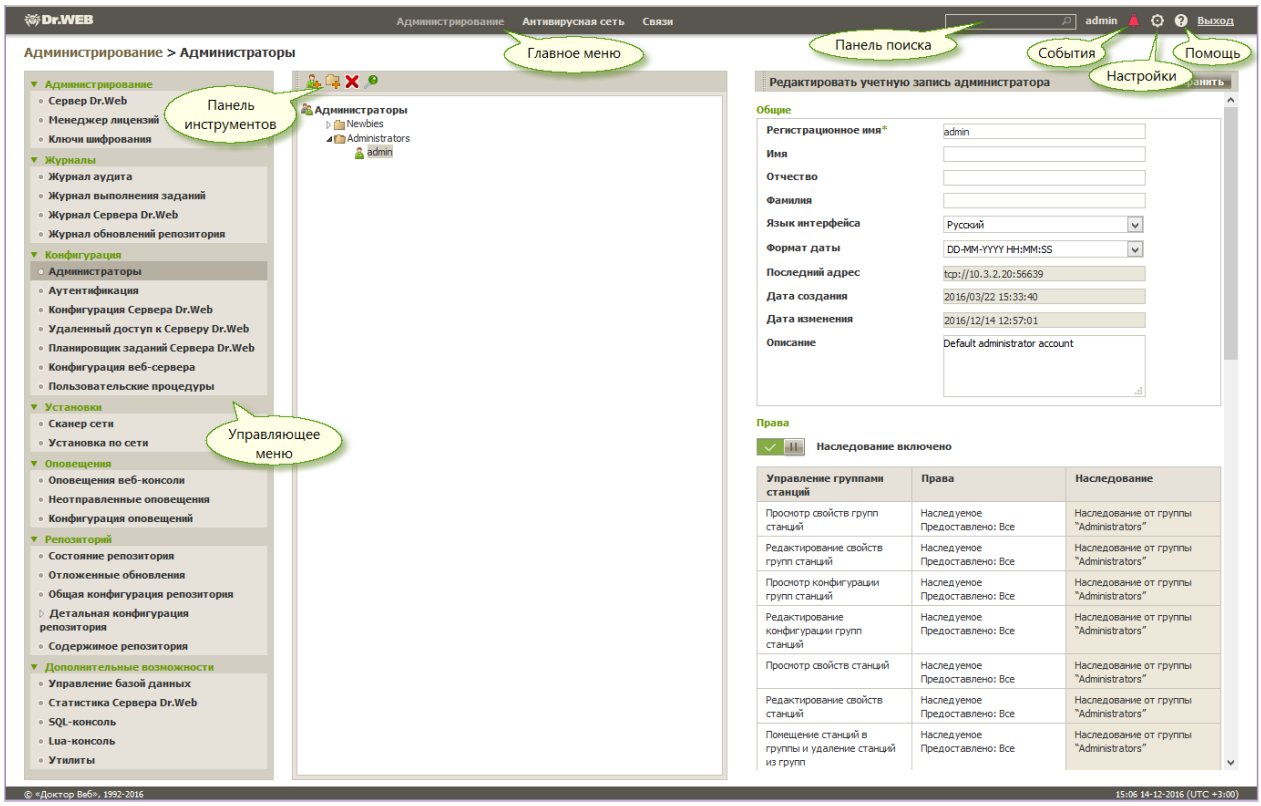


Рисунок 4-1. Окно Центра управления безопасностью Dr.Web. Нажмите на пункт главного меню для перехода к описанию

Меню межсерверных связей

Информация по организации многосерверной антивирусной сети и настройке межсерверных связей приведена в разделе Особенности сети с несколькими Серверами Dr.Web.

При наличии межсерверных связей с другими Серверами Dr.Web добавляются следующие функции для регистрационного имени администратора в главном меню:

- Рядом с именем администратора выводится имя текущего Сервера Dr.Web.
- При нажатии на имя администратора открывается выпадающий список со связными Серверами. Если для связи не задано имя, приводится ее идентификатор.

  При нажатии на связь возможны два варианта действий:

  - Откроется Центр управления связного Сервера, если при настройке связи был указан IP-адрес Центра управления.
    Действие аналогично кнопке на панели инструментов в разделе **Связи** главного меню.
  - Если адрес Центра управления соседнего Сервера не задан для данной связи, откроется настройка раздела **Связи** для задания IP-адреса.

4.3.1. 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**
   - **Сервер Dr.Web** – 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. Также, при наличии загруженных обновлений Сервера Dr.Web, из данного раздела доступен раздел Обновления Сервера Dr.Web со списком версий Сервера для обновления и резервного копирования.
   - Менеджер лицензий – позволяет управлять лицензионными ключевыми файлами.
   - **Ключи шифрования** – позволяет экспортировать (сохранить локально) открытый и закрытый ключи шифрования.
2. **Журналы**
   - Журнал аудита – позволяет просмотреть список событий и изменений, осуществленных при помощи управляющих подсистем Dr.Web Enterprise Security Suite.
   - **Журнал выполнения заданий** – содержит список назначенных заданий на Сервере с пометкой о выполнении и комментариями.
   - Журнал Сервера Dr.Web – содержит список журналов событий, связанных с работой Сервера.
   - Журнал обновлений репозитория – содержит список обновлений с ВСО, включающий подробную информацию об обновленных ревизиях продуктов.
3. **Конфигурация**
   - Администраторы – открывает панель управления учетными записями администраторов антивирусной сети.
   - Аутентификация – открывает панель управления аутентификацией администраторов в Центре управления.
   - Конфигурация Сервера Dr.Web – открывает панель основных настроек Сервера.
   - Удаленный доступ к Серверу Dr.Web – содержит настройки для подключения утилиты дистанционной диагностики Сервера.
   - Планировщик заданий Сервера Dr.Web – открывает панель настройки расписания заданий Сервера.
   - Конфигурация веб-сервера – открывает панель основных настроек Веб-сервера.

- Пользовательские процедуры.

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.
- **Установка по сети** – позволяет упростить установку ПО Агента на конкретные рабочие станции (см. **Руководство по установке**, п. Установка Агента Dr.Web с использованием Центра управления безопасностью Dr.Web).

5. **Оповещения**

- Оповещения веб-консоли – позволяет просматривать и управлять оповещениями администратора, полученными методом **Веб консоль**.
- Неотправленные оповещения – позволяет отслеживать и управлять оповещениями администратора, которые не удалось отправить согласно настройкам раздела **Конфигурация оповещений**.
- Конфигурация оповещений – позволяет осуществлять настройку оповещений администратора о событиях в антивирусной сети.

6. **Репозиторий**

- Состояние репозитория – позволяет проверить состояние репозитория: дату последнего обновления компонентов репозитория и их состояние. А также произвести обновление репозитория с ВСО.
- Отложенные обновления – содержит список продуктов, для которых были временно запрещены обновления продуктов в разделе **Детальная конфигурация репозитория**.
- Общая конфигурация репозитория – открывает окно настроек подключения к ВСО и обновления репозитория для всех продуктов.
- Детальная конфигурация репозитория – позволяет настроить конфигурацию ревизий для каждого продукта репозитория в отдельности.
- Содержимое репозитория – позволяет просматривать и управлять текущим содержимым репозитория на уровне каталогов и файлов репозитория.

7. **Дополнительные возможности**

- Управление базой данных – позволяет осуществлять непосредственное обслуживание базы данных, с которой работает Сервер Dr.Web.
- Статистика Сервера Dr.Web – содержит статистику работы данного Сервера.
- **SQL-консоль** – предоставляет возможность выполнять SQL-запросы к базе данных, используемой Сервером Dr.Web.
- **Lua-консоль** – предоставляет возможность исполнять LUA-скрипты, как набранные непосредственно в консоли, так и загруженные из файла.

Администратор с доступом к lua-консоли получает доступ ко всей файловой системе в пределах каталога Сервера и некоторым системным командам на компьютере с установленным Сервером.

Чтобы запретить доступ к lua-консоли, отключите право **Дополнительные возможности** для соответствующего администратора (см. п. Администраторы и административные группы).

- **Утилиты** – открывает раздел для загрузки дополнительных утилит для работы с Dr.Web Enterprise Security Suite:
  - Загрузчик репозитория Dr.Web для скачивания продуктов Dr.Web Enterprise Security Suite из Всемирной системы обновлений. Графическая версия Загрузчика репозитория Dr.Web доступна только под ОС Windows.
  - Утилита дистанционной диагностики Сервера Dr.Web позволяет удаленно подключаться к Серверу Dr.Web для базового управления и просмотра статистики работы. См. также п. Удаленный доступ к Серверу Dr.Web.
  - Мобильный центр управления Dr.Web для администрирования антивирусной сети, построенной на основе Dr.Web Enterprise Security Suite. Предназначен для установки и запуска на мобильных устройствах под управлением iOS и ОС Android.

4.3.2. Антивирусная сеть

Выберите в главном меню Центра управления пункт **Антивирусная сеть**.

Управляющее меню

Для просмотра и редактирования информации в открывшемся окне служит управляющее меню, расположенное в левой части окна.

Управляющее меню содержит следующие пункты:

1. **Общие**
   - Графики
   - Запущенные компоненты
   - Установленные компоненты
   - Карантин
   - Сравнение оборудования и программ (при выборе группы или нескольких станций)
   - **Сессии пользователей**
   - **Неактивные станции**
   - Оборудование и программы (при выборе станции)
   - Свойства
   - Правила членства в группе (при выборе пользовательской группы)

2. Статистика
3. **Конфигурация**
   - Права
   - Планировщик заданий
   - Устанавливаемые компоненты
   - Ограничения обновлений
   - Список антивирусных компонентов для операционной системы выбранной станции или по спискам операционных систем при выборе группы.

> Детальное описание настроек антивирусных компонентов, задаваемых через Центр управления, приведено в **Руководствах администратора** по управлению станциями для соответствующей операционной системы.

Иерархический список антивирусной сети

В центральной части окна расположен иерархический список антивирусной сети. Иерархический список 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 и краткой сводки по станции на панели свойств (в правой части окна);
- нажмите левой кнопкой мыши на значок группы, чтобы отобразить или скрыть содержимое группы;
- нажмите левой кнопкой мыши на значок станции для перехода в раздел свойств этой станции.

> 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 4-1).

Таблица 4-1. Значки элементов иерархического списка

Значок	Описание
Группы. Основные значки	
	Группы, всегда отображаемые в иерархическом списке.

Значок	Описание
	Группы не будут отображаться в иерархическом списке, если: • для групп было применено действие **Настроить видимость группы** → **Скрывать, если пустая** и в данный момент группы не содержат станций, • для групп было применено действие **Настроить видимость группы** → **Скрывать** и в данный момент в разделе **Настройки вида дерева** снят флаг **Показывать скрытые группы**.
Рабочие станции. Основные значки	
	Доступная рабочая станция с установленным антивирусным ПО.
	Станция недоступна.
	Антивирусное ПО на станции деинсталлировано.
	Состояние станции при удаленной установке Агента по сети. Станция находится в данном состоянии с момента удачной установки Агента на станции до момента первого подключения станции к Серверу.
Дополнительные значки	
	Значок персональных настроек отображается на основных значках станций и групп, для которых заданы персональные настройки (для групп в том числе, если в группе есть станции с персональными настройками). Для отображения значка выберите пункт **Настройки вида дерева** на панели инструментов и установите флаг **Показывать значок персональных настроек**. Например, если персональные настройки заданы для рабочей станции с установленным антивирусным ПО, находящейся в данный момент в сети, то ее значок будет выглядеть следующим образом:  .
	Значок ошибки обновления отображается рядом с основными значками станций, на которых произошли ошибки при обновлении антивирусного ПО. Для отображения значка выберите пункт **Настройки вида дерева** на панели инструментов и установите флаг **Показывать значок ошибки обновления**. Например, если произошла ошибка обновления антивирусного ПО на рабочей станции, находящейся в данный момент в сети, то ее значок будет выглядеть следующим образом:  .
	Значок правил членства отображается рядом со основными значками групп, для которых установлены правила автоматического размещения станций. Для отображения значка выберите пункт **Настройки вида дерева** на панели инструментов и установите флаг **Показывать значок правил членства**.

Значок	Описание
	Например, если для группы, которая всегда отображается в иерархическом списке, заданы правила членства, то ее значок будет выглядеть следующим образом: .

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

Панель инструментов

Панель инструментов иерархического списка содержит следующие элементы:

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

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

Удалить выбранные объекты. Позволяет удалить объекты иерархического списка. Для этого выберите в списке объект или несколько объектов и нажмите **Удалить выбранные объекты**.

Удалить правила членства. Позволяет удалить правила для автоматического включения станций в группы.

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

Назначить первичную группу для станций. Позволяет назначить для выделенных в иерархическом списке станций первичную группу. При этом, если в иерархическом списке выделена группа, то для всех входящих в нее станций будет назначена выбранная 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.

Удалить персональные настройки. 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 также удалены у всех входящих в нее станций.

Отправить сообщение станциям. Позволяет отправить пользователям сообщение произвольного содержания.

Сбросить пароль. Позволяет удалить пользовательский пароль для доступа к настройкам антивирусных компонентов на выбранных станциях. Опция доступна только для станций под ОС Windows.

Перезагрузить станцию. Позволяет удаленно запустить процесс перезагрузки станции.

Деинсталлировать Агент Dr.Web. Удаляет Агента и антивирусное ПО с выбранной станции или группы станций.

Установить Агент Dr.Web. 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. Данный пункт активен только при выборе станций из подгруппы **Deleted** в группе **Status**.

Разослать инсталляционные файлы. Позволяет разослать инсталляционный файлы для выбранных в списке станций на адреса электронной почты, задаваемые в настройках данного раздела.

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. **Руководство по установке**, п. Создание новой учетной записи).

Создать группу. Позволяет создать новую группу станций.

Экспортировать данные:

Сохранить в формате CSV – записать общие данные о выбранных станциях антивирусной сети в файл формата CSV.

Сохранить в формате HTML – записать общие данные о выбранных станциях антивирусной сети в файл формата HTML.

Сохранить в формате XML – записать общие данные о выбранных станциях антивирусной сети в файл формата XML.

Сохранить в формате PDF – записать общие данные о выбранных станциях антивирусной сети в файл формата PDF.

При выборе перечисленных выше опций из раздела **Экспортировать данные** будет экспортирована информация только о выбранных станциях и станциях, входящих в выбранные группы.

Экспортировать конфигурацию – сохранить в файл конфигурацию выбранного объекта антивирусной сети. Для данной опции будет предложено выбрать сохраняемые разделы конфигурации.

Импортировать конфигурацию – загрузить из файла конфигурацию выбранного объекта антивирусной сети. Для данной опции будет предложено выбрать файл, из которого будет загружена конфигурация, а также загружаемые разделы конфигурации.

Распространить конфигурацию – распространить конфигурацию выбранного объекта на другие объекты антивирусной сети. Для данной опции будет предложено выбрать объекты, на которые будет распространена конфигурация, а также распространяемые разделы конфигурации.

Настроить видимость 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. табл. 4-1):

Скрывать – 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 сбойные компоненты. Предписывает принудительно синхронизировать компоненты, обновление которых прошло с ошибкой.

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).

Прервать запущенные компоненты. Предписывает остановить работу запущенных на станции антивирусных компонентов.

Сканировать. Позволяет провести сканирование станции в одном из режимов, выбираемых в выпадающем списке:

Сканер Dr.Web. Быстрое сканирование. В данном режиме производится сканирование при помощи Dr.Web Agent Сканера 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.

Сканер Dr.Web. Полное сканирование. В данном режиме производится полное сканирование всех жестких дисков и сменных носителей (включая загрузочные секторы) при помощи Dr.Web Agent Сканера.

Сканер Dr.Web. Выборочное сканирование. Данный режим предоставляет возможность выбрать любые папки и файлы для последующего сканирования при помощи Dr.Web Agent Сканера.

Неподтвержденные станции. Позволяет управлять списком новичков – станций, регистрация которых не подтверждена (подробнее см. раздел Политика подключения станций). Данный пункт активен только при выборе станций из подгруппы **Newbies** в группе **Status**.

При подтверждении регистрации или при отказе в доступе к Серверу станции будут автоматически удалены из предустановленной подгруппы **Newbies**. Для этого выберите в выпадающем списке один из следующих вариантов:

Разрешить доступ выбранным станциям и назначить первичную группу. Предписывает подтвердить доступ станции к Серверу и задать для нее первичную группу из предложенного списка.

Отменить действие, заданное для выполнения при подключении. Предписывает отменить действие над неподтвержденной станцией, которое было ранее назначено для выполнения в момент, когда станция подключится к Серверу.

Отказать в доступе выбранным станциям. Предписывает запретить доступ станции к Серверу.

Настройки вида дерева. Позволяют изменять внешний вид дерева антивирусной сети. Для включения параметра установите соответствующие флаги в выпадающем меню:

- для групп:
  - **Членство во всех группах** – дублировать отображение станции в списке, если она входит в несколько групп одновременно (только для групп, идущих под значком белой папки – см. табл. 4-1). Если флаг установлен, будут показаны все вхождения станции. Если снят – станция будет отображена в списке единожды.
  - **Показывать скрытые группы** – отображать 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 идентификаторы станций** – отображать уникальные идентификаторы станций в иерархическом списке.
  - **Показывать названия станций** – отображать имена (названия) станций.

> Нельзя отключить отображение идентификаторов и названий станций одновременно. Один из параметров **Показывать идентификаторы станций** и **Показывать названия станций** всегда будет выбран.

  - **Показывать адреса станций** – отображать IP-адреса станций в иерархическом списке.
  - **Показывать серверы станций** – отображать имена или IP-адреса антивирусных Серверов, к котором подключены станции.
  - **Показывать значок ошибки обновления** – отображать маркер на значках станций, последнее обновление на которых завершилось ошибкой.
- для всех элементов:
  - **Показывать значок персональных настроек** – отображать маркер на значках станций и групп, обозначающий наличие персональных настроек.
  - **Показывать описания** – отображать описания групп и станций (описания задаются в свойствах элемента).

- **Показывать число станций** – отображать количество станций для всех групп антивирусной сети.
- **Показывать значок правил членства** – отображать маркер на значках станций, которые были добавлены в группу автоматически согласно правилам членства, а также на значках групп, в которые станции были добавлены автоматически.

Настройки сортировки станций. Позволяют изменять параметр, по которому осуществляется сортировка, и порядок сортировки станций в дереве антивирусной сети.

- Для выбора параметра, по которому будет производиться сортировка, установите один из следующих флагов (допускается выбор только одного параметра):
  - **Идентификатор** – сортировать по уникальным идентификаторам станций.
  - **Название** – сортировать по именам станций.
  - **Адрес** – сортировать по сетевым адресам станций. Те станции, у которых нет сетевого адреса, будут выводиться в произвольном порядке без сортировки.
  - **Дата создания** – сортировать по дате создания учетной записи станции на Сервере.
- Для выбора порядка сортировки установите один из следующих флагов:
  - **Сортировать по возрастанию**.
  - **Сортировать по убыванию**.

Разделы **Настройки вида дерева** и **Настройки сортировки станций** взаимозависимы:

- Если вы выбираете параметр сортировки в разделе **Настройки сортировки станций**, отображение этого параметра автоматически включается в разделе **Настройки вида дерева**, если оно было отключено.
- Если в разделе **Настройки вида дерева** вы отключаете отображение параметра, выбранного для сортировки в разделе **Настройки сортировки станций**, то сортировка по этому параметру автоматически переключается на сортировку по названию станций. Если отображение названий станций при этом отключено, то сортировка переключается на идентификатор станций (название и идентификатор одновременно не могут быть отключены).

Панель свойств

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

Для отображения панели свойств:

1. В иерархическом списке нажмите на название станции или группы.
2. В правой части окна Центра управления откроется панель со свойствами выбранной группы или рабочей станции. Подробное описание данных настроек приведено в п. Редактирование групп и Свойства станции.

4.3.3. 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 Dr.Web).

В иерархическом списке приведены все Серверы Dr.Web, связанные с данным Сервером.

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

Таблицы

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

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

4.3.4. 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,
   - **Имя пользователя** – для поиска станций по имени пользователя на станции,
   - **IP-адрес** – для поиска станций по IP-адресу,
   - **Оборудование** – для поиска станций по названию или категории аппаратного обеспечения, установленного на станции,

- **Программа** – для поиска станций по названию программного обеспечения, установленного на станции.

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. Откроется расширенная панель поиска и дерево антивирусной сети.
4. В дереве антивирусной сети отображаются 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**.

4.3.5. События

Для оповещения администратора о событиях, требующих внимания, служит раздел, отображаемый в главном меню значком **События**.

Значок может находиться в следующих состояниях:

– нет новых оповещений о событиях в сети.

– есть новые оповещения о малозначительных событиях.

– есть новые оповещения о важных событиях, требующих вмешательства администратора.

Для списка событий возможны следующие действия:

1. При нажатии на значок открывается выпадающий список событий антивирусной сети. При этом значок автоматически меняется на .
2. При нажатии на строку оповещения о событии осуществляется переход в раздел Центра управления, отвечающий за соответствующий функционал.
3. Корешок каждого оповещения в списке событий помечается цветом, соответствующим важности события (аналогично значку). При переходе в раздел, отвечающий за функционал оповещения, оповещение считается прочитанными, и корешок меняет цвет на серый.

Таблица 4-2. Список возможных оповещений о событиях в антивирусной сети

Событие	Важность	Раздел Центра управления	Описание
Установить расширение браузера для Центра управления безопасностью Dr.Web	малозначительное	Страница для скачивания расширения Центра управления безопасностью Dr.Web	Требуется установка расширения Центра управления безопасностью Dr.Web.
Непрочитанные новости	малозначительное	**Помощь** → **Новости**	Доступны непрочитанные новости компании «Доктор Веб».
Новые оповещения	малозначительное	**Администрирование** → **Оповещения веб-консоли**	Доступны новые оповещения администратора, полученные методом **Веб-консоль**.
Критические оповещения	важное		
Доступны обновления Сервера	важное	**Администрирование** → **Сервер Dr.Web**	Обновление Сервера Dr.Web было загружено в репозиторий и доступно для установки.
Конфигурация Сервера была изменена. Требуется перезапуск Сервера.	важное	**Администрирование** → **Конфигурация Сервера Dr.Web**	Настройки конфигурационного файла Сервера были изменены после запуска Сервера. Требуется перезагрузка Сервера для принятия новых настроек.
Конфигурация веб-сервера была изменена. Требуется перезапуск Сервера.	важное	**Администрирование** → **Конфигурация веб-сервера**	Настройки конфигурационного файла веб-сервера были изменены после запуска Сервера. Требуется перезагрузка Сервера для принятия новых настроек.

4.3.6. Настройки

Для перехода в раздел настроек Центра управления нажмите в главном меню кнопку **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**.

- **Подписка**.

Моя учетная запись

При помощи данного раздела осуществляется управление текущей учетной записью администратора антивирусной сети (см. также п. Администраторы и административные группы).

Общие

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

При необходимости отредактируйте следующие параметры:

- **Регистрационное имя** администратора – логин для доступа к Центру управления.
- 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 смены пароля нажмите кнопку **Изменить пароль** на панели инструментов.

Следующие параметры доступны только для чтения:

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

Права

Описание прав администраторов и их редактирование приведено в разделе Редактирование администраторов.

После изменения параметров нажмите кнопку **Сохранить**.

Интерфейс

Настройки вида дерева

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

- для групп:
  - **Членство во всех группах** – дублировать отображение станции в списке, если она входит в несколько групп одновременно (только для групп, идущих под значком белой папки – см. табл. 4-1). Если флаг установлен, будут показаны все вхождения станции. Если снят – станция будет отображена в списке единожды.
  - **Показывать скрытые группы** – отображать 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 идентификаторы станций** – отображать уникальные идентификаторы станций в иерархическом списке.
  - **Показывать названия станций** – отображать имена (названия) станций.

> Нельзя отключить отображение идентификаторов и названий станций одновременно. Один из параметров **Показывать идентификаторы станций** и **Показывать названия станций** всегда будет выбран.

  - **Показывать адреса станций** – отображать IP-адреса станций в иерархическом списке.
  - **Показывать серверы станций** – отображать имена или IP-адреса антивирусных Серверов, к котором подключены станции.
  - **Показывать значок ошибки обновления** – отображать маркер на значках станций, последнее обновление на которых завершилось ошибкой.
- для всех элементов:
  - **Показывать значок персональных настроек** – отображать маркер на значках станций и групп, обозначающий наличие персональных настроек.
  - **Показывать описания** – отображать описания групп и станций (описания задаются в свойствах элемента).
  - **Показывать число станций** – отображать количество станций для всех групп антивирусной сети.
  - **Показывать значок правил членства** – отображать маркер на значках станций, которые были добавлены в группу автоматически согласно правилам членства, а также на значках групп, в которые станции были добавлены автоматически.

Сканер сети

Для работы Сканера сети необходимо, чтобы было установлено расширение Центра управления безопасностью Dr.Web.

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 выберите пункт **Сканер сети**.

Задайте следующие параметры Сканера сети:

1. В поле **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 использованием префикса сети (например, `10.4.0.0/24`).
2. При необходимости измените **Порт** и значение параметра **Тайм-аут (с)**.
3. Для сохранения значений по умолчанию нажмите 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 статистики по рабочей станции):

- В выпадающем списке **Интервал по умолчанию для 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 списке **Интервал по умолчанию для 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 Центра управления безопасностью Dr.Web, будут сохранены имя и пароль, которые администратор укажет при следующей авторизации в Центре управления.

Для функционирования автоматической авторизации необходимо, чтобы было установлено расширение Центра управления безопасностью Dr.Web.

В дальнейшем, при открытии любого Центра управления безопасностью 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 главном меню 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**.

В выпадающем списке **Длительность сессии** выберите период времени, по истечении которого сессия работы с Центром управления в веб-браузере автоматически прерывается.

Экспорт в PDF

В данном подразделе задаются настройки текста при экспорте статистических данных в формат PDF:

- В выпадающем списке **Шрифт отчетов** вы можете выбрать шрифт текста, используемый при экспорте отчетов в формат PDF.
- В поле **Размер шрифта отчетов** задается размер шрифта основного текста статистических таблиц, используемый при экспорте отчетов в формат PDF.

Отчеты

В данном подразделе задаются настройки отображения статистических данных в разделе **Отчеты** Центра управления:

- В поле **Количество строк на странице** задается максимальное количество строк на одной странице отчета при постраничном отображении статистики.
- Установите флаг **Показывать графики**, чтобы отображать графические данные на страницах статистических отчетов. Если флаг снят, отображение графических данных отключается.

Подписка

В данном подразделе настраивается подписка на новости компании «Доктор Веб».

Установите флаг **Автоматическая подписка на новые разделы** для автоматического добавления новых разделов в разделе новостей в Центре управления.

4.3.7. Помощь

Для перехода в раздел помощи Центра управления нажмите в главном меню кнопку **Помощь**.

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

1. **Общие**
   - **Форум** – перейти на форум компании «Доктор Веб».
   - **Новости** – перейти на страницу новостей компании «Доктор Веб».
   - **Обратиться в службу технической поддержки** – перейти на страницу технической поддержки «Доктор Веб».
   - **Прислать подозрительный файл** – открыть форму для отправки вируса в лабораторию «Доктор Веб».
   - **Википедия «Доктор Веб»** – перейти на страницу Википедии – базы знаний, посвященной продуктам компании «Доктор Веб».
   - **Сообщить о ложном срабатывании в Офисном контроле** – открыть форму для отправки сообщения о ложном срабатывании или пропуске вредных ссылок в модуле Офисного контроля.
2. **Документация администратора**
   - **Руководство администратора** – открыть документацию администратора в формате HTML.
   - **Руководство по установке** – открыть документацию по установке Dr.Web Enterprise Security Suite в формате HTML.

- **Инструкция по развертыванию антивирусной сети** – открыть краткую инструкцию по развертыванию антивирусной сети в формате HTML. Рекомендуется ознакомиться с данной инструкцией перед началом развертывания антивирусной сети, установкой и настройкой компонентов.
- **Приложения** – открыть приложения к руководству администратора в формате HTML.
- **Руководство по Web API** – открыть документацию администратора по Web API (см. также документ **Приложения**, п. Приложение L. Интеграция 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. **Документация пользователя** – открыть документацию пользователя в формате HTML для соответствующей операционной системы, представленной в списке.

4.4. Компоненты Центра управления безопасностью Dr.Web

4.4.1. Сканер сети

В состав Сервера Dr.Web 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 было установлено расширение Центра управления безопасностью Dr.Web.

Для корректной работы Сканера сети под веб-браузером Windows Internet Explorer необходимо в настройках веб-браузера добавить адрес Центра управления, в котором запускается Сканер Сети, в доверенную зону: **Сервис** → **Свойства обозревателя** → **Безопасность** → **Надежные узлы**.

Сканер сети реализует следующие функции:

- Сканирование (обзор) сети с целью обнаружения рабочих станций.
- Определение наличия Агента Dr.Web на станциях.
- Установка Агента Dr.Web на обнаруженные станции по указанию администратора. Установка Агента Dr.Web подробно описана в **Руководстве по установке**, п. Установка Агента Dr.Web с использованием Центра управления безопасностью 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. Установите флаг **Поиск по IP-адресам**, чтобы осуществлять поиск станций в сети по заданным IP-адресам. Укажите в поле **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`).
3. Для ОС Windows: установите флаг **Поиск в Active Directory**, чтобы осуществлять поиск станций в домене Active Directory. При этом задайте следующие параметры:
   - **Домены** – список доменов, в которых будет осуществляться поиск станций. В качестве разделителя для нескольких доменов используйте запятую.
   - **Контроллер Active Directory** – контроллер Active Directory, например, dc.example.com.

   
   Для поиска станций в домене Active Directory при помощи Сканера сети необходимо, чтобы веб-браузер, в котором открыт Центр управления, был запущен от имени доменного пользователя с правами на поиск объектов в домене Active Directory.
4. Для ОС семейства UNIX: установите флаг **Поиск по LDAP**, чтобы осуществлять поиск станций по LDAP. При этом задайте следующие параметры:
   - **Домены** – список доменов, в которых будет осуществляться поиск станций. В качестве разделителя для нескольких доменов используйте запятую.
   - **Сервер LDAP** – сервер LDAP, например, ldap://ldap.example.com.
   - **Регистрационное имя** – регистрационное имя пользователя LDAP.
   - **Пароль** – пароль пользователя LDAP.
5. В поле **Порт** укажите номер порта, по которому следует обращаться через протокол UDP к Агентам при поиске.
6. При необходимости в поле **Тайм-аут (с)** измените значение тайм-аута в секундах, в течение которого будет ожидаться ответ от опрашиваемых станций.
7. 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.
8. 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 обнаружены 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.

9. Нажмите кнопку **Сканировать**. После этого начнется сканирование сети.
10. В процессе сканирования сети в окно будет загружаться каталог (иерархический список) компьютеров с указанием наличия на них Агента Dr.Web.

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

Таблица 4-3. Возможные виды значков

Значок	Описание
Рабочие группы	
	Рабочие группы, содержащие в числе прочих компьютеры, на которые можно установить антивирус Dr.Web Enterprise Security Suite.
	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.

Взаимодействие с Агентами Dr.Web

Инструмент **Сканер сети** включен в состав Dr.Web Enterprise Security Suite 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.

4.4.2. Менеджер лицензий

Подробная информация о принципах и особенностях лицензирования Dr.Web Enterprise Security Suite приведена в разделе Глава 2: Лицензирование.

Интерфейс Менеджера лицензий

В состав Центра управления входит Менеджер лицензий. Данный компонент используется для управления лицензированием объектов антивирусной сети.

Для того чтобы открыть окно Менеджера лицензий, выберите в главном меню Центра управления пункт **Администрирование**, в открывшемся окне выберите пункт управляющего меню **Менеджер лицензий**.

Иерархический список ключей

Главное окно Менеджера лицензий содержит дерево ключей – иерархический список, узлами которого являются лицензионные ключи, а также станции и группы, для которых назначены лицензионные ключи.

Панель инструментов содержит следующие элементы управления:

Опция	Описание	Зависимость от объектов в дереве ключей
Добавить ключ	Добавить новую запись о лицензионном ключе.	Опция всегда доступна. Особенности функционала зависят от того, выбран ли объект в дереве ключей или нет (см. Добавление нового лицензионного ключа).
Удалить выбранные объекты	Удалить связь между ключом и объектом лицензирования.	Опция доступна, если в дереве выбран объект лицензирования (стан-

Опция	Описание	Зависимость от объектов в дереве ключей
		ция или группа) или лицензионный ключ.
Распространить ключ на группы и станции	Заменить или добавить выбранный ключ к объекту лицензирования.	Опция доступна, если в дереве выбран лицензионный ключ.
Экспортировать ключ	Сохранить локальную копию файла лицензионного ключа.	
Распространить ключ на соседние Серверы	Передать лицензии из выбранного ключа соседним Серверам.	

Настройки вида дерева позволяют изменять вид иерархического дерева:

- Флаг **Показывать количество лицензий** включает/выключает отображение в дереве ключей общего количества лицензий, предоставляемых ключевыми файлами.
- Для изменения структуры дерева используйте следующие опции:
  - Опция **Ключи** предписывает отображать все лицензионные ключи антивирусной сети в качестве корневых узлов иерархическое дерева. При этом вложенными элементами лицензионных ключей являются все группы и станции, для которых назначены эти ключи. Данное представление дерева является основным и позволяет управлять объектами лицензирования и лицензионными ключами.
  - Опция **Группы** предписывает отображать в качестве корневых узлов иерархического дерева те группы, для которых непосредственно назначены лицензионные ключи. При этом вложенными элементами групп являются станции, входящие в данные группы, и лицензионные ключи, которые назначены для этих групп. Данное представление дерева служит для удобства визуализации информации о лицензировании и не позволяет управлять объектами дерева.

Работа с лицензиями

При помощи Менеджера лицензий вы можете осуществлять следующие действия над лицензионными ключами:

1. Просмотр информации о лицензии.
2. Добавление нового лицензионного ключа.
3. Обновление лицензионного ключа.
4. Замена лицензионного ключа.
5. Расширение списка лицензионных ключей объекта.
6. Удаление лицензионного ключа и удаление объекта из списка лицензирования.

7. Передача лицензий на соседний Сервер.
8. Редактирование лицензий, переданных на соседний Сервер.

Просмотр информации о лицензии

Для того чтобы просмотреть сводную информацию о лицензионном ключе, выберите в главном окне Менеджера лицензий учетную запись ключа, информацию о котором вы хотите просмотреть (нажмите на название учетной записи ключа). В открывшейся панели будет выведена такая информация, как:

- пользователь лицензии,
- продавец, у которого была приобретена данная лицензия,
- идентификационный и серийный номера лицензии,
- дата окончания срока действия лицензии,
- включает ли данная лицензия поддержку модуля Антиспам,
- количество станций, лицензируемых данным ключевым файлом,
- MD5-хэш лицензионного ключа,
- список антивирусных компонентов, которые позволяет использовать данная лицензия.

Добавление нового лицензионного ключа

Для того чтобы добавить новый лицензионный ключ:

1. В главном окне Менеджера лицензий нажмите кнопку **Добавить ключ** на панели инструментов.
2. На открывшейся панели нажмите кнопку и выберите файл с лицензионным ключом.
3. Нажмите кнопку **Сохранить**.
4. Лицензионный ключ будет добавлен в дерево ключей, но не привязан ни к одному из объектов. В этом случае для задания объектов лицензирования выполните процедуры Замена лицензионного ключа или Расширение списка лицензионных ключей объекта, описанные ниже.

Обновление лицензионного ключа

При обновлении лицензионного ключа, новый лицензионный ключ будет назначен для тех же объектов лицензирования, для которых был назначен обновляемый ключ.

Воспользуйтесь процедурой обновления ключа для замены ключа с истекшим сроком действия или для замены на ключ с другим списком устанавливаемых компонентов с сохранением структуры дерева ключей.

Для того чтобы обновить лицензионный ключ:

1. В главном окне Менеджера лицензий в дереве ключей выберите ключ, который хотите обновить.
2. На открывшейся панели свойств ключа нажмите кнопку  и выберите файл с лицензионным ключом.
3. Нажмите кнопку **Сохранить**. Откроется окно настроек устанавливаемых компонентов, описанное в подразделе Настройки при замене лицензионного ключа.
4. Нажмите кнопку **Сохранить** для обновления лицензионного ключа.

Замена лицензионного ключа

При замене лицензионного ключа, для объекта лицензирования удаляются все текущие лицензионные ключи и добавляется новый ключ.

Для того чтобы заменить текущий лицензионный ключ:

1. В главном окне Менеджера лицензий в дереве ключей выберите ключ, который хотите назначить объекту лицензирования.
2. На панели инструментов нажмите кнопку **Распространить ключ на группы и станции**. Откроется окно с иерархическим списком станций и групп антивирусной сети.
3. Выберите в списке объекты лицензирования. Для выбора нескольких станций и групп используйте кнопки CTRL и SHIFT.
4. Нажмите кнопку **Заменить ключ**. Откроется окно настроек устанавливаемых компонентов, описанное в подразделе Настройки при замене лицензионного ключа.
5. Нажмите кнопку **Сохранить** для замены лицензионного ключа.

Расширение списка лицензионных ключей объекта

При добавлении лицензионного ключа, для объекта лицензирования сохраняются все текущие ключи, и в список ключей добавляется новый лицензионный ключ.

Для того чтобы добавить лицензионный ключ к списку лицензионных ключей объекта:

1. В главном окне Менеджера лицензий в дереве ключей выберите ключ, который хотите добавить в список ключей объекта.
2. На панели инструментов нажмите кнопку **Распространить ключ на группы и станции**. Откроется окно с иерархическим списком станций и групп антивирусной сети.
3. Выберите в списке объекты лицензирования. Для выбора нескольких станций и групп используйте кнопки CTRL и SHIFT.

4. Нажмите кнопку **Добавить ключ**. Откроется окно настроек устанавливаемых компонентов, описанное в подразделе Настройки при добавлении лицензионного ключа в список ключей.
5. Нажмите кнопку **Сохранить** для добавления лицензионного ключа.

Удаление лицензионного ключа и удаление объекта из списка лицензирования

Нельзя удалить последнюю учетную запись ключа группы **Everyone**.

Для того чтобы удалить лицензионный ключ или объект из списка лицензирования:

1. В главном окне Менеджера лицензий выберите ключ, который вы хотите удалить, или объект (станцию или группу), для которого назначен этот ключ, и нажмите кнопку **Удалить выбранные объекты** на панели инструментов. При этом:
   - Если был выбран объект лицензирования, то он удаляется из списка объектов, на которых распространяется действие назначенного для него ключа. Для объекта, у которого удаляется персональный лицензионный ключ, устанавливается наследование лицензионного ключа.
   - Если был выбран лицензионный ключ, удаляется учетная запись ключа из антивирусной сети. Для всех объектов, для которых был назначен данный лицензионный ключ, будет установлено наследование лицензионного ключа.
2. Откроется окно настроек устанавливаемых компонентов, описанное в подразделе Настройки при замене лицензионного ключа.
3. Нажмите кнопку **Сохранить** для удаления выбранного объекта и переключения на наследуемый ключ.

Передача лицензий на соседний Сервер

При передаче части свободных лицензий на соседний Сервер из лицензионного ключа на данном Сервере, переданное количество лицензий будет недоступно для использования на данном Сервере до окончания срока распространения этих лицензий.

Для того чтобы передать лицензии на соседний Сервер:

1. В главном окне Менеджера лицензий в дереве ключей выберите ключ, свободные лицензии из которого хотите передать на соседний Сервер.
2. На панели инструментов нажмите кнопку **Распространить ключ на соседние Серверы**. Откроется окно с иерархическим списком соседних Серверов.
3. Выберите в списке Серверы, на которые хотите распространить лицензии.
4. Напротив каждого из Серверов задайте следующие параметры:

- **Количество лицензий** – количество свободных лицензий, которые вы хотите передать из данного ключа на соседний Сервер.
- **Дата окончания лицензии** – срок действия передачи лицензий. По истечении указанного срока, все лицензии будут отозваны с соседнего Сервера и вернутся в список свободных лицензий данного лицензионного ключа.

5. Нажмите одну из кнопок:
   - **Добавить ключ** – чтобы добавить лицензии к списку имеющихся лицензий соседних Серверов. Откроется окно настроек устанавливаемых компонентов, описанное в подразделе Настройки при добавлении лицензионного ключа в список ключей.
   - **Заменить ключ** – чтобы удалить текущие лицензии соседних Серверов и задать только распространяемые лицензии. Откроется окно настроек устанавливаемых компонентов, описанное в подразделе Настройки при замене лицензионного ключа.
6. Нажмите кнопку **Сохранить** для распространения лицензий на соседние Серверы.

Редактирование лицензий, переданных на соседний Сервер

Для того чтобы отредактировать лицензии, распространенные на соседний Сервер:

1. В главном окне Менеджера лицензий в дереве ключей выберите соседний Сервер, на который были распространены лицензии.
2. На открывшейся панели свойств отредактируйте следующие параметры:
   - **Количество лицензий** – количество свободных лицензий, которые переданы из ключа с данного Сервера на соседний Сервер.
   - **Дата окончания лицензии** – срок действия передачи лицензий. По истечении указанного срока, все лицензии будут отозваны с данного Сервера и вернутся в список свободных лицензий соответствующего лицензионного ключа.
3. Нажмите кнопку **Сохранить** для обновления информации по распространяемым лицензиям.

Изменение списка устанавливаемых компонентов

Настройки при замене лицензионного ключа

В данном подразделе описана настройка устанавливаемых компонентов при выполнении процедур:

- Обновление лицензионного ключа.
- Замена лицензионного ключа.
- Удаление лицензионного ключа.
- Передача лицензий на соседний Сервер с заменой ключа.

При выполнении данных процедур для настройки устанавливаемых компонентов:

1. В окне настроек устанавливаемых компонентов в списке объектов приведены:
   - Станции и группы со своими списками устанавливаемых компонентов.
   - В столбце **Текущий ключ** приведен список ключей объекта и настройки устанавливаемых компонентов, актуальные для объекта на данный момент.
   - В столбце **Назначаемый ключ** приведен ключ и настройки устанавливаемых компонентов, заданные в ключе, который будет назначен для выбранных объектов.
   - При необходимости установите флаг **Показывать только различающиеся**, чтобы в списке отображались только те компоненты, настройки которых в текущем и назначаемом ключах различаются.
2. Для настройки списка устанавливаемых компонентов:
   a) В столбце **Назначаемый ключ** вы можете настроить результирующий список устанавливаемых компонентов.
      - Настройки устанавливаемых компонентов в столбце **Назначаемый ключ** рассчитываются исходя из того, разрешено ли использование компонента в текущих настройках и новом ключе (+) или не разрешено (–), следующим образом:

Текущие настройки	Настройки назначаемого ключа	Результирующие настройки
+	+	+
–	+	+
+	–	–
–	–	–

      - Вы можете изменить настройки устанавливаемых компонентов (понизить права на установку) только если в настройках, полученных в столбце **Назначаемый ключ**, разрешено использование этого компонента.

   b) Установите флаги для тех объектов (станций и групп), для которых будет разорвано наследование настроек и заданы настройки устанавливаемых компонентов из столбца **Назначаемый ключ** в качестве персональных. Для остальных объектов (для которых флаги не установлены) будет установлено наследование изначальных настроек из столбца **Назначаемый ключ**.

Настройки при добавлении лицензионного ключа в список ключей

В данном подразделе описана настройка устанавливаемых компонентов при выполнении процедур:

- Расширение списка лицензионных ключей объекта.
- Передача лицензий на соседний Сервер с добавлением ключа.

При выполнении данных процедур для настройки устанавливаемых компонентов:

1. В окне настроек устанавливаемых компонентов в списке объектов приведены:
   - Станции и группы со своими списками устанавливаемых компонентов.
   - В столбце **Текущий ключ** приведен список ключей объекта и настройки устанавливаемых компонентов, актуальные для объекта на данный момент.
   - В столбце **Назначаемый ключ** приведен ключ и настройки устанавливаемых компонентов, заданные в ключе, который вы хотите добавить для выбранных объектов.
2. При необходимости установите флаг **Показывать только различающиеся**, чтобы в списке отображались только те компоненты, настройки которых в текущем и наследуемом ключах различаются. Обратите внимание, что в разделе **Назначаемый ключ** приведены не сами настройки назначаемого ключа, а результирующие настройки устанавливаемых компонентов.
3. Для настройки списка устанавливаемых компонентов:
   a) В столбце **Назначаемый ключ** вы можете настроить результирующий список устанавливаемых компонентов.
      - Настройки устанавливаемых компонентов в столбце **Назначаемый ключ** рассчитываются исходя из того, разрешено ли использование компонента в текущих настройках и новом ключе (+) или не разрешено (–), следующим образом:

Текущие настройки	Настройки назначаемого ключа	Результирующие настройки
+	+	+
–	+	–
+	–	–
–	–	–

      - Вы можете изменить настройки устанавливаемых компонентов (понизить права на установку) только если в настройках, полученных в столбце Назначаемый ключ, разрешено использование этого компонента.

   b) Установите флаги для тех объектов (станций и групп), для которых будет разорвано наследование настроек и заданы настройки устанавливаемых компонентов из столбца **Назначаемый ключ** в качестве персональных. Для остальных объектов (для которых флаги не установлены) будет установлено наследование настроек из столбца **Назначаемый ключ**.

4.5. Схема взаимодействия компонентов антивирусной сети

На рисунке 4-2 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 Dr.Web Enterprise Security Suite и антивирусных пакетов нахождение компьютеров в пределах какой-либо ЛВС необязательно, достаточно доступа в Интернет.

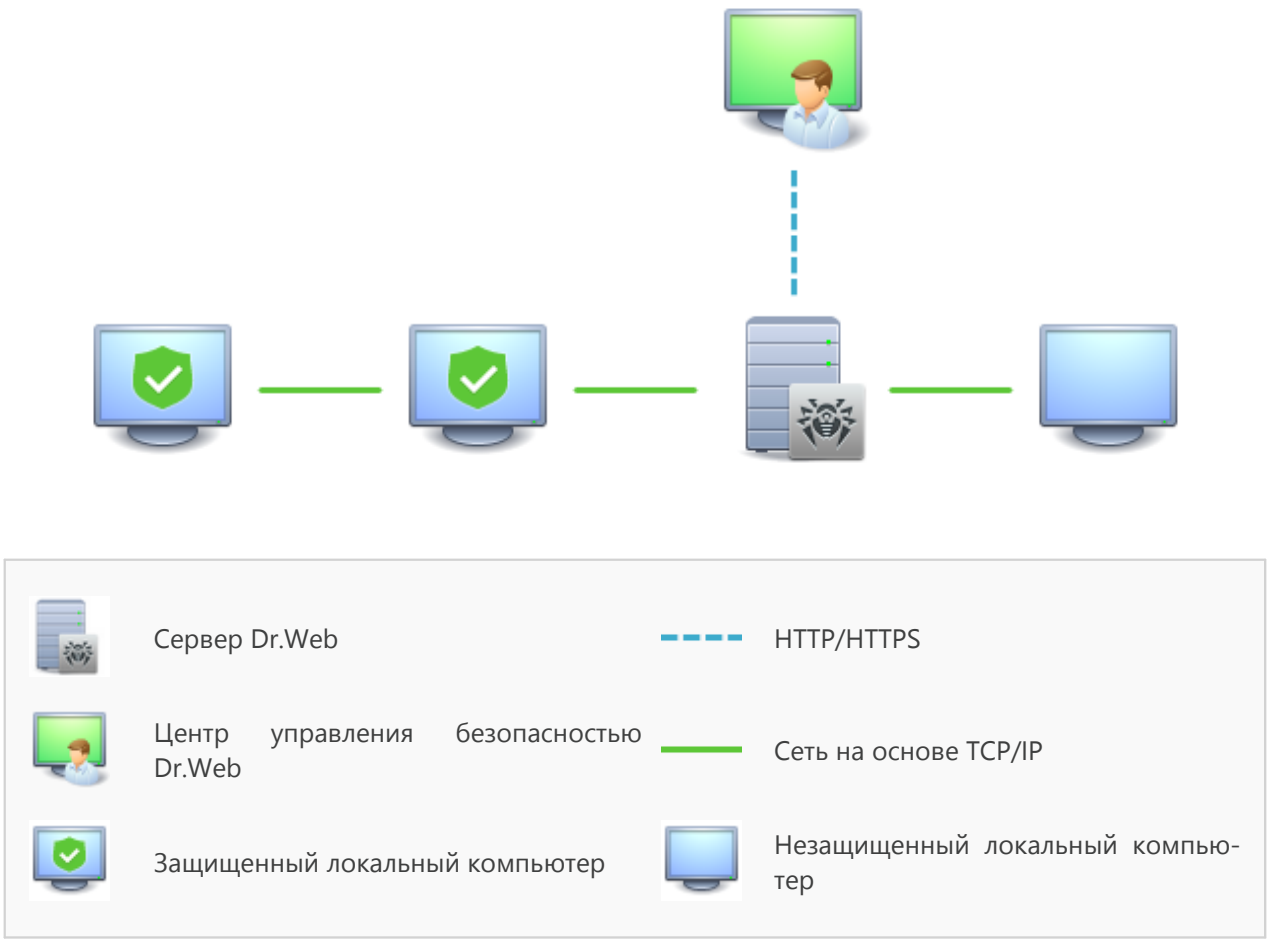


Рисунок 4-2. Структура антивирусной сети

При запуске Сервера Dr.Web выполняется следующая последовательность действий:

1. Загрузка файлов Сервера Dr.Web 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 Агентов Dr.Web и команд от Центров управления.

Весь поток команд, данных и статистической информации в антивирусной сети в обязательном порядке проходит через Сервер Dr.Web. Центр управления также обменивается информацией только с Сервером; изменения в конфигурации рабочей станции и передача команд Агенту Dr.Web осуществляется Сервером на основе команд Центра управления.

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

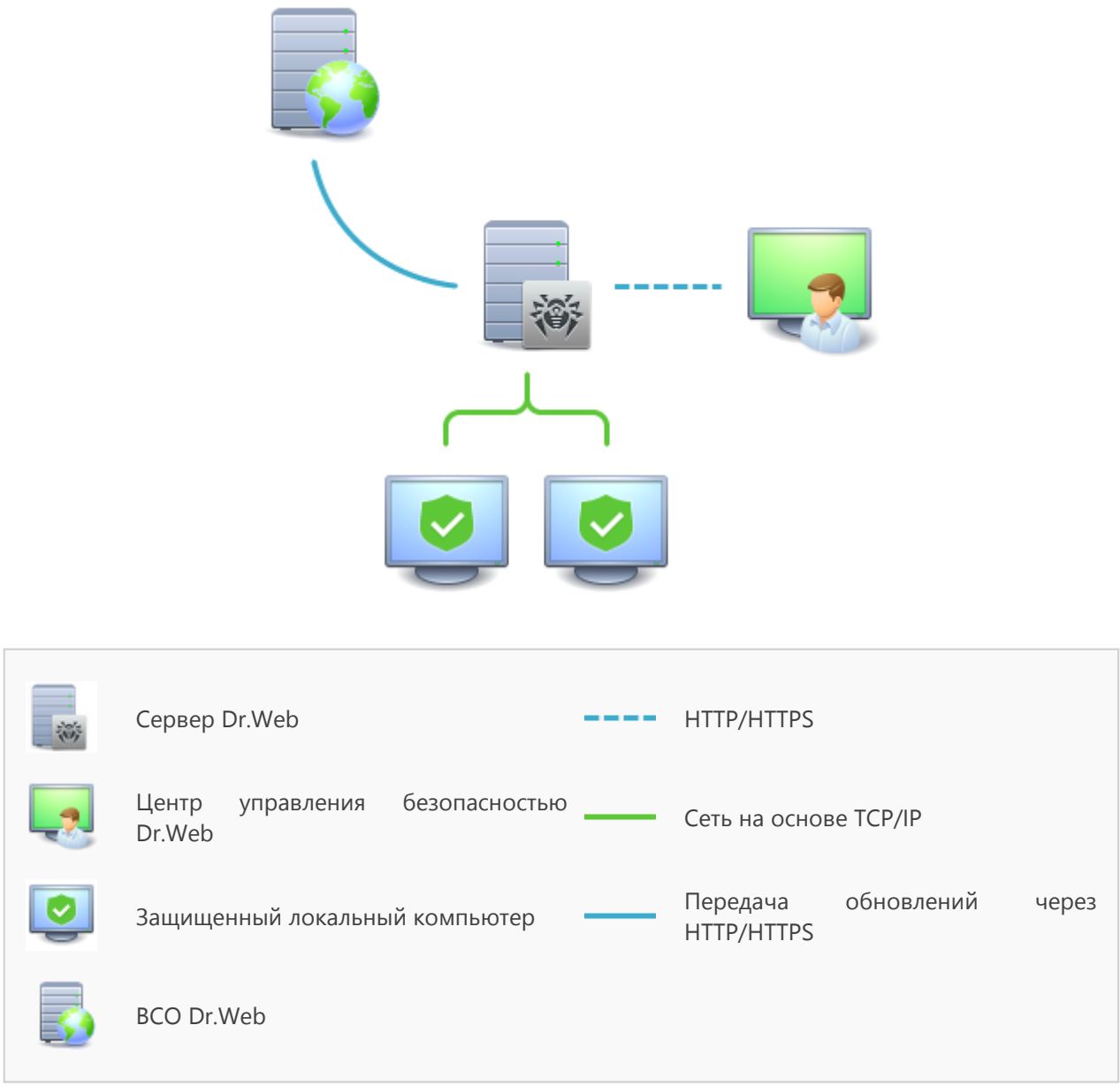


Рисунок 4-3. Логическая структура антивирусной сети

Между Сервером и рабочими станциями (сплошная тонкая линия на рисунке 4-3) 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 Enterprise Security Suite 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 Серверу Dr.Web (сплошная толстая линия на рисунке 4-3) 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 Enterprise Security Suite 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 4-3) 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 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 Сервера Dr.Web. 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 Сервера Dr.Web – полного доступа к каталогу его установки.

5.1. Аутентификация администраторов

Аутентификация администратора для подключения к Серверу Dr.Web 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.
5. С ипользованием PAM (только под ОС семейства UNIX).

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. Под ОС семейства UNIX пятой используется аутентификация PAM.
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 аутентификации:

1. Выберите пункт **Администрирование** в главном меню Центра управления.
2. В управляющем меню выберите раздел **Аутентификация**.
3. В открывшемся окне представлен список типов аутентификации в том порядке, в котором они используются. Для изменения порядка следования перетащите (drag'n'drop) методы аутентификации в списке и разместите их в таком порядке, в каком необходимо проводить аутентификацию.
4. Для принятия изменений перезагрузите Сервер.

Регистрационное имя администратора должно быть уникальным.

Подключение администраторов через внешние системы аутентификации будет невозможно, если на Сервере уже существует администратор с таким же регистрационным именем.

При каждом сохранении изменений раздела **Аутентификация** автоматически сохраняется резервная копия предыдущей версии конфигурационного файла с параметрами аутентификации администраторов. Хранению подлежат 10 последних копий.

Резервные копии располагаются в том же каталоге, что и сам конфигурационный файл, и называются в соответствии со следующим форматом:

<имя_файла>;<время_создания>

где *<имя_файла>* зависит от системы аутентификации: `auth-ads.xml`, `auth-ldap.xml`, `auth-radius.xml`, `auth-pam.xml`.

Вы можете использовать созданные резервные копии, в частности, для восстановления конфигурационного файла в случае, если интерфейс Центра управления недоступен.

5.1.1. 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 администраторов Сервера.

   Подробнее см. п. Администраторы и административные группы.

5.1.2. Аутентификация с использованием Active Directory

Для включения аутентификации через Active Directory:

1. Выберите пункт **Администрирование** в главном меню Центра управления.
2. В управляющем меню выберите раздел **Аутентификация**.
3. В открывшемся окне зайдите в раздел **Microsoft Active Directory**.
4. Установите флаг **Использовать аутентификацию Microsoft Active Directory**.
5. Нажмите **Сохранить**.
6. Для принятия изменений перезагрузите Сервер.

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 `drweb-esuite-modify-ad-schema-xxxxxxxxxxxxxx-windows-nt-xYY.exe` (входит в дистрибутив Сервера Dr.Web).
   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.

Если ранее была произведена модификация схемы Active Directory с использованием данной утилиты от 6 версии Сервера, нет необходимости повторно выполнять модификацию с использованием утилиты от 10 версии Сервера.

   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-xxxxxxxxxxxxx-windows-nt-xYY.msi` (входит в дистрибутив Dr.Web Enterprise Security Suite 10) 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 доступен следующий параметр (значение атрибута может быть **yes**, **no** или **not set**):

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

> Алгоритмы принципа работы и разбора атрибутов при аутентификации приведены в документе **Приложения**, в Приложении С1.

5.1.3. Аутентификация с использованием LDAP

Для включения аутентификации через LDAP:

1. Выберите пункт **Администрирование** в главном меню Центра управления.
2. В управляющем меню выберите раздел **Аутентификация**.
3. В открывшемся окне зайдите в раздел **LDAP-аутентификация**.
4. Установите флаг **Использовать LDAP-аутентификацию**.
5. Нажмите **Сохранить**.
6. Для принятия изменений перезагрузите Сервер.

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

> Настройки LDAP-аутентификации сохраняются в файле конфигурации `auth-ldap.xml`.
>
> Описание основных xml-атрибутов аутентификации приведено в документе **Приложения**, в Приложении С2.

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 аутентификации 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.

5.1.4. Аутентификация с использованием RADIUS

Для включения аутентификации через RADIUS:

1. Выберите пункт **Администрирование** в главном меню Центра управления.
2. В управляющем меню выберите раздел **Аутентификация**.
3. В открывшемся окне зайдите в раздел **RADIUS-аутентификация**.
4. Установите флаг **Использовать RADIUS-аутентификацию**.
5. Нажмите **Сохранить**.
6. Для принятия изменений перезагрузите Сервер.

Для использования протокола аутентификации RADIUS необходимо развернуть сервер, реализующий этот протокол, например, freeradius (подробности см. на http://freeradius.org/).

В Центре управления настраиваются следующие параметры работы с сервером RADIUS:

- **Сервер**, **Порт**, **Пароль** – параметры подключения к серверу RADIUS: IP-адрес/DNS-имя, номер порта, пароль (секрет) соответственно.
- **Тайм-аут** – время ожидания ответа от сервера RADIUS в секундах.

- **Количество повторных попыток** – количество повторных попыток соединения с сервером RADIUS.

Также для настройки дополнительных параметров RADIUS могут использоваться:

- Конфигурационный файле `auth-radius.xml`, расположенный в каталоге etc Сервера.

  Помимо параметров, настраиваемых через Центр управления, через конфигурационный файл вы можете задать значение идентификатора NAS. Данный идентификатор согласно RFC 2865 может быть использован вместо IP-адреса/DNS-имени в качестве идентификатора клиента при подключении к серверу RADIUS. В конфигурационном файле хранится в следующем виде:

```
<!-- NAS identifier, optional, default - hostname -->
<nas-id value="drwcs"/>
```

- Словарь `dictionary.drweb`, расположенный в каталоге `etc` Сервера.

  Словарь хранит набор атрибутов RADIUS компании «Доктор Веб» (VSA – Vendor-Specific Attributes).

5.1.5. Аутентификация с использованием PAM

Для включения аутентификации через PAM:

1. Выберите пункт **Администрирование** в главном меню Центра управления.
2. В управляющем меню выберите раздел **Аутентификация**.
3. В открывшемся окне зайдите в раздел **PAM-аутентификация**.
4. Установите флаг **Использовать PAM-аутентификацию**.
5. Нажмите **Сохранить**.
6. Для принятия изменений перезагрузите Сервер.

Аутентификация на основе PAM под ОС семейства UNIX осуществляется посредством подключаемых модулей аутентификации.

Для настройки параметров PAM-аутентификации вы можете использовать следующие способы:

- Настройки метода аутентификации через Центр управления: в разделе **Администрирование** → **Аутентификация** → **PAM-аутентификация**.
- Конфигурационный файл `auth-pam.xml`, расположенный в каталоге `etc` Сервера. Пример конфигурационного файла:

```
...
<!-- Enable this authorization module -->
  <enabled value="no" />
<!-- This authorization module number in the stack -->
  <order value="50" />
<!-- PAM service name>" -->
  <service name="drwcs" />
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->
  <admin-flag mandatory="no" name="DrWeb_ESuite_Admin" />
...
```

Описание параметров PAM-аутентификации, настраиваемых на стороне Dr.Web Enterprise Security Suite

Элемент Центра управления	Элементы файла auth-pam.xml			Описание
	Блок	Параметр	Допустимые значения	
Флаг **Использовать PAM-аутентификацию**	<enabled>	value	yes | no	Флаг, определяющий, будет ли использоваться метод PAM-аутентификации.
Используйте Drag and Drop	<order>	value	целочисленное значение, согласованное со значениями других методов	Порядковый номер PAM-аутентификации при использовании нескольких методов аутентификации.
Поле **Название службы**	<service>	name	-	Имя сервиса, которое будет использовано для создания PAM-контекста. PAM может считать политики для данного сервиса из /etc/pam.d/<*имя сервиса*> или из /etc/pam.conf, если файл не существует. Если параметр не задан (нет тега <service> в конфигурационном файле), то по умолчанию используется имя drwcs.
Флаг **Управляющий флаг обязателен**	<admin-flag>	mandatory	yes | no	Параметр, определяющий, является ли обязательным управляющий флаг для идентификации пользователя как администратора. По умолчанию – yes.
Поле **Название управляющего флага**	<admin-flag>	name	-	Ключ-строка, по которой у PAM-модулей будет прочитан флаг. По умолчанию – DrWeb_ESuite_Admin.

При настройке работы модулей PAM-аутентификации, используйте параметры, задаваемые на стороне Dr.Web Enterprise Security Suite, в том числе учитывайте значения, присваиваемые по умолчанию, даже если параметр не был задан.

5.2. Администраторы и административные группы

Чтобы открыть раздел управления административными учетными записями, выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Администраторы**.

Раздел **Администраторы** доступен всем администраторам Центра управления. Однако полное иерархическое дерево администраторов доступно только администраторам из группы **Administrators**, для которых разрешено право **Просмотр свойств и конфигурации групп администраторов**. Для остальных администраторов в иерархическом дереве будет отображаться только собственная группа и ее подгруппы с входящими в них учетными записями.

5.2.1. Иерархия администраторов

Иерархический список администраторов отображает древовидную структуру административных групп и учетных записей администраторов. Узлами данной структуры являются административные группы и входящие в них администраторы. Каждый администратор входит только в одну группу. Уровень вложенности групп не ограничен.

Предустановленные группы

После установки Сервера автоматически создаются две группы:

- **Administrators**. Изначально в группу входит только администратор **admin** с полным набором прав, автоматически создаваемый при установке Сервера (см. ниже).
- **Newbies**. Изначально группа пуста. В эту группу автоматически перемещаются администраторы с внешним типом аутентификации через LDAP, Active Directory и RADIUS.

  Администраторам из группы **Newbies** по умолчанию назначаются права только на чтение.

Предустановленные администраторы

После установки Сервера автоматически создается одна учетная запись администратора:

Параметр	Значение
Регистрационное имя	**admin**
Пароль	Задается при установке Сервера (шаг 9 в процедуре установки).
Права	Полный набор прав.

Параметр	Значение
Редактирование учетной записи	Права администратора нельзя редактировать, самого администратора невозможно удалить.

Отображение иерархических списков

- В иерархическом списке антивирусной сети: администратор видит только те пользовательские группы, которые разрешены в праве **Просмотр свойств групп станций**. Все системные группы также отображаются в дереве антивирусной сети, но в них видны только станции из указанного списка пользовательских групп.
- В иерархическом списке администраторов: администратор из группы **Newbies** видит дерево, корнем которого является группа, в которой он находится, т.е. видит администраторов из своей группы и её подгрупп. Администратор из группы **Administrators** видит всех администраторов, независимо от их групп.

5.2.2. Права администраторов

Все действия администраторов в Центре управления ограничиваются набором прав, который может быть определен как для отдельной учетной записи, так и для группы администраторов.

Система административных прав включает следующие возможности управления правами:

- **Назначение прав**

  Назначение прав осуществляется при создании администратора или административной группы. Права наследуются от родительской группы, в которую администратор или административная группа помещаются при создании. При создании возможность изменения прав не предоставляется.

- **Наследование прав**

  По умолчанию права администраторов и административных групп наследуются от родительской группы, но наследование может быть отключено.

  - Если наследование отключено, администратор использует независимый набор персональных прав, который задается непосредственно для его учетной записи. Права родительской группы при этом не учитываются.
  - При наследовании прав администратора или группы осуществляется не переназначение правами родительской группы, а перерасчет назначенного права исходя из всех прав родительских групп вверх по иерархическому дереву. Таблица для расчета результирующего права объекта в зависимости от назначенных прав и прав родительской групп приведена в п. Объединение прав.

- **Редактирование прав**

  При создании администраторов и административных групп возможность редактирования прав не предоставляется. Редактирование прав доступно только для уже созданных объектов и осуществляется в разделе настроек учетной записи или группы. При редактировании собственных настроек допускается только понижение прав. Редактирование прав предустановленного администратора **admin** и предустановленных групп **Administrators** и **Newbies** не предоставляется.

  Процедура редактирования прав приведена в разделе Редактирование прав.

Редактирование прав

Для редактирования прав администратора или административной группы:

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 отредактировать. Откроется раздел редактирования свойств.
3. В подразделе **Права** вы можете отредактировать список разрешенных действий для выбранного администратора или административной группы.
4. Для управления наследованием прав выбранного объекта от родительской группы используйте переключатель:

    **Наследование включено**

    **Наследование выключено**
5. Основные настройки задаются в таблице прав:

   a) В первом столбце приведены названия прав. Заголовок столбца зависит от конкретной секции, объединяющей права по типам.

   > Краткое описание прав администраторов и разделов Центра управления, за которые отвечают конкретные права, приведено в документе **Приложения**, в Приложении С3.

   b) В столбце **Права** приведены настройки для соответствующих прав из первого столбца.

Объекты управления	**Список настроек в столбце Права**	**Принцип задания права**
Право задается для всех объектов		
Право не подразумевает разделение на группы по объектам управления.	Может быть приведен один из следующих типов прав:	Установите/снимите флаг **Предоставить** в строке соответствующего права.

Объекты управления	Список настроек в столбце Права	Принцип задания права
	• **Персональное** – для данного объекта заданы собственные настройки. • **Наследуемое** – настройки унаследованы от родительской группы.	
Право задается для списка объектов (станций, администраторов или групп)		
• *Предоставлено всё* – право предоставлено для всех объектов управления. • *Запрещено всё* – право запрещено для всех объектов управления. • *Предоставлено для некоторых объектов*. При этом должен быть задан список объектов, для которых данное право предоставлено. Для всех остальных объектов право считается запрещенным. • *Запрещено для некоторых объектов*. При этом должен быть задан список объектов, для которых данное право запрещено. Для всех остальных объектов право считается предоставленным.	В случае объединения настроек приводятся одновременно следующие типы прав: • **Персональное** – собственные настройки, заданные для данного объекта. • **Результирующее** – результат слияния персонального права объекта и права родительской группы. В случае наследования настроек приводится только тип права **Наследуемое**.	Нажмите на список объектов (в том числе, если задан вариант **Все**). Откроется окно с деревом антивирусной сети, деревом групп администраторов или деревом тарифов в зависимости от редактируемого права. Выберите нужные объекты в дереве. Для выбора нескольких объектов используйте кнопки CTRL и SHIFT. При необходимости установите флаг **Для всех прав секции**, чтобы применить данные настройки для всех прав, приведенных в той же секции, что и редактируемое. Нажмите кнопку: • **Предоставить** для разрешения права на выбранные объекты. • **Запретить** для запрещения права на выбранные объекты.

Для одного и того же права, задаваемого на список объектов, не могут быть заданы одновременно списки запрещенных и разрешенных объектов. Данные понятия являются взаимоисключающими.

c) В столбце **Наследование** отражено состояние данного права относительно родительской группы:

- **Наследование от группы** – включено наследование от указанной родительской группы, персональные права не заданы.
- **Персональные настройки** – наследование от родительской группы отключено, заданы персональные права.
- **Объединение с группой** – включено наследование от указанной родительской группы, персональные права заданы. Результирующее право объекта рассчитано путем объединения прав родительской группы и персональных прав (см. п. Объединение прав).

В этом случае персональные права объекта можно удалить. Для этого нажмите кнопку  в столбце **Наследование**. После удаления персональных прав будет установлено **Наследование от группы**.

Объединение прав

Расчет результирующего права объекта (администратора или группы администраторов) при включенном наследовании зависит от прав родительских групп и прав, заданных самому объекту. Таблица ниже описывает принцип получения результирующего права объекта:

Право родительской группы	**Право рассматриваемого потомка**	**Результирующее право**
Предоставлено всё	Предоставлено для некоторых объектов	Предоставлено для объектов потомка
Предоставлено для некоторых объектов	Предоставлено для некоторых объектов	Списки разрешенных объектов объединяются
Предоставлено для некоторых объектов	Предоставлено всё	Предоставлено всё
Права родителя и потомка запрещающие, и одно из них запрещает всё		Запрещено всё
Запрещено для некоторых объектов	Запрещено для некоторых объектов	Списки запрещенных объектов объединяются
Запрещено всё	Предоставлено всё	Предоставлено всё
Запрещено для некоторых объектов	Предоставлено всё	Запрещено для объектов родителя
Запрещено для некоторых объектов	Предоставлено для некоторых объектов	Из запрещенных объектов вычитаются разрешенные объекты. Если после этого список запрещённых объектов не пуст, то результат – запрещены оставшиеся объекты. В противном случае результат – разрешены все объекты потомка
Предоставлено для некоторых объектов	Запрещено всё	Запрещено всё
Предоставлено всё	Запрещено для некоторых объектов	Запрещено для объектов потомка
Предоставлено для некоторых объектов	Запрещено для некоторых объектов	Из разрешенных объектов вычитаются запрещенные объекты. Если после этого список разрешённых объектов

Право родительской группы	Право рассматриваемого потомка	Результирующее право
		пуст, то результат – запрещено всё. В противном случае, результат – разрешены оставшиеся объекты.

5.3. Управление учетными записями администраторов и административными группами

5.3.1. Создание и удаление административных записей и групп

Регистрационное имя администратора должно быть уникальным.

Подключение администраторов через внешние системы аутентификации будет невозможно, если на Сервере уже существует администратор с таким же регистрационным именем.

Добавление администраторов

Для возможности создания учетных записей администраторов необходимо обладать правом **Создание администраторов, групп администраторов**.

Для добавления новой учетной записи администратора:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Администраторы**.
2. На панели инструментов нажмите значок  **Создать учетную запись**. Откроется окно настроек создаваемой учетной записи.
3. В подразделе **Общие** задайте следующие параметры:
   - В поле **Регистрационное имя** задайте регистрационное имя администратора, которое будет использоваться для доступа к Центру управления. Разрешается использовать строчные буквы (a-z), заглавные буквы (A-Z), цифры (0-9), символы "_" и ".".
   - В списке **Тип аутентификации** выберите один из вариантов:
     - **Внутренняя** – аутентификация такого администратора в Центре управления осуществляется на основе учетных данных в БД Сервера Dr.Web.
     - **Внешняя** – аутентификация такого администратора в Центре управления осуществляется через внешние системы LDAP, Active Directory, RADIUS или PAM.

Подробнее см. в разделе Аутентификация администраторов.

- В полях **Пароль** и **Еще раз пароль** задайте пароль для доступа к Серверу и, соответственно, к Центру управления.

При задании пароля администратора не допускается использование национальных символов.

Поля для задания пароля активны только для администраторов с внутренней аутентификацией.

Значения данных полей, заданных в Центре управления для администраторов с внешней аутентификацией, не имеют значения.

- В полях **Фамилия**, **Имя** и **Отчество** можете указать личные данные администратора.
- В выпадающем списке **Язык интерфейса** выберите язык интерфейса Центра управления, который будет использоваться создаваемым администратором (по умолчанию задан язык веб-браузера или английский).
- 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.

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

4. В подразделе **Группы** задается родительская административная группа. В списке приведены группы, доступные для назначения администратора. Напротив группы, для которой будет назначен создаваемый администратор, установлен флаг. По умолчанию создаваемые администраторы размещаются в родительской группе текущего администратора. Чтобы изменить назначенную группу, установите флаг напротив нужной группы.

   Каждый администратор может входить только в одну группу.

   От родительской группы администратор наследует права (см. п. Права администраторов).
5. После задания всех необходимых параметров нажмите кнопку **Сохранить** для создания учетной записи администратора.

Добавление административных групп

Для возможности создания административных групп необходимо обладать правом **Создание администраторов, групп администраторов**.

Для добавления новой учетной записи административной группы:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Администраторы**.
2. На панели инструментов нажмите значок **Создать группу**. Откроется окно настроек создаваемой группы.
3. В подразделе **Общие** задайте следующие параметры:
   - В поле **Группа** задайте название административной группы. Разрешается использовать строчные буквы (a-z), заглавные буквы (A-Z), цифры (0-9), символы "_" и ".".
   - В поле **Описание** можете задать произвольное описание группы.
4. В подразделе **Группы** задается родительская административная группа. В списке приведены группы, доступные для назначения в качестве родительской группы. Напротив группы, в которую будет входить создаваемая группа, установлен флаг. По умолчанию создаваемые группы размещаются в родительской группе текущего администратора. Чтобы изменить назначенную группу, установите флаг напротив нужной группы.

   Может быть назначена только одна родительская группа.

   От родительской группы административная группа наследует права (см. п. Права администраторов).
5. После задания всех необходимых параметров нажмите кнопку **Сохранить** для создания административной группы.

Удаление администраторов и административных групп

Для возможности удаления учетных записей администраторов и административных групп необходимо обладать правами **Удаление учетных записей администраторов** и **Редактирование свойств и конфигурации групп администраторов** соответственно.

Для удаления учетной записи администратора или группы:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Администраторы**.
2. В иерархическом списке администраторов выберите учетную запись администратора или административную группу, которую вы хотите удалить.
3. На панели инструментов нажмите значок **Удалить выбранные объекты**.

5.3.2. Редактирование административных записей и групп

Для возможности редактирования учетных записей администраторов и административных групп необходимо обладать правами **Редактирование учетных записей администраторов** и **Редактирование свойств и конфигурации групп администраторов** соответственно.

Для возможности редактирования собственной учетной записи необходимо обладать правом **Редактирование собственных настроек**.

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

Редактирование администраторов

Для редактирования учетной записи администратора:

1. В списке администраторов выберите учетную запись, которую вы хотите отредактировать. Откроется раздел редактирования свойств.
2. В подразделе **Общие** вы можете отредактировать параметры, которые были заданы при создании, при этом:
   a) Чтобы изменить пароль для доступа к учетной записи администратора, выберите на панели инструментов значок **Изменить пароль**.

   Администратор с соответствующими правами может редактировать пароли всех других администраторов.

   При задании регистрационного имени администратора не допускается использование национальных символов.

   b) Следующие параметры администратора доступны только для чтения:
      - Даты создания учетной записи и последнего изменения ее параметров,
      - **Состояние** – отображает сетевой адрес последнего подключения под данной учетной записью.
3. В подразделе **Группы** вы можете изменить административную группу. В списке приведены группы, доступные для назначения администратора. Напротив текущей родительской группы администратора установлен флаг. Чтобы изменить назначенную группу, установите флаг напротив нужной группы.

   Родительская группа для администратора обязательно должна быть назначена. Каждый администратор может входить только в одну группу. От заданной родительской группы наследуются права.

   См. также подраздел Редактирование членства.
4. В подразделе **Права** вы можете отредактировать список разрешенных действий для выбранного администратора.

   Процедура редактирования прав приведена в подразделе Редактирование прав.
5. Для применения внесенных изменений нажмите кнопку **Сохранить**.

Редактирование административных групп

Для редактирования административной группы:

1. В списке администраторов выберите группу, которую вы хотите отредактировать. Откроется раздел редактирования свойств.
2. В подразделе **Общие** вы можете отредактировать параметры, которые были заданы при создании.
3. В подразделе **Группы** вы можете изменить родительскую группу. В списке приведены группы, доступные для назначения в качестве родительской группы. Напротив текущей родительской группы установлен флаг. Чтобы изменить назначенную группу, установите флаг напротив нужной группы.

   Родительская группа для административной группы обязательно должна быть назначена. От заданной родительской группы наследуются права.

   См. также подраздел Редактирование членства.
4. В подразделе **Права** вы можете отредактировать список разрешенных действий для выбранной административной группы.

   Процедура редактирования прав приведена в подразделе Редактирование прав.
5. Для применения внесенных изменений нажмите кнопку **Сохранить**.

Редактирование членства

Существует несколько способов назначить родительскую группу для администраторов и административных групп:

1. Изменить настройки администратора или группы как описано выше.
2. Перетащить (drag-and-drop) администратора или административную группу в иерархическом списке на группу, которую хотите назначить родительской.

Глава 6: Группы. Комплексное управление рабочими станциями

Механизм групп предназначен для облегчения управления рабочими станциями антивирусной сети.

Объединение станций в группы может использоваться в следующих целях:

- 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

Системные группы

Изначально Dr.Web Enterprise Security Suite содержит набор предустановленных системных групп. Эти группы создаются в момент инсталляции Сервера Dr.Web 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.

После установки Сервера до момента подключения к нему станций в списке системных групп отображается только группа **Everyone**. Для отображения всех системных групп воспользуйтесь опцией **Показывать скрытые группы** в разделе **Настройки вида дерева** на панели инструментов.

Everyone

Группа, содержащая в себе все станции, известные Серверу Dr.Web. Группа **Everyone** содержит настройки всех групп и станций по умолчанию.

Configured

Группа содержит станции, для которых заданы персональные настройки.

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 **OS X**. Данное семейство включает набор групп, которые соответствуют конкретной версии операционной системы 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.

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 Агента Dr.Web, станция автоматически переходит в группу **Deinstalled**.
- Группа **Deleted**. Содержит станции, ранее удаленные администратором с Сервера. Возможно восстановление данных станций (см. п. Удаление и восстановление станции).
- Группа **New**. Содержит новые станции, которые были созданы администратором через Центр управления, но Агент на них еще не был установлен.
- Группа **Newbies**. Содержит все неподтвержденные станции, регистрация которых на Сервере в данный момент не была подтверждена. При подтверждении регистрации или при отказе в доступе к Серверу станции будут автоматически исключены из данной группы (подробнее см. раздел Политика подключения станций).
- Группа **Offline**. Содержит все неподключенные в данный момент станции.
- Группа **Online**. Содержит все подключенные в данный момент станции (реагирующие на запросы Сервера).

- Группа **Update Errors**. Содержит станции, обновление антивирусного ПО на которых прошло с ошибками.

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 версии 4.
- Группа **TCP/IP Version 6**. Группа содержит станции, подключенные в данный момент по протоколу TCP/IP версии 6.

Ungrouped

Группа содержит станции, которые не входят ни в одну из пользовательских групп.

Пользовательские группы

Это группы, создаваемые 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 6-1 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 6-1. Группы и поддерживаемые параметры

Группа/тип групп	Параметр			
	Автоматическое членство	**Управление членством**	**Первичная группа**	**Содержание настроек**
Everyone	+	–	+	+
Configured	+	–	–	–
Operating System	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
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**.
6. Нажмите кнопку **Сохранить**.

Созданные вами группы первоначально пусты. Процедура включения рабочих станций в группы описана в разделе Размещение рабочих станций в пользовательских группах.

Удаление группы

Для удаления существующей группы:

1. Выберите пользовательскую группу в иерархическом списке Центра управления.
2. На панели инструментов нажмите **Общие** → **Удалить выбранные объекты**.

> Предустановленные группы удалить невозможно.

6.2.2. Редактирование групп

Чтобы отредактировать настройки группы:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке выберите группу.
2. Откройте раздел свойств группы одним из следующих способов:
   a) Нажмите на название группы в иерархическом списке антивирусной сети. В правой части окна Центра управления автоматически откроется секция со свойствами группы.
   b) Выберите пункт **Свойства** управляющего меню. Откроется окно со свойствами группы станции.
3. Окно свойств группы содержит разделы **Общие** и **Конфигурация**. Их содержание и настройка описаны ниже.

> При открытии свойств группы в правой части окна Центра управления (см. пункт **2.a)**), также будет доступен раздел **Сведения о станциях**, в котором приведена общая информация о станциях, входящих в данную группу.

4. Для сохранения внесенных изменений нажмите кнопку **Сохранить**.

Общие

В разделе **Общие** приведена следующая информация:

- **Идентификатор** – уникальный идентификатор группы. Не доступен для редактирования.

- **Название** – название группы. При необходимости можете изменить название пользовательской группы. Для предустановленных групп поле **Название** не доступно 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.

Сведения о станциях

В разделе **Сведения о станциях** приведена следующая информация:

- **Станций** – общее количество станций, входящих в данную группу.
- **Первичная группа для** – количество станций, для которых данная группа является первичной.
- **Станций в сети** – количество станций в данной группе, которые находятся в данный момент в сети (online).

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** вы можете изменить конфигурацию групп, которая включает:

Значок	Настройки	Раздел с описанием
	Права пользователей рабочих станций, которые наследуют данную настройку от группы, если она является первичной. Настройка прав групп аналогична настройке прав отдельных рабочих станций.	Права пользователей станции
	Централизованное расписание запуска заданий на рабочих станциях, которые наследуют данную настройку от группы, если она является первичной. Настройка расписания для групп аналогична настройке централизованного расписания для станций.	Расписание заданий рабочей станции
	Лицензионные ключи для станций, для которых данная группа является первичной.	Менеджер лицензий
	Ограничения при распространении обновлении антивирусного ПО на станциях, которые наследуют данную настройку от группы, если она является первичной.	Ограничение обновлений рабочих станций

Значок	Настройки	Раздел с описанием
	Список компонентов, устанавливаемых на станциях, которые наследуют данную настройку от группы, если она является первичной. Редактирование списка компонентов для групп аналогично редактированию списка компонентов для станций.	Устанавливаемые компоненты антивирусного пакета
	Настройка автоматического размещения станций в данной группе. Доступна только для пользовательских групп.	Настройка автоматического членства в группе
	Настройки компонентов антивирусного пакета. Настройка компонентов антивирусного пакета для группы аналогична настройке компонентов для станции.	Настройка антивирусных компонентов

Для групп, у которых заданы персональные настройки, в разделе **Конфигурация** указывается количество вложенных групп с разорванным наследованием и собственными персональными настройками, при наличии таковых. При нажатии на данную опцию открывается окно со списком групп, для которых указаны их названия и идентификаторы.

6.3. Размещение рабочих станций в пользовательских группах

Dr.Web Enterprise Security Suite предоставляет следующие способы размещения станций в пользовательских группах:

1. Размещение станций в группах вручную.
2. Использование правил автоматического членства в группе.

6.3.1. Размещение станций в группах вручную

Существует несколько способов добавления рабочих станций в пользовательские группы вручную:

1. Изменение настроек станции.
2. Перетаскивание станции в иерархическом списке (drag-and-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. Откроется панель свойств станции. Также вы можете открыть раздел свойств станции выбрав в управляющем меню пункт **Свойства**.

3. На открывшейся панели **Свойства станции** перейдите в раздел **Группы**.

   В списке **Членство** перечислены все группы, в которые входит рабочая станция и в которые ее можно включить.

4. Для добавления станции в пользовательскую группу установите флаг напротив этой группы в списке **Членство**.
5. Для удаления рабочей станции из пользовательской группы снимите флаг напротив этой группы в списке **Членство**.

   Удаление станций из предустановленных групп невозможно.

6. Для сохранения внесенных изменений нажмите кнопку **Сохранить**.

Также в разделе **Свойства** 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-and-drop).
3. Чтобы переместить станцию из одной пользовательской группы в другую, перетащите станцию при помощи мыши (drag-and-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.

6.3.2. Настройка автоматического членства в группе

Dr.Web Enterprise Security Suite предоставляет возможность настройки правил автоматического включения станций в пользовательские группы.

Чтобы задать правила автоматического включения станций в группу:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В иерархическом списке антивирусной сети выберите пользовательскую группу, для которой вы хотите создать правила членства.
3. Перейдите в раздел редактирования правил членства одним из следующих способов:
   - На панели свойств группы в правой части окна, в разделе **Конфигурация** нажмите **Правила членства в группе**.

- В управляющем меню, в секции **Общие** выберите пункт **Правила членства в группе**.
- В управляющем меню, в секции **Общие** выберите пункт **Свойства**, перейдите на вкладку **Конфигурация**, нажмите **Правила членства в группе**.

4. В открывшемся окне задайте список условий, при выполнении которых станции будут помещены в данную группу:
   a) Если для группы не были ранее заданы правила членства, нажмите **Добавить правило**.
   b) Установите флаг **Назначить группу первичной**, чтобы группа, для которой создается правило, автоматически назначалась первичной для всех станций, которые будут перемещены в данную группу по этому правилу.
   c) Для каждого блока правил задайте следующие настройки:
      - Выберите одну из опций, задающую принцип объединения правил в пределах данного блока: **Соответствует всем условиям**, **Соответствует любому из условий**, **Не соответствует ни одному из условий**.
      - В выпадающих списках условий выберите: один из параметров станции, который будет проверяться на соответствие условиям; принцип соответствия данному условию и, если подразумевает параметр станции, введите строку условия.

При задании параметра **Платформа станции** необходимо выбирать из списка конечное полное название платформы, которое располагается на последнем уровне иерархии представленного дерева. Все вышележащие уровни приведены исключительно для удобства группировки списка платформ и сами по себе не являются значениями параметра **Платформа станции**.

Например: **Windows** и **Windows 7** не являются верными значениями параметра. Верным будет выбор **Windows 7 Professional Edition**.

При задании параметра **LDAP DN из Active Directory** необходимо:

1. Включить задание **Синхронизация с Active Directory** в расписании Сервера (раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web**).
2. В правилах членства в качестве строки условия для параметра **LDAP DN из Active Directory** задать требуемое значение DN, например:
   `OU=OrgUnit,DC=Department,DC=domain,DC=com`

      - Для добавления еще одного условия в данный блок правил нажмите  справа от строки условия.

   d) Для добавления нового блока правил нажмите  справа от блока. При этом задайте принцип объединения данного блока условий с остальными блоками:
      - **И** – условия блоков должны выполняться одновременно.
      - **ИЛИ** – должны выполняться условия хотя бы одного из блоков.

При задании строки условий допускается задание регулярных выражений.

Использование регулярных выражений кратко описано в документе **Приложения**, в разделе Приложение J. Использование регулярных выражений в Dr.Web Enterprise Security Suite.

Обратите внимание: при использовании параметров фильтра **начинается с** и **заканчивается на** строка условия автоматически дополняется следующими управляющими символами соответственно: ^ (строка начинается с последовательности указанных символов) или $ (строка заканчивается последовательностью указанных символов).

Для полноценного использования регулярных выражений рекомендуется выбирать параметр фильтра **содержит**.

5. Для сохранения и применения заданных правил нажмите одну из следующих кнопок:
   - **Применить сейчас** – сохранить заданные правила членства и применить данные правила сразу ко всем станциям, зарегистрированным на данном Сервере. При большом количестве станций, подключенных к Серверу, выполнение данного действия может занять некоторое время. Правила перегруппировки станций применяются ко всем уже зарегистрированным станциям сразу при задании действия и будут применяться в дальнейшем ко всем станциям, в том числе впервые зарегистрированным на Сервере, в момент их подключения.
   - **Применить при подключении станций** – сохранить заданные правила членства и применять данные правила к станциям в момент их подключения к Серверу. Правила перегруппировки станций применяется ко всем уже зарегистрированным станциям в момент их следующего подключения к Серверу и будут применяться ко всем станциям, впервые зарегистрированным на Сервере, в момент их первого подключения.
6. При задании правил автоматического членства для пользовательской группы, в иерархическом списке антивирусной сети рядом со значком этой группы появится значок , при условии, что установлен флаг **Показывать значок правил членства** в списке **Настройки вида дерева** на панели инструментов.

Если станция была автоматически перемещена в пользовательскую группу на основе правил членства, то удаление станции из этой группы вручную не имеет смысла, поскольку при следующем подключении к Серверу, станция будет автоматически возвращена в эту группу.

Чтобы удалить правила автоматического включения станций в группу:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В иерархическом списке антивирусной сети выберите пользовательскую группу, для которой вы хотите удалить правила членства.
3. Выполните одно из следующих действий:
   - На панели инструментов нажмите кнопку **Удалить правила членства**.

- На панели свойств группы в правой части окна, в разделе **Конфигурация** нажмите **Удалить правила членства**.
- В управляющем меню, в секции **Общие** выберите пункт **Свойства**, перейдите на вкладку **Конфигурация**, нажмите **Удалить правила членства**.

4. После удаления правил членства группы, все станции, помещенные в данную группу согласно правилам членства, будут удалены из этой группы. Если для каких-либо из этих станций данная группа была назначена администратором первичной, то при удалении станций из группы, первичной для них будет назначена группа **Everyone**.

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. Свойства станции – Конфигурация). 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 кнопку **Удалить персональные настройки** на панели инструментов Центра управления в разделе соответствующих настроек или в разделе свойств станции.

6.4.1. Наследование элементов конфигурации рабочей станции

Принцип наследования 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 первичная группа – **Everyone**.

> Если первичная группа не **Everyone**, и у указанной первичной группы, которая является корневой в иерархическом дереве антивирусной сети, нет персональных настроек, то наследуются настройки группы **Everyone**.

В условиях вложенных групп, если для станции не заданы персональные настройки, наследование элементов конфигурации осуществляется в соответствии со структурой вложенных групп. Поиск осуществляется вверх по иерархическому дереву, начиная с первичной группы станции, ее родительской группы и далее до корневого элемента дерева. Если при этом не были обнаружены персональные настройки, то наследуются элементы конфигурации группы **Everyone**.

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. Откроется панель свойств станции. Также вы можете открыть раздел свойств станции выбрав в управляющем меню пункт **Свойства**. В открывшемся окне перейдите в подраздел **Группы**.
3. При необходимости изменить первичную группу нажмите на значок нужной группы в разделе Членство. При этом на значке группы появится **1**.
4. Нажмите 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 станций (можно также выбирать группы – при этом действие будет распространено на все входящие в них станции), для которых вы хотите назначить первичную группу. 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 для станций**. 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 иерархическом списке, 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 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,

 в окне настройки прав пользователей станции.

Откроется окно с иерархическим списком антивирусной сети.

2. Выберите в этом списке группы и станции, на которые вы хотите распространить настройки.
3. Для того чтобы выполнить изменения в конфигурации этих групп, нажмите 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 нажмите пункт **Сравнение**.
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.
     - **Персональная конфигурация** – список компонентов, для которых назначены персональные настройки, не унаследованные от родительской группы.
   - Параметры сравнения для станций:
     - **Дата создания** станции.
     - **Первичная группа** для станции.
     - **Персональная конфигурация** – 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 учетными записями рабочих станций

7.1.1. Политика подключения станций

> Процедура создания станции через Центр управления описана в **Руководстве по установке**, п. Создание новой учетной записи.

Возможность управления авторизацией станций на Сервере Dr.Web зависит от следующих параметров:

1. Если при установке Агента на станции был снят флаг **Ручная авторизация на сервере**, 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 установлен флаг **Ручная авторизация на сервере** 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 `drweb-esuite-install` – см. **Руководство по установке**, п. Инсталляционные файлы).

> Задание типа авторизации Агента при его установке описано в **Руководстве пользователя**.

Чтобы изменить режим доступа станций к Серверу Dr.Web:

1. Откройте настройки конфигурации Сервера. Для этого выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**.
2. На вкладке **Общие** в выпадающем списке **Режим регистрации новичков** выберите одно из следующих значений:
   - **Подтверждать доступ вручную** (режим устанавливается по умолчанию, если не был изменен при установке Сервера),
   - **Всегда отказывать в доступе**,
   - **Автоматически разрешать доступ**.

Ручное подтверждение доступа

В режиме **Подтверждать доступ вручную** новые станции помещаются в системную подгруппу **Newbies** группы **Status** до их непосредственного рассмотрения администратором.

Для управления доступом неподтвержденных станций:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления. В дереве антивирусной сети выберите станции в группе **Status** → **Newbies**.

   Группа **Status** → **Newbies** в дереве антивирусной сети доступна только при выполнении следующих условий:

   1. В разделе **Администрирование** → **Конфигурации Сервера Dr.Web** → **Общие** для параметра **Режим регистрации новичков** задано значение **Подтверждать доступ вручную**.
   2. Для администратора разрешено право **Подтверждение новичков**.

2. Для задания доступа к Серверу на панели инструментов в разделе **Неподтвержденные станции** задайте действие, которое будет применено для выбранных станций:

   Разрешить доступ выбранным станциям и назначить первичную группу – подтвердить доступ станции к Серверу и задать для нее первичную группу из предложенного списка.

   Отменить действие, заданное для выполнения при подключении – отменить действие над неподтвержденной станцией, которое было ранее назначено для выполнения в момент, когда станция подключится к Серверу.

   Отказать в доступе выбранным станциям – запретить доступ станции к Серверу.

Автоматический 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.

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, заданная в выпадающем списке **Первичная группа** в разделе **Конфигурация Сервера Dr.Web** на вкладке **Общие**.

7.1.2. Удаление и восстановление станции

Удаление станций

Чтобы удалить запись о рабочей станции:

1. Выберите пункт главного меню **Антивирусная сеть**, в открывшемся окне на панели инструментов нажмите **Общие** → **Удалить выбранные объекты**.
2. Откроется окно подтверждения удаления станции. Нажмите **OK**.

После удаления станций из иерархического списка, они помещаются в таблицу удаленных станций, из которой возможно восстановление объектов при помощи Центра управления.

Восстановление станций

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** вы можете изменить список групп, в которые будет входить станция. По умолчанию задан список групп, в которые станция входила до удаления. В списке **Членство** приведен список групп, в которые возможно включение станции. Установите флаги напротив тех групп, в которые будет включена станция.

4. Для восстановления станции с заданными параметрами нажмите кнопку **Восстановить**.

7.1.3. 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 столбце выберите станцию, которая будет считаться главной. Все остальные станции будут удалены, а их данные будут приписаны выбранной.
4. В столбце выберите станцию, настройки которой будут заданы для выбранной главной станции.
5. Нажмите **Сохранить**.

7.2. Общие настройки рабочей станции

7.2.1. Свойства 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 выберите станцию.

2. Откройте раздел свойств станции одним из следующих способов:
   a) Нажмите на название станции в иерархическом списке антивирусной сети. В правой части окна Центра управления автоматически откроется секция со свойствами станции.
   b) Выберите пункт **Свойства** управляющего меню. Откроется окно со свойствами станции.
3. Окно свойств станции содержит следующие группы параметров: **Общие**, **Конфигурация**, **Группы**, **Безопасность**, **Расположение**. Их содержание и настройка описаны ниже.
4. Для сохранения внесенных изменений нажмите кнопку **Сохранить**.

Удаление персональных 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 на панели инструментов нажмите **Общие** → **Удалить персональные настройки**. Откроется список настроек данной станции, персональные настройки будут отмечены флагами.
2. Для персональных настроек, которые необходимо удалить, оставьте флаги установленными. Для тех настроек, которые вы хотите оставить персональными, снимите флаги. Нажмите **Удалить**. Для настроек, отмеченных флагами, будут восстановлено наследование от первичной группы.

7.2.1.1. Общие

В разделе **Общие** приведены следующие поля, доступные только для чтения:

- **Идентификатор** – уникальный идентификатор станции.
- **Название** – название станции.
- **Дата создания** – дата создания станции на Сервере.
- **Последняя регистрация** – дата последнего подключения данной станции к Серверу.

Также вы можете задать или изменить 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** вы можете указать дополнительную информацию о станции.

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

Также в данном разделе приведены следующие ссылки:

- В пункте **Инсталляционный файл** – ссылка для загрузки инсталлятора Агента для данной станции.

  Сразу после создании станции, до момента, когда будет задана операционная система станции, в разделе скачивания дистрибутива ссылки предоставляются отдельно для всех ОС, поддерживаемых Dr.Web Enterprise Security Suite.
- В пункте **Конфигурационный файл** – ссылка для загрузки файла с настройками подключения к Серверу Dr.Web станций под управлением ОС Android, OS X и ОС Linux.

7.2.1.2. Конфигурация

В разделе **Конфигурация** вы можете изменить конфигурацию станций, которая включает:

Значок	Настройки	Раздел с описанием
	Права пользователей рабочей станции	Права пользователей станции
	Централизованное расписание запуска заданий на рабочей станции	Расписание заданий рабочей станции
	Лицензионные ключи для станции	Менеджер лицензий
	Ограничения при распространении обновлении антивирусного ПО	Ограничение обновлений рабочих станций
	Список устанавливаемых компонентов	Устанавливаемые компоненты антивирусного пакета
	Настройки компонентов антивирусного пакета для данной станции	Настройка антивирусных компонентов

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.

При изменении настроек SplDer Gate и/или Офисного контроля необходимо учитывать, что настройки данных компонентов взаимосвязаны, поэтому, если были удалены персональные настройки одного из них при помощи кнопки  **Удалить персональные настройки**, то также будут удалены настройки второго компонента (устанавливается наследование настроек от родительской группы).

7.2.1.3. Группы

В разделе **Группы** настраивается список групп, в которые входит данная рабочая станция. В списке **Членство** перечислены все группы, в которые входит рабочая станция и в которые ее можно включить.

Для управления членством рабочей станции необходимо:

1. Для добавления станции в пользовательскую группу установите флаг напротив этой группы в списке **Членство**.
2. Для удаления рабочей станции из пользовательской группы снимите флаг напротив этой группы в списке **Членство**.

   Удаление станций из предустановленных групп невозможно.

3. При необходимости назначить другую первичную группу нажмите на значок нужной группы в списке Членство. При этом на значке группы появится **1**.

7.2.1.4. Безопасность

В разделе **Безопасность** задаются ограничения на сетевые адреса, с которых Агент, установленный на данной станции, может подключаться к Серверу.

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 в виде: <*IP-адрес*>/[<*префикс сети*>].
2. Для добавления нового поля адреса, нажмите кнопку  соответствующего раздела.
3. Для удаления поля нажмите кнопку  напротив удаляемого адреса.
4. Для применения настроек нажмите кнопку **Сохранить**.

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.

Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлен ли флаг **Приоритетность запрета**. Если флаг установлен, список **Запрещено** имеет более высокий приоритет, чем список **Разрешено**. Адреса, не включенные ни в один из списков или включенные в оба, запрещаются. Разрешаются только адреса, которые включены в список **Разрешено** и не включены в список **Запрещено**.

7.2.1.5. Расположение

В разделе **Расположение** вы можете задать дополнительную информацию о физическом расположении станции.

Также на данной вкладке вы можете просмотреть расположение станции на географической карте.

Для просмотра расположения станции на карте:

1. Задайте в полях **Широта** и **Долгота** географические координаты станции в формате десятичных градусов (Decimal Degrees).
2. Нажмите кнопку **Сохранить** для сохранения введенных данных.
3. На вкладке **Расположение** отобразится превью карты OpenStreetMaps с меткой, соответствующей заданным координатам.

   В случае, если загрузка превью невозможна, отображается текст **Показать на карте**.
4. Для просмотра полноразмерной карты нажмите на превью или на текст **Показать на карте**.

7.2.2. Установленные компоненты 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 выберите из подраздела **Общие** пункт **Установленные компоненты**.

3. Откроется окно с информацией об установленных компонентах: название компонента; время установки; адрес Сервера, с которого был установлен данный компонент; каталог установки компонента на станции.

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. Устанавливаемые компоненты 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.
2. В открывшемся управляющем меню выберите из подраздела **Статистика** пункт **Вирусные базы**.
3. Откроется окно с информацией об установленных вирусных базах: название файла, содержащего конкретную вирусную базу; версия вирусной базы; дата создания вирусной базы; количество записей в вирусной базе.

Если отображение пункта **Вирусные базы** отключено, для его включения выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**. На вкладке **Статистика** установите флаги **Мониторинг вирусных баз** и **Мониторинг состояния станций**, после чего перезагрузите Сервер.

7.2.3. Аппаратно-программное обеспечение на станциях под ОС Windows®

Dr.Web Enterprise Security Suite позволяет накапливать и просматривать информацию об аппаратном и программном обеспечении, установленном на защищаемых станциях под ОС Windows.

Для сбора информации об аппаратном и программном обеспечении станций:

1. Включите сбор статистики на Сервере:
   a) Выберите пункт **Администрирование** главного меню Центра управления.
   b) Выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**.
   c) В настройках Сервера откройте вкладку **Статистика** и установите флаг **Состав оборудования и программ**, если он снят.
   d) Для принятия внесенных изменений нажмите **Сохранить** и перезапустите Сервер.
2. Разрешите сбор статистики на станциях:
   a) Выберите пункт **Антивирусная сеть** главного меню Центра управления.
   b) В иерархическом списке антивирусной сети выберите станцию или группу станций, для которых вы хотите разрешить сбор статистики. При выборе группы станций обратите внимание на наследование настроек: если для станций выбранной группы задаются персональные настройки, то изменения настроек группы не приведет к изменению настроек станции.
   c) В управляющем меню, в секции **Конфигурация** → **Windows** выберите пункт **Агент Dr.Web**.
   d) В настройках Агента на вкладке **Общие** установите флаг **Собирать информацию о станциях**, если он снят. При необходимости отредактируйте значение параметра **Период сбора информации о станциях (мин.)**.
   e) Для принятия внесенных изменений нажмите **Сохранить**. Настройки будут переданы на станции.

Для просмотра аппаратного и программного обеспечения станции:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В иерархическом списке антивирусной сети выберите интересующую вас станцию.
3. В управляющем меню, в секции **Общие** выберите пункт **Оборудование и программы**.
4. В открывшемся окне приводится дерево со списком аппаратного и программного обеспечения, содержащее следующую информацию о данной станции:
   - **Application** – список программных продуктов, установленных на станции.
   - **Hardware** – список аппаратного обеспечения, установленного на станции.
   - **Operating System** – информация об операционной системе станции.
   - **Windows Management Instrumentation** – информация об инструментарии управления ОС Windows.
5. Чтобы отфильтровать отображаемые параметры аппаратно-программного обеспечения станции, в разделе **Настройки вида дерева** задайте соответствующие опции:
   - **Скрыть системные компоненты** – скрыть отображение системных приложений из раздела **Application**. Если флаг установлен, будет выведен список со всеми остальными приложениями, кроме системных. Если флаг снят, то в списке, помимо остальных, будут выводиться также системные компоненты.

- **Скрыть расширенную информацию** – отображать только минимальный набор компонентов, который позволит получить общее представление о станции. Данный набор определяется предустановленными фильтрами и не может быть изменен пользователем. Если флаг установлен, будут показаны только основные компоненты. Если флаг снят, будут показаны все компоненты.

6. Для отображения подробной информации о конкретном оборудовании или программе, выберите нужный объект в дереве.
7. При необходимости вы можете экспортировать данные о программно-аппаратном обеспечении станции в файл. Экспорту подлежат данные, выведенные в данный момент в дереве согласно заданным настройкам (см. п. 5).

   Для экспорта данных нажмите одну из следующих кнопок на панели инструментов:

   Сохранить данные в CSV-файл,

   Сохранить данные в HTML-файл,

   Сохранить данные в XML-файл,

   Сохранить данные в PDF-файл.

Для сравнения аппаратного и программного обеспечения нескольких станций:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В иерархическом списке антивирусной сети выберите несколько станций или групп станций. Для отображения страницы сравнения должно быть выбрано две или более станции под ОС Windows.
3. В управляющем меню, в секции **Общие** выберите пункт **Сравнение оборудования и программ**.
4. В открывшемся окне будет доступна следующая информация:
   - дерево со списком аппаратного и программного обеспечения;
   - таблица сравнения для выбранных станций.
5. Для отображения сравниваемых данных, выберите необходимый пункт в дереве аппаратно-программного обеспечения. Все доступные значения выбранного пункта будут отображены в дереве сравнения.

7.3. Настройка конфигурации рабочей станции

7.3.1. Права пользователей станции

Чтобы настроить права пользователей рабочей станции при помощи Центра управления безопасностью Dr.Web:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции. В открывшемся управляющем меню выберите пункт **Права**. Откроется окно настройки прав.

2. Редактирование прав осуществляется на вкладках, соответствующих операционной системе рабочей станции. Для того чтобы изменить (предоставить или отнять) какое-либо из прав, установите или снимите флаг для этого права.
3. Редактирование прав для станций под ОС Windows, OS X, Linux и Android 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 Агентом Dr.Web и его функциями:

Флаг раздела Права	Действие флага	Результат на станции, если флаг снят
Станции под ОС Windows		
Запуск в мобильном режиме	Установите флаг, чтобы разрешить пользователям на станции переключаться в мобильный режим и получать обновления непосредственно из Всемирной системы обновления Dr.Web, если отсутствует подключение к Серверу Dr.Web.	В настройках Агента, в разделе **Основные** → **Режим** недоступна настройка **Использовать Мобильный режим, если отсутствует подключение к серверу**.
Изменение режима работы	Установите флаг, чтобы разрешить пользователям на станции устанавливать режимы работы Агента Dr.Web.	В настройках Агента, в разделе **Основные** → **Режим** недоступны следующие настройки: • **Принимать обновления от сервера**, • **Принимать задачи от сервера**, • **Накапливать события**.
Изменение конфигурации Агента Dr.Web	Установите флаг, чтобы разрешить пользователям на станции изменять настройки Агента Dr.Web.	В настройках Агента, в разделе **Основные** недоступны настройки следующих подразделов: • **Уведомления**: недоступны все настройки. • **Режим**: недоступны настройки подключения к Серверу и флаг **Синхронизировать системное время с временем сервера**. • **Самозащита**: недоступны настройки **Запрещать изменение даты и времени системы**, **Запрещать эмуляцию действий пользователя**. • **Дополнительно**: в настройках подраздела **Журнал** недоступны

Флаг раздела Права	Действие флага	Результат на станции, если флаг снят
		пункты **Обновление Dr.Web**, **Службы Dr.Web**, **Создавать дампы памяти при ошибках проверки**.
Отключение самозащиты	Установите флаг, чтобы разрешить пользователям на станции останавливать самозащиту.	В настройках Агента, в разделе **Основные** → **Самозащита** недоступна настройка **Включить самозащиту** и настройка **Включить поддержку аппаратной виртуализации**.
Деинсталляция Агента Dr.Web	Установите флаг, чтобы разрешить пользователям на станции деинсталлировать Агент Dr.Web.	Запрещает удаление Агента на станции как при помощи инсталлятора, так и штатными средствами ОС Windows. В этом случае удаление Агента можно осуществить только при помощи пункта **Общие** → **Деинсталлировать Агент Dr.Web** на панели инструментов Центра управления.
Станции под OS X		
Запуск в мобильном режиме	Установите флаг, чтобы разрешить пользователям на станции переключаться в мобильный режим и получать обновления непосредственно из Всемирной системы обновления Dr.Web, если отсутствует подключение к Серверу Dr.Web.	В главном окне приложения раздел **Обновление** недоступен.
Станции под ОС семейства Linux		
Запуск в мобильном режиме	Установите флаг, чтобы разрешить пользователям на станции переключаться в мобильный режим и получать обновления непосредственно из Всемирной системы обновления Dr.Web, если отсутствует подключение к Серверу Dr.Web.	Для консольного режима работы приложения: команда `drweb-ctl update` для обновления вирусных баз с ВСО недоступна.
Станции под ОС Android		
Запуск в мобильном режиме	Установите флаг, чтобы разрешить пользователям мобильных устройств переключаться	На главном экране приложения, запущенного на мобильном устройстве, раздел **Обновление** недоступен.

Флаг раздела Права	Действие флага	Результат на станции, если флаг снят
	в мобильный режим и получать обновления непосредственно из Всемирной системы обновления Dr.Web, если отсутствует подключение к Серверу Dr.Web.	

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 для Windows. Руководство пользователя**.

4. Вы также можете распространить эти настройки на другой объект, нажав кнопку **Распространить эти настройки на другой объект**.
5. Чтобы экспортировать эти настройки в файл, нажмите **Экспортировать настройки из данного раздела в файл**.
6. Чтобы импортировать эти настройки из файла, нажмите **Импортировать настройки в данный раздел из файла**.
7. Для того чтобы принять сделанные изменения прав, нажмите кнопку **Сохранить**.

Если на момент редактирования настроек рабочая станция не подключена к Серверу, то настройки будут приняты, как только Агент восстановит связь с Сервером.

7.3.2. Расписание заданий рабочей станции

Dr.Web Enterprise Security Suite предоставляет возможность ведения *централизованного расписания заданий*, которое создается администратором антивирусной сети и подчиняется всем правилам наследования конфигураций.

Расписание заданий – это список действий, выполняемых автоматически в заданное время на станциях. Основное применение расписаний – сканирование станций на вирусы в наиболее удобное для пользователей время без необходимости ручного запуска Сканера. Кроме этого, Агент Dr.Web позволяет выполнять некоторые другие типы действий, описанные ниже.

Редактирование централизованного расписания регулярного выполнения заданий определенных рабочих станций и групп осуществляется при помощи Центра управления безопасностью Dr.Web.

Просмотр и редактирование заданий централизованного расписания пользователям на станции не предоставляется.

Результаты выполнения заданий по централизованному расписанию не заносятся в статистические данные на стороне Агента, а отправляются на Сервер и хранятся в статистических данных Сервера.

Для редактирования централизованного расписания выполните следующие действия:

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 выберите пункт **Планировщик заданий**. Откроется список заданий для станций.

   По умолчанию для станций под управлением ОС Windows расписание содержит задание **Daily scan** – ежедневное сканирование станции (запрещено).

2. Для управления расписанием используются соответствующие элементы на панели инструментов:

   a) Общие элементы панели инструментов служат для создания новых заданий и управления разделом расписания в целом. Данные инструменты всегда доступны на панели инструментов.

   Создать задание – добавить новое задание. Данное действие подробно описывается ниже, в подразделе Редактор заданий.

   Распространить эти настройки на другой объект – скопировать задания расписания в другие объекты – станции и группы. Подробнее см. в разделе Копирование настроек в другие группы/станции.

   Экспортировать настройки из данного раздела в файл – экспортировать расписание в файл специального формата.

   Импортировать настройки в данный раздел из файла – импортировать расписание из файла специального формата.

   b) Для управления уже существующими заданиями установите флаги напротив нужных заданий или в заголовке таблицы для выбора всех заданий в списке. При этом станут доступны элементы панели инструментов для управления выбранными заданиями:

Настройка		Действие
Состояние	**Разрешить выполнение**	Активировать выполнение выбранных заданий согласно заданному для них расписанию, если они были запрещены.
	Запретить выполнение	Запретить выполнение выбранных заданий. При этом задания будет присутствовать в списке, но не будет выполняться.

Настройка		Действие
Аналогичная настройка задается в редакторе задания на вкладке **Общие** при помощи флага **Разрешить выполнение**.		
Важность	**Сделать критическим**	Осуществить внеочередной запуск задания при следующем запуске Агента Dr.Web, если выполнение данного задания было пропущено по расписанию.
	Сделать не критическим	Выполнять задание только в указанное для него время, вне зависимости от того, был пропущен запуск задания или нет.
Аналогичная настройка задается в редакторе задания на вкладке **Общие** при помощи флага **Критическое задание**.		
Дублировать настройки		Дублировать задания, выбранные в списке текущего расписания. При задании действия **Дублировать настройки** создаются новые задания с настройками, аналогичными выбранным заданиям.
Запланировать повторно		Для однократных заданий: выполнить задание еще один раз в соответствии с заданными для него настройкам времени (изменение кратности выполнения задания описано ниже, в подразделе Редактор заданий).
Удалить выбранные задания		Удалить выбранное задание из расписания.

3. Для того чтобы изменить параметры задания, выберите его в списке заданий. При этом откроется окно **Редактор заданий**, описанное ниже.
4. По окончании редактирования расписания нажмите кнопку **Сохранить**, чтобы принять изменения.

Если в результате редактирования будет создано пустое (не содержащее заданий) расписание, Центр управления предложит 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.

Редактор заданий

При помощи редактора заданий вы можете задать настройки, чтобы:

1. Создать новое задание.

   Для этого нажмите кнопку **Создать задание** на панели инструментов.
2. Отредактировать существующее задание.

   Для этого нажмите на название одного из заданий в списке заданий.

При этом откроется окно редактирования параметров задания. Настройки задания при редактировании существующего задания аналогичны настройкам при создании нового задания.

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

Для редактирования параметров задания:

1. На вкладке **Общие** настраиваются следующие параметры:
   - В поле **Название** задается наименование задания, под которым оно будет отображаться в расписании.
   - Установите флаг **Разрешить выполнение**, чтобы активировать выполнение задания. Если флаг не установлен, задание будет присутствовать в списке, но не будет выполняться.

     Аналогичная настройка задается в главном окне Планировщика при помощи элемента панели инструментов **Состояние**.

   - Установите флаг **Критическое задание**, чтобы осуществлять внеочередной запуск задания при следующем запуске Агента Dr.Web, если выполнение задания было пропущено в назначенное время (Агент Dr.Web отключен на момент выполнения задания). Если на момент запуска задание было пропущено несколько раз, то оно выполнится только 1 раз.

     Аналогичная настройка задается в главном окне Планировщика при помощи элемента панели инструментов **Важность**.

     Если при этом должны выполниться несколько заданий на сканирование, то будет выполнено только одно из них – первое, стоящее в очереди.

     Например, если разрешено задание **Daily scan** и при этом было отложено критичное задание на сканирование при помощи Agent Сканера, то будет выполняться **Daily scan**, а отложенное критическое сканирование не сможет быть выполнено.

На вкладке **Действие** выберите тип задания из выпадающего списка **Действие** и настройте параметры задания, требуемые для выполнения:

Тип задания	Параметры и описание
Запись в файл журнала	**Строка** – текст сообщения, записываемого в файл отчета.
Запуск программы	Задайте следующие параметры: • В поле **Путь –** полное имя (с путем) исполняемого файла программы, которую предполагается запускать.

Тип задания	Параметры и описание
	• В поле **Аргументы –** параметры командной строки для запускаемой программы. • Установите флаг **Ожидать завершения программы** для ожидания завершения программы, запущенной данным заданием. При этом Агент протоколирует запуск программы, код возврата и время завершения программы. Если флаг **Ожидать завершения программы** снят, задание считается завершенным сразу после запуска программы, и Агент протоколирует только запуск программы.
Сканер Dr.Web. Быстрое сканирование	Параметры настройки сканирования описаны в п. Настройка параметров Сканера.
Сканер Dr.Web. Выборочное сканирование	
Сканер Dr.Web. Полное сканирование	

Удаленный запуск Сканера возможен только на станциях, работающих под ОС Windows, ОС семейства UNIX и OS X.

2. На вкладке **Время**:
   - В выпадающем списке **Периодичность** выберите режим запуска задания и настройте время в соответствии с выбранной периодичностью:

Режим запуска	Параметры и описание
Стартовое	Задание будет запускаться при старте работы Агента. Запускается без дополнительных параметров.
Через N минут после исходного задания	Необходимо выбрать в выпадающем списке **Исходное задание** то задание, относительно которого устанавливается время выполнения текущего задания. В поле **Минута** задайте или выберите из предлагаемого списка количество минут, которое должно пройти после выполнения исходного задания, чтобы началось выполнение редактируемого задания.
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.

Режим запуска	Параметры и описание
Ежечасно	Необходимо ввести число от 0 до 59, задающее минуту каждого часа, в которую будет запускаться задание.
Каждые N минут	Необходимо ввести значение **N** для задания временного интервала выполнения задания. При **N** равном `60` или больше задание будет запускаться каждые **N** минут. При **N** меньше `60` задание будет запускаться в каждую минуту часа, кратную **N**.

- Установите флаг **Запретить после первого выполнения** для однократного выполнения задания в соответствии с указанным временем. Если флаг снят, задание будет выполняться многократно с указанной периодичностью.
  Чтобы повторить выполнение однократного задания, которое уже было выполнено, воспользуйтесь кнопкой **Запланировать повторно** на панели инструментов раздела расписания.
- Установите флаг **Запускать задание по UTC**, чтобы запускать задание относительного всемирного времени (часовой пояс UTC+0). Если флаг снят, задание будет запущено по локальному времени на станции.

3. По окончании редактирования параметров задания нажмите кнопку **Сохранить** для принятия изменений в параметрах задания, если вы редактировали уже существующее задание, или для создания задания с заданными параметрами, если вы выполняли процедуру создания нового задания.

7.3.3. Устанавливаемые компоненты 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 выберите пункт **Устанавливаемые компоненты**.
2. Для необходимых компонентов выберите в выпадающем списке один из вариантов:
   - **Должен быть установлен** – задает обязательное наличие компонента на станции. При создании новой станции компонент входит в состав устанавливаемого антивирусного пакета в обязательном порядке. При задании значения **Должен быть установлен** для уже существующей станции компонент будет добавлен в состав имеющегося антивирусного пакета.
   - **Может быть установлен** – определяет возможность установки антивирусного компонента. Решение об установке принимает пользователь при установке Агента.
   - **Не может быть установлен** – запрещает наличие компонента на станции. При создании новой станции компонент не входит в состав устанавливаемого антивирусного пакета. При задании значения **Не может быть установлен** 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.

Задано 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.

7.4. Настройка антивирусных компонентов

Детальное описание настроек антивирусных компонентов, задаваемых через Центр управления, приведено в **Руководствах администратора** по управлению станциями для соответствующей операционной системы.

7.4.1. Компоненты

В зависимости от операционной системы станции предоставляются соответствующие функции защиты, приведенные далее.

Станции под ОС Windows®

Сканер Dr.Web, Dr.Web Agent Сканер

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления, в том числе на наличие руткитов.

SpIDer Guard

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

SpIDer Mail

Проверка всей входящей и исходящей почты при использовании почтовых клиентов.

Также возможно использование спам-фильтра (при условии, что лицензия позволяет использование такой функции).

SpIDer Gate

Проверка всех обращений к веб-сайтам по протоколу HTTP. Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Офисный контроль

Управление доступом к локальным и сетевым ресурсам, в частности, контроль доступа к веб-сайтам. Позволяет контролировать целостность важных файлов от случайного изменения или заражения вирусами, и запрещает служащим доступ к нежелательной информации.

Брандмауэр

Защита компьютеров от несанкционированного доступа извне и предотвращение утечки важных данных по сети Интернет. Контроль подключения и передачи данных по сети Интернет и блокировка подозрительных соединений на уровне пакетов и приложений.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

Самозащита

Защита файлов и каталогов Dr.Web Enterprise Security Suite от несанкционированного или невольного удаления или модификации пользователем, а также вредоносным ПО. При включенной самозащите доступ к файлам и каталогам Dr.Web Enterprise Security Suite разрешен только для процессов Dr.Web.

Превентивная защита (настройки предоставляются в рамках настроек Агента Dr.Web)

Предотвращение потенциальных угроз безопасности. Контроль доступа к критическим объектам операционной системы, контроль за загрузкой драйверов, автоматическим запуском программ и работой системных служб, а также отслеживание запущенных процессов и их блокировка в случае обнаружения вирусной активности.

Станции под ОС семейства UNIX®

Сканер Dr.Web, Dr.Web Agent Сканер

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

SpIDer Guard

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

SplDer Gate

Проверка всех обращений к веб-сайтам по протоколу HTTP. Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

Остальные компоненты, настройки которых приведены в Центре управления для станций под ОС семейства UNIX, являются дополнительными и служат для внутренней настройки работы антивирусного ПО.

Станции под OS X®

Сканер Dr.Web, Dr.Web Agent Сканер

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

SplDer Guard

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

SplDer Gate (настройки доступны только на станции)

Проверка всех обращений к веб-сайтам по протоколу HTTP. Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

Мобильные устройства под ОС Android

Сканер Dr.Web, Dr.Web Agent Сканер

Сканирование мобильного устройства по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

SplDer Guard

Постоянная проверка файловой системы в режиме реального времени. Сканирование всех файлов при попытке их сохранения в памяти мобильного устройства.

Фильтр звонков и сообщений

Фильтрация SMS-сообщений и телефонных звонков позволяет блокировать нежелательные сообщения и звонки, например, рекламные рассылки, а также звонки и сообщения с неизвестных номеров.

Антивор

Обнаружение местоположения или оперативная блокировка функций мобильного устройства в случае его утери или кражи.

Cloud Checker

URL-фильтр позволяет оградить пользователя мобильного устройства от нежелательных интернет-ресурсов.

Брандмауэр (настройки доступны только на мобильном устройстве)

Защита мобильного устройства от несанкционированного доступа извне и предотвращение утечки важных данных по сети. Контроль подключения и передачи данных по сети Интернет и блокировка подозрительных соединений на уровне пакетов и приложений.

Аудитор безопасности (настройки доступны только на мобильном устройстве)

Диагностика и анализ безопасности мобильного устройства и устранение выявленных проблем и уязвимостей.

Фильтр приложений

Запрет запуска на мобильном устройстве тех приложений, которые не включены в список разрешенных администратором.

Серверы под ОС Novell® NetWare®

Сканер Dr.Web

Сканирование компьютера по запросу пользователя, а также согласно расписанию.

SplDer Guard

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

7.5. Антивирусная проверка рабочих станций

Пользователь рабочей станции может производить антивирусное сканирование станции самостоятельно, используя компонент Сканер Dr.Web 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.

Через Центр управления 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.

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 выберите пункт **Запущенные компоненты**.

   Откроется список всех активных в настоящее время компонентов, как запущенных через Центр управления вручную администратором или по расписанию, так и запущенных пользователем на станции.
2. При необходимости прервать какой-либо из компонентов, установите флаг напротив этого компонента, после чего на панели инструментов нажмите кнопку **Прервать**. Компонент будет остановлен и удален из списка работающих компонентов.

При использовании данной опции текущие сканирования будут прерваны, Сканер остановлен, работа запущенных мониторов приостановлена.

Внимание! Запуск мониторов SpIDer Guard, SpIDer Mail и SpIDer Gate из Центра управления невозможен.

7.5.2. Прерывание работы запущенных компонентов по типам

При использовании данной опции текущие сканирования будут прерваны, Сканер остановлен, работа запущенных мониторов приостановлена.

Внимание! Запуск мониторов SpIDer Guard, SpIDer Mail и SpIDer Gate из Центра управления невозможен.

Чтобы прервать работу всех компонентов определенного типа, запущенных на рабочих станциях:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке выберите необходимую группу или отдельные станции.

2. На панели инструментов каталога антивирусной сети нажмите **Управление компонентами**. В выпадающем списке выберите пункт **Прервать запущенные компоненты**.
3. На открывшейся панели установите флаги напротив типов компонентов, которые вы хотите немедленно прервать:
   - **Прервать Dr.Web Agent Сканер, запущенный Планировщиком заданий** – для остановки активного сканирования при помощи Dr.Web Agent Сканера, которое было запущено согласно заданиям централизованного расписания.
   - **Прервать Dr.Web Agent Сканер, запущенный администратором** – для остановки активного сканирования при помощи Dr.Web Agent Сканера, которое было запущено вручную администратором через Центр управления.
   - **Прервать Сканер Dr.Web, запущенный пользователем** – для остановки активного сканирования при помощи Сканера Dr.Web, которое было запущено пользователем на станции.
   - **Прервать SpIDer Guard, SpIDer Mail, SpIDer Gate, Офисный контроль, Брандмауэр, Самозащиту и Превентивную защиту** – для приостановки работы соответствующих компонентов.

   Для выбора всех типов прерываемых компонентов установите флаг напротив заголовка панели **Прерывание запущенных компонентов**.
4. Нажмите кнопку **Прервать**.

7.5.3. Запуск проверки рабочей станции

Чтобы запустить антивирусную проверку рабочих станций:

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**. В открывшемся списке на панели инструментов выберите один из режимов сканирования:

   Сканер Dr.Web. Быстрое сканирование. В данном режиме сканируются следующие объекты:
   - 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.

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

Сканер Dr.Web. Выборочное сканирование. Данный режим предоставляет возможность выбрать любые каталоги и файлы для последующего сканирования, а также настроить расширенные параметры проверки.

Удаленный запуск Сканера возможен только при выборе активных станций, работающих под операционной системой, позволяющей запуск Сканера: ОС Windows, ОС семейства UNIX и OS X.

4. После выбора варианта сканирования откроется окно настроек Сканера. При необходимости измените параметры сканирования (см. раздел Настройка параметров Сканера).
5. Нажмите кнопку **Сканировать** для запуска процесса сканирования на выбранных рабочих станциях.

Сканирование станции при помощи Dr.Web Agent Сканера, запущенного удаленно, проводится в фоновом режиме без отображения уведомлений для пользователя станции.

7.5.4. Настройка параметров Сканера

При помощи Центра управления вы можете задать следующие настройки антивирусной проверки:

- Настройки Сканера Dr.Web. Данный Сканер запускается пользователями на станциях и не доступен для удаленного запуска из Центра управления. Однако администратор может централизованно изменить его настройки, которые в последствии будут переданы и сохранены на станциях.
- Настройки Dr.Web Agent Сканера. Данный Сканер запускается удаленно из Центра управления и осуществляет проверку станции аналогично Сканеру Dr.Web. Настройки Dr.Web Agent Сканера представляют собой расширенные настройки Сканера Dr.Web и задаются при запуске антивирусной проверки станций.

Настройка параметров Сканера Dr.Web

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 в разделе **Конфигурация** выберите в подразделе нужной вам операционной системы пункт **Сканер**. Откроется окно настроек Сканера.
4. Задайте необходимые параметры сканирования. Описание параметров Сканера Dr.Web приведены в **Руководстве пользователя** для соответствующей операционной системы.
5. Нажмите кнопку **Сохранить**. Настройки будут сохранены в Центре управления и переданы на соответствующие станции.

Настройка параметров Dr.Web Agent Сканера

Параметры Dr.Web Agent Сканера задаются при запуске проверки рабочих станций как описано в п. Запуск проверки рабочей станции.

Список разделов настроек Сканера, которые будут доступны (+) или не доступны (–), зависит от варианта запуска сканирования станций и приведен в таблице ниже.

Таблица 7-2. Список разделов настроек сканера в зависимости от варианта запуска

Вариант запуска сканирования	Разделы настроек			
	Общие	**Действия**	**Ограничения**	**Исключения**
Сканер Dr.Web. Выборочное сканирование	+	+	+	+
Сканер Dr.Web. Быстрое сканирование	–	+	+	–
Сканер Dr.Web. Полное сканирование	–	+	+	–

В зависимости от операционной системы станции, на которой запускается удаленное сканирование, будет доступна только та часть настроек Сканера, которая поддерживается системой станции.

Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и OS X, заключены в квадратные скобки **[ ]**.

7.5.4.1. Общие

Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и OS X, заключены в квадратные скобки **[ ]**.

В разделе **Общие** вы можете задать следующие настройки антивирусной проверки:

- Установите флаг **Использовать эвристический анализ**, чтобы Сканер осуществлял поиск неизвестных вирусов при помощи эвристического анализатора. В данном режиме возможны ложные срабатывания Сканера.
- Установите флаг **Проверять загрузочные секторы**, чтобы Сканер осуществлял проверку загрузочных секторов. Проверяются как загрузочные секторы логических дисков, так и главные загрузочные секторы физических дисков.
- Установите флаг **[Проверять автоматически запускаемые программы]**, чтобы проверять программы, автоматически запускаемые при старте операционной системы.

- Установите флаг **Следовать символическим ссылкам**, чтобы следовать символическим ссылкам при сканировании.
- Установите флаг **[Проверять работающие программы и модули]**, чтобы проверять процессы, запущенные в оперативной памяти.
- Установите флаг **[Проверять на наличие руткитов]**, чтобы включить сканирование на наличие вредоносных программ, скрывающих свое присутствие в системе.
- Установите флаг **[Прерывать проверку при переходе на питание от аккумулятора]**, чтобы прерывать антивирусную проверку при переходе компьютера пользователя на питание от аккумулятора.
- Выпадающий список **Приоритет сканирования** определяет приоритет процесса проверки относительно имеющихся вычислительных ресурсов операционной системы.
- Установите флаг **[Уровень загрузки ресурсов компьютера]**, чтобы ограничивать использование ресурсов компьютера при проверке, и выберите из выпадающего списка максимально допустимую загрузку ресурсов Сканером. При отсутствии других задач ресурсы компьютера будут использоваться максимально.

  Опция **Уровень загрузки ресурсов компьютера** не оказывает влияния на фактическую величину загрузки ресурсов при запуске сканирования на однопроцессорной системе с одним ядром.

- Выпадающий список **Действия после сканирования** определяет автоматическое выполнение заданного действия сразу после окончания процесса проверки:
  - **ничего не делать** – после завершения проверки не предпринимать никаких действий с компьютером пользователя.
  - **[выключить станцию]** – после завершения проверки выключить компьютер пользователя. Перед выключением компьютера Сканер применит заданные действия к обнаруженным угрозам.
  - **перезагрузить станцию** – после завершения проверки перезагрузить компьютер пользователя. Перед перезагрузкой компьютера Сканер применит заданные действия к обнаруженным угрозам.
  - **перевести станцию в ждущий режим**.
  - **перевести станцию в спящий режим**.
- Установите флаг **Отключить сеть при сканировании**, чтобы отключить компьютер от локальной сети и Интернета на время сканирования.
- Установите флаг **Проверять стационарные диски** для проверки стационарных жестких дисков (винчестер и т.п.).
- Установите флаг **Проверять объекты на съемных носителях** для проверки всех сменных носителей информации, таких как накопители на магнитных дисках (дискеты), CD/DVD-диски, flash-накопители и т.д.
- В поле **Пути, выбранные для сканирования** задайте список проверяемых путей (способ их задания описывается ниже).
  - Для того чтобы добавить новую строку в список, нажмите кнопку  и в открывшуюся строку введите требуемый путь.

- Для того чтобы удалить элемент из списка, нажмите кнопку  напротив соответствующей строки.

При установке флага **Пути, выбранные для сканирования** осуществляется антивирусная проверка только указанных путей. Если флаг снят, проводится проверка всех дисков.

7.5.4.2. Действия

Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и OS X, заключены в квадратные скобки **[ ]**.

В разделе **Действия** задается реакция Сканера на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов.

Dr.Web Agent Сканер автоматически применяет действия, заданные для обнаруженных вредоносных объектов.

Предусмотрены следующие действия над обнаруженными угрозами:

- **Лечить** – восстановить состояние инфицированного объекта до заражения. Если объект неизлечим или попытка лечения не была успешной, будет применено действие, заданное 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.
- **Перемещать в карантин** – переместить зараженные объекты в каталог Карантина на станции.
- **Информировать** – отправить в Центр управления уведомление об обнаружении вируса (о настройке режима оповещений см. в п. Настройка оповещений).
- **Игнорировать** – пропустить объект без выполнения каких-либо действий, в том числе не присылать оповещения в статистике сканирования.

Таблица 7-3. Действия Сканера над обнаруженными вредоносными объектами

Объект	Действие				
	Лечить	Удалять	Перемещать в карантин	Информировать	Игнорировать
Инфицированные	+/*	+	+		
Подозрительные		+	+/*		+
Неизлечимые		+	+/*		

Объект	Действие				
	Лечить	**Удалять**	**Перемещать в карантин**	**Информировать**	**Игнорировать**
Контейнеры		+	+/*		
Архивы		+	+/*		
Почтовые файлы			+/*		+
Загрузочные секторы	+/*			+	
Рекламные программы		+	+/*		+
Программы дозвона		+	+/*		+
Программы-шутки		+	+/*		+
Потенциально опасные		+	+/*		+
Программы взлома		+	+/*		+

Условные обозначения

+	действие разрешено для данного типов объектов
+/*	действие установлено как реакция по умолчанию для данного типов объектов

Для задания действий над обнаруженными угрозами служат следующие настройки:

- Выпадающий список **Инфицированные** 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.
- Выпадающий список **Инфицированные контейнеры** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в составе файлового контейнера.
- Выпадающий список **Инфицированные архивы** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в составе файлового архива.

- Выпадающий список **Инфицированные почтовые файлы** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в формате электронной почты.

> При обнаружении вирусов или подозрительного кода внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров) действия по отношению к угрозам внутри таких объектов выполняются над всем объектом, а не только над зараженной его частью. По умолчанию во всех этих случаях предусмотрено информирование.

- Выпадающий список **Инфицированные загрузочные секторы** задает реакцию Сканера на обнаружение вирусов или подозрительного кода в области загрузочных секторов.
- Следующие выпадающие списки задают реакцию Сканера на обнаружение соответствующего нежелательного ПО:
  - **Рекламные программы**;
  - **Программы дозвона**;
  - **Программы-шутки**;
  - **Потенциально опасные**;
  - **Программы взлома**.

> При задании действия **Игнорировать** не будет произведено никаких действий: в Центр управления не будет отправлено уведомление, как в случае включенной опции **Информировать** при обнаружении вируса.

Установите флаг **[Перезагружать компьютер автоматически]** для автоматической перезагрузки компьютера пользователя после окончания сканирования, если в процессе проверки были обнаружены инфицированные объекты, для завершения лечения которых требуется перезагрузка операционной системы. Если флаг снят, перезагрузка компьютера пользователя не будет осуществляться. В статистике сканирования станции, получаемой Центром управления, будет сообщено о необходимости перезагрузки станции для завершения лечения. Информация о состоянии, требующем перезагрузку, отображается в таблице Состояния. При необходимости администратор может перезагрузить станцию из Центра управления (см. раздел Антивирусная сеть).

Установите флаг **Показывать ход проверки**, чтобы отображать в Центре управления индикатор и строку состояния процесса сканирования станции.

7.5.4.3. Ограничения

> Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и OS X, заключены в квадратные скобки **[ ]**.

В разделе **Ограничения** доступны следующие настройки антивирусной проверки:

- **Максимальное время сканирования (мс)** – максимальное время проверки одного объекта в миллисекундах. По истечении указанного времени проверка объекта будет прекращена.

- **Максимальный уровень вложенности в архив** – максимальное количество вложенных архивов. Если уровень вложенности в архив превышает заданное ограничение, проверка будет производиться только до указанного уровня вложенности.
- **[Максимальный размер архива (КБ)]** – максимальный размер проверяемого архива в килобайтах. Если размер архива превышает заданное ограничение, распаковка и проверка производиться не будет.
- **Максимальный коэффициент сжатия архива** – если Сканер определяет, что коэффициент сжатия архива превышает заданное ограничение, распаковка и проверка производиться не будет.
- **[Максимальный размер распакованного объекта (КБ)]** – максимальный размер файла при распаковке в килобайтах. Если Сканер определяет, что после распаковки размер файлов архива превышает заданное ограничение, распаковка и проверка производиться не будет.
- **[Порог проверки уровня сжатия (КБ)]** – минимальный размер файла в килобайтах внутри архива, начиная с которого будет производиться проверка коэффициента сжатия.

7.5.4.4. Исключения

В разделе **Исключения** задается список каталогов и файлов, исключаемых из антивирусной проверки.

Для редактирования списков исключаемых путей и файлов:

1. Введите путь к требуемому файлу или каталогу в строку **Исключаемые пути и файлы**.
2. Для того чтобы добавить новую строку в список, нажмите кнопку  и в открывшуюся строку введите требуемый путь.
3. Для того чтобы удалить элемент из списка, нажмите 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 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

Регулярное выражение	Значение
`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 документе **Приложения**, в разделе Приложение J. Использование регулярных выражений в Dr.Web Enterprise Security Suite.

В подразделе **Проверять содержимое следующих файлов** вы можете отключить проверку составных объектов. Для этого снимите следующие флаги:

- Флаг **Архивы** предписывает Сканеру искать вирусы в файлах, упакованных в файловые архивы.
- Флаг **Почтовые файлы** предписывает проверять почтовые ящики.
- Флаг **Инсталляционные пакеты** предписывает Сканеру проверять пакеты для установки программ.

7.6. Просмотр статистики по рабочей станции

При помощи управляющего меню раздела **Антивирусная сеть** вы можете просматривать следующую информацию:

- Статистика – данные по статистике работы антивирусных средств на станции, по состоянию рабочих станций и антивирусных средств, для просмотра и сохранения отчетов, содержащих все сводные статистические данные или выборочные сводки по заданным типам таблиц.
- Графики – графики с информацией о заражениях, обнаруженных на станциях.
- Карантин – удаленный доступ к содержимому Карантина на рабочей станции.

7.6.1. Статистика

Также вы можете настроить автоматическое создание статистического отчета, включающего нужный вам набор статистических таблиц. Данный отчет в выбранном формате может не только сохраняться на Сервере, но и отправляться на электронную почту.

Для этого настройте задание **Создание статистического отчета** в расписании Сервера.

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 выберите нужный пункт из подраздела **Статистика**.

Раздел меню **Статистика** содержит следующие пункты:

- **Суммарная статистика** – для получения суммарной статистики без разбиения на сеансы.
- 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 **Статистика**.
- **Угрозы** – для просмотра информации об обнаруженных угрозах безопасности защищаемых станций: перечень зараженных объектов, расположение по станциям, названия угроз, действия антивируса и т.п.

- **Ошибки** – для просмотра списка ошибок сканирования на выбранной рабочей станции за определенный период.
- Статистика сканирования – для получения статистики о работе антивирусных средств на станции.
- **Запуск/Завершение** – для просмотра списка компонентов, запускавшихся на рабочей станции.
- **Статистика угроз** – для просмотра сведений об обнаружении угроз безопасности защищаемых станций, сгруппированных по типам угроз и по количеству угроз на станциях.
- Состояние – для просмотра сведений о необычном состоянии рабочих станций, возможно требующем вмешательства.
- **Задания** – для просмотра списка заданий, назначенных для рабочей станции в заданный период.
- **Продукты** – для просмотра информации об установленных продуктах на выбранных станциях. Под продуктами в данном случае понимаются продукты репозитория Сервера.
- **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.
- **Инсталляции Агентов** – для просмотра списка установок Агента на рабочую станцию или группу рабочих станций.
- **Деинсталляции Агентов** – для просмотра списка рабочих станций, с которых было удалено антивирусное ПО Dr.Web.

Для отображения скрытых пунктов раздела **Статистика** выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**. На вкладке **Статистика** установите соответствующие флаги (см. ниже), после чего нажмите **Сохранить** и перезагрузите Сервер.

Таблица 7-4. Соответствие пунктов раздела Статистика и флагов раздела Статистика в конфигурации Сервера

Пункты раздела Статистика	Флаги раздела Статистика в конфигурации Сервера
Суммарная статистика	Статистика сканирования
Угрозы	Обнаруженные угрозы безопасности
Ошибки	Ошибки сканирования
Статистика сканирования	Статистика сканирования
Запуск/Завершение	Запуск/Завершение компонентов

Пункты раздела Статистика	Флаги раздела Статистика в конфигурации Сервера
Статистика угроз	Обнаруженные угрозы безопасности
Состояние	Состояние станций
Задания	Журнал выполнения заданий на станциях
Вирусные базы	Состояние станций Мониторинг вирусных баз Журнал выполнения заданий на станциях
Модули	Список модулей станций
Инсталляции Агентов	Инсталляции Агентов

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.

7.6.1.1. Сводные данные

Для просмотра сводных данных:

1. В иерархическом списке выберите станцию или группу.
2. В управляющем меню в разделе **Статистика** выберите пункт **Сводные данные**.
3. Откроется окно, содержащее табличные данные отчета. Для того чтобы включить в отчет определенные статистические данные, нажмите кнопку **Сводные данные** на панели инструментов и выберите требуемые типы в выпадающем списке: **Статистика сканирования**, **Угрозы**, **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 кнопку **Обновить**.
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 просмотра данных нажмите кнопку **Обновить**.
5. При необходимости сохранить отчет для распечатки или дальнейшей обработки нажмите на одну из кнопок:

   Сохранить данные в CSV-файл,

Сохранить данные в HTML-файл,

Сохранить данные в XML-файл,

Сохранить данные в PDF-файл.

7.6.1.2. Статистика сканирования

Для получения статистики о работе антивирусных средств на станции:

1. В иерархическом списке выберите 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 в разделе **Статистика** выберите пункт **Статистика сканирования**.
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 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 отчет для распечатки или дальнейшей обработки нажмите на одну из кнопок:

   Сохранить данные в CSV-файл,

   Сохранить данные в HTML-файл,

Сохранить данные в XML-файл,

Сохранить данные в PDF-файл.

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 выберите пункт **Графики**. Откроется окно просмотра статистических диаграмм (подробное описание см. ниже).

7.6.1.3. Состояние

Для просмотра сведений о состоянии рабочих станций:

1. В иерархическом списке выберите станцию или группу.
2. В управляющем меню в разделе **Статистика** выберите пункт **Состояние**.
3. Сведения о состоянии станций отображаются в соответствии с настройками фильтра. На панели инструментов доступны следующие параметры фильтра:
   - В выпадающем списке **Период** выберите период, в течение которого произошло событие. В поле периода отображается количество дней, соответствующих выбранному значению: в списке будут отображаться станции, события на которых произошли в течение заданного времени.
   - В списке **Серьезность** установите опцию для выбора минимального уровня важности сообщений: список сообщений о состоянии будет содержать сообщения с выбранным уровнем и выше.
   - В списке **Источник** установите флаги для тех источников появления событий, которые будут отображаться в списке:
     - **Агент** – отображать события, пришедшие от Агентов Dr.Web, подключенных к данному Серверу.
     - **Сервер** – отображать события, пришедшие от данного Сервера Dr.Web.
     - **Подключенные** – отображать события для станций, которые подключены к данному Серверу и находятся в данный момент в сети (online).
     - **Отключенные** – отображать события для станций, которые подключены к данному Серверу и в данный момент не в сети (offline).
     - **Деинсталлированные** – отображать последнее событие для станций, на которых было удалено антивирусное ПО Dr.Web.
4. Нажмите кнопку **Обновить**, чтобы применить выбранные настройки фильтра и отобразить соответствующие данные.
5. Действия по детализации и форматированию информации данной таблицы аналогичны описанным выше для таблицы статистики сканирования.

Вы также можете просмотреть результаты работы и статистику нескольких рабочих станций. Для этого необходимо выбрать эти станции в иерархическом списке сети.

6. При необходимости сохранить отчет для распечатки или дальнейшей обработки нажмите на одну из кнопок:

   Сохранить данные в CSV-файл,

   Сохранить данные в HTML-файл,

   Сохранить данные в XML-файл,

   Сохранить данные в PDF-файл.

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 выберите в разделе **Общие** пункт **Графики**.
2. Откроется окно, содержащее следующие графические данные:
   - **Вирусная активность** – на графике отображается общее количество вредоносных объектов, найденных в пределах каждого временного промежутка для всех выбранных станций и групп. График отображается, если задан временной период, превышающий одни сутки.
   - **Наиболее распространенные угрозы** – приводится список из десяти угроз, встречающихся в наибольшем количестве файлов. На графике отображаются численные данные по объектам, соответствующим конкретной угрозе.
   - **Классы угроз** – приводится список угроз в соответствии с классификацией вредоносных объектов. На круговой диаграмме отображается процентное соотношение между всеми обнаруженными угрозами.
   - **Наиболее зараженные станции** – приводится список станций, на которых были обнаружены угрозы безопасности. На графике отображается общее количество угроз для каждой станции.
   - **Произведенные действия** – приводится список действий, произведенных над обнаруженными вредоносными объектами. На круговой диаграмме отображается процентное соотношение между всеми произведенными действиями.
3. Для просмотра графических данных за предопределенный период выберите диапазон из выпадающего списка на панели инструментов: отчет за определенный день или месяц. Либо вы можете выбрать произвольный диапазон дат, для этого введите требуемые даты или выберите даты в выпадающих календаря. Для просмотра данных нажмите кнопку **Обновить**.

4. Чтобы исключить какой-либо пункт из отображения на графике (кроме графика **Вирусная активность**), нажмите на название этого пункта в легенде под графиком.

Графики итоговой статистики

Графические данные приводятся в пункте **Графики** раздела **Общие** и в некоторых пунктах раздела **Статистика** управляющего меню. В таблице ниже приведен список возможных графиков и разделы управляющего меню, в которых данные графики отображаются.

Таблица 7-5. Соответствие графиков разделам управляющего меню

Графики	Разделы
Вирусная активность	Графики
Наиболее распространенные угрозы	Графики Угрозы Статистика угроз
Классы угроз	Графики Статистика угроз
Наиболее зараженные станции	Графики
Произведенные действия	Графики Угрозы
Количество ошибок по станциям	Ошибки
Количество ошибок по компонентам	Ошибки
Угрозы по компонентам	Запуск/Завершение
Ошибки по компонентам	Запуск/Завершение

- **Количество ошибок по станциям** – приводится список станций, на которых возникали ошибки в функционировании антивирусных компонентов. На графике отображается общее количество ошибок для каждой станции.
- **Количество ошибок по компонентам** – приводится список антивирусных компонентов, в функционировании которых возникали ошибки. На круговой диаграмме отображается процентное соотношение между ошибками всех компонентов.
- **Угрозы по компонентам** – приводится список антивирусных компонентов, которыми были обнаружены угрозы. На графике отображается общее количество угроз, обнаруженных каждым из компонентов.

- **Ошибки по компонентам** – приводится список антивирусных компонентов, в функционировании которых возникали ошибки. На графике отображается общее количество ошибок каждого из компонентов.

7.6.3. Карантин

Содержимое Карантина

Файлы в Карантин могут быть добавлены одним из антивирусных компонентов, например, Сканером.

Пользователь может сам повторно сканировать файлы, находящиеся в Карантине, через Центр 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 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.

   Статистика о повторном сканировании объекта в Карантине, приведенная в столбце **Информация**, учитывает только повторное сканирование, запущенное через Центр управления.

   Если для объекта в Карантине заявлен статус **не инфицирован**, это означает, что после перемещения в Карантин объекта, квалифицированного как угроза, было произведено повторное сканирование, и объекту присвоен статус безопасного.

   Восстановление объектов из Карантина осуществляется только вручную.

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:

  Сохранить данные в CSV-файл,

  Сохранить данные в HTML-файл,

  Сохранить данные в XML-файл,

  Сохранить данные в PDF-файл.

7.7. Рассылка инсталляционных файлов

При создании новой учетной записи станции в Центре управления генерируется персональный инсталляционный пакет для установки Агента Dr.Web. Инсталляционный пакет включает в себя инсталлятор Агента Dr.Web и набор параметров подключения к Серверу Dr.Web и авторизации станции на Сервере Dr.Web (описание инсталляционного пакета и процесса установки Агента с его помощью приведено в **Руководстве по установке**, в разделе Локальная установка Агента Dr.Web).

После создания инсталляционных пакетов, для удобства их распространения, вы можете отправить конкретные инсталляционные пакеты на электронную почту пользователей.

При отправке инсталляционных пакетов содержимое письма формируется следующим образом:

1. Операционная система станции известна:

   a) ОС Windows: к письму прикладывается инсталляционный пакет Агента Dr.Web для Windows.

   b) ОС Linux, OS X, ОС Android: к письму прикладывается инсталляционный файл Агента Dr.Web для соответствующей операционной системы и конфигурационный файл с настройками подключения к Серверу Dr.Web.

2. Операционная система станции не известна – новая учетная запись станции, Агент еще не установлен:
   a) Если на Сервере нет пакетов для станций под ОС Linux, OS X, ОС Android (в частности, на Сервере не установлен дополнительный (extra) дистрибутив): к письму прикладывается инсталляционный пакет Агента Dr.Web для Windows, а также конфигурационный файл с настройками подключения к Серверу Dr.Web для станций под ОС Linux, OS X, ОС Android.
   b) Если на Сервере есть хотя бы один пакет, кроме пакета для станций под ОС Windows: к письму прикладывается инсталляционный пакет Агента Dr.Web для Windows, конфигурационный файл с настройками подключения к Серверу Dr.Web для станций под ОС Linux, OS X, ОС Android, а также ссылка на скачивание инсталляционных файлов для станций под ОС Linux, OS X, ОС Android.

Для рассылки инсталляционных пакетов по электронной почте:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке выберите следующие объекты:
   - выберите станцию, чтобы отправить по электронной почте инсталляционный пакет, сгенерированный для данной станции.
   - выберите группу станций, чтобы отправить по электронной почте все инсталляционные пакеты, сгенерированные для станций данной группы.

   Для одновременного выбора нескольких объектов используйте кнопки CTRL или SHIFT.
2. На панели инструментов нажмите **Общие** → **Разослать инсталляционные файлы**.
3. В открывшемся разделе **Рассылка инсталляционных файлов** задайте следующие параметры:
   - В секции **Электронная почта получателей** задайте адрес электронной почты, на который будет отправлен инсталляционный пакет. Если было выбрано несколько станций или групп, то задайте адреса электронной почты для отправки инсталляционных пакетов для каждой станции в отдельности напротив имени этой станции.
   - В секции **Дополнительно** установите флаг **Упаковать в zip-архив**, чтобы упаковать файлы инсталляционных пакетов в zip-архив. Упаковка в архив может быть полезна при наличии фильтров электронной почты на стороне пользователя, блокирующих передачу исполняемых файлов во вложениях электронных писем.
   - В секции **Отправитель** укажите адрес электронной почты, который будет указан в качестве отправителя электронного письма с инсталляционными файлами.
   - В секции **Настройки SMTP сервера** задаются параметры SMTP-сервера, который будет использоваться для отправки электронной почты. Если параметры известны, например, уже были ранее заданы, данный раздел будет свернут, вы можете развернуть его и отредактировать заданные параметры при необходимости. При первой отправке инсталляционных пакетов в открывшемся разделе необходимо задать следующие параметры:
     - **Адрес** – адрес SMTP-сервера, который будет использоваться для отправки электронной почты.

- **Порт** – порт для подключения к SMTP-серверу. По умолчанию порт 465 при открытии отдельного защищенного TLS-соединения или порт 25 в противном случае.
- **Пользователь**, **Пароль** – при необходимости задайте имя пользователя и пароль пользователя SMTP-сервера, если SMTP-сервер требует авторизации.
- Установите флаг **STARTTLS шифрование** для шифрованного обмена данными. При этом переключение на защищенное соединение осуществляется через команду `STARTTLS`. По умолчанию для соединения предусматривается использование 25 порта.
- Установите флаг **SSL шифрование** для шифрованного обмена данными. При этом будет открыто отдельное защищенное TLS-соединение. По умолчанию для соединения предусматривается использование 465 порта.
- Установите флаг **Использовать CRAM-MD5 аутентификацию** для использования *CRAM-MD5* аутентификации на почтовом сервере.
- Установите флаг **Использовать DIGEST-MD5 аутентификацию** для использования *DIGEST-MD5* аутентификации на почтовом сервере.
- Установите флаг **Использовать обычную аутентификацию** для использования *plain text* аутентификации на почтовом сервере.
- Установите флаг **Использовать LOGIN аутентификацию** для использования *LOGIN* аутентификации на почтовом сервере.
- Установите флаг **Проверять правильность SSL сертификата сервера** чтобы проверять правильность SSL-сертификата почтового сервера.
- Установите флаг **Отладочный режим** для получения детального журнала SMTP-сессии.Нажмите кнопку **Отправить**.

7.8. Отправка сообщений станциям

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).

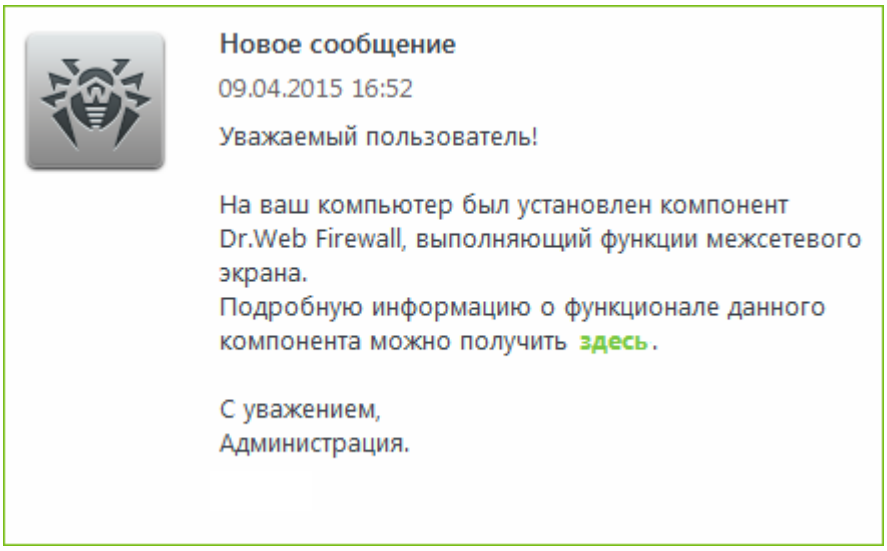


Рисунок 7-1. Окно сообщения на станции под ОС Windows

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 на панели инструментов нажмите **Общие** → **Отправить сообщение станциям**.
3. В открывшемся окне заполните следующие поля:
   - **Текст сообщения** – обязательное поле. Содержит непосредственно само сообщение.
   - Установите флаг **Показывать логотип в сообщении**, чтобы отображать графический объект в заголовке окна сообщения. Задайте следующие параметры логотипа:
     - Установите флаг **Использовать прозрачность** для использования прозрачности в изображении логотипа (см. Формат файла логотипа, п. 4).
     - В поле **URL** можете задать ссылку на веб-страницу, которая будет открываться при нажатии на логотип и заголовок окна.
     - В поле **Заголовок сообщения** можете задать заголовок сообщения, например, название компании. Данный текст будет отображен в заголовке окна сообщения справа от логотипа. Если данное поле останется пустым, то на месте заголовка в окне сообщения будет выводится информация о сообщении.
     - Справа от поля **Файл логотипа** нажмите кнопку для загрузки файла логотипа с локального ресурса и выберите необходимый объект в открывшемся браузере по файловой системе (см. Формат файла логотипа).

   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 Агента Dr.Web.
   - Установите флаг **Показывать ссылку в сообщении**, чтобы включить в сообщение гиперссылку на веб-ресурсы.

   Для добавления ссылки:
   1. В поле **URL** задайте ссылку на интернет-ресурс.

2. В поле **Текст** укажите название ссылки – текст, который будет отображаться на месте ссылки в сообщении.
3. В поле **Текст сообщения** добавьте маркер `{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**.

- Установите флаг **Отправлять только станциям в сети**, чтобы отправлять сообщение только станциям в сети (online). Если флаг установлен, отправка станциям не в сети осуществляться не будет. Если флаг снят, отправка станциям не в сети будет отложена до момента их подключения.
- Установите флаг **Показывать статус отправки**, чтобы выводить уведомление со статусом отправки сообщения.

4. Нажмите кнопку **Отправить**.

Формат файла логотипа

Файл с графическим изображением (логотипом), включаемый в сообщение, должен удовлетворять следующим условиям:

1. Графический формат файла: BMP, JPG, PNG, GIF, SVG.
2. Размер файла логотипа не должен превышать 512 КБ.
3. Габаритные размеры изображения – 72x72 пикселя. Изображения другого размера будут масштабироваться при отправке до размера по умолчанию.
4. Глубина цвета (bit depth) – любая (8 – 24 бит).
5. В случае, если при отправке сообщения установлен флаг **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 используете опцию **Использовать прозрачность** для прямоугольного логотипа, рекомендуется сделать прямоугольную рамку во избежание некорректного задания пикселей самого изображения логотипа в качестве прозрачных.

   Использование 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 7-2, фиолетовый фон будет исключаться (станет прозрачным).

Рисунок 7-2. Логотип нестандартной формы

Если вы хотите использовать в сообщении логотип с прозрачным фоном, используйте файлы в формате PNG или GIF.

Перед отправкой пользовательского сообщения (особенно многоадресного), рекомендуется предварительно отправить его на любой компьютер с установленным Агентом, чтобы проверить корректность результата.

Пример отправки сообщения

Для отправки сообщения, приведенного на рисунке 7-1, были заданы следующие параметры:

Текст сообщения:

```
Уважаемый пользователь!


На ваш компьютер был установлен компонент Dr.Web Firewall, выполняющий функ-
ции межсетевого экрана.

Подробную информацию о функционале данного компонента можно получить {link}.


С уважением,

Администрация.
```

URL: `http://drweb.com/`

Текст: `здесь`

Глава 8: Настройка Сервера Dr.Web

В данной главе приведено описание следующих возможностей по управлению параметрами работы антивирусной сети и Сервера Dr.Web:

- Ведение журнала – просмотр и управление журналами работы Сервера, просмотр подробных статистических данных по работе Сервера;
- Настройка конфигурации Сервера Dr.Web – настройка параметров работы Сервера;
- Настройка расписания Сервера Dr.Web – настройка расписания заданий для обслуживания Сервера;
- Настройка конфигурации веб-сервера – настройка параметров работы веб-сервера;
- Пользовательские процедуры – подключение и настройка пользовательских процедур;
- Настройка оповещений – настройка системы оповещения администратора о событиях антивирусной сети с различными методами доставки сообщений;
- Управление репозиторием Сервера Dr.Web – настройка репозитория для обновления всех компонентов антивирусной сети с ВСО и дальнейшего распространения обновлений на станции;
- Управление базой данных – непосредственное обслуживание базы данных Сервера;
- Особенности сети с несколькими Серверами Dr.Web – конфигурация многосерверной антивирусной сети и настройка межсерверных связей.

8.1. Ведение журнала

8.1.1. Журнал аудита

Журнал аудита позволяет просмотреть список событий и изменений, осуществленных при помощи управляющих подсистем Dr.Web Enterprise Security Suite.

Для просмотра журнала аудита:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Журнал аудита**.
3. Откроется окно с таблицей зарегистрированных действий. Для настройки просмотра журнала задайте на панели инструментов период, в течение которого осуществлялись действия. Для этого вы можете выбрать в выпадающем списке один из предлагаемых периодов или задать произвольные даты в календарях, открываемых при нажатии на поля дат. Нажмите **Обновить** для отображения журнала за выбранные даты.
4. Таблица журнала содержит следующие данные:
   - **Дата** – дата и время, когда было произведено действие.

- **Регистрационное имя** – регистрационное имя администратора Сервера. Указывается, если действие было инициировано непосредственно администратором или при подключении к Серверу согласно учетным данным администратора.
- **Адрес** – IP-адрес, с которого было инициировано выполнение данного действия. Указывается только в случае внешнего подключения к Серверу, в частности через Центр управления или через Web API.
- **Подсистема** – название подсистемы, которой или через которую было инициировано действие. Запись аудита осуществляется для следующих подсистем:
  - **Центр управления** – действие было произведено через Центр управления безопасностью Dr.Web, в частности администратором.
  - **Web API** – действие было произведено через Web API, например, из внешнего приложения, подключенного согласно учетным данным администратора (см. также документ **Приложения**, п. Приложение L. Интеграция Web API и Dr.Web Enterprise Security Suite).
  - **Сервер** – действие было произведено Сервером Dr.Web, например, согласно его расписанию.
  - **Утилиты** – действие было инициировано через внешние утилиты, в частности через утилиту дистанционной диагностики Сервера.
- **Результат** – краткий результат выполнения действия:
  - **ОК** – операция выполнена успешно.
  - **неуспешно** – во время выполнения операции произошла ошибка. Операция не выполнена.
  - **начато** – выполнение операции было инициировано. Результат выполнения операции будет известен только после ее завершения.
  - **нет прав** – у администратора, запустившего выполнение операции, нет прав для ее выполнения.
  - **отложено** – выполнение действия было отложено до наступления определенного срока или выполнения определенного события.
  - **невозможно** – выполнение запрошеного действия запрещено. Например, удаление системных групп.

Для действий, завершившихся с ошибкой (значение **неуспешно** в столбце **Результат**), строки отмечаются красным цветом.

- **Операция** – описание действия.

5. При необходимости вы можете экспортировать в файл данные за выбранный период. Для этого на панели инструментов нажмите одну из следующих кнопок:

 **Сохранить данные в CSV-файл**,

 **Сохранить данные в HTML-файл**,

 **Сохранить данные в XML-файл**,

 **Сохранить данные в PDF-файл**.

8.1.2. Журнал работы Сервера Dr.Web

Сервер Dr.Web ведет журнал событий, связанных с его работой.

Журнал Сервера используется для отладки, а также устранения неполадок в случае нештатной работы компонентов антивирусной сети.

По умолчанию файл журнала называется `drwcsd.log` и располагается:

- Под ОС **UNIX**:
  - для ОС Linux и ОС Solaris: `/var/opt/drwcs/log/drwcsd.log`;
  - для ОС FreeBSD: `/var/drwcs/log/drwcsd.log`.
- Под ОС **Windows**: в подкаталоге `var` каталога установки Сервера.

Файл имеет простой текстовый формат (см. документ **Приложения**, раздел Приложение К. Формат файлов журнала).

Для просмотра журнала работы Сервера через Центр управления:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Журнал Сервера Dr.Web**.
3. Откроется окно со списком журналов работы Сервера. Согласно настройкам режима ротации используется следующий формат именования файлов журнала работы Сервера: <*file_name*>.<*N*>.`log` или <*file_name*>.<*N*>.`log.gz`, где <*N*> – порядковый номер: 1, 2, и т.д. Например, при названии файла `drwcsd`, список файлов журнала работы будет следующий:
   - `drwcsd.log` – текущий файл (в который идет запись),
   - `drwcsd.1.log.gz` – предыдущий,
   - `drwcsd.2.log.gz` и так далее – чем больше число, тем более старая версия.
4. Для управления файлами журнала установите флаг напротив нужного файла или нескольких файлов. Для выбора всех файлов журнала установите флаг в заголовке таблицы. На панели инструментов станут доступны следующие кнопки:

   Экспортировать выбранные файлы журнала – сохранить локальную копию выбранных файлов журнала. Сохранение копии журнала может использоваться, например, для просмотра содержимого файла журнала с удаленного компьютера.

   Удалить выбранные файлы журнала – для удаления выбранных файлов журнала без возможности восстановления.

Настройка журнала работы для UNIX

В Серверах Dr.Web под ОС семейства UNIX включена возможность настройки ведения журнала работы Сервера через отдельный конфигурационный файл:

- для ОС Linux и ОС Solaris: `/var/opt/drwcs/etc/local.conf`;

- для ОС FreeBSD: `/var/drwcs/etc/local.conf`.

Содержимое файла `local.conf`:

```
# Log level.

DRWCS_LEV=trace3

# Log rotation.

DRWCS_ROT=10,10m
```

Значения параметров соответствуют значениям ключей командной строки для запуска Сервера:

- `-verbosity=`<*уровень_подробности*> – уровень детализации журнала работы Сервера.
- `-rotate=`<*N*><*f*>`,`<*M*><*u*> – режим ротации журнала работы Сервера.

Подробное описание ключей приведено в документе **Приложения**, раздел H4.8.

Если файл `local.conf` был отредактирован в процессе работы Сервера, необходимо перезагрузить Сервер, чтобы изменения в настройках ведения журнала вступили в силу. Перезагрузка должна осуществляться средствами операционной системы.

При обновлении и удалении Сервера файл `local.conf` проходит резервное копирование, что позволяет управлять уровнем ведения журнала при пакетном обновлении Сервера.

8.1.3. Журнал обновлений репозитория

Журнал обновлений репозитория содержит список обновлений с ВСО, включающий подробную информацию об обновленных ревизиях продуктов.

Для просмотра журнала обновлений репозитория:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Журнал обновлений репозитория**.
3. Откроется окно с таблицей зарегистрированных действий. Для настройки просмотра журнала задайте на панели инструментов период, в течение которого осуществлялись действия. Для этого вы можете выбрать в выпадающем списке один из предлагаемых периодов или задать произвольные даты в календарях, открываемых при нажатии на поля дат. Нажмите **Обновить** для отображения журнала за выбранные даты.
4. Таблица журнала содержит следующие данные:
   - **Начало** – дата и время начала загрузки обновлений конкретного продукта с ВСО.
   - **Окончание** – дата и время завершения загрузки обновлений конкретного продукта с ВСО.

- **Название продукта** – название продукта репозитория, который был загружен или загрузка которого запрашивалась.
- **Результат обновления** – результат обновления репозитория. Приводится краткая информация об удачном завершении обновления или причина ошибки.

> Для действий, завершившихся с ошибкой, ячейки **Результат обновления** отмечаются красным цветом.

- **Исходная ревизия** – номер ревизии (ревизии нумеруются согласно дате их создания), которая была последней для данного продукта перед началом процесса обновления.
- **Ревизия из обновления** – номер ревизии (ревизии нумеруются согласно дате их создания), которая была загружена в процессе обновления.
- **Обновленные файлы** – краткая сводка по измененным файлам. Приводится в формате: *<количество файлов> – <действие над файлами>*.
- **Инициатор** – система, инициировавшая процесс обновления:
  - **Запущено из командной строки** – обновление инициировано администратором при помощи соответствующей консольной команды.
  - **Запущено Планировщиком заданий** – обновление было запущено согласно заданию в расписании Сервера Dr.Web.
  - **Межсерверное обновление** – обновление было получено по межсерверной связи от главного Сервера. Данный инициатор присутствует только в случае многосерверной конфигурации антивирусной сети с распространением обновлений по межсерверным связям.
  - **Запущено из Центра управления** – обновление было запущено администратором через Центр управления безопасностью Dr.Web, в разделе Состояние репозитория.
  - **Импорт репозитория** – обновление было загружено администратором через раздел Содержимое репозитория Центра управления.
- **Администратор** – регистрационное имя администратора Сервера. Указывается, если действие было инициировано непосредственно администратором.
- **Сетевой адрес** – IP-адрес, с которого было инициировано выполнение данного действия. Указывается только в случае внешнего подключения к Серверу, в частности через Центр управления или через Web API.
- **Каталог в репозитории** – название каталога репозитория Сервера, который был модифицирован согласно процессу обновления.

5. Чтобы просмотреть подробную информацию о конкретном обновлении, нажмите на строку данного обновления. Откроется окно с таблицей о файлах продукта, измененных в процессе выбранного обновления. Для каждого файла приводится следующая информация: **Имя файла**, **Хэш файла**, **Размер** и **Состояние**.
6. При необходимости вы можете экспортировать в файл данные за выбранный период. Для этого на панели инструментов нажмите одну из следующих кнопок:

   Сохранить данные в CSV-файл,

   Сохранить данные в HTML-файл,

Сохранить данные в XML-файл,

Сохранить данные в PDF-файл.

8.2. Настройка конфигурации Сервера Dr.Web

При каждом сохранении изменений раздела **Конфигурация Сервера Dr.Web** автоматически сохраняется резервная копия предыдущей версии конфигурационного файла Сервера. Хранению подлежат 10 последних копий.

Резервные копии располагаются в том же каталоге, что и сам конфигурационный файл, и называются в соответствии со следующим форматом:

`drwcsd.conf;<время_создания>`

Вы можете использовать созданные резервные копии, в частности, для восстановления конфигурационного файла в случае, если интерфейс Центра управления недоступен.

Чтобы настроить конфигурационные параметры Сервера Dr.Web:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**. Откроется окно настроек Сервера.

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

3. На панели инструментов доступны следующие кнопки управления настройками раздела:

   Перезапустить Сервер Dr.Web – перезапустить Сервер для принятия изменений, внесенных в данном разделе. Кнопка становится активной после внесения изменений в настройки раздела и нажатия кнопки **Сохранить**.

   Восстановить конфигурацию из резервной копии – выпадающий список, содержащий сохраненные копии настроек всего раздела, к которым можно вернуться после внесения изменений. Кнопка становится активной после внесения изменений в настройки раздела и нажатия кнопки **Сохранить**.

   Установить все параметры в начальные значения – восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).

   Установить все параметры в значения по умолчанию – установить для всех параметров данного раздела значения, заданные по умолчанию.

4. Чтобы принять изменения, внесенные в настройки раздела, нажмите кнопку **Сохранить**, после чего потребуется перезагрузка Сервера. Для этого нажмите кнопку **Перезапустить Сервер Dr.Web** на панели инструментов данного раздела.

8.2.1. Общие

На вкладке **Общие** задаются следующие настройки работы Сервера:

- **Название Сервера Dr.Web** – имя данного Сервера. Если значение поля не задано, используется имя компьютера, на котором установлен Сервер Dr.Web.
- **Язык Сервера** – язык, который используется по умолчанию компонентами и системами Сервера Dr.Web, если не удалось получить настройки языка из базы данных Сервера. В частности используется для Центра управления безопасностью Dr.Web и системы оповещений администратора, если база данных была повреждена, и получить настройки языка не представляется возможным.
- **Количество параллельных запросов от клиентов** – количество потоков для обработки данных, поступающих от клиентов: Агентов, инсталляторов Агентов, соседних Серверов. Данный параметр влияет на производительность Сервера. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой технической поддержки.
- **Количество соединений с БД** – количество соединений Сервера с базой данных. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой поддержки.

Начиная с версии 10, возможность редактирования параметра **Очередь авторизации** через Центр управления не предоставляется.

По умолчанию, при установке нового Сервера, данный параметр задается равным 50. При обновлении с предыдущей версии с сохранением файла конфигурации, значение очереди авторизации сохраняется из конфигурации предыдущей версии.

При необходимости изменения длины очереди авторизации, отредактируйте значение следующего параметра в конфигурационном файле Сервера:

```
<!-- Maximun authorization queue length -->
<maximum-authorization-queue size='50'/>
```

- Установите флаг **Ограничить трафик обновлений**, чтобы ограничить объем сетевого трафика при передаче обновлений между Сервером и Агентами.

  Если флаг установлен, задайте в поле **Максимальная скорость передачи (КБ/с)** значение максимальной скорости передачи обновлений. При этом обновления будут передаваться в пределах заданной полосы пропускания совокупного сетевого трафика обновлений всех Агентов.

  Если флаг снят, обновления для Агентов передаются без ограничения полосы пропускания сетевого трафика.

- В выпадающем списке **Режим регистрации новичков** задается политика подключения новых рабочих станций (см. п. Политика подключения станций).
  - Выпадающий список **Первичная группа по умолчанию** определяет первичную группу, в которую будут помещены станции при автоматическом подтверждении доступа станций к Серверу.

- Установите флаг **Переводить неавторизованных в новички**, чтобы сбрасывать параметры получения доступа к Серверу у станций, не прошедших авторизацию. Данная опция может быть полезна при изменении настроек Сервера (таких как открытый ключ шифрования) или при смене БД. В подобных случаях станции не смогут подключиться, и потребуется повторное получение новых параметров для доступа к Серверу.
- В выпадающем списке **Шифрование** выбирается политика шифрования трафика, передаваемого по каналу связи между Сервером Dr.Web и подключаемыми к нему клиентами: Агентами, соседними Серверами, Сетевыми инсталляторами.

  Подробнее об этих параметрах см. в п. Использование шифрования и сжатия трафика.
- В выпадающем списке **Сжатие** выбирается режим сжатия трафика, передаваемого по каналу связи между Сервером Dr.Web и подключаемыми к нему клиентами: Агентами, соседними Серверами, Сетевыми инсталляторами. Подробнее об этих параметрах см. в п. Использование шифрования и сжатия трафика.
  - При выборе значений **Да** и **Возможно** для сжатия трафика, станет доступен выпадающий список **Уровень сжатия**. В этом списке вы можете выбрать уровень сжатия данных от 1 до 9, где 1 – минимальный уровень, а 9 – максимальный уровень сжатия.
- В поле **Допустимая разница между временем Сервера и** Агента задается допустимая разница между системным временем Dr.Web Сервера и Агентов Dr.Web в минутах. Если расхождение больше указанного значения, это будет отмечено в статусе станции на Сервере Dr.Web. По умолчанию допускается разница в 3 минуты. Значение 0 означает, что проверка не будет проводиться.
- Установите флаг **Заменять IP-адреса**, чтобы заменять IP-адреса DNS-именами компьютеров в файле журнала Сервера Dr.Web.
- Установите флаг **Заменять NetBIOS-имена**, чтобы отображать в каталоге антивирусной сети Центра управления не NetBIOS-имена рабочих станций, а их DNS-имена (при невозможности определения доменных имен отображаются IP-адреса).

  Оба флага **Заменять IP-адреса** 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.
- Установите флаг **Синхронизировать описания станций**, чтобы синхронизировать описание компьютера пользователя с описанием станции в Центре управления (поле Computer description на странице System properties). 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.
- Установите флаг **Отслеживать эпидемии**, чтобы включить режим оповещения администратора о случаях вирусных эпидемий. Если флаг снят, оповещения о вирусных зараже-

ниях будут осуществляться в обычном режиме. При установленном флаге вы также можете задать следующие параметры отслеживания вирусных эпидемий:

- **Период (с)** – промежуток времени в секундах, за который должно прийти заданное количество сообщений о заражениях, чтобы Сервер Dr.Web отправлял администратору единое уведомление об эпидемии на все случаи заражения.
- **Количество сообщений** – количество сообщений о заражениях, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправлял администратору единое уведомление об эпидемии на все случаи заражения.

- Установите флаг **Синхронизировать географическое положение**, чтобы активировать синхронизацию географического расположения станций между Серверами Dr.Web в многосерверной антивирусной сети. При установленном флаге вы также можете задать следующий параметр:
  - **Стартовая синхронизация** – количество станций без географических координат, информация о которых запрашивается при установлении соединения между Серверами Dr.Web.

8.2.1.1. Использование шифрования и сжатия трафика

Антивирусная сеть Dr.Web Enterprise Security Suite позволяет зашифровать трафик между Сервером и рабочими станциями (Агентами Dr.Web), между Серверами Dr.Web (при многосерверной конфигурации антивирусной 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 в процессе взаимодействия компонентов.

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 отдельно на каждом из компонентов антивирусной сети, при этом настройки остальных компонентов должны быть согласованы с настройками Сервера.

Ввиду того, что трафик между компонентами, в особенности между Серверами, может быть весьма значительным, антивирусная сеть позволяет установить сжатие этого трафика. Настройка политики сжатия и совместимость таких настроек на разных компонентах аналогичны настройкам для шифрования.

При настройке шифрования и сжатия на стороне Сервера обратите внимание на особенности клиентов, которые планируется подключать к данному Серверу. Не все клиенты поддерживают шифрование и сжатия трафика (например, Антивирус Dr.Web для Android и Антивирус Dr.Web для OS X не поддерживают ни шифрование, ни сжатие). Подключение к Серверу таких клиентов будет невозможно, если задано значение **Да** для шифрования и/или сжатия на стороне Сервера.

Чтобы задать политики сжатия и шифрования для Сервера Dr.Web:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**.
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 и сжатия на Сервере и другом компоненте (Агенте или Сетевом инсталляторе) следует иметь ввиду, что ряд сочетаний настроек является недопустимым, и их выбор приведет к невозможности установки соединения между Сервером и компонентом.

В таблице 8-1 приведены сведения о том, при каких установках соединение между Сервером и компонентом будет шифрованным/сжатым (+), при каких – нешифрованным/несжатым (–), и о том, какие сочетания являются недопустимыми (**Ошибка**).

Таблица 8-1. Совместимость настроек политик шифрования и сжатия

Настройки компонента	**Настройки Сервера**		
	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).

Для отключения режима шифрования 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.

Использование сжатия уменьшает трафик, но значительно увеличивает вычислительную нагрузку на компьютеры, в большей степени, чем шифрование.

Значение **Возможно**, установленное на стороне Агента Dr.Web, означает, что по умолчанию шифрование/сжатие будет производиться, но может быть отменено редактированием настроек Сервера Dr.Web без изменений настроек на стороне Агента.

8.2.2. Сеть

8.2.2.1. DNS

На вкладке **DNS** задаются параметры обращений к DNS-серверу:

- **Таймаут для DNS-запросов (сек.)** – таймаут в секундах для разрешения прямых/обратных DNS-запросов. Установите значение 0, чтобы не ограничивать время ожидания до окончания разрешения DNS-запроса.
- **Количество повторных DNS-запросов** – максимальное количество повторных DNS-запросов при неуспешном разрешении DNS-запроса.
- Установите флаг **Задать время хранения ответов от DNS-сервера**, чтобы задать время хранения в кэше ответов от DNS-сервера (TTL).
  - **Для положительных ответов (мин.)** – время хранения в кэше (TTL) положительных ответов от DNS-сервера в минутах.
  - **Для отрицательных ответов (мин.)** – время хранения в кэше (TTL) отрицательных ответов от DNS-сервера в минутах.
- **Серверы DNS** – список серверов DNS, заменяющий системный список по умолчанию.
- **Домены DNS** – список доменов DNS, заменяющий системный список по умолчанию.

8.2.2.2. Прокси

На вкладке **Прокси** задаются параметры прокси-сервера.

Установите флаг **Использовать прокси-сервер**, чтобы настроить соединения Сервера Dr.Web через прокси-сервер. При этом станут доступны следующие настройки:

- **Прокси-сервер** – IP-адрес или DNS-имя прокси-сервера.
- Чтобы использовать авторизацию для доступа к прокси-серверу согласно заданным методам, установите флаг **Использовать авторизацию** и задайте следующие параметры:
  - Заполните поля **Пользователь прокси-сервера** и **Пароль пользователя прокси-сервера**.
  - Выберите один из методов авторизации:

Опция		Описание
Любой метод из поддерживаемых		Использовать любой способ авторизации, поддерживаемый прокси-сервером. Если прокси-сервер поддерживает несколько методов авторизации, будет использоваться наиболее надежный.
Любой безопасный метод из поддерживаемых		Использовать любой безопасный способ авторизации, поддерживаемый прокси-сервером. В данном режиме метод авторизации Basic не используется. Если прокси-сервер поддерживает несколько методов авторизации, будет использоваться наиболее надежный.
Указанные ниже методы:	Basic-авторизация	Использовать Basic-авторизацию. Не рекомендуется использовать этот метод, поскольку передача учетных данных авторизации не шифруется.
	Digest-авторизация	Использовать Digest-авторизацию. Криптографический метод авторизации.
	NTLM-авторизация	Использовать NTLM-авторизацию. Криптографический метод авторизации. Для авторизации используется протокол NTLM компании Microsoft.
	GSS-Negotiate авторизация	Использовать GSS-Negotiate авторизацию. Криптографический метод авторизации.

8.2.2.3. Транспорт

На вкладке **Транспорт** настраиваются параметры транспортных протоколов, используемых Сервером для соединения с клиентами.

В подразделе **TCP/IP** настраиваются параметры соединений с Сервером по протоколам TCP/IP:

- **Адрес** и **Порт** – соответственно IP-адрес и номер порта сетевого интерфейса, к которому привязывается данный транспортный протокол. Интерфейс с указанными настройками прослушивается Сервером для взаимодействия с Агентами, установленными на рабочих станциях.
- **Название** – имя Сервера Dr.Web. Если оно не задано, используется имя, заданное на вкладке **Общие** (см. выше, в частности, если на указанной вкладке имя не задано, используется имя компьютера). Если для протокола задано иное имя, чем определенное на вкладке **Общие**, используется имя из описания протокола. Данное имя используется службой обнаружения для поиска Сервера Агентами и т.д.
- Установите флаг **Обнаружение**, чтобы включить службу обнаружения Сервера.
- Установите флаг **Multicasting**, чтобы использовать режим *Multicast over UDP* при обнаружении Сервера.

- **Multicast-группа** – IP-адрес multicast-группы, в которой зарегистрирован Сервер. Используется для взаимодействия с Агентами и Сетевыми инсталляторами при поиске активных Серверов Dr.Web сети. Если значение данного поля не задано, по умолчанию используется группа `231.0.0.1`.
- Только под ОС семейства UNIX: в поле **Путь** задается путь до сокета связи, например, с Агентом.

> Более подробная информация приведена в разделе Настройка сетевых соединений.

Данные параметры задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

8.2.2.4. Кластер

На вкладке **Кластер** настраиваются параметры кластера Серверов Dr.Web для обмена информацией при многосерверной конфигурации антивирусной сети.

Для использования кластера задайте следующие параметры:

- **Multicast-группа** – IP-адрес multicast-группы, через которую Серверы будут осуществлять обмен информацией.
- **Порт** – номер порта сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу.
- **Интерфейс** – IP-адрес сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу.

> Особенности создания кластера Серверов Dr.Web приведены в разделе Кластер Серверов Dr.Web.

8.2.2.5. Загрузка

На вкладке **Загрузка** настраиваются параметры Сервера, используемые при формировании файлов инсталляции Агента для станций антивирусной сети. В дальнейшем эти параметры используются при подключении инсталлятора Агента к Серверу:

- **Адрес Сервера Dr.Web** – IP-адрес или DNS-имя Сервера Dr.Web.

  Если адрес Сервера не задан, то используется имя компьютера, возвращаемое операционной системой.
- **Порт** – номер порта, который будет использоваться при подключении инсталлятора Агента к Серверу.

  Если номер порта не задан, то используется порт 2193 (настраивается в Центре управления в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → вкладка **Сеть** → вкладка **Транспорт**).

Настройки раздела **Загрузка** сохраняются в конфигурационном файле `download.conf` (см. документ **Приложения**, п. G3. Конфигурационный файл download.conf).

8.2.2.6. Групповые обновления

На вкладке **Групповые обновления** настраивается передача групповых обновлений на рабочие станции по multicast-протоколу.

Чтобы включить передачу обновлении на станции по multicast-протоколу, установите флаг **Включить групповые обновления**, при этом:

- Если групповые обновления отключены, обновление для всех станций осуществляется только штатным способом – по протоколу TCP.
- Если групповые обновления включены, то для всех станций, подключенных к данному Серверу, обновление будет осуществляться в два этапа:
  1. Обновление по multicast-протоколу.
  2. Стандартное обновление по протоколу TCP.

Для настройки групповых обновлений используются следующие параметры:

- **Размер UDP-датаграммы (байты)** – размер в байтах UDP-датаграмм, используемых multicast-протоколом.

  Допустимый диапазон 512 – 8192. Во избежании фрагментации рекомендуется задавать значение меньше MTU (Maximum Transmission Unit) используемой сети.
- **Время передачи файла (мс.)** – в течение заданного интервала осуществляется передача одного файла обновления, после чего Сервер начинает отправку следующего файла.

  Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP.
- **Длительность групповых обновлений (мс.)** – длительность процесса обновления по multicast-протоколу.

  Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP.
- **Интервал отправки пакетов (мс.)** – интервал отправки пакетов в multicast-группу.

  Малое значение интервала может привести к значительным потерям при передаче пакетов и перегрузить сеть. Не рекомендуется изменять этот параметр.
- **Интервал между запросами на повторную передачу (мс.)** – с данным интервалом Агенты отправляют запросы на повторную передачу потерянных пакетов.

  Сервер Dr.Web накапливает эти запросы, после чего пересылает потерянные блоки.
- **Интервал “тишины” на линии (мс.)** – в случае завершения передачи файла до истечения отведенного времени, если в течение заданного интервала “тишины” от Агентов не поступило запросов на повторную передачу потерянных пакетов, Сервер Dr.Web считает, что все Агенты успешно получили файлы обновления, и начинает отправку следующего файла.

- **Интервал накопления запросов на повторную передачу (мс.)** – в течение указанного интервала Сервер накапливает запросы от Агентов на повторную передачу потерянных пакетов.

  Агенты перезапрашивают потерянные пакеты. Сервер накапливает эти запросы в течение указанного времени, после чего пересылает потерянные блоки.

Чтобы задать список multicast-групп, через которые будет доступно групповое обновление, настройте следующие параметры в подразделе **Multicast-группы**:

- **Multicast-группа** – IP-адрес multicast-группы, через которую станции будут получать групповые обновления.
- **Порт** – номер порта сетевого интерфейса Сервера Dr.Web, к которому привязывается транспортный multicast-протокол для передачи обновлений.

> Для групповых обновлений необходимо задавать любой свободный порт, в частности, отличный от порта, который назначен в настройках для работы транспортного протокола самого Сервера.

- **Интерфейс** – IP-адрес сетевого интерфейса Сервера Dr.Web, к которому привязывается транспортный multicast-протокол для передачи обновлений.

  В каждой строке задаются настройки одной multicast-группы. Для добавления еще одной multicast-группы нажмите  .

При задании нескольких multicast-групп, обратите внимание на следующие особенности:

- Для разных Серверов Dr.Web, которые будут рассылать групповые обновления, должны задаваться различные multicast-группы.
- Для разных Серверов Dr.Web, которые будут рассылать групповые обновления, необходимо задавать различные параметры **Интерфейс** и **Порт**.
- При использовании нескольких multicast-групп, наборы станций, входящие в данные группы, не должны пересекаться. Таким образом, каждая станция антивирусной сети может входить только в одну multicast-группу.

8.2.3. Статистика

На вкладке **Статистика** задается статистическая информация, которая записывается в журнал протокола и заносится в базу данных Сервера.

Для регистрации и добавления в БД соответствующего типа информации установите следующие флаги:

- **Состояние карантина** – разрешает мониторинг состояния Карантина на станциях и запись информации в базу данных.
- **Состав оборудования и программ** – разрешает мониторинг состава аппаратно-программного обеспечения станций и запись информации в базу данных.
- **Список модулей станций** – разрешает мониторинг списка модулей Антивируса, установленных на станциях, и запись информации в базу данных.

- **Список установленных компонентов** – разрешает мониторинг списка установленных компонентов Антивируса (Сканер, мониторы и т.п.), установленных на рабочей станции, и запись информации в базу данных.
- **Сессии пользователей станции** – разрешает мониторинг сессий пользователей рабочих станций и запись в базу данных регистрационных имен пользователей, вошедших в систему на компьютере с установленным Агентом.
- **Запуск/Завершение компонентов** – разрешает мониторинг информации о запуске и завершении работы компонентов Антивируса (Сканер, мониторы и т.п.) на рабочих станциях и запись информации в базу данных.
- **Обнаруженные угрозы безопасности** – разрешает мониторинг обнаружения угроз безопасности рабочих станций и запись информации в базу данных.

  Если флаг **Обнаруженные угрозы безопасности** установлен, вы также можете настроить дополнительные параметры статистики по угрозам.

  Для активации отправки статистики по обнаруженным угрозам безопасности станций в компанию «Доктор Веб» установите флаг Отправлять статистику в компанию «Доктор Веб». Станут доступны следующие поля:

  - **Интервал** – интервал отправки статистики в минутах;
  - **Идентификатор** – MD5-ключ (находится в конфигурационном файле Сервера).

  Обязательным полем является только **Интервал** отправки статистики.
- **Ошибки сканирования** – разрешает мониторинг обнаружения ошибок при сканировании на рабочих станциях и запись информации в базу данных.
- **Статистика сканирования** – разрешает мониторинг результатов сканирования на рабочих станциях и запись информации в базу данных.
- **Инсталляции Агентов** – разрешает мониторинг информации об инсталляциях Агентов на рабочих станциях и запись ее в базу данных.
- **Журнал выполнения заданий на станциях** – разрешает мониторинг результатов выполнения задания на станциях и запись их в базу данных.
- **Состояние станций** – разрешает мониторинг изменений состояния станций и запись информации в базу данных.
  - **Состояние вирусных баз** – разрешает мониторинг состояния (состава, изменения) вирусных баз на станции и запись информации в базу данных. Флаг доступен, только если установлен флаг **Состояние станций**.

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 статистики по рабочей станции.

В таблице ниже приведено соответствие флагов из раздела **Статистика** в настройках Сервера и пунктов управляющего меню на странице **Антивирусная сеть**.

При снятии флагов на вкладке **Статистика**, соответствующие им пункты будут скрыты из управляющего меню.

Таблица 8-2. Соответствие настроек Сервера и пунктов управляющего меню

Настройки Сервера	Пункты меню
Состояние карантина	Общие → Карантин Конфигурация → Windows → Агент Dr.Web → флаг Разрешить удаленное управление карантином
Состав оборудования и программ	Общие → Оборудование и программы Общие → Сравнение оборудования и программ
Список модулей станции	Статистика → Модули
Список установленных компонентов	Общие → Установленные компоненты
Сессии пользователей станции	Общие → Сессии пользователей
Запуск/Завершение компонентов	Статистика → Запуск/Завершение
Обнаруженные угрозы безопасности	Статистика → Угрозы Статистика → Статистика угроз
Ошибки сканирования	Статистика → Ошибки
Статистика сканирования	Статистика → Статистика сканирования Таблицы → Суммарная статистика
Инсталляции Агентов	Статистика → Инсталляции Агентов
Журнал выполнения заданий на станции	Статистика → Задания Статистика → Вирусные базы
Состояние станций	Статистика → Состояние Статистика → Вирусные базы
Состояние вирусных баз	Статистика → Вирусные базы

8.2.4. Безопасность

На вкладке **Безопасность** задаются ограничения на сетевые адреса, с которых Агенты, сетевые инсталляторы и другие (соседние) Серверы Dr.Web смогут получать доступ к данному Серверу.

Управление журналом аудита Сервера осуществляется при помощи следующих флагов:

- **Аудит операций администратора** 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 Dr.Web и запись журнала в БД.
- **Аудит операций Web API** разрешает ведение журнала аудита операций через XML API и запись журнала в БД.

Журнал аудита можно посмотреть, выбрав в главном меню **Администрирование** пункт **Журнал аудита**.

На вкладке **Безопасность** размещаются дополнительные вкладки, на которых настраиваются ограничения для соответствующих типов соединений:

- **Агенты** – список ограничений на IP-адреса, с которых Агенты Dr.Web могут подключаться к данному Серверу.
- **Инсталляторы** – список ограничений на IP-адреса, с которых инсталляторы Агентов Dr.Web могут подключаться к данному Серверу.
- **Соседи** – список ограничений на IP-адреса, с которых соседние Серверы Dr.Web могут подключаться к данному Серверу.
- **Служба обнаружения** – список ограничений на IP-адреса, с которых принимаются широковещательные запросы службой обнаружения Сервера.

Для того чтобы настроить ограничения доступа для какого-либо типа соединения:

1. Перейдите на соответствующую вкладку (**Агенты**, **Инсталляции**, **Соседи** или **Служба обнаружения**).
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 кнопку **Сохранить**.

2. Для добавления нового поля адреса, нажмите кнопку  соответствующего раздела.
3. Для удаления поля нажмите 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.*.*.*`

Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлен ли флаг **Приоритетность запрета**. Если флаг установлен, список **Запрещено** имеет более высокий приоритет, чем список **Разрешено**. Адреса, не включенные ни в один из списков или включенные в оба, запрещаются. Разрешаются только адреса, которые включены в список **Разрешено** и не включены в список **Запрещено**.

8.2.5. Кэш

На вкладке **Кэш** задаются параметры очистки серверного кэша:

- **Период очистки кэша** – периодичность полной очистки кэша.
- **Файлы в карантине** – периодичность удаления файлов в Карантине на стороне Сервера.
- **Файлы репозитория** – периодичность удаления файлов в репозитории.
- **Инсталляционные пакеты** – периодичность удаления персональных инсталляционных пакетов.

При задании числовых значений обратите внимание на выдающие списки с единицами измерения периодичности.

8.2.6. База данных

На вкладке **База данных** задается выбор СУБД, необходимой для функционирования Сервера Dr.Web.

Структуру БД Сервера Dr.Web можно получить на основе `sql`-скрипта `init.sql`, расположенного в подкаталоге etc каталога установки Сервера Dr.Web.

1. В выпадающем списке **База данных** выберите тип базы данных:
   - **IntDB** – встроенная БД SQLite2 (компонент Сервера Dr.Web),
   - **ODBC** – для использования внешней БД через ODBC-соединение,

   При возникновении предупреждений или ошибок в работе Сервера Dr.Web с СУБД Microsoft SQL Server через ODBC следует убедиться, что вы используете последнюю доступную версию СУБД для данной редакции.

   С тем, как определить наличие исправлений, вы можете ознакомиться на следующей странице компании Microsoft: https://support.microsoft.com/en-us/kb/321185.

   - **Oracle** – внешняя БД для платформ, кроме FreeBSD,

   При использовании внешней **СУБД Oracle** через ODBC-подключение необходимо установить последнюю версию ODBC-драйвера, поставляемую с данной СУБД. Использование ODBC-драйвера Oracle, поставляемого Microsoft, категорически не рекомендовано.

   - **PostgreSQL** – внешняя БД,
   - **SQLite3** – встроенная БД (компонент Сервера Dr.Web). Рекомендуемый вариант при использовании встроенной БД.
2. Задайте необходимые настройки для работы с БД:
   - Для встроенных БД, при необходимости, введите в поле **Имя файла** полный путь к файлу с базой данных и задайте размер кэш-памяти и режим записи данных.
   - Параметры для внешних БД описаны в документе **Приложения**, в разделе Приложение В. Настройки, необходимые для использования СУБД. Параметры драйверов СУБД.
3. Для применения заданных настроек нажмите **Сохранить**.

   Дистрибутив Сервера Dr.Web содержит встроенные клиенты для поддерживаемых СУБД, поэтому:

   - Если вы планируете использовать поставляемые вместе с Сервером Dr.Web встроенные клиенты СУБД, то при установке (обновлении) Сервера, в настройках инсталлятора убедитесь, что разрешена установка соответствующего встроенного клиента для СУБД в разделе **Поддержка баз данных**.
   - Если вы планируете подключаться к внешним базам данных через ODBC, то при установке (обновлении) Сервера, в настройках инсталлятора отмените установку соответствующего встроенного клиента в разделе **Поддержка баз данных**.
     В противном случае работа с БД через ODBC будет невозможна из-за конфликта библиотек.

   Инсталлятор Сервера поддерживает режим изменения продукта. Для добавления или удаления отдельных компонентов, например, драйверов для управления базами данных, достаточно запустить инсталлятор Сервера и выбрать вариант **Изменить**.

По умолчанию предусмотрено использование встроенной СУБД. Выбор этого режима создает значительную вычислительную нагрузку на Сервер. При значительном размере антивирусной сети рекомендуется использовать внешнюю СУБД. Процедура смены типа СУБД

описана в документе **Приложения**, в разделе Смена типа СУБД Dr.Web Enterprise Security Suite.

Использование встроенной БД допустимо при подключении к Серверу не более 200-300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен Сервер Dr.Web, 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 Сервера Dr.Web, от 8 ГБ – для сервера БД,
- ОС семейства UNIX.

Предусмотрена возможность осуществления операций, связанных с очисткой базы данных, используемой Сервером Dr.Web, 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.

8.2.7. Модули

На вкладке **Модули** задается режим взаимодействия Сервера Dr.Web с другими компонентами Dr.Web Enterprise Security Suite:

- Установите флаг **Расширение Центра управления безопасностью Dr.Web** для возможности использования расширения Центра управления безопасностью Dr.Web для управления Сервером и антивирусной сетью через Центр управления.

При снятии флага **Расширение Центра управления безопасностью Dr.Web**, после перезагрузки Сервера Dr.Web будет недоступен Центр управления безопасностью Dr.Web. При этом управление Сервером и антивирусной сетью будет возможно только через утилиту дистанционной диагностики, при условии, что флаг **Расширение Dr.Web Server FrontDoor** установлен.

- Установите флаг **Расширение Dr.Web Server FrontDoor** для возможности использования расширения Dr.Web Server FrontDoor, позволяющего подключение утилиты дистанционной диагностики Сервера (см. также п. Удаленный доступ к Серверу Dr.Web).
- Установите флаг **Протокол Агента Dr.Web** для включения протокола взаимодействия Сервера с Агентами Dr.Web.
- Установите флаг **Протокол Microsoft NAP Health Validator** для включения протокола взаимодействия Сервера с компонентом проверки работоспособности системы Microsoft NAP Validator.

- Установите флаг **Протокол инсталлятора Агента Dr.Web** для включения протокола взаимодействия Сервера с инсталляторами Агентов Dr.Web.
- Установите флаг **Протокол кластера Серверов Dr.Web** для включения протокола взаимодействия между Серверами в кластерной системе.
- Установите флаг **Протокол Сервера Dr.Web** для включения протокола взаимодействия Сервера Dr.Web с другими Серверами Dr.Web. Протокол по умолчанию отключен. При задании многосерверной конфигурации сети (см.п. Особенности сети с несколькими Серверами Dr.Web) включите этот протокол, установив флаг **Протокол Сервера Dr.Web**.

8.2.8. Расположение

На вкладке **Расположение** вы можете задать дополнительную информацию о физическом расположении компьютера, на котором установлено ПО Сервера Dr.Web.

Также на данной вкладке вы можете просмотреть расположение Сервера на географической карте.

Для просмотра расположения Сервера на карте:

1. Задайте в полях **Широта** и **Долгота** географические координаты Сервера в формате десятичных градусов (Decimal Degrees).
2. Нажмите кнопку **Сохранить** для сохранения введенных данных в конфигурационном файле Сервера.

   Для отображения карты перезагрузка Сервера не требуется. Однако, для применения измененных географических координат перезагрузка Сервера потребуется.
3. На вкладке **Расположение** отобразится превью карты OpenStreetMaps с меткой, соответствующей заданным координатам.

   В случае, если загрузка превью невозможна, отображается текст **Показать на карте**.
4. Для просмотра полноразмерной карты нажмите на превью или на текст **Показать на карте**.

8.2.9. Лицензии

На вкладке **Лицензии** задаются настройки распространения лицензий между Серверами Dr.Web:

- **Срок действия выдаваемых лицензий** – период времени, на который выдаются лицензии из ключа на данном Сервере. Настройка используется, если данный Сервер выдает лицензии соседним Серверам.
- **Период для продления получаемых лицензии** – период до окончания срока действия лицензии, начиная с которого данный Сервер инициирует продление лицензии, полученной от соседнего Сервера. Настройка используется, если данный Сервер получает лицензии от соседних Серверов.

- **Период синхронизации лицензий** – периодичность синхронизации информации о выдаваемых лицензиях между Серверами.

Подробную информацию о распространении лицензий между Серверами см. в разделе Менеджер лицензий.

8.3. Удаленный доступ к Серверу Dr.Web

Для возможности подключения утилиты дистанционной диагностики Сервера необходимо включить расширение Dr.Web Server FrontDoor. Для этого в разделе **Конфигурация Сервера Dr.Web**, на вкладке Модули установите флаг **Расширение Dr.Web Server FrontDoor**.

Для возможности подключения утилиты дистанционной диагностики Сервера необходимо, чтобы для администратора, который подключается через утилиту, было разрешено право **Использование дополнительных возможностей**. В противном случае доступ к Серверу через утилиту дистанционной диагностики будет запрещен.

Чтобы настроить параметры подключения утилиты дистанционной диагностики Сервера:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Удаленный доступ к Серверу Dr.Web**.
2. Задайте настройки протокола подключения:
   - Установите флаг **Использовать SSL**, чтобы разрешить подключение утилиты дистанционной диагностики к Серверу Dr.Web по протоколу SSL. Если флаг снят, подключение будет возможно только по протоколу TCP.
     Для подключения по протоколу SSL задайте следующие настройки:
     - **SSL-сертификат** – файл SSL-сертификата, который будет проверяться при подключении. В выпадающем списке приводятся доступные сертификаты из каталога Сервера.
     - **Закрытый ключ SSL** – файл закрытого ключа SSL, который будет проверяться при подключении. В выпадающем списке приводятся доступные закрытые ключи SSL из каталога Сервера.
3. Задайте настройки узлов подключения:
   - **Адрес** – адрес, с которого разрешается подключение утилиты дистанционной диагностики Сервера.
   - **Порт** – порт для подключения утилиты дистанционной диагностики Сервера. По умолчанию используется порт 10101.

   Чтобы добавить еще один разрешенный адрес, нажмите  и задайте значения добавленных полей.

Чтобы запретить подключение с разрешенного адреса, удалите данный адрес из списка, нажав  напротив строки с этим адресом.

4. Нажмите **Сохранить**.

> Описание использования консольной версии утилиты дистанционной диагностики Сервера приведено в документе **Приложения**, в разделе Н10. Утилита дистанционной диагностики Сервера Dr.Web.

8.4. Настройка расписания Сервера Dr.Web

Чтобы настроить расписание выполнения заданий для Сервера Dr.Web:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Планировщик заданий Сервера Dr.Web**. Откроется список заданий Сервера.
2. Для управления расписанием используются соответствующие элементы на панели инструментов:
   a) Общие элементы панели инструментов служат для создания новых заданий и управления разделом расписания в целом. Данные инструменты всегда доступны на панели инструментов:

    **Создать задание** – добавить новое задание. Данное действие подробно описывается ниже, в подразделе Редактор заданий.

    **Экспортировать настройки из данного раздела в файл** – экспортировать расписание в файл специального формата.

    **Импортировать настройки в данный раздел из файла** – импортировать расписание из файла специального формата.

   b) Для управления уже существующими заданиями установите флаги напротив нужных заданий или в заголовке таблицы для выбора всех заданий в списке. При этом станут доступны элементы панели инструментов для управления выбранными заданиями:

Настройка		Действие
Состояние	**Разрешить выполнение**	Активировать выполнение выбранных заданий согласно заданному для них расписанию, если они были запрещены.
	Запретить выполнение	Запретить выполнение выбранных заданий. При этом задания будет присутствовать в списке, но не будет выполняться.
> Аналогичная настройка задается в редакторе задания на вкладке **Общие** при помощи флага **Разрешить выполнение**.		
Важность	**Сделать критическим**	Осуществить внеочередной запуск задания, если выполнение данного задания было пропущено по расписанию.

Настройка		Действие
	Сделать не критическим	Выполнять задание только в заданное время, вне зависимости от того, был пропущен запуск задания или нет.
Аналогичная настройка задается в редакторе задания на вкладке **Общие** при помощи флага **Критическое задание**.		
Дублировать настройки		Дублировать задания, выбранные в списке текущего расписания. При задании действия **Дублировать настройки** создаются новые задания с настройками, аналогичными выбранным заданиям.
Запланировать повторно		Для однократных заданий: выполнить задание еще один раз в соответствии с заданными для него настройкам времени (изменение кратности выполнения задания описано ниже, в подразделе Редактор заданий).
Удалить выбранные задания		Удалить выбранное задание из расписания.

3. Для того чтобы изменить параметры задания, выберите его в списке заданий. При этом откроется окно **Редактор заданий**, описанное ниже.
4. По окончании редактирования расписания нажмите кнопку **Сохранить**, чтобы принять изменения.

Редактор заданий

При помощи редактора заданий вы можете задать настройки, чтобы:

1. Создать новое задание.

   Для этого нажмите кнопку **Создать задание** на панели инструментов.
2. Отредактировать существующее задание.

   Для этого нажмите на название задания в списке заданий.

При этом откроется окно редактирования параметров задания. Настройки задания при редактировании существующего задания аналогичны настройкам при создании нового задания.

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

Для редактирования параметров задания:

1. На вкладке **Общие** настраиваются следующие параметры:
   - В поле **Название** задается наименование задания, под которым оно будет отображаться в расписании.

- Установите флаг **Разрешить выполнение**, чтобы активировать выполнение задания. Если флаг не установлен, задание будет присутствовать в списке, но не будет выполняться.

Аналогичная настройка задается в главном окне Планировщика при помощи элемента панели инструментов **Состояние**.

- Установите флаг **Критическое задание**, чтобы осуществлять внеочередной запуск задания, если его выполнение было пропущено в назначенное время по какой-либо причине. Планировщик ежеминутно просматривает список заданий и, при обнаружении пропущенного критического задания, осуществляет его запуск. Если на момент запуска задание было пропущено несколько раз, то оно выполнится только 1 раз.

Аналогичная настройка задается в главном окне Планировщика при помощи элемента панели инструментов **Важность**.

На вкладке **Действие** выберите тип задания из выпадающего списка **Действие** и настройте параметры задания, требуемые для выполнения:

Тип задания	Параметры и описание
Выполнение процедуры	Задание предназначено для выполнения пользовательских процедур (подробнее см. п. Пользовательские процедуры). Необходимо задать следующие параметры: • **Группа процедур** – группа пользовательских процедур, для которой будет выполняться процедура. • **Процедура** – название конкретной выполняемой пользовательской процедуры из группы, выбранной в списке **Группа процедур**. • Установите флаг **Выполнить для всех групп процедур**, чтобы выполнять выбранную пользовательскую процедуру во всех группах процедур, в которых данная процедур задана. При этом для каждой группы будет выполняться та процедура, которая определена непосредственно для нее.
Выполнение скрипта	Задание предназначено для выполнения lua-скрипта, приведенного в поле **Скрипт**. Одновременное выполнение задания типа **Выполнение скрипта** на нескольких Серверах, использующих одну БД, может приводить к ошибкам выполнения данного задания. При выполнении lua-скриптов администратор получает доступ ко всей файловой системе в пределах каталога Сервера и некоторым системным командам на компьютере с установленным Сервером. Чтобы запретить доступ к расписанию, отключите право **Редактирование расписания Сервера** для соответствующего администратора (см. п. Администраторы и административные группы).

Тип задания	Параметры и описание
Замена ключа шифрования	Задание предназначено для периодической замены ключей шифрования: • закрытого ключа `drwcsd.pri` на Сервере, • открытого ключа `drwcsd.pub` на рабочих станциях. Поскольку некоторые рабочие станции могут оказаться выключены на момент замены, процедура делится на два этапа. Необходимо создать два задания для выполнения каждого из этих этапов, при этом второй этап рекомендуется выполнять спустя некоторое время после первого этапа, за которое станции наверняка подключатся к Серверу. При создании задания выберите соответствующий этап замены ключа из выпадающего списка: • **Добавление нового ключа** – первый этап процедуры, на котором создается новая неактивная пара ключей шифрования. Станции получают новый открытый ключ, когда подключаются к Серверу. • **Удаление старого ключа и переход на новый ключ** – второй этап, на котором рабочие станции информируются о переходе на новые ключи шифрования, после чего осуществляется замена действующих ключей на новые: открытые ключи на станциях и закрытый ключ на Сервере. Те станции, которые по каким-либо причинам не получили новый открытый ключ, не смогут подключиться к Серверу. Для разрешения данной проблемы возможны следующие варианты действий: • Вручную подложить новый открытый ключ на станции (с процедурой замены ключа на станции можно ознакомиться в документе **Приложения**, в разделе Подключение Агента Dr.Web к другому Серверу Dr.Web). • Разрешить Агентам авторизацию на Сервере с неверным открытым ключом (см. п. **Сеть** в настройках Агента).
Запись в файл журнала	Задание предназначено для записи в файл отчета Сервера заданной строки. **Строка** – текст сообщения, записываемого в файл отчета.
Запуск программы	Задание предназначено для запуска произвольной программы. Программы, запущенные в рамках данного задания, выполняются в фоновом режиме. Необходимо задать следующие параметры: • В поле **Путь** – полное имя (с путем) исполняемого файла программы, которую предполагается запускать. • В поле **Аргументы** – параметры командной строки для запускаемой программы. • Установите флаг **Ожидать завершения программы** для ожидания завершения программы, запущенной данным заданием. При этом Сервер протоколирует запуск программы, код возврата и время завершения программы.

Тип задания	Параметры и описание
	Если флаг **Ожидать завершения программы** снят, задание считается завершенным сразу после запуска программы, и Сервер протоколирует только запуск программы.
Напоминание об окончании лицензии	Задание предназначено для выдачи оповещения об окончании срока действия лицензии на продукт Dr.Web. Необходимо задать период до окончания срока действия лицензии, начиная с которого будет выдаваться напоминание.
Обновление репозитория	Информация о данном задании приведена в разделе Обновление по расписанию.
Останов Сервера Dr.Web	Задание предназначено для завершения работы Сервера. Запускается без дополнительных параметров.
Отправка сообщения на станцию	Задание предназначено для отправки произвольного сообщения пользователям станции или группы станций. Настройки сообщения приведены в разделе Отправка сообщений станциям.
Очистка базы данных	Задание предназначено для сборки и удаления неиспользуемых записей в базе данных Сервера посредством выполнения команды `vacuum`. Запускается без дополнительных параметров.
Очистка неотправленных событий	Задание предназначено для удаления неотправленных событий из базы данных. Необходимо указать период хранения неотправленных событий, по истечении которого они будут удаляться. Здесь имеются в виду события, передаваемые подчиненным Сервером главному Серверу. При неудачной передаче события, оно заносится в список неотправленных. Подчиненный Сервер с заданной периодичностью осуществляет попытки передачи. При выполнении задания **Очистка неотправленных событий** осуществляется удаление всех событий, длительность хранения которых достигла и превысила заданный период.
Очистка старых записей	Задание предназначено для удаления устаревшей информации о станциях из базы данных. 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.

Тип задания	Параметры и описание
Очистка старых станций	Задание предназначено для удаления устаревших станций из базы данных. Необходимо указать временной период (по умолчанию 90 дней), в течение которого не посещавшие Сервер станции, признаются старыми и удаляются с Сервера.
 Старые данные автоматически удаляются из базы данных с целью экономии дискового пространства. По умолчанию период для заданий **Очистка старых записей** и **Очистка 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.	
Очистка устаревших сообщений	Задание предназначено для удаления из базы данных следующих сообщений: • агентские оповещения, • оповещения для веб-консоли, • отчеты, созданные по расписанию. При этом удаляются сообщения, помеченные как устаревшие, т.е. сообщения с истекшим сроком хранения, который вы можете настроить: • для оповещений: при создании оповещений для соответствующего способа отправки (см. п. Конфигурация оповещений). • для отчетов: в задании на создание отчетов. Задание запускается без дополнительных параметров.
Перезапуск Сервера Dr.Web	Задание предназначено для перезапуска Сервера. Запускается без дополнительных параметров.
Пробуждение станций	Задание предназначено для включения станций, например, перед запуском задания на сканирование. Включаемые станции задаются при помощи следующих параметров задания: • **Будить все станции** – предписывает включить все станции, подключенные к данному Серверу. • **Будить станции по заданным параметрам** – предписывает включить только станции, соответствующие указанным ниже параметрам: ▫ **IP-адреса** – список IP-адресов станций, которые необходимо включить. Задается в формате: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. При задании списка адресов используйте запятую или переход на новую строку в качестве разделителя. Также IP-адреса можно заменять на DNS-имена компьютеров. ▫ **MAC-адреса** – список MAC-адресов станций, которые необходимо включить. Октеты MAC-адреса разделяются знаком ':'. При задании

Тип задания	Параметры и описание
	списка адресов используйте запятую или переход на новую строку в качестве разделителя. ▫ **Группы** – список групп, станции которых необходимо включить. Для выбора нескольких групп используйте кнопки CTRL и SHIFT.  Для выполнения данного задания на включаемых станциях должны быть установлены сетевые карты с поддержкой опции Wake-on-LAN. Поддержку опции Wake-on-LAN вы можете проверить в документации к сетевой карте или в свойствах сетевой карты (**Панель управления** → **Сеть и Интернет** → **Сетевые подключения** → **Настройка параметров подключения** → **Настроить** → **Дополнительно**).
Резервное копирование критичных данных сервера	Задание предназначено для создания резервной копии следующих критичных данных Сервера: • база данных, • лицензионный ключевой файл, • закрытый ключ шифрования. Необходимо задать следующие параметры: • **Путь** – путь к каталогу, в который будут сохранены данные (пустой путь означает каталог по умолчанию). • **Максимальное количество копий –** максимальное количество резервных копий (значение 0 означает отмену этого ограничения). Подробнее см. в документе **Приложения**, п. Приложение Н4.5.  Каталог для резервного копирования должен быть пуст. В противном случае содержимое каталога будет удалено при выполнении резервного копирования.
Резервное копирование репозитория	Задание предназначено для периодического сохранения резервных копий репозитория. Необходимо задать следующие параметры: • **Путь** – полный путь до каталога, в котором будет сохраняться резервная копия. • **Максимальное количество копий** – максимальное количество резервных копий репозитория, сохраняемых заданием в указанном каталоге. При достижении максимального количества копий репозитория, для сохранения новой копии, удаляется самая старая из имеющихся копий. • **Область репозитория** определяет, какой блок информации об антивирусном компоненте будет сохраняться:

Тип задания	Параметры и описание
	▫ **Весь репозиторий** – сохранять все ревизии из репозитория, для тех компонентов, которые выбраны в списке ниже. ▫ **Только важные ревизии** – сохранять только ревизии, помеченные как важные, для тех компонентов, которые выбраны в списке ниже. ▫ **Только конфигурационные файлы** – сохранять только конфигурационные файлы тех компонентов, которые выбраны в списке ниже. • Установите флаги напротив компонентов, выбранные области которых буду сохраняться. ⚠ Каталог для резервного копирования должен быть пуст. В противном случае содержимое каталога будет удалено при выполнении резервного копирования.
Синхронизация с Active Directory	Задание предназначено для синхронизации структуры сети: контейнеры Active Directory, содержащие компьютеры, становятся группами антивирусной сети, в которые помещаются рабочие станции. Запускается без дополнительных параметров. ⓘ По умолчанию данное задание отключено. Для активации выполнения задания установите опцию **Разрешить выполнение** в настройках задания или на панели инструментов как описано выше.
Соседний сервер давно не подключался	Задание предназначено для выдачи оповещения о том, что соседние Серверы давно не подключались к данному Серверу. Настройка отображения оповещения осуществляется в разделе Конфигурация оповещений при помощи пункта **Соседний сервер давно не подключался**. В полях **Часов** и **Минут** задайте периоды времени, по истечении которых соседний Сервер будет считаться давно не подключавшимся.
Станция давно не подключалась	Задание предназначено для выдачи оповещения о том, что станции давно не подключались к данному Серверу. Настройка отображения оповещения осуществляется в разделе Конфигурация оповещений при помощи пункта **Станция давно не подключалась к серверу**. В поле **Дней** задайте период времени, по истечении которого станция будет считаться давно неподключавшейся.
Создание статистического отчета	Задание предназначено для создания отчета со статистическими данными по антивирусной сети.

Тип задания	Параметры и описание
	Для возможности создания отчета необходимо, чтобы было включено оповещение **Периодический отчет** (см. п. Конфигурация оповещений). Созданный отчет сохраняется на компьютере с установленным Сервером. Получение отчета зависит от типа оповещения: • Для метода отправки сообщения **Электронная почта**: на адрес почтового ящика, заданного в настройках оповещения, отправляется письмо со ссылкой на местоположение отчета и сам отчет во вложениях к письму. • Для всех остальных методов отправки: отправляется соответствующее оповещение, которое содержит ссылку на местоположение отчета. Для создания задания в расписании необходимо задать следующие параметры: • **Профили уведомлений** – название группы оповещений с настройками, согласно которым будет создаваться отчет. Название заголовка задается при создании новой группы оповещений. • **Язык отчета** – язык, на котором будут представлены данные в отчете. • **Формат даты** – формат, в котором будет отображаться статистическая информация, содержащая даты. Доступны следующие форматы: ▫ европейский: `DD-MM-YYYY HH:MM:SS` ▫ американский: `MM/DD/YYYY HH:MM:SS` • **Формат отчета** – формат документа, в котором будет сохранен статистический отчет. • **Отчетный период** – период времени, статистические данные за который будут внесены в отчет. • **Группы** – список групп станций антивирусной сети, данные о которых будут занесены в отчет. Для выбора нескольких групп используйте кнопки CTRL или SHIFT. • **Таблицы отчета** – список статистических таблиц, данные из которых будут занесены в отчет. Для выбора нескольких таблиц используйте кнопки CTRL или SHIFT. • **Срок хранения отчета** – временной период хранения отчета на компьютере с установленным Сервером, начиная с момента создания отчета.

2. На вкладке **Время**:
   - В выпадающем списке **Периодичность** выберите режим запуска задания и настройте время в соответствии с выбранной периодичностью:

Режим запуска	Параметры и описание
Завершающее	Задание будет запускаться при завершении работы Сервера. Запускается без дополнительных параметров.
Стартовое	Задание будет запускаться при запуске Сервера.

Режим запуска	Параметры и описание
	Запускается без дополнительных параметров.
Через N минут после исходного задания	Необходимо выбрать в выпадающем списке **Исходное задание** то задание, относительно которого устанавливается время выполнения текущего задания. В поле **Минута** задайте или выберите из предлагаемого списка количество минут, которое должно пройти после выполнения исходного задания, чтобы началось выполнение редактируемого задания.
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 N минут	Необходимо ввести значение **N** для задания временного интервала выполнения задания. При **N** равном `60` или больше задание будет запускаться каждые **N** минут. При **N** меньше `60` задание будет запускаться в каждую минуту часа, кратную **N**.

- Установите флаг **Запретить после первого выполнения** для однократного выполнения задания в соответствии с указанным временем. Если флаг снят, задание будет выполняться многократно с указанной периодичностью.

Чтобы повторить выполнение однократного задания, которое уже было выполнено, воспользуйтесь кнопкой **Запланировать повторно** на панели инструментов раздела расписания.

3. По окончании редактирования параметров задания нажмите кнопку **Сохранить** для принятия изменений в параметрах задания, если вы редактировали уже существующее задание, или для создания задания с заданными параметрами, если вы выполняли процедуру создания нового задания.

8.5. Настройка конфигурации веб-сервера

При каждом сохранении изменений раздела **Конфигурация веб-сервера** автоматически сохраняется резервная копия предыдущей версии конфигурационного файла веб-сервера. Хранению подлежат 10 последних копий.

Резервные копии располагаются в том же каталоге, что и сам конфигурационный файл, и называются в соответствии со следующим форматом:

`webmin.conf;<время_создания>`

Вы можете использовать созданные резервные копии, в частности, для восстановления конфигурационного файла в случае, если интерфейс Центра управления недоступен.

Чтобы настроить конфигурационные параметры веб-сервера:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация веб-сервера**. Откроется окно настроек веб-сервера.

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

3. На панели инструментов доступны следующие кнопки управления настройками раздела:

   Перезапустить Сервер Dr.Web – перезапустить Сервер для принятия изменений, внесенных в данном разделе. Кнопка становится активной после внесения изменений в настройки раздела и нажатия кнопки **Сохранить**.

   Восстановить конфигурацию из резервной копии – выпадающий список, содержащий сохраненные копии настроек всего раздела, к которым можно вернуться после внесения изменений. Кнопка становится активной после внесения изменений в настройки раздела и нажатия кнопки **Сохранить**.

   Установить все параметры в начальные значения – восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).

   Установить все параметры в значения по умолчанию – установить для всех параметров данного раздела значения, заданные по умолчанию.

4. Чтобы принять изменения, внесенные в настройки раздела, нажмите кнопку **Сохранить**, после чего потребуется перезагрузка Сервера. Для этого нажмите кнопку **Перезапустить Сервер Dr.Web** на панели инструментов данного раздела.

8.5.1. Общие

На вкладке **Общие** задаются следующие настройки работы веб-сервера:

- **Адрес Сервера Dr.Web** – IP-адрес или DNS-имя Сервера Dr.Web.

  Задается в формате:

  <IP-адрес или DNS-имя Сервера> [**:** *<порт>*]

  Если адрес Сервера не задан, то используется имя компьютера, возвращаемое операционной системой или сетевой адрес Сервера: DNS-имя, если доступно, в противном случае – IP-адрес.

Если номер порта не задан, используется порт, заданный в запросе (например, при обращении к Серверу из Центра управления или через **Web API**). В частности, при запросе из Центра управления – это порт, заданный в адресной строке при подключении Центра управления к Серверу.

Значение хранится в параметре `<server-name />` в конфигурационном файле `webmin.conf`.

Значение параметра используется также при формировании ссылки на скачивание файла инсталляции Агента для станций антивирусной сети.

- **Количество параллельных запросов** – количество параллельных запросов, обрабатываемых веб-сервером. Данный параметр влияет на производительность сервера. Не рекомендуется изменять его значение без необходимости.
- **Количество потоков ввода/вывода** – количество потоков, обрабатывающих данные, передаваемые по сети. Данный параметр влияет на производительность Сервера. Не рекомендуется изменять его значение без необходимости.
- **Тайм-аут (с)** – тайм-аут HTTP-сессии. При использовании постоянных соединений Сервер разрывает соединение, если в течение указанного времени от клиента не приходят запросы.
- **Минимальная скорость отправки (Б/с)** – минимальная скорость отправки данных. Если исходящая скорость передачи по сети ниже данного значения, в соединении будет отказано. Задайте значение 0, чтобы снять данное ограничение.
- **Минимальная скорость приема (Б/с)** – минимальная скорость получения данных. Если входящая скорость передачи по сети ниже данного значения, в соединении будет отказано. Задайте значение 0, чтобы снять данное ограничение.
- **Размер буфера отправки (КБ)** – размер буферов, используемых при отправке данных. Данный параметр влияет на производительность Сервера. Не рекомендуется изменять его значение без необходимости.
- **Размер буфера приема (КБ)** – размер буферов, используемых при получении данных. Данный параметр влияет на производительность Сервера. Не рекомендуется изменять его значение без необходимости.
- **Максимальная длина запроса (КБ)** – максимально допустимый размер HTTP-запроса.
- **Использовать сжатие** – установите флаг, чтобы использовать сжатие трафика при передаче данных по каналу связи с веб-сервером через HTTP/HTTPS.
  - Если флаг установлен, доступен выпадающий список **Уровень сжатия**. В этом списке вы можете выбрать уровень сжатия данных от 1 до 9, где 1 – минимальный уровень, а 9 – максимальный уровень сжатия.
- **Заменять IP-адреса** – установите флаг, чтобы заменять IP-адреса DNS-именами компьютеров в файле журнала Сервера.
- **Поддерживать SSL-сессию активной** – установите флаг, чтобы использовать постоянное соединение для SSL. Устаревшие версии браузеров могут некорректно работать с постоянными SSL-соединениями. Отключите этот параметр, если возникают проблемы с работой по SSL-протоколу.

- **SSL-сертификат** – путь к файлу SSL-сертификата. В выпадающем списке приводятся доступные сертификаты из каталога Сервера.
- **Закрытый ключ SSL** – путь к файлу закрытого ключа SSL. В выпадающем списке приводятся доступные закрытые ключи SSL из каталога Сервера.

8.5.2. Дополнительно

На вкладке **Дополнительно** задаются следующие настройки работы веб-сервера:

- Установите флаг **Отображать ошибки скриптов** чтобы показывать ошибки скриптов в веб-браузере. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.
- Установите флаг **Трассировать работу скриптов** чтобы включить трассировку работы скриптов. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.
- Установите флаг **Разрешать завершение скриптов** чтобы разрешить прерывание работы скриптов. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.

8.5.3. Транспорт

На вкладке **Транспорт** настраиваются "прослушиваемые" сетевые адреса, с которых веб-сервер принимает входящие соединения, например, для подключения Центра управления или выполнения запросов через Web API:

- В разделе **Адреса, прослушиваемые по HTTP** настраивается список интерфейсов, которые будут прослушиваться для приема соединений по протоколу HTTP:

  В полях **Адрес** и **Порт** необходимо указать соответственно IP-адрес и номер порта сетевого интерфейса, с которого разрешен прием соединений по протоколу HTTP.

  По умолчанию для "прослушивания" веб-сервером устанавливаются:

  - **Адрес**: `0.0.0.0` – использовать "все сетевые интерфейсы" для данной машины, на которой установлен веб-сервер.
  - **Порт**: `9080` – использовать стандартный порт `9080` для протокола HTTP.
- В разделе **Адреса, прослушиваемые по HTTPS** настраивается список интерфейсов, которые будут прослушиваться для приема соединений по протоколу HTTPS:

  В полях **Адрес** и **Порт** необходимо указать соответственно IP-адрес и номер порта сетевого интерфейса, с которого разрешен прием соединений по протоколу HTTPS.

  По умолчанию для "прослушивания" веб-сервером устанавливаются:

  - **Адрес**: `0.0.0.0` – использовать "все сетевые интерфейсы" для данной машины, на которой установлен веб-сервер.
  - **Порт**: `9081` – использовать стандартный порт `9081` для протокола HTTPS.

Для добавления нового поля адреса, нажмите кнопку  соответствующего раздела. Для удаления поля нажмите кнопку  напортив удаляемого поля.

8.5.4. Безопасность

На вкладке **Безопасность** задаются ограничения на сетевые адреса, с которых веб-сервер принимает HTTP и HTTPS запросы.

Для того чтобы настроить ограничения доступа для какого-либо типа соединения:

1. Для того чтобы разрешить доступ по HTTP или по HTTPS с определенных адресов, включите их в списки **HTTP: Разрешено** или **HTTPS: Разрешено** соответственно.
2. Для того чтобы запретить доступ по HTTP или по HTTPS с каких-либо адресов, включите их в списки **HTTP: Запрещено** или **HTTPS: Запрещено**.
3. Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлены ли флаги **Приоритетность запрета для HTTP** и **Приоритетность запрета для HTTPS**: при установленном флаге адреса, не включенные ни в один из списков (или включенные в оба), запрещаются. В противном случае, такие адреса разрешаются.

Для редактирования списка адресов:

1. Введите сетевой адрес в соответствующее поле и нажмите кнопку **Сохранить**.
2. Сетевой адрес задается в виде: *<IP-адрес>*/[*<префикс>*].

   Списки для ввода адресов TCPv6 будут отображены, только если на компьютере установлен интерфейс IPv6.

3. Для добавления нового поля адреса, нажмите кнопку  соответствующего раздела.
4. Для удаления поля нажмите кнопку  .

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.*.*.*`

8.6. Пользовательские процедуры

При выполнении lua-скриптов администратор получает доступ ко всей файловой системе в пределах каталога Сервера и некоторым системным командам на компьютере с установленным Сервером.

Чтобы запретить доступ к пользовательским процедурам, отключите право **Редактирование конфигурации Сервера и конфигурации репозитория** для соответствующего администратора (см. п. Администраторы и административные группы).

Для упрощения и автоматизации выполнения определенных заданий Сервера Dr.Web возможно использование пользовательских процедур, реализованных в виде lua-скриптов.

Пользовательские процедуры располагаются в следующем подкаталоге каталога установки Сервера:

- для ОС Windows: `var\extensions`
- для ОС FreeBSD: `/var/drwcs/extensions`
- для ОС Linux и ОС Solaris: `/var/opt/drwcs/extensions`

После инсталляции Сервера в данном подкаталоге размещаются предустановленные пользовательские процедуры.

Редактирование пользовательских процедур рекомендуется осуществлять через Центр управления.

Чтобы настроить выполнение пользовательских процедур:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Пользовательские процедуры**. Откроется окно настроек пользовательских процедур.

Дерево процедур

Иерархический список процедур отображает древовидную структуру, узлами которой являются группы процедур и входящие в них пользовательские процедуры.

Изначально в дереве процедур представлены следующие предустановленные группы:

- **Examples of the hooks** – содержит шаблоны всех доступных пользовательских процедур. На основе данных шаблонов вы можете создавать собственные пользовательские процедуры.
- **IBM Tivoli integration** – содержит шаблоны пользовательских процедур, используемых при интеграции с системой IBM Tivoli.

Значок элемента дерева зависит от типа или состояния этого элемента (см. таблицу 8-6).

Таблица 8-6. Значки элементов дерева процедур

Значок	Описание
Группы процедур	
	Группа процедур, для которой разрешено выполнение процедур.
	Группа процедур, для которой запрещено выполнение процедур.
Процедуры	
	Процедура, для которой разрешено выполнение.
	Процедура, для которой запрещено выполнение.

Управление деревом процедур

Для управления объектами в дереве процедур используются следующие элементы панели инструментов:

 – выпадающий список для добавления элемента дерева процедур:

 **Добавить процедуру** – добавить новую пользовательскую процедуру.

 **Добавить группу процедур** – создать новую пользовательскую группу для размещения в ней процедур.

 **Удалить отмеченные объекты** – удалить пользовательскую процедуру или группу, выбранную в дереве процедур.

 **Разрешить выполнение процедуры** – аналогичное действие производится из редактора процедур при помощи установки флага **Разрешить выполнение процедуры**. См. также Активация процедур.

 **Запретить выполнение процедуры** – аналогичное действие производится из редактора процедур при помощи снятия флага **Разрешить выполнение процедуры**. См. также Активация процедур.

Управление группами процедур

Чтобы создать новую группу:

1. На панели инструментов выберите  →  **Добавить группу процедур**.
2. В открывшемся окне задайте следующие параметры:
   - Установите флаг **Разрешить выполнение процедуры**, чтобы активировать процедуры, которые будут входить в эту группу. См. также Активация процедур.
   - В поле **Название группы** задайте произвольное название для создаваемой группы.
3. Нажмите кнопку **Сохранить**.

Чтобы изменить порядок использования групп:

1. В дереве процедур перетащите (drag and drop) группу процедур и разместите ее в нужном порядке относительно других групп.
2. Порядок использования процедур автоматически изменится при изменении порядка групп: первыми будут выполняться процедуры из групп, расположенных выше в дереве процедур.

Чтобы переместить процедуру в другую группу:

1. В дереве процедур выберите процедуру, которую вы хотите переместить.
2. На открывшейся панели свойств, в выпадающем списке **Родительская группа** выберите группу, в которую необходимо переместить процедуру.
3. Нажмите кнопку **Сохранить**.

Управление процедурами

Чтобы добавить новую процедуру:

1. На панели инструментов выберите → **Добавить процедуру**.
2. В открывшемся окне задайте следующие параметры:
   - Установите флаг **Разрешить выполнение процедуры**, чтобы активировать создаваемую процедуру. См. также Активация процедур.
   - В выпадающем списке **Родительская группа** выберите группу, в которой будет размещаться создаваемая процедура. В дальнейшем можно переместить процедуру в другую группу – см. выше.
   - В выпадающем списке **Процедура** выберите тип процедуры. Тип процедуры определяет действие, для которого будет вызываться данная процедура.
   - В поле **Текст процедуры** введите lua-скрипт, который будет выполняться при вызове данной процедуры.
     В подразделе **Информация о процедуре** приводится событие, для которого будет вызываться данная процедура; информация о том, доступна ли база данных Сервера для данной процедуры; а также приводятся списки входных параметров и возвращаемых значений для данного типа процедуры.
3. Нажмите кнопку **Сохранить**.

Чтобы отредактировать процедуру:

1. В дереве процедур выберите процедуру, которую вы хотите отредактировать.
2. В правой части окна автоматически откроется панель свойств данной процедуры. Для редактирования доступны все параметры, которые задавались при создании процедуры, кроме параметра **Процедура**. Данный параметр определяет событие, для которого бу-

дет вызываться данная процедура, и не подлежит редактированию после создания процедуры.

3. Нажмите кнопку **Сохранить**.

Активация процедур

Активация процедур и групп процедур определяет, будут ли выполняться процедуры при наступлении соответствующего им события или нет.

Чтобы активировать процедуру или группу процедур:

1. В дереве процедур выберите процедуру или группу, которую вы хотите активировать.
2. Выполните одно из следующих действий:
   - На панели инструментов нажмите кнопку **Разрешить выполнение процедуры**.
   - В правой части окна на панели свойств выбранного объекта установите флаг **Разрешить выполнение процедуры**, если он снят. Нажмите кнопку **Сохранить**.

Особенности активации процедур:

Для того чтобы процедура выполнялась при наступлении соответствующего ей события, необходимо следующее:

a) должна быть активирована сама процедура;

b) должна быть активирована группа, в которую входит данная процедура.

> Если группа процедур отключена, входящие в нее процедуры не будут выполняться, даже если сами они активированы.
>
> При активации группы будут выполняться только те процедуры, которые сами непосредственно активированы.

8.7. Настройка оповещений

Dr.Web Enterprise Security Suite поддерживает отправку оповещений о вирусных атаках, состояниях компонентов антивирусной сети и других событиях администраторам антивирусной сети Dr.Web Enterprise Security Suite.

8.7.1. Конфигурация оповещений

Для настройки оповещений о событиях в антивирусной сети:

1. Выберите пункт **Администрирование** главного меню Центра управления. В открывшемся окне выберите пункт управляющего меню **Конфигурация оповещений**.

2. При первоначальной настройке список оповещений пуст. Нажмите **Добавить уведомление**.
3. Чтобы включить отправку оповещений установите переключатель слева от заголовка блока оповещения в соответствующее положение:

    – отправка оповещений для данного блока включена.

    – оповещения данного блока отправляться не будут.
4. В данном разделе вы можете создать несколько блоков (профилей) оповещений, например, для различных способов отправки. Для добавления еще одного блока нажмите  справа от настроек блока оповещений. Внизу страницы будет добавлен еще один блок оповещений. Настройка различных блоков оповещений, как и текстов их шаблонов, осуществляется независимо.
5. В поле **Заголовок** задайте название добавленного блока оповещений. Это название будет использоваться, например, при настройке задания **Статистические отчеты** в расписании Сервера. В дальнейшем для редактирования заголовка нажмите на него левой кнопкой мыши и введите необходимое название. При наличии более чем одного блока оповещений, при нажатии на текст заголовка, будет предложен выпадающий список с заголовками существующих блоков оповещений.
6. Чтобы настроить рассылку оповещений, выберите необходимый тип отправки оповещения в выпадающем списке **Метод отправки оповещений**:
   - Веб-консоль – отправлять оповещения для просмотра в Веб-консоли.
   - Электронная почта – отправлять оповещения по электронной почте.
   - SNMP – отправлять оповещения через SNMP-протокол.
   - Push-оповещения – отправлять push-оповещения на Мобильный Центр управления безопасностью Dr.Web. Данный пункт будет доступен в выпадающем списке **Метод отправки оповещений** только после подключения Мобильного Центра управления безопасностью Dr.Web к данному Серверу Dr.Web.
   - Windows Message – отправлять оповещения, используя **Windows Messenger** (только для Серверов под ОС Windows).

   Описание настроек каждого из типов отправки оповещений приведено ниже в данном разделе.
7. Для отправки оповещений предоставляется предопределенный набор стандартных оповещений Сервера.

   Описание предопределенных оповещений и их параметров приведено в документе **Приложения**, в Приложение D1. Описание предопределенных оповещений.

   Чтобы настроить конкретные оповещения, необходимо:

   a) В списке оповещений установите флаги напротив тех оповещений, которые будут отправляться в соответствии с методом отправки текущего блока оповещений.

   b) Для изменения настроек оповещений нажмите ⚙ напротив редактируемого оповещения. Откроется шаблон оповещения. При необходимости отредактируйте текст отправляемого сообщения. В тексте оповещения можете использовать переменные ша-

блона (в фигурных скобках). Для добавления переменных предоставляются выпадающие списки в заголовке сообщения. При подготовке сообщения система оповещения заменяет переменные шаблона на конкретный текст, зависящий от ее текущих настроек. Список доступных переменных указан в документе **Приложения**, в Приложении D3. Параметры шаблонов системы оповещения.

c) Для оповещений по электронной почте предоставляется возможность добавить произвольные пользовательские поля в дополнительном разделе **Заголовки** в редакторе шаблона для каждого оповещения (см. п. **b)**). Заголовки должны формироваться в соответствии со стандартами RFC 822, RFC 2822 и не пересекаться с полями, определенными в стандартах для сообщений электронной почты. В частности, стандарт RFC 822 гарантирует отсутствие в спецификации заголовков, начинающихся с `X-`, поэтому рекомендуется задавать названия в формате `X-`<*название-заголовка*>. Например: `X-Template-Language: Russian`.

d) Для оповещений подраздела **Станция** вы также можете задать список станций, о событиях на которых будут отправляться оповещения. В окне редактирования шаблона, в дереве **Группы отслеживаемых станций** выберите группы станций, для которых будут отслеживаться события и отправляться соответствующие оповещения. Для выбора нескольких групп используйте кнопки CTRL или SHIFT.

> Для метода отправки **SNMP** тексты шаблонов оповещений задаются на стороне получателя (*управляющая станция* в терминах RFC 1067). Через Центр управления в подразделе **Станция** вы можете задать только список станций, о событиях на которых будут отправляться оповещения.

8. После окончания редактирования нажмите кнопку **Сохранить**, чтобы применить все внесенные изменения.

Оповещения, отображаемые в Веб-консоли

Для оповещений, отображаемых в Веб-консоли, задайте следующие параметры:

- **Количество повторных отправок** – количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию – 10.
- **Тайм-аут повторной отправки** – период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- **Время хранения оповещения** – время, в течение которого требуется хранить оповещение, начиная с момента его получения. По умолчанию 1 день. По истечении указанно срока оповещение помечается как устаревшее и удаляется согласно заданию **Удаление устаревших сообщений** в настройках расписания Сервера.

  Для оповещений, полученных данным методом отправки, вы можете задать неограниченный срок хранения в разделе Оповещения Веб-консоли.
- **Отправить тестовое сообщение** – отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.

Оповещения по электронной почте

Для оповещений по электронной почте задайте следующие параметры:

- **Количество повторных отправок** – количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию – 10.
- **Тайм-аут повторной отправки** – период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- **Электронная почта отправителя** – адрес электронной почты отправителя оповещений.
- **Электронная почта получателей** – адреса электронной почты получателей сообщения. В каждое поле вводится только один адрес электронной почты получателя. Для добавления еще одного поля получателя нажмите кнопку  . Для удаления поля нажмите кнопку  .
- В разделе **Настройки SMTP сервера** задайте следующие параметры:
  - **Адрес** – адрес SMTP-сервера, который будет использоваться для отправки электронной почты.
  - **Порт** – порт для подключения к SMTP-серверу. По умолчанию порт 465 при открытии отдельного защищенного TLS-соединения или порт 25 в противном случае.
  - **Пользователь**, **Пароль** – при необходимости задайте имя пользователя и пароль пользователя SMTP-сервера, если SMTP-сервер требует авторизации.
  - Установите флаг **STARTTLS шифрование** для шифрованного обмена данными. При этом переключение на защищенное соединение осуществляется через команду `STARTTLS`. По умолчанию для соединения предусматривается использование 25 порта.
  - Установите флаг **SSL шифрование** для шифрованного обмена данными. При этом будет открыто отдельное защищенное TLS-соединение. По умолчанию для соединения предусматривается использование 465 порта.
  - Установите флаг **Использовать CRAM-MD5 аутентификацию** для использования *CRAM-MD5* аутентификации на почтовом сервере.
  - Установите флаг **Использовать DIGEST-MD5 аутентификацию** для использования *DIGEST-MD5* аутентификации на почтовом сервере.
  - Установите флаг **Использовать обычную аутентификацию** для использования *plain text* аутентификации на почтовом сервере.
  - Установите флаг **Использовать LOGIN аутентификацию** для использования *LOGIN* аутентификации на почтовом сервере.
  - Установите флаг **Проверять правильность SSL сертификата сервера** чтобы проверять правильность *SSL*-сертификата почтового сервера.
  - Установите флаг **Отладочный режим** для получения детального журнала SMTP-сессии.

- **Отправить тестовое сообщение** – отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.

Оповещения через SNMP протокол

Для оповещений через SNMP-протокол задайте следующие параметры:

- **Количество повторных отправок** – количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию – 10.
- **Тайм-аут повторной отправки** – период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- **Получатель** – сущность, принимающая SNMP-запрос. Например, IP-адрес или DNS-имя компьютера. В каждое поле вводится только один получатель. Для добавления еще одного поля получателя нажмите кнопку  . Для удаления поля нажмите кнопку  .
- **Отправитель** – сущность, отправляющая SNMP-запрос. Например, IP-адрес или DNS-имя компьютера (должно распознаваться DNS-сервером).

  Если отправитель не задан, по умолчанию используется `"localhost"` для ОС Windows и `"."` для ОС семейства UNIX.
- **Общность** – SNMP-общность или контекст. По умолчанию `public`.
- **Отправить тестовое сообщение** – отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.

Push-оповещения

Для Push-оповещений, отправляемых на Мобильный центр управления, задайте следующие параметры:

- **Количество повторных отправок** – количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию – 10.
- **Тайм-аут повторной отправки** – период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- **Отправить тестовое сообщение** – отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.

Оповещения 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 следующие параметры:

- **Количество повторных отправок** – количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию – 10.
- **Тайм-аут повторной отправки** – период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- **Получатель** – список имен компьютеров получателей сообщений. В каждое поле вводится только одно имя компьютера. Для добавления еще одного поля получателя нажмите кнопку  Для удаления поля нажмите кнопку  .
- **Отправить тестовое сообщение** – отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.

8.7.2. Оповещения веб-консоли

Через Центр управления вы можете просматривать и управлять оповещениями администратора, полученными методом **Веб-консоль** (отправка оповещений администратора описана в разделе Конфигурация оповещений).

Для просмотра и управления оповещениями:

1. Выберите пункт **Администрирование** главного меню Центра управления. В открывшемся окне выберите пункт управляющего меню **Оповещения веб-консоли**. Откроется список оповещений, отправленных на Веб-консоль.
2. Для просмотра оповещения нажмите на соответствующую строку таблицы. Откроется окно с текстом оповещения. При этом оповещение будет автоматически помечено как прочитанное.
3. Для управления списком оповещений используйте следующие элементы:
   a) Общие элементы панели инструментов служат для управления разделом оповещений в целом. Данные инструменты всегда доступны на панели инструментов:

Настройка		Действие
Серьезность	**Максимальная**	Отображать только оповещения с серьезностью **Максимальная**
	Высокая	Отображать оповещения с серьезностью от **Высокой** до **Максимальной**
	Средняя	Отображать оповещения с серьезностью от **Средней** до **Максимальной**
	Низкая	Отображать оповещения с серьезностью от **Низкой** до **Максимальной**

Настройка		Действие
	Минимальная	Отображать все оповещения с серьезностью от **Минимальной** до **Максимальной**
Источник	**Агент**	Отображать оповещения, связанные с событиями на станциях
	Сервер	Отображать оповещения, связанные с событиями на Сервере

Для отображения оповещений, полученных в течение определенного временного промежутка, воспользуйтесь одним из следующих способов:

- Выберите в выпадающем списке на панели инструментов один из предопределенных временных промежутков.
- Выберите в выпадающих календарях произвольные даты начала и окончания временного промежутка.

После изменения значений данных настроек нажмите кнопку **Обновить** для отображения списка оповещений в соответствии с заданными настройками.

b) Для управления отдельными оповещениями установите флаги напротив нужных оповещений или общий флаг в заголовке таблицы для выбора всех оповещений в списке. При этом станут доступны элементы панели инструментов для управления выбранными оповещениями:

   Удалить оповещения – удалить все выбранные оповещения без возможности восстановления.

   Пометить оповещения как прочитанные – отметить все выбранные оповещения как прочитанные.

c) Установите значок **Хранить сообщение без автоматического удаления** в списке оповещений напротив тех оповещений, которые не должны быть удалены по истечении срока хранения (срок хранения задается перед отправкой оповещений в разделе Конфигурация оповещений в настройках метода отправки **Веб-консоль**). Такие оповещения будут храниться до тех пор, пока вы не удалите их вручную в разделе **Оповещения веб-консоли** или не снимите значок напротив этих оповещений.

8.7.3. Неотправленные оповещения

Через Центр управления вы можете отслеживать и управлять оповещениями администратора, которые не удалось отправить согласно настройкам раздела Конфигурация оповещений.

Для просмотра и управления неотправленными оповещениями:

1. Выберите пункт **Администрирование** главного меню Центра управления. В открывшемся окне выберите пункт управляющего меню **Неотправленные оповещения**. Откроется список неотправленных оповещений данного Сервера.

2. В список неотправленных оповещения помещаются оповещения, которые не удалось отправить адресатам, но количество попыток повторной отправки, заданное в настройках этого оповещения, еще не истекло.
3. Таблица неоправленных оповещений содержит следующую информацию:
   - **Оповещение** – название оповещения из списка предустановленных оповещений.
   - **Заголовок** – название блока оповещений, согласно настройкам которого осуществляется отправка данного оповещения.
   - **Осталось отправок** – количество оставшихся повторных попыток, предпринимаемых при неудачной отправке оповещения. Изначальное количество попыток повторной отправки задается при настройке оповещений в разделе Конфигурация оповещений. После отправки оповещения возможность изменить количество попыток повторных отправок для данного оповещения не предоставляется.
   - **Время следующей отправки** – дата и время следующей попытки повторной отправки оповещения. Периодичность, с которой будут осуществляться попытки повторной отправки оповещения, задается при настройке оповещений в разделе Конфигурация оповещений. После отправки оповещения возможность изменить периодичность повторных попыток отправки для данного оповещения не предоставляется.
   - **Получатель** – адреса получателей оповещения.
   - **Ошибка** – ошибка, из-за которой не удалось отправить оповещение.
4. Для управления неотправленными оповещениями:
   a) Установите флаги напротив конкретных оповещений или флаг в заголовке таблицы оповещений, чтобы выбрать все оповещения в списке.
   b) Используйте следующие кнопки на панели инструментов:

      Отправить повторно – отправить выбранные оповещения немедленно. При этом будет осуществлена внеочередная попытка отправки оповещения. В случае неудачной отправки количество оставшихся попыток уменьшится на единицу, и время следующей попытки будет отсчитываться от момента текущей отправки с периодичностью, заданной в разделе Конфигурация оповещений.

      Удалить – удалить все выбранные неотправленные оповещения без возможности восстановления.
5. Неотправленные оповещения удаляются из списка в следующих случаях:
   a) Оповещение было удачно отправлено адресату.
   b) Оповещение было удалено администратором вручную при помощи кнопки **Удалить** на панели инструментов.
   c) Количество попыток повторной отправки закончилось, и оповещение не было отправлено.
   d) В разделе Конфигурация оповещений удален блок оповещений, согласно настройкам которого отправлялись данные оповещения.

8.8. Управление репозиторием Сервера Dr.Web

Репозиторий Сервера Dr.Web 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:

a) на Сервер Dr.Web с сайта обновления продукта (по протоколу HTTP),

b) между различными Серверами Dr.Web в многосерверной конфигурации (в соответствии с заданной политикой обмена),

c) с Сервера Dr.Web 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:

- Сервер Dr.Web,
- Агенты Dr.Web (ПО Агента, антивирусное ПО рабочей станции для соответствующих операционных систем),
- Прокси-сервер Dr.Web,
- Вирусные базы Dr.Web,
- Базы SplDer Gate,

- Базы Антиспама Dr.Web,
- Новости компании «Доктор Веб».

8.8.1. Состояние репозитория

Чтобы проверить текущее состояние репозитория или обновить компоненты антивирусной сети:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**.
2. В открывшемся окне приведен список продуктов репозитория, дата используемой в данный момент ревизии, дата последней загруженной ревизии и состояние продуктов.

   В столбце **Состояние** указано состояние продуктов в репозитории Сервера на момент последнего обновления.

3. Для управления содержимым репозитория используйте следующие кнопки:
   - Нажмите кнопку **Проверить обновления** для проверки наличия обновлений всех продуктов на ВСО и загрузки имеющихся обновлений с серверов ВСО.
   - Нажмите кнопку **Перезагрузить репозиторий с диска**, чтобы произвести перезагрузку текущей версии репозитория с диска.

   При запуске Сервер загружает содержимое репозитория в память, и если в процессе работы Сервера содержимое репозитория было изменено администратором в обход Центра управления, например, при обновлении содержимого репозитория при помощи внешней утилиты или вручную, для использования загруженной на диск версии репозитория необходимо осуществить его перезагрузку.

8.8.2. Отложенные обновления

В разделе **Отложенные обновления** приведен список продуктов, для которых были временно запрещены обновления продуктов в разделе **Детальная конфигурация репозитория** → *<Продукт>* → Отложенные обновления. Отложенная ревизия считается *замороженной*.

Таблица замороженных продуктов содержит следующую информацию:

- **Каталог в репозитории** – название каталога замороженного продукта в репозитории:
  - 10-drwgatedb – базы SplDer Gate,
  - 10-drwspamdb – базы AntiSpam,
  - 20-drwagent – Агент Dr.Web для Windows,
  - 20-drwandroid – Агент Dr.Web для Android,
  - 20-drwcs – Сервер Dr.Web,
  - 20-drwunix – Агент Dr.Web для UNIX,

- 80-drwnews – новости компании «Доктор Веб».

- **Ревизия** – номер замороженной ревизии.
- **Отложено до** – время, до которого были отложены обновления данного продукта.

При нажатии на строку таблицы замороженных продуктов открывается таблица с подробной информации о замороженной ревизии данного продукта.

Функционал отложенных обновлений может использоваться, если необходимо временно отменить распространение последней ревизии продукта на все станции антивирусной сети, например, при необходимости предварительного тестирования данной ревизии на ограниченном количестве станций.

Чтобы использовать функционал отложенных обновлений, выполните действия, описанные в разделе **Детальная конфигурация репозитория** → Отложенные обновления.

Для управления отложенными обновлениями:

1. Установите флаг напротив тех продуктов, для которых вы хотите задать действие над отложенными обновлениями. Для выбора всех продуктов установите флаг в заголовке таблицы замороженных продуктов.
2. На панели инструментов выберите необходимое действие:

   Выполнить немедленно – снять заморозку продукта и включить данную ревизию в список ревизий с распространением на станции по общей процедуре.

   Отменить обновление – снять заморозку продукта и запретить данную ревизию. Процесс получения обновлений с ВСО будет восстановлен. Размороженная ревизия будет удалена из списка ревизий продукта. При приходе следующей ревизии, размороженная ревизия будет также удалена с диска.

   Изменить время задержки обновлений – задать время, на которое ревизия данного продукта откладывается. Начало времени заморозки считается с момента получения ревизии с ВСО.
3. Если над замороженным продуктом не было задано действие по его разморозке, то по истечении времени, заданном в списке **Время задержки обновлений**, ревизия будет автоматически разморожена и включена в список ревизий с распространением на станции по общей процедуре.

8.8.3. Общая конфигурация репозитория

Раздел **Общая конфигурация репозитория** позволяет задать параметры подключения к ВСО и обновления репозитория для всех продуктов.

Чтобы отредактировать конфигурацию репозитория:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Общая конфигурация репозитория**.

3. Настройте все необходимые параметры обновлений с ВСО, описанные ниже.
4. Если в процессе редактирования параметров необходимо отменить все внесенные изменения, используйте следующие кнопки на панели инструментов:

   Установить все параметры в начальные значения – сбросить значения всех параметров данного раздела в значения, которые они имели до текущего редактирования. Для аналогичного действия над отдельными параметрами используйте кнопки напротив каждого параметра.

   Установить все параметры в значения по умолчанию – сбросить значения всех параметров данного раздела в значения, сохраненные в конфигурационном файле Сервера. Для аналогичного действия над отдельными параметрами используйте кнопки напротив каждого параметра.
5. Нажмите одну из кнопок на панели инструментов:
   - **Сохранить и повторно синхронизировать** – сохранить все внесенные изменения и осуществить обновление репозитория с ВСО согласно новым настройкам.
   - **Сохранить и перезагрузить с диска** – сохранить все внесенные изменения без обновления репозитория с ВСО. При этом осуществляется перезагрузка текущей версии репозитория с диска (см. также раздел Состояние репозитория).

Настройка ВСО Dr.Web

На вкладке **ВСО Dr.Web** осуществляется настройка параметров подключения к Всемирной системе обновлений Dr.Web.

Для редактирования подключения к ВСО используются следующие настройки:

- **Базовый URI** – каталог на серверах обновлений, содержащий обновления продуктов Dr.Web.
- Установите флаг **Использовать CDN**, чтобы разрешить использование Content Delivery Network при загрузке репозитория.
- Установите флаг **Использовать SSL**, чтобы осуществлять загрузку репозитория через защищенное SSL-соединение.

  При этом в выпадающем списке **Допустимые сертификаты** выберите тип SSL-сертификатов, которые будут автоматически приниматься.
- При необходимости отредактируйте список серверов ВСО, с которых осуществляется обновление репозитория, в секции **Список серверов Всемирной системы обновления Dr.Web**:
  - Чтобы добавить сервер ВСО в список серверов, используемых для обновления, нажмите кнопку и введите адрес сервера ВСО в добавленное поле.
  - Чтобы удалить сервер ВСО из списка используемых, нажмите кнопку напротив сервера, который необходимо удалить.

- Порядок серверов ВСО в списке определяет порядок обращения Сервера Dr.Web при обновлении репозитория. Для изменения порядка серверов ВСО, перетащите требуемый сервер, захватив строку сервера за корешок слева.

При установке Сервера Dr.Web в список входят только серверы обновлений компании «Доктор Веб». При необходимости вы можете настроить собственные зоны обновлений и внести их в список серверов для получения обновлений.

Настройка обновлений Агента Dr.Web

Конфигурация обновления репозитория для ПО Агента и антивирусного пакета настраивается отдельно для различных версий ОС, на которые будет устанавливаться данное ПО:

- На вкладке **Агент Dr.Web 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 **Агент Dr.Web для UNIX** укажите, для каких ОС семейства UNIX требуется обновление компонентов, устанавливаемых на рабочие станции.

Чтобы полностью отключить получение обновлений с ВСО для Агента для UNIX, перейдите в раздел **Детальная конфигурация репозитория**, пункт **Агент Dr.Web для UNIX**, и на вкладке **Синхронизация** установите флаг **Отключить обновление продукта**.

Настройка обновлений Сервера Dr.Web

На вкладке **Сервер Dr.Web** укажите, для каких ОС будет осуществляться обновление файлов Сервера:

- Чтобы получать обновления для Серверов под всеми поддерживаемыми ОС, установите флаг **Обновлять все платформы, доступные на ВСО**.
- Чтобы получать обновления для Сервера только под некоторыми из поддерживаемых ОС, установите флаги только напротив этих ОС.

Чтобы полностью отключить получение обновлений с ВСО для Сервера, перейдите в раздел **Детальная конфигурация репозитория**, пункт **Сервер Dr.Web**, и на вкладке **Синхронизация** установите флаг **Отключить обновление продукта**.

Новости компании «Доктор Веб»

На вкладке **Новости компании «Доктор Веб»** задайте список языков, на которых будет скачиваться новостная лента.

Настройка подписки на разделы новостей осуществляется в разделе Настройки → **Подписка**.

С новостями компании «Доктор Веб» вы можете ознакомиться в разделе главного меню Центра управления **Помощь** → **Новости**.

Языки Агента Dr.Web для Windows

На вкладке **Языки Агента Dr.Web для Windows** задайте список языков интерфейса Агента и антивирусного пакета для ОС Windows, которые будут скачиваться с ВСО.

8.8.4. Детальная конфигурация репозитория

Раздел **Детальная конфигурация репозитория** позволяет настроить конфигурацию ревизий для каждого продукта репозитория в отдельности.

Чтобы отредактировать конфигурацию репозитория:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите в подразделе управляющего меню **Детальная конфигурация репозитория** пункт, соответствующий продукту, который вы хотите отредактировать.
3. Настройте все необходимые параметры репозитория выбранного продукта, описанные ниже.
4. Нажмите кнопку на панели инструментов **Сохранить и перезагрузить с диска**, чтобы сохранить все внесенные изменения. При этом осуществляется перезагрузка текущей версии репозитория с диска (см. также раздел Состояние репозитория).

Список ревизий

На вкладке **Список ревизий** приведена информация обо всех ревизиях данного продукта, доступных на данном Сервере.

Таблица ревизий содержит следующие столбцы:

Название столбца	Описание содержимого
Распространяемая	Автоматический маркер в данном столбце определяет состояние ревизий продукта. В столбце могут стоят два типа маркеров: ✔ – *Распространяемая ревизия*. Ревизия используется для обновлений Агентов и антивирусного ПО на станциях. Ревизия для распространения выбирается следующим образом: 1. Распространяется ревизия, отмеченная маркером ✔ в столбце **Текущая**. Отмечена может быть только одна ревизия. Для продукта **Агент Dr.Web для Windows** от-

Название столбца	Описание содержимого
	сутствует возможность установить маркер на ревизии, полученной ранее, чем распространяемая в данный момент ревизия. 2. Если в столбце **Текущая** ревизия не отмечена, распространяется последняя ревизия, отмеченная маркером в столбце **Хранимая**. 3. Если в столбцах **Текущая** и **Хранимая** не отмечена ни одна ревизия, распространяется самая последняя ревизия. Автоматический маркер всегда указывает на распространяемую ревизию. – *Замороженная ревизия*. Данная ревизия не распространяется на станции, новые ревизии не скачиваются с Сервера. О действиях при заморозке ревизии см. подраздел Отложенные обновления. При наличии замороженной ревизии, ревизия для распространения выбирается следующим образом: 1. Если маркер в столбце **Текущая** установлен, станциям раздается текущая ревизия. 2. Если маркер в столбце **Текущая** не установлен, станциям раздается ревизия, предшествующая замороженной.
Текущая	Установите маркер, чтобы задать ревизию продукта, которая будет использоваться для обновлений Агентов и антивирусного ПО на станциях. Может быть установлена только одна текущая ревизия. Также маркер, задающий текущую ревизию, может быть не установлен.
Хранимая	Установите маркер, чтобы сохранять данную ревизию при автоматической очистке репозитория. Маркер может быть установлен для нескольких ревизий одновременно. Также ни один маркер может быть не установлен. Сервер хранит на диске определенное количество ревизий продукта, задаваемое на вкладке **Синхронизация**. При достижении максимально допустимого количества временно хранимых ревизий, для сохранения новой скачанной с ВСО ревизии, самая старая временно хранимая ревизия удаляется. При автоматической очистке репозитория не удаляются следующие ревизии: • Ревизии, отмеченные маркером в столбце **Хранимая**. • Ревизия, отмеченная маркером в столбце **Текущая**. Если ревизия продукта работает стабильно, ее можно отметить как хранимую, и в случае, если с ВСО придет нестабильная ревизия, можно откатится на предыдущую.
Ревизия	Дата получения ревизии продукта.

Название столбца	Описание содержимого
	Если ревизия заморожена, в данном столбце дополнительно выводится статус блокировки.

Синхронизация

На вкладке **Синхронизация** настраиваются параметры обновления репозитория Сервера с ВСО:

- В выпадающем списке **Количество хранимых ревизий** задается количество ревизий продукта, временно хранимых на диске, не считая ревизий, отмеченных хотя бы в одном из столбцов на вкладке **Список ревизий**. В случае если пришла новая ревизия, а количество ревизий продукта уже достигло заданного значения, то удаляется самая старая ревизия. Ревизии, помеченные как **Текущая**, **Хранимая** и **Распространяемая** не подлежат удалению.
- Установите флаг **Отключить обновление продукта**, чтобы отключить получение обновлений данного продукта с серверов ВСО. Агенты при этом будут обновляться до текущей ревизии на Сервере (или согласно процедуре выбора распространяемой ревизии).

Для некоторых продуктов также доступны следующие настройки:

- Установите флаг **Обновлять только следующие файлы**, чтобы получать обновления с ВСО только указанных ниже файлов.
- Установите флаг **Не обновлять только следующие файлы**, чтобы отключить обновление с ВСО только указанных ниже файлов.

  Списки файлов задаются в формате регулярных выражений.

  Если установлены оба флага, то выборка файлов осуществляется следующим образом:

  1. Из полного списка файлов продукта выбираются файлы по спискам **Обновлять только следующие файлы**.
  2. Из списка, полученного на шаге 1, удаляются файлы по спискам **Не обновлять только следующие файлы**.
  3. С ВСО обновляются только файлы, полученные в результате выборки на шаге 2.

Оповещения

На вкладке **Оповещения** настраиваются оповещения об обновлениях репозитория:

- Установите флаг **Не оповещать только о следующих файлах**, чтобы отключить отправку уведомлений только на события, связанные с файлами, которые заданы в списке ниже.
- Установите флаг **Оповещать только о следующих файлах**, чтобы отправлять уведомления только на события, связанные с файлами, которые заданы в списке ниже.

  Списки файлов задаются в формате регулярных выражений.

Если списки исключений не заданы, то будут отправляться все оповещения, включенные на странице Конфигурация оповещений.

Параметры оповещений об обновлениях репозитория настраиваются на странице конфигурации оповещений в подразделе **Репозиторий**.

Отложенные обновления

На вкладке **Отложенные обновления** вы можете отложить распространение обновлений на станции на определенный срок. Отложенная ревизия считается замороженной.

Данный функционал может использоваться, если необходимо временно отменить распространение последней ревизии продукта на все станции антивирусной сети, например, при необходимости предварительного тестирования данной ревизии на ограниченном количестве станций.

Чтобы использовать функционал отложенных обновлений, выполните следующие действия:

1. Для продукта, который необходимо заморозить, настройте отложенные обновления как описано ниже.
2. Чтобы отменить распространение последней ревизии, установите в качестве текущей ревизии одну из предыдущих ревизий на вкладке Список ревизий.
3. Для группы станций, на которые будет распространяться последняя ревизия, установите флаг **Получать все последние обновления** в разделе **Антивирусная сеть** → Ограничение обновлений рабочих станций. На остальные станции будет распространяться ревизия, которую вы отметили в качестве текущей на шаге 2.
4. Следующая загруженная с ВСО ревизия, которая удовлетворяет условиям опции **Отложить обновления только следующих файлов**, будет заморожена и отложена на срок, выбранный в списке **Время задержки обновлений**.

Чтобы настроить отложенные обновления:

1. Установите флаг **Отложить обновления**, чтобы временно отменить загрузку обновлений данного продукта, получаемых с серверов ВСО.
2. В выпадающем списке **Время задержки обновлений** выберите время, на которое откладывается загрузка обновлений, начиная с момента их получения с серверов ВСО.
3. При необходимости установите флаг **Отложить обновления только следующих файлов**, чтобы отложить распространение обновлений, содержащих файлы, которые соответствуют маскам, заданным в списке ниже. Список масок задается в формате регулярных выражений.

   Если флаг не установлен, будут заморожены все обновления, приходящие с ВСО.

Чтобы снять заморозку:

- На вкладке **Список ревизий** нажмите **Выполнить немедленно**, чтобы снять заморозку продукта и включить данную ревизию в список ревизий с распространением на станции по общей процедуре.
- На вкладке **Список ревизий** нажмите **Отменить обновление**, чтобы снять заморозку продукта и запретить данную ревизию. Процесс получения обновлений с ВСО будет восстановлен. Размороженная ревизия будет удалена из списка ревизий продукта. При приходе следующей ревизии, размороженная ревизия будет также удалена с диска.
- По истечении времени, заданном в списке **Время задержки обновлений**, ревизия будет автоматически разморожена и включена в список ревизий с распространением на станции по общей процедуре.

Управление замороженными ревизиями для всех продуктов осуществляется в разделе Отложенные обновления.

8.8.5. Содержимое репозитория

Раздел **Содержимое репозитория** позволяет просматривать и управлять текущим содержимым репозитория на уровне каталогов и файлов репозитория.

Главное окно раздела **Содержимое репозитория** содержит иерархическое дерево содержимого репозитория, отражающее все каталоги и файлы в текущей версии репозитория со списком всех имеющихся ревизий каждого продукта.

Просмотр информации о репозитории

Чтобы просмотреть информацию об объектах репозитория, в иерархическом дереве содержимого репозитория выберите объект. Откроется панель свойств со следующей информацией:

- В подразделе **Выбранные объекты** приведена подробная информация об объекте, выбранном в дереве содержимого репозитория: **Тип**, **Размер** (только для отдельных файлов), **Дата создания** и **Дата изменения**.
- В подразделе **Состояние репозитория** приведена общая информация обо всех объектах репозитория: текущий список объектов и дата их последнего обновления.

Управление репозиторием

Для управления содержимым репозитория используйте следующие кнопки на панели инструментов:

Экспортировать файлы репозитория в архив,

Импортировать архив с файлами репозитория,

Удалить выбранные объекты – удалить объекты, выбранные в дереве содержимого репозитория, без возможности восстановления.

> После изменения содержимого репозитория, например, при удалении или импорте объектов репозитория, для использования Сервером измененных данных необходимо перезагрузить репозиторий.
>
> См. раздел Состояние репозитория.

Экспорт репозитория

Чтобы сохранить файлы репозитория в zip-архив, выполните следующие действия:

1. В иерархическом дереве содержимого репозитория выберите продукт, отдельную ревизию продукта или весь репозиторий. Весь репозиторий будет экспортирован, если ничего не выбрано в дереве или выбран заголовок дерева – **Репозиторий**. Для выбора нескольких объектов используйте кнопки CTRL или SHIFT.

   При экспорте объектов репозитория обратите внимание на основные типы экспортируемых объектов:

   a) Zip-архивы продуктов репозитория. Такие архивы содержат один из следующих типов объектов репозитория:

   - Весь репозиторий целиком.
   - Весь продукт целиком.
   - Вся отдельная ревизия продукта целиком.

   Архивы, полученные при экспорте данных объектов, могут быть импортированы через раздел **Содержимое репозитория**. Название таких архивов содержит префикс `repository_`.

   b) Zip-архивы отдельных файлов репозитория.

   Архивы, полученные при экспорте отдельных файлов и каталогов, находящиеся в иерархическом дереве ниже объектов из п. **a)**, не подлежат импорту через раздел **Содержимое репозитория**. Название таких архивов включает префикс `files_`.

   Такие архивы могут использоваться в качестве резервных копий файлов для ручной замены. Однако, не рекомендуется осуществлять замену файлов репозитория вручную, в обход раздела **Содержимое репозитория**.
2. Нажмите кнопку **Экспортировать файлы репозитория в архив** на панели инструментов.
3. Задание пути для сохранения zip-архива с выбранным объектом репозитория осуществляется в соответствии с настройками веб-браузера, в котором открыт Центр управления.

Импорт репозитория

Чтобы загрузить файлы репозитория из zip-архива, выполните следующие действия:

1. Нажмите кнопку **Импортировать архив с файлами репозитория** на панели инструментов.
2. В открывшемся окне в разделе **Выбор файла** задайте zip-архив с файлами репозитория. Для выбора файла можете воспользоваться кнопкой .

   Импорту подлежат только zip-архивы, которые были получены при экспорте одного из следующих типов объектов репозитория:

   - Весь репозиторий целиком.
   - Весь продукт целиком.
   - Вся отдельная ревизия продукта целиком.

   Название таких архивов при экспорте содержит префикс `repository_`.
3. В разделе **Настройки импорта** задайте следующие параметры:
   - **Только добавить отсутствующие ревизии** – в данном режиме импорта осуществляется только добавление тех ревизий репозитория, которые отсутствуют в текущей версии. Остальные ревизии остаются без изменений.
   - **Заменить весь репозиторий** – в данном режиме импорта осуществляется полная замена текущего репозитория на импортируемый.
   - Установите флаг **Импортировать конфигурационные файлы**, чтобы при импорте репозитория также импортировать конфигурационные файлы.
4. Нажмите кнопку **Импортировать** для начала процесса импорта.

8.9. Дополнительные возможности

8.9.1. Управление базой данных

Раздел **Управление базой данных** позволяет осуществлять непосредственное обслуживание базы данных, с которой работает Сервер Dr.Web.

Секция **Общие** содержит следующие параметры:

- Поле **Последнее обслуживание БД** – дата последнего запуска команд обслуживания базы данных из этого раздела.
- Список команд для обслуживания базы данных, включающий:
  - Команды, аналогичные заданиям из расписания Сервера Dr.Web. Названия команд соответствуют названиям заданий из раздела **Действия** в расписании Сервера (описание соответствующих заданий расписания приведено в таблице Типы заданий и их параметры).

- Команда **Анализ базы данных**. Предназначена для оптимизации базы данных Сервера посредством выполнения команды `analyze`.

Для выполнения команд обслуживания базы данных:

1. В списке команд установите флаги для тех команд, которые вы хотите выполнить.

   При необходимости, измените временные периоды для команд очистки базы данных, по прошествии которых хранимая информация признается устаревшей и подлежит удалению с Сервера.
2. Нажмите кнопку **Применить сейчас**. Все выбранные команды будут выполнены незамедлительно.

   Для отсроченного и/или периодического автоматического выполнения данных команд (кроме команды **Анализ базы данных**) воспользуйтесь Планировщиком заданий Сервера.

Для управления базой данных используйте следующие кнопки на панели инструментов:

 Импорт,

 Экспорт,

 Резервное копирование.

Экспорт базы данных

Чтобы сохранить информацию из базы данных в файл, выполните следующие действия:

1. Нажмите кнопку  **Экспорт** на панели инструментов.
2. В окне настроек экспорта выберите один из вариантов:
   - **Экспортировать всю базу данных** для сохранения всей информации из базы данных в gz-архив. XML-файл, полученный при экспорте, аналогичен файлу экспорта базы данных, получаемому при запуске исполняемого файла Сервера из командной строки с ключом `xmlexportdb`. Данный файл экспорта может быть импортирован при запуске исполняемого файла Сервера из командной строки с ключом `xmlimportdb`.
     Подробное описание данных команд приведено в документе **Приложения**, в разделе Н4.3. Команды для управления базой данных.
   - **Экспортировать информацию о станциях и группах** для сохранения информации об объектах антивирусной сети в zip-архив. В результате выполнения данной операции в файл специального формата сохраняется все информация о группах станций и самих учетных записях станций антивирусной сети, обслуживаемой данным Сервером. Файл экспорта включает следующую информацию о станциях: свойства, конфигурацию компонентов, права, настройки ограничений обновлений, расписание, список устанавливаемых компонентов, статистику, информацию об удаленных станциях; о группах: свойства, конфигурацию компонентов, права, настройки ограничений обновлений, расписание, список устанавливаемых компонентов, идентификатор родительской группы.

В дальнейшем файл экспорта может быть импортирован через раздел **Управление базой данных**.

3. Нажмите кнопку **Экспортировать**.
4. Задание пути для сохранения архива с базой данных осуществляется в соответствии с настройками веб-браузера, в котором открыт Центр управления.

Импорт базы данных

Процедура импорта файла базы данных, содержащего информацию об объектах антивирусной сети, может использоваться для переноса информации как на новый Сервер, так и на Сервер, уже функционирующий в составе антивирусной сети, в частности для объединения списков обслуживаемых станций двух Серверов.

К Серверу, на котором осуществляется импорт, смогут подключаться все станции, информация о которых импортируется. При осуществлении импорта обратите внимание на необходимость соответствующего количества доступных лицензий для подключения перенесенных станций. Например, при необходимости, в разделе Менеджер лицензий добавьте лицензионный ключ с Сервера, с которого переносилась информация о станциях.

Чтобы загрузить базу данных из файла, выполните следующие действия:

1. Нажмите кнопку  **Импорт** на панели инструментов.
2. В окне импорта задайте zip-архив с файлом базы данных. Для выбора файла можете воспользоваться кнопкой  .

   Импорту подлежат только zip-архивы, которые были получены при экспорте базы данных для варианта **Экспортировать информацию о станциях и группах**.
3. Нажмите кнопку **Импортировать** для начала процесса импорта.
4. Если при импорте будут обнаружены станции и/или группы с одинаковыми идентификаторами, которые входят как в импортируемые данные, так и в базу данных текущего Сервера, откроется раздел **Коллизии** для задания действий над продублированными объектами.

   Списки групп и станций приводятся в отдельных таблицах.

   Для соответствующей таблицы объектов в выпадающем списке **Режим импорта групп** или **Режим импорта станций** выберите вариант разрешения коллизии:

   - **Сохранить данные импорта для всех** – удалить всю информацию о дублированных объектах из базы данных текущего Сервера и перезаписать ее информацией из импортируемой базы данных. Действие применяется одновременно для всех дублированных объектов в данной таблице.
   - **Сохранить текущие данные для всех** – сохранить всю информацию о дублированных объектах из базы данных текущего Сервера. Информация о дублированных объектах из импортируемой базы данных будет проигнорирована. Действие применяется одновременно для всех дублированных объектов в данной таблице.

- **Выбрать вручную** – задать действие вручную для каждого дублированного объекта в отдельности. В этом режиме список дублированных объектов станет доступен для редактирования. Установите опции напротив тех объектов, которые будут сохранены.

Нажмите **Сохранить**.

Резервное копирование

Чтобы создать резервную копию критичных данных Сервера, нажмите кнопку **Резервное копирование** на панели инструментов. Данные будут сохранены в gz-архив. Файлы, полученные в результате резервного копирования, аналогичны файлам, получаемым при запуске исполняемого файла Сервера из командной строки с ключом `backup`.

Подробное описание данной команды приведено в документе **Приложения**, в разделе H4.5. Резервное копирование критичных данных Сервера Dr.Web.

8.9.2. Статистика Сервера Dr.Web

При помощи Центра управления вы можете ознакомиться со статистикой работы Сервера Dr.Web на уровне использования системных ресурсов компьютера, на котором установлен Сервер Dr.Web, а также сетевого взаимодействия с компонентами антивирусной сети и внешними ресурсами, такими как ВСО.

Чтобы ознакомиться со статистикой работы Сервера Dr.Web:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Статистика Сервера Dr.Web**.
3. В открывшемся окне представлены следующие разделы статистических данных:
   - **Активность клиентов** – данные по количеству обслуживаемых клиентов, подключенных к данному Серверу: Агентов Dr.Web, соседних Серверов Dr.Web и инсталляторов Агентов Dr.Web.
   - **Сетевой трафик** – параметры входящего и исходящего сетевого трафика при обмене данными с Сервером.
   - **Использование системных ресурсов** – параметры использования системных ресурсов компьютера, на котором установлен Сервер.
   - **Microsoft NAP** – параметры работы Dr.Web NAP Validator.
   - **Использование базы данных** – параметры обращения к базе данных Сервера.
   - **Использование файлового кэша** – параметры обращения к файловому кэшу компьютера, на котором установлен Сервер.
   - **Использование DNS кэша** – параметры обращения к кэшу, хранящему запросы к DNS-серверам, на компьютере, на котором установлен Сервер.
   - **Оповещения** – параметры работы подсистемы оповещений администратора.
   - **Репозиторий** – параметры обмена данными репозитория Сервера с серверами ВСО.

- **Web-статистика** – параметры обращения к Веб-серверу.
- **Кластер** – параметры обращений по протоколу межсерверной синхронизации при использовании кластера Серверов в многосерверной конфигурации сети.

4. Чтобы посмотреть статистические данные конкретного раздела, нажмите на название нужного раздела.
5. В открывшемся списке приведены параметры раздела с динамическими счетчиками значений.
6. Одновременно при раскрытии статистического раздела включается графическое представление изменений для каждого из параметров. При этом:
   - Чтобы отключить графическое представление, нажмите на название нужного раздела. При отключении графического представления числовое значение параметров продолжит динамически обновляться.
   - Чтобы повторно включить графическое представление данных, повторно нажмите на название нужного раздела.
   - Названия разделов и их параметров, для которых включено графическое отображение, выделяются полужирным шрифтом.
7. Для изменения частоты обновления параметров воспользуйтесь следующими инструментами на панели управления:
   - В выпадающем списке **Частота обновления** выберите требуемый период обновления данных. При изменении значения выпадающего списка, автоматически применяется временной период обновления числовых и графических данных.
   - Нажмите кнопку **Обновить**, чтобы единожды обновить все значения статистических данных одновременно.
8. При наведении указателя мыши на графические данные выводится числовое значение выбранной точки в виде:
   - **Abs** – абсолютное значение параметра.
   - **Delta** – прирост значения параметра относительно его предыдущего значения согласно частоте обновления данных.
9. Чтобы скрыть параметры раздела, нажмите на стрелку слева от названия этого раздела. При скрытии параметров раздела графическое представление статистики очищается и при повторном открытии параметров отрисовка начинается заново.

8.10. Особенности сети с несколькими Серверами Dr.Web

Dr.Web Enterprise Security Suite позволяет создавать антивирусную сеть с несколькими Серверами Dr.Web. 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.

Для обмена информацией между Серверами используется специальный *протокол межсерверной синхронизации*.

Возможности, предоставляемые протоколом межсерверной синхронизации:

- Распространение обновлений между Серверами в пределах антивирусной сети.
- Оперативность передачи обновлений при их получении с серверов ВСО Dr.Web.
- Передача между связанными Серверами статистической информации о состоянии защищаемых станций.
- Передача лицензий для защищаемых станций между соседними Серверами.

8.10.1. Строение сети с несколькими Серверами Dr.Web

В антивирусной сети можно установить несколько Серверов Dr.Web. При этом каждый Агент Dr.Web 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 Серверами Dr.Web.

Сервер Dr.Web может передавать другому Серверу Dr.Web:

- обновления ПО и вирусных баз. При этом получать обновления с серверов ВСО Dr.Web будет только один из них;
- информацию о вирусных событиях, статистику работы и т.д.;
- лицензии для защищаемых станций (передача лицензий между Серверами настраивается в Менеджере лицензий).

Dr.Web Enterprise Security Suite выделяет два типа связей между Серверами Dr.Web:

- *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.

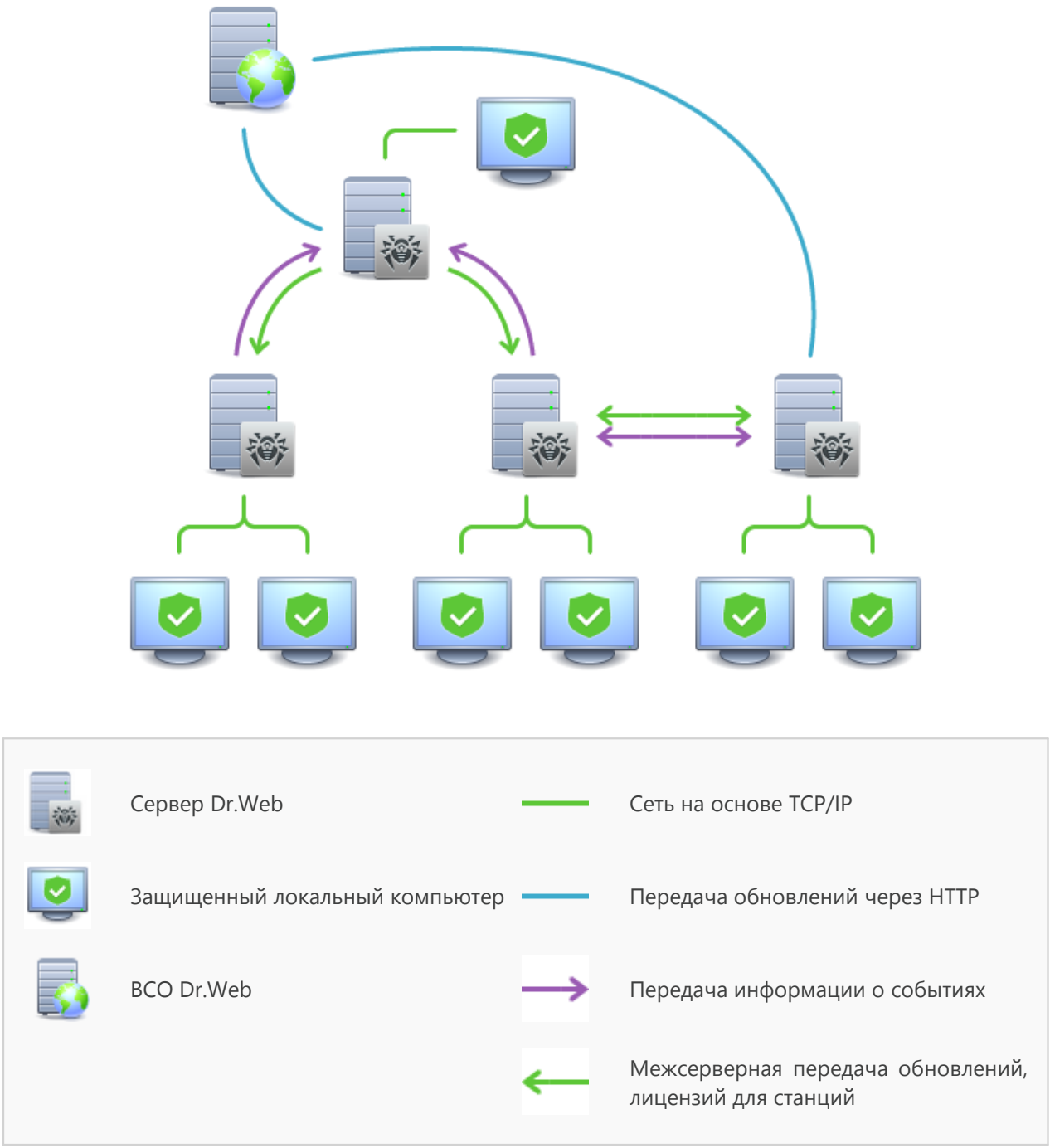


Рисунок 8-1. Сеть с несколькими Серверами

Некоторые из преимуществ антивирусной сети с несколькими Серверами Dr.Web:

1. Возможность получения обновлений с серверов ВСО Dr.Web через один Сервер Dr.Web с последующей передачей на остальные Серверы напрямую или через промежуточные звенья.

Серверы, принимающие обновления от вышестоящего Сервера, не принимают обновления с ВСО, даже при наличии такого задания в расписании.

Однако, на тот случай, если главный Сервер будет временно недоступен, рекомендуется оставить в расписание подчиненного Сервера задание на обновление с серверов ВСО. Это позволит Агентам, подключенным к подчиненному Серверу, получать обновление вирусных баз и программных модулей (см. также п. Общая конфигурация репозитория).

В задании на обновление с ВСО на главном Сервере, раздающем обновления, необходимо настроить получение обновлений серверного ПО для всех операционных систем, установленных на всех подчиненных Серверах, получающих обновления от этого главного Сервера (см. п. Общая конфигурация репозитория).

2. Возможность распределения рабочих станций по нескольким Серверам с уменьшением нагрузки на каждый из них.
3. 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.

4. Возможность передачи свободных лицензий для защиты станций на соседний Сервер. При этом сам лицензионный ключ остается в распоряжении раздающего Сервера, свободные лицензии выдаются соседнему Серверу на определенный промежуток времени, по истечении которого отзываются обратно.

8.10.2. Настройка связей между Серверами Dr.Web

Для того чтобы воспользоваться возможностями работы с несколькими Серверами, необходимо настроить связи между ними.

Рекомендуется предварительно спланировать 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" Серверы связывает хотя бы один информационный поток).

Пример настройки соединения главного и подчиненного Серверов Dr.Web:

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

1. Убедитесь, что оба Сервера Dr.Web нормально функционируют.
2. Каждому из Серверов Dr.Web дайте «говорящие» имена, так как это поможет не совершить ошибку при настройке соединения Серверов Dr.Web и при дальнейшем управлении. Сделать это можно в меню Центра управления **Администрирование** → **Конфигу-**

рация Сервера Dr.Web на вкладке **Общие** в поле **Название**. В данном примере назовем главный Сервер `MAIN`, а подчиненный – `AUXILIARY`.

3. На обоих Серверах Dr.Web включите серверный протокол. Для этого в меню Центра управления **Администрирование** → **Конфигурация Сервера Dr.Web** на вкладке **Модули** установите флаг **Протокол Сервера Dr.Web** (см. п. Модули).

   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.

4. Перезапустите оба Сервера Dr.Web.
5. Через Центр управления подчиненного Сервера (`AUXILIARY`) добавьте главный Сервер (`MAIN`) в список соседних Серверов. Для этого выберите пункт **Связи** в главном меню. Откроется окно, содержащее иерархический список Серверов антивирусной сети, соседних с данным Сервером. Для того чтобы добавить Сервер в этот список, нажмите кнопку **Создать связь** на панели инструментов.

   Откроется окно описания связей между текущим и добавляемым Сервером. Задайте следующие параметры:

   - **Тип** создаваемой связи – **Главный**.
   - **Название** – название главного Сервера (`MAIN`).
   - **Пароль*** – произвольный пароль для доступа к главному Серверу.
   - **Собственные ключи Сервера Dr.Web** – список открытых ключей шифрования настраиваемого Сервера. Нажмите кнопку и выберите ключ `drwcsd.pub`, относящийся к текущему Серверу. Для добавления еще одного ключа, нажмите и добавьте ключ в новое поле.
   - **Ключи соседнего Сервера Dr.Web*** – список открытых ключей шифрования подключаемого главного Сервера. Нажмите кнопку и выберите ключ `drwcsd.pub`, относящийся к главному Серверу. Для добавления еще одного ключа, нажмите и добавьте ключ в новое поле.
   - **Адрес*** – сетевой адрес главного Сервера и порт для подключения. Задается в формате *<адрес_Сервера>*:*<порт>*.

   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 кнопку . Начнется обзор сети на наличие доступных Серверов.

   d) Выберите Сервер в списке доступных Серверов. Его адрес будет записан в поле **Адрес** для создания связи.

- **Адрес Центра управления безопасностью Dr.Web** – можете указать адрес начальной страницы Центра управления главного Сервера (см. п. Центр управления безопасностью Dr.Web).
- В выпадающем списке **Параметры соединения** задается принцип соединения Серверов создаваемой связи.
- В выпадающих списках **Шифрование** и **Сжатие** задайте параметры шифрования и сжатия трафика между соединяемыми Серверами (см. п. Использование шифрования и сжатия трафика).
- **Срок действия выдаваемых лицензий** – период времени, на который выдаются лицензии из ключа на главном Сервере. Настройка используется, если главный Сервер будет выдавать лицензии текущему Серверу.
- **Период для продления получаемых лицензии** – настройка не используется при создании связи до главного Сервера.
- **Период синхронизации лицензий** – периодичность синхронизации информации о выдаваемых лицензиях между Серверами.
- Флаги в разделах **Лицензии**, **Обновления** и **События** установлены в соответствии с принципом связи *главный-подчиненный* и не подлежат изменению:
  - главный Сервер отправляет лицензии на подчиненный Сервер;
  - главный Сервер отправляет обновления на подчиненный Сервер;
  - главный Сервер принимает информацию о событиях от подчиненного Сервера.
- В разделе **Ограничения обновлений** → **События** можете задать расписание передачи событий от текущего Сервера главному (редактирование таблицы **Ограничения обновлений** осуществляется аналогично редактированию таблицы расписания в разделе Ограничение обновлений рабочих станций).

Нажмите кнопку **Сохранить**.

В результате главный Сервер (MAIN) попадет в папки **Главные** и **Отключенные** (см. рис. 8-2).

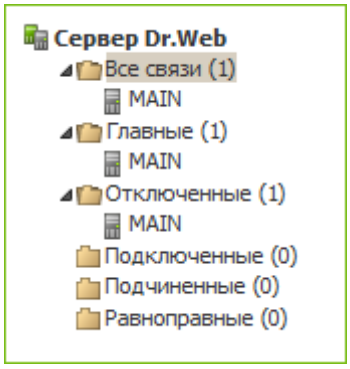


Рисунок 8-2.

6. Откройте Центр управления главного Сервера (MAIN) и добавьте подчиненный Сервер (AUXILIARY) в список соседних Серверов. 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 кнопку **Создать связь** на панели инструментов.

Откроется окно описания связей между текущим и добавляемым Сервером. Задайте следующие параметры:

- **Тип** создаваемой связи – **Подчиненный**.
- **Название** – название подчиненного Сервера (`AUXILIARY`).
- **Пароль*** – введите тот же пароль, что был указан в п. **5**.
- **Собственные ключи Сервера Dr.Web** – список открытых ключей шифрования настраиваемого Сервера. Нажмите кнопку  и выберите ключ `drwcsd.pub`, относящийся к текущему Серверу. Для добавления еще одного ключа, нажмите  и добавьте ключ в новое поле.
- **Ключи соседнего Сервера Dr.Web*** – список открытых ключей шифрования подключаемого подчиненного Сервера. Нажмите кнопку  и выберите ключ `drwcsd.pub`, относящийся к подчиненному Серверу. Для добавления еще одного ключа, нажмите  и добавьте ключ в новое поле.
- **Адрес Центра управления безопасностью Dr.Web** – можете указать адрес начальной страницы Центра управления подчиненного Сервера (см. п. Центр управления безопасностью Dr.Web).
- В выпадающем списке **Параметры соединения** задается принцип соединения Серверов создаваемой связи.
- В выпадающих списках **Шифрование** и **Сжатие** задайте параметры шифрования и сжатия трафика между соединяемыми Серверами (см. п. Использование шифрования и сжатия трафика).
- **Срок действия выдаваемых лицензий** – настройка не используется при создании связи до подчиненного Сервера.
- **Период для продления получаемых лицензии** – период до окончания срока действия лицензии, начиная с которого подчиненный Сервер инициирует продление лицензии, полученной от текущего Сервера. Настройка используется, если подчиненный Сервер будет получать лицензии от текущего Сервера.
- **Период синхронизации лицензий** – периодичность синхронизации информации о выдаваемых лицензиях между Серверами.
- Флаги в разделах **Лицензии**, **Обновления** и **События** установлены в соответствии с принципом связи *главный-подчиненный* и не подлежат изменению:
  - подчиненный Сервер принимает лицензии с главного Сервера;
  - подчиненный Сервер принимает обновления с главного Сервера;
  - подчиненный Сервер отправляет информацию о событиях на главный Сервер.
- В разделе **Ограничения обновлений** → **Обновления** можете задать расписание передачи обновлений от текущего Сервера подчиненному (редактирование таблицы **Ограничения обновлений** осуществляется аналогично редактированию таблицы расписания в разделе Ограничение обновлений рабочих станций).

Нажмите кнопку **Сохранить**.

В результате подчиненный Сервер (`AUXILIARY`) будет включен в папки **Подчиненные** и **Отключенные** (см. рис. 8-3).

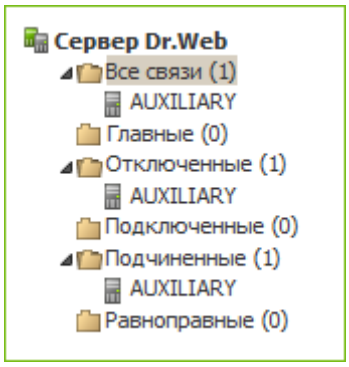


Рисунок 8-3.

7. Дождитесь установления соединения 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. 8-4).

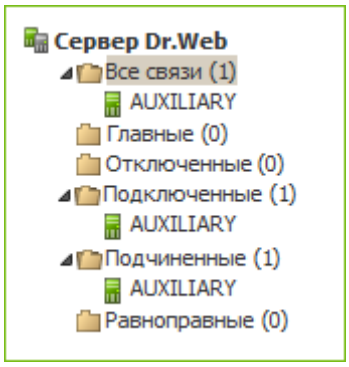


Рисунок 8-4.

8. Откройте Центр управления подчиненного Сервера (`AUXILIARY`) и убедитесь в том, что главный Сервер (`MAIN`) подключен к подчиненному (`AUXILIARY`) (см. рис. 8-5).

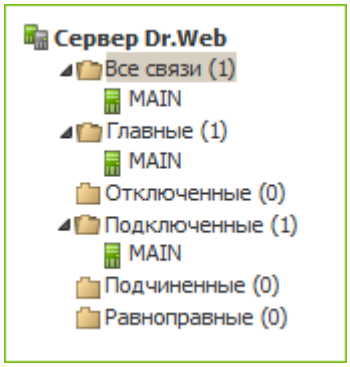


Рисунок 8-5.

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 журнале работы Серверов.

Установка соединения между Серверами Dr.Web невозможна в следующих случаях:

- Проблемы связи по сети.
- При настройке связи задан неверный адрес главного Сервера.
- Заданы неверные открытые ключи шифрования `drwcsd.pub` на одном из Серверов.
- Задан неверный пароль доступа на одном из Серверов (заданы несовпадающие пароли на соединяемых Серверах).

8.10.3. Использование антивирусной сети с несколькими Серверами Dr.Web

Особенностью сети с несколькими Серверами является получение обновлений с серверов ВСО Dr.Web через часть Серверов Dr.Web (как правило, один или несколько главных Серверов). При этом только на этих Серверах следует настраивать расписание, содержащее задание на обновление (см. п. Настройка расписания Сервера Dr.Web). 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, 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 кнопку **Обновить**.
6. При необходимости сохранить таблицу для распечатки или дальнейшей обработки, на панели инструментов нажмите

   Сохранить данные в CSV-файл,

   Сохранить данные в HTML-файл,

   Сохранить данные в XML-файл,

   Сохранить данные в PDF-файл.

8.10.4. Кластер Серверов Dr.Web

Обновлять Серверы в пределах кластера следует только из установочных пакетов. При этом требуется остановить все Серверы и осуществить обновление по очереди. Обновление через Центр управления (переход на новую ревизию) применять не следует, поскольку при использовании общей базы данных после обновления первого Сервера, все оставшиеся Серверы не смогут продолжить функционирование и обновление.

При создании в антивирусной сети кластера Серверов Dr.Web необходимо выполнение следующих предписаний:

1. **Одинаковые конфигурационные файлы**

   На всех Серверах должны быть одинаковые ключи шифрования `drwcsd.pub` и `drwcsd.pri`.

   Если ключи шифрования ранее не создавались, то в ходе установки первого Сервера кластера ключи шифрования будут сформированы автоматически.

   Получить необходимые ключи шифрования для установки последующих Серверов кластера можно через Центр управления: меню **Администрирование** → **Ключи шифрования**. При этом в зависимости от того, как в дальнейшем будет разворачиваться кластер, могут потребоваться или оба ключа, или только `drwcsd.pri`:

- При задании закрытого ключа `drwcsd.pri` во время установки Сервера, открытый ключ `drwcsd.pub` формируется автоматически.
- Если не задать нужный закрытый ключ при установке Сервера, то после установки необходимо заменить оба ключа вручную.

Местоположение конфигурационных файлов приведено в разделе Сервер Dr.Web.

2. Единое имя Сервера

Для всех Серверов должны быть заданы одинаковые IP-адрес или DNS-имя Сервера, используемые при формировании файлов инсталляции Агента для станций антивирусной сети.

Данное имя задается через Центр управления: **Администрирование** → **Конфигурация Сервера Dr.Web** → вкладка **Сеть** → вкладка Загрузка → поле **Адрес Сервера Dr.Web**. Настройки этого раздела хранятся в конфигурационном файле `download.conf` (описание файла приведено в документе **Приложения**, в п. G3. Конфигурационный файл download.conf).

3. Настройка использования кластера

На DNS сервере в сети необходимо зарегистрировать общее имя кластера для каждого отдельного Сервера и задать метод балансировки нагрузки.

Для автоматического применения настроек в кластере Серверов Dr.Web необходимо использование специального кластерного протокола.

Для настройки кластерного протокола необходимо для каждого из Серверов в Центре управления перейти в меню **Администрирование** → **Конфигурация Сервера Dr.Web** и задать следующие настройки:

a) Для включения кластерного протокола на вкладке Модули установите флаг **Протокол кластера Серверов Dr.Web**.

b) Для настройки параметров взаимодействия Серверов в составе кластера на вкладке Кластер задайте соответствующие параметры.

c) После задания всех необходимых параметров, нажмите **Сохранить** и перезагрузите Серверы.

Например

- Multicast-группа: `232.0.0.1`
- Порт: `11111`
- Интерфейс: `0.0.0.0`

В данном примере для всех Серверов кластера настраиваются транспорты для всех интерфейсов. В иных случаях, например, когда одна из сетей является внешней для кластера, и через нее подключаются Агенты, а вторая сеть является внутрикластерной, то кластерный протокол лучше открывать только для интерфейсов внутренней сети. В этом

случае в качестве интерфейсов необходимо задавать адреса вида `192.168.1.1`, ..., `192.168.1.N`.

4. **Единая база данных**

Для возможности работы с одной базой данных все Серверы Dr.Web должны быть одинаковой версии.

Все Серверы Dr.Web в пределах одного кластера должны работать с единой внешней базой данных.

Как и в случае использования базы данных без организации кластера, каждый из Серверов обращается к базе данных независимо, и все данные Серверов хранятся раздельно. Везде, где это актуально, Сервер забирает из базы данных только записи, привязанные к его ID, который является уникальным для каждого Сервера. Использование единой базы данных позволяет Серверам работать с Агентами, изначально зарегистрированными на других Серверах кластера.

При создании кластера Серверов с единой базой данных необходимо учитывать следующие особенности:

- База данных может быть установлена как отдельно от всех Серверов, так и на одном из компьютеров, на котором установлен Сервер кластера.
- База данных должна быть создана до установки первого Сервера кластера или до момента подключения первого Сервера к базе данных.
- В процессе добавления новых узлов в кластер (за исключением первого Сервера), при установке Серверов не рекомендуется сразу задание единой базы данных, которая используется в данном кластере. Иначе это может привести к удалению информации, уже хранящейся в базе данных. Рекомендуется устанавливать Серверы изначально с внутренней базой данных, а после установки переключать их на единую внешнюю базу данных.
  Переключить Серверы на использование внешней базы данных можно через Центр управления: в меню **Администрирование** → **Конфигурация Сервера Dr.Web** → на вкладке База данных или через конфигурационный файл Серверов `drwcsd.conf`.
- За исключением первого Сервера кластера, не рекомендуется вводить в кластер Серверы, уже функционирующие в антивирусной сети с иной внешней или внутренней базой данных. Это приведет к потере данных: информации о станциях, статистике, настройках (за исключением настроек, хранящихся в конфигурационных файлах), так как при импорте данные в базе полностью удаляются. В данном случае возможен только частичный импорт некоторых настроек.

5. **Одна версия репозитория**

На всех Серверах кластера репозитории должны содержать обновления одной и той же версии.

Достижение данного требования возможно одним из следующих способов:

- Одновременно обновлять все Серверы кластера с ВСО. В данном случае все Серверы будут содержать самую последнюю версию обновлений. Обновление репозиториев всех Серверов также возможно настроить с локальной зоны обновлений, с которой будет раздаваться одна и та же подтвержденная версия обновлений продуктов, или же самая последняя в случае создания зеркала ВСО.
- Допускается создание гибридной структуры, сочетающей в себе как кластер Серверов, так и иерархическую структуру на основе межсерверных связей. При этом один из Серверов (может быть как Сервером кластера, так и не входящим в кластер) назначается главным и получает обновления с ВСО. Остальные Серверы кластера – подчиненные – получают обновления с главного Сервера по межсерверным связям.

В случае настройки обновления Серверов кластера с локальной зоны (зеркала ВСО) или с главного Сервера необходимо следить за функционированием этой зоны или главного Сервера. В случае выхода из строя узла, раздающего обновления, необходимо перенастроить один из других Серверов на роль главного Сервера или создать новую зону обновлений для получения обновлений с ВСО соответственно.

6. Особенности распределения лицензий для станций

Для распределения лицензий между Серверами кластера могут использоваться следующие подходы:

a) Создание гибридной структуры, сочетающей в себе как кластер Серверов, так и иерархическую структуру на основе межсерверных связей. Подобная структура будет полезна, если при обслуживании Агентов в пределах кластерной системы Серверов осуществляется динамическое распределение станций между Серверами кластера. В этом случае осуществляется распространение необходимого количества лицензий от главного Сервера (может быть как Сервером кластера, так и не входящим в кластер) подчиненным Серверам по межсерверной связи непосредственно в процессе работы.

   Таким образом, достаточно расположения на главном Сервере одного лицензионного файла с количеством лицензий, соответствующем общему количеству обслуживаемых станций, и распределение необходимого количества лицензий на подчиненные Серверы в процессе работы кластера. Настройка раздачи подчиненным Серверам необходимого количества лицензий на необходимый срок осуществляется вручную администратором антивирусной сети.

   Для настройки распространения лицензий на соседние Серверы воспользуйтесь Менеджером лицензий.

   Например, можете настроить иерархическую структуру Серверов и выделить главный Сервер (может быть как Сервером кластера, так и не входящим в кластер), который будет раздавать как обновления репозитория, так и лицензии из лицензионного файла всем узлам кластера.

b) При отказе от настройки иерархической структуры Серверов, возможность разделения лицензий из единого лицензионного файла между всеми Серверами отсутствует. В таком случае необходимо заранее планировать структуру антивирусной сети с учетом наличия кластера Серверов и использовать несколько лицензионных файлов – по одному на каждый Сервер кластера. Общее количество лицензий во всех лицензион-

ных файлах приравнивается к общему количеству станций в сети, однако распределение количества лицензий по Серверам кластера необходимо рассчитать заранее, исходя из предполагаемого количества станций, которые планируется подключать к каждому из Серверов.

7. **Задания в расписании Серверов**

Чтобы исключить дублирование запросов к БД, рекомендуется выполнять только на одном из Серверов следующие задания из расписания Сервера: **Purge Old Data**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge unsent IS events**. Например, на Сервере, который расположен на том же компьютере, что и единая внешняя база данных. Или на наиболее производительном компьютере кластера, если конфигурации Серверов различаются, и база данных установлена на отдельном компьютере.

Глава 9: Обновление компонентов Dr.Web Enterprise Security Suite

Перед началом обновления Dr.Web Enterprise Security Suite 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. Общая конфигурация репозитория).

9.1. Обновление Сервера Dr.Web и восстановление из резервной копии

Центр управления предоставляет следующие возможности по управлению ПО Сервера Dr.Web:

- Обновление ПО Сервера на одну из доступных версий, скачанных из ВСО, и хранящихся в репозитории Сервера. Описание настроек обновления репозитория с ВСО приведены в разделе Управление репозиторием Сервера Dr.Web.
- Откат ПО Сервера к сохраненной резервной копии. Резервные копии Сервера создаются автоматически при переходе к новой версии в разделе **Обновления Сервера Dr.Web** (шаг 4 в процедуре ниже).

Обновление Сервера в пределах версии 10 также возможно осуществлять при помощи дистрибутива Сервера. Описание процедуры приведено в **Руководстве по установке**, в разделе Обновление Сервера Dr.Web для ОС Windows® или Обновление Сервера Dr.Web для ОС семейства UNIX®.

Не все обновления Сервера в пределах версии 10 содержат файл дистрибутива. Некоторые их них возможно установить только через Центр управления.

При обновлении Сервера под ОС семейства UNIX через Центр управления, версия Сервера в пакетном менеджере ОС не изменится.

Для управления ПО Сервера Dr.Web:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Сервер Dr.Web**.

2. Для перехода к списку версий Сервера выполните одно из следующих действий:
   - Нажмите на текущую версию Сервера в главном окне.
   - Нажмите кнопку **Список версий**.
3. Откроется раздел **Обновления Сервера Dr.Web** со списком доступных обновлений и резервных копий Сервера. При этом:
   - В списке **Текущая версия** указана версия Сервера, которая используется в данный момент. В разделе **Список изменений** приведен краткий список новых возможностей и список ошибок, исправленных в данной версии относительно предыдущей версии обновления.
   - В списке **Все версии** приведен список обновлений для данного Сервера, скачанных с ВСО. В разделе **Список изменений** приведен краткий список новых возможностей и исправленных ошибок для каждого из обновлений.
     Для версии, соответствующей первоначальной установке Сервера из инсталляционного пакета, раздел **Список изменений** пуст.
   - В списке **Резервные копии** приведен список резервных копий, сохраненных для данного Сервера. В разделе **Дата** приводится информация о дате резервного копирования.
4. Для обновления ПО Сервера установите опцию напротив нужной версии Сервера в списке **Все версии** и нажмите кнопку **Сохранить**.

   Произвести обновление можно только на более позднюю версию Сервера относительно используемой в данный момент.

   В процессе обновления Сервера текущая версия сохраняется как резервная копия (помещается в раздел **Резервные копии**), а версия, на которую осуществляется обновление, перемещается из раздела **Все версии** в раздел **Текущая версия**.

   Резервные копии сохраняются в следующем каталоге:

   `var → update_backup_<`*старая_версия*`>_<`*новая_версия*`>`.

   В процессе обновления создается или дополняется файл журнала `var → dwupdater.log`.
5. Для отката ПО Сервера к сохраненной резервной копии установите опцию напротив нужной версии Сервера в списке **Резервные копии** и нажмите кнопку **Сохранить**.

   В процессе отката ПО Сервера, резервная копия, на которую осуществляется переход, помещается в раздел **Текущая версия**.

9.2. Ручное обновление компонентов Dr.Web Enterprise Security Suite

Проверка наличия обновлений с ВСО

Чтобы проверить наличие обновления продуктов Dr.Web Enterprise Security Suite 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 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 Сервера Dr.Web).

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 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 перезагрузка станции. Следуйте указаниям Агента.

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 Сервера Dr.Web).

Чтобы настроить расписание выполнения задания на обновление на Сервере Dr.Web:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Планировщик заданий Сервера Dr.Web**. Откроется текущий список заданий Сервера.
2. Для того чтобы добавить задание в список, на панели инструментов нажмите 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 репозитория**.
5. В открывшемся списке установите флаги напротив тех компонентов, которые будут обновляться согласно этому заданию.
6. Перейдите на вкладку **Время** и укажите в выпадающем списке периодичность запуска задания, после чего настройте время в соответствии с выбранной периодичностью.
7. Для того чтобы сохранить изменения, нажмите кнопку **Сохранить**.

9.4. Обновление репозитория Сервера Dr.Web, не подключенного к Интернету

9.4.1. Копирование репозитория другого Сервера Dr.Web

Если Сервер Dr.Web не подключен к Интернету, его репозиторий можно обновить вручную, скопировав репозиторий другого, обновленного, Сервера Dr.Web.

Данный способ не предназначен для обновления Сервера до новой версии.

Для переноса обновлений репозитория с другого Сервера Dr.Web:

1. Обновите репозиторий Сервера, подключенного к Интернету, из раздела **Администрирование** → Состояние репозитория в Центре управления.
2. Экспортируйте репозиторий или его часть (нужные вам продукты) при помощи Центра управления, из раздела Содержимое репозитория. При этом необходимо осуществлять экспорт только тех типов объектов, которые поддерживаются для последующего импорта.
3. Скопируйте архив с экспортированным репозиторием на компьютер с Сервером, требующим обновлений.

   Импортируйте загруженный репозиторий на Сервер при помощи Центра управления, из раздела **Администрирование** → Содержимое репозитория.

Если вы используете особые настройки репозитория, такие как заморозка ревизий или обновление Агентов только с заданной (непоследней) ревизии, то при импорте репозитория необходимо включить опцию **Только добавить отсутствующие ревизии** и отключить опцию **Импортировать конфигурационные файлы**.

9.4.2. Загрузчик репозитория Dr.Web

Если нет возможности подключить какой-либо из Серверов Dr.Web к Интернету, вы можете скачать репозиторий с ВСО без использования ПО Сервера. Для этого предоставляется штатная утилита Загрузчик репозитория Dr.Web.

Особенности использования

- Для загрузки репозитория с ВСО необходим лицензионный ключ Dr.Web Enterprise Security Suite либо его MD5-хэш, который доступен для просмотра в Центре управления, в разделе **Администрирование** → **Менеджер лицензий**.
- Загрузчик репозитория Dr.Web доступен в следующих версиях:
  - графическая версия утилиты (только в версии под ОС Windows),
  - консольная версия утилиты.
- При загрузке репозитория с ВСО возможно использование прокси-сервера.

Возможные варианты использования

Загрузка с ручной заменой репозитория

1. Загрузите с ВСО репозиторий Сервера через утилиту Загрузчик репозитория Dr.Web.

   При загрузке создайте архив репозитория:

   a) Для графической утилиты: выберите режим **Загрузить репозиторий** и установите флаг **Архивировать репозиторий** в главном окне утилиты.

   b) Для консольной утилиты: используйте ключ `--archive`.

2. Скопируйте архив с загруженным репозиторием на компьютер с Сервером Dr.Web, требующим обновлений.

   Импортируйте загруженный репозиторий на Сервер Dr.Web при помощи Центра управления, из раздела **Администрирование** → Содержимое репозитория.

Если вы используете особые настройки репозитория, такие как заморозка ревизий или обновление Агентов только с заданной (непоследней) ревизии, то при импорте репозитория необходимо включить опцию **Только добавить отсутствующие ревизии** и отключить опцию **Импортировать конфигурационные файлы**.

Режим создания зеркала обновлений доступен только в графическом загрузчике только последней версии, которую можно скачать на официальном сайте компании в форматах версии x64 и версии x32.

Создание зеркала репозитория на сервере локальной сети

1. Загрузите с ВСО репозиторий Сервера через графическую утилиту Загрузчик репозитория Dr.Web.

   При загрузке выберите режим **Синхронизировать зеркало обновлений** в главном окне утилиты.

2. Загруженный репозиторий выложите на веб-сервер вашей локальной сети, который будет служить для раздачи обновлений репозитория.

3. В разделе **Администрирование** → Общая конфигурация репозитория настройте получение обновлений Сервером Dr.Web с вашего локального зеркала, а не с серверов ВСО Dr.Web.

   Убедитесь, что зеркало располагается в каталоге с названием `10.01.0`. При этом путь в поле **Базовый URI** необходимо указывать вплоть до этого каталога, не включая сам каталог.

9.4.2.1. Графическая утилита

Графическая версия утилиты Загрузчик репозитория Dr.Web может быть скачана при помощи Центра управления, в разделе **Администрирование** → **Утилиты**. Запускать данную версию утилиты можно на любом компьютере под ОС Windows, имеющем доступ в Интернет. Исполняемый файл – `drwreploader-gui-<`*версия*`>.exe`.

Режим загрузки обновлений, а также некоторые разделы дополнительных параметров доступны только в последней версии загрузчика, которую можно скачать на официальном сайте компании в форматах версии x64 и версии x32.

Для скачивания репозитория при помощи графической версии Загрузчика репозитория Dr.Web:

1. Запустите графическую версию утилиты Загрузчик репозитория Dr.Web.
2. В главном окне утилиты задайте следующие параметры:
   a) **Лицензионный ключ или MD5 ключа** – укажите файл лицензионного ключа Dr.Web. Для этого нажмите **Обзор** и выберите действующий файл лицензионного ключа. Вместо файла лицензионного ключа вы можете задать только MD5-хэш лицензионного ключа, который доступен для просмотра в Центре управления, в разделе **Администрирование** → **Менеджер лицензий**.
   b) **Каталог загрузки** – задайте каталог, в который будет осуществляться загрузка репозитория.

c) В списке **Режим** выберите один из режимов загрузки обновлений:

- **Загрузить репозиторий** – осуществляется скачивание репозитория в формате репозитория Сервера. Загруженные файлы могут быть непосредственно импортированы через Центр управления в качестве обновления репозитория Севера.
- **Синхронизировать зеркало обновлений** – осуществляется скачивание репозитория в формате зоны обновлений ВСО. Загруженные файлы могут выть выложены на зеркало обновлений в вашей локальной сети. В дальнейшем Серверы могут быть настроены на получение обновлений непосредственно с данного зеркала обновлений, содержащего последнюю версию репозитория, а не с серверов ВСО.

d) Установите флаг **Архивировать репозиторий**, чтобы автоматически упаковать загруженный репозиторий в zip-архив. Данная опция позволяет получить готовый архивный файл для импорта загруженного репозитория на Сервер при помощи Центра управления, из раздела **Администрирование** → Содержимое репозитория.

3. Если вы хотите изменить дополнительные настройки соединения с ВСО и загрузки обновлений, нажмите **Дополнительные параметры**. В открывшемся окне настроек доступны следующие вкладки:

a) На вкладке **Продукты** вы можете изменить список загружаемых продуктов. В окне настроек приведен список всех продуктов репозитория, доступных для загрузки с ВСО:

- Чтобы обновить список продуктов, доступных на ВСО в данный момент, нажмите кнопку **Обновить**.
- Установите флаги напротив тех продуктов, которые вы хотите загрузить с ВСО, или флаг в заголовке таблицы, чтобы выбрать все продукты из списка.

b) На вкладке **ВСО Dr.Web** вы можете настроить параметры серверов обновления:

- Порядок серверов ВСО в списке определяет порядок обращения к ним утилиты при загрузке репозитория. Для изменения порядка серверов ВСО используйте кнопки **Вверх** и **Вниз**.
- Чтобы добавить сервер ВСО в список серверов, используемых для загрузке, введите адрес сервера ВСО в поле над списком серверов и нажмите кнопку **Добавить**.
- Чтобы удалить сервер ВСО из списка используемых, выберите в списке сервер, который необходимо удалить, и нажмите кнопку **Удалить**.
- В поле **Базовый URI** указан каталог на серверах ВСО, содержащий обновления продуктов Dr.Web.
- В выпадающем списке **Протокол** выберите тип протокола для получения обновлений с серверов обновлений. Для всех протоколов загрузка обновлений осуществляется согласно настройкам списка серверов ВСО.
- В выпадающем списке **Допустимые сертификаты** выберите тип SSL-сертификатов, которые будут автоматически приниматься. Данная настройка используется только для защищенных протоколов, поддерживающих шифрование.
- **Регистрационное имя** и **Пароль** – регистрационные данные пользователя для аутентификации на сервере обновлений, если сервер требует авторизации.

- Установите флаг **Использовать CDN**, чтобы разрешить использование Content Delivery Network при загрузке репозитория.

c) На вкладке **Прокси** вы можете задать параметры подключения к ВСО через прокси-сервер:

- **Адрес прокси-сервера** и **Порт** – соответственно сетевой адрес и номер порта используемого прокси-сервера.
- **Регистрационное имя** и **Пароль** – параметры авторизации на прокси-сервере, если используемый прокси-сервер требует авторизацию.

d) На вкладке **Планировщик** вы можете настроить расписание периодических обновлений. Для выполнения расписания используется планировщик задач ОС Windows. При этом нет необходимости запускать утилиту вручную, загрузка репозитория будет осуществляться автоматически согласно заданным промежуткам времени.

e) На вкладке **Журнал** вы можете настроить параметры ведения журнала загрузок обновлений.

Нажмите **ОК** для принятия внесенных изменений и возвращения в главное окно Загрузчика репозитория Dr.Web.

4. После настройки всех параметров нажмите кнопку **Загрузить** в главном окне Загрузчика репозитория Dr.Web, чтобы начать подключение к ВСО и загрузку репозитория.

9.4.2.2. Консольная утилита

Консольная версия утилиты Загрузчик репозитория Dr.Web располагается в подкаталоге bin каталога установки Сервера Dr.Web. Запускать данную версию утилиты допускается только из данного каталога Сервера. Исполняемый файл – `drwreploader`.

Допустимые ключи

- `--help` – вывести справку по ключам.
- `--show-products` – показать список продуктов на ВСО.
- `--path` <*аргумент*> – загрузить репозиторий с ВСО в каталог, указанный в параметре <*аргумент*>.
- `--etc` <*аргумент*> – путь до каталога `etc` Сервера (используется для поиска корневых сертификатов и обновления открытых ключей).
- `--archive` – упаковать репозиторий в архив.
- `--key` <*аргумент*> – путь к файлу лицензионного ключа (должен быть указан ключ или его MD5).
- `--key-md5` <*аргумент*> – MD5-хэш лицензионного ключа (должен быть указан ключ или его MD5).
- `--product` <*аргумент*> – обновляемый продукт. По умолчанию загружается весь репозиторий.
- `--only-bases` – загрузить только вирусные базы.

- `--update-url` <*аргумент*> – каталог на серверах ВСО, содержащий обновления продуктов Dr.Web (рекомендуется оставить значение по умолчанию).
- `--servers` <*аргумент*> – адреса серверов ВСО (рекомендуется оставить значение по умолчанию).
- `--prohibit-cdn` – запретить использовать CDN при загрузке обновлений (по умолчанию отключено, т.е. разрешено использование CND).
- `--prohibit-ssl` – использовать незащищенный HTTP вместо HTTPS (по умолчанию отключено, т.е. используется HTTPS).
- `--cert-mode` [<*аргумент*>] – автоматически принимать сертификаты HTTPS.

  <*аргумент*> может принимать одно из значений:

  - `any` – принимать все сертификаты,
  - `valid` – принимать только проверенные сертификаты,
  - `drweb` – принимать только сертификаты Dr.Web.

  По умолчанию используется значение `drweb`.
- `--proxy-host` <*аргумент*> – прокси-сервер в формате <*сервер*>`[:`<*порт*>`]`.
- `--proxy-auth` <*аргумент*> – информация для аутентификации на прокси-сервере: регистрационное имя пользователя и пароль в формате <*пользователь*>`[:`<*пароль*>`]`.
- `--strict` – остановить загрузку в случае возникновения ошибки.
- `--log` <*аргумент*> – создать журнал в формате журналов Сервера по процедуре загрузки репозитория и разместить его в каталог, указанный в параметре <*аргумент*>.

Примеры использования

1. Создать импортируемый архив со всеми продуктами:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:
\Program Files\DrWeb Server\etc\agent.key" --etc "C:\Program Files\DrWeb
Server\etc"
```

2. Создать импортируемый архив с вирусными базами:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:
\Program Files\DrWeb Server\etc\agent.key" --only-bases --etc "C:\Program
Files\DrWeb Server\etc"
```

3. Создать импортируемый архив только с Сервером:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:
\Program Files\DrWeb Server\etc\agent.key" --product=20-drwcs --etc "C:
\Program Files\DrWeb Server\etc"
```

9.5. Ограничение обновлений рабочих станций

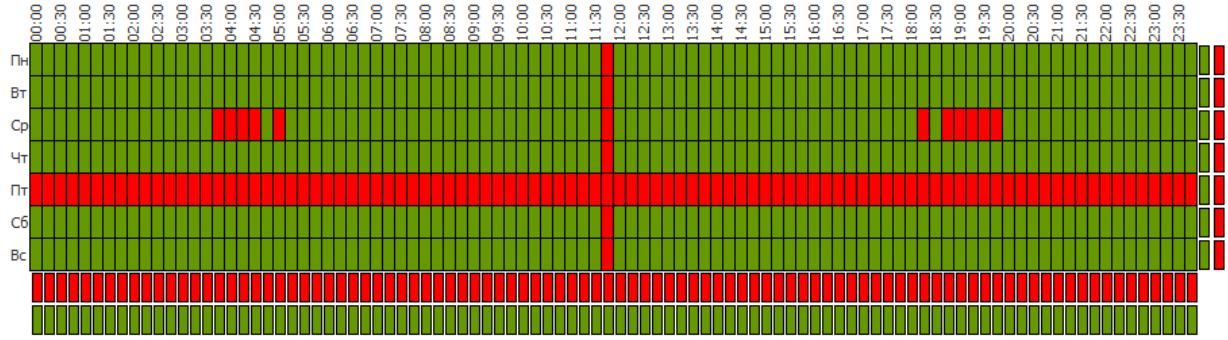
При помощи Центра управления вы можете задать режим обновлений компонентов Dr.Web Enterprise Security Suite на защищаемых станциях в определенные промежутки времени.

Для настройки режима обновлений станций выполните следующие действия:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В управляющем меню выберите пункт **Ограничения обновлений**.
2. В выпадающем списке **Ограничение обновлений** выберите режим ограничений:
   - **Без ограничений** – не устанавливать ограничения на распространение обновлений на станции.
   - **Запретить все обновления** – запретить распространение всех обновлений на станции в промежутках времени, заданных ниже в таблице **Расписание обновления станций**.
   - **Обновлять только базы** – запретить распространение только обновлений программных модулей в промежутках времени, заданных ниже в таблице **Расписание обновления станций**. Обновление вирусных баз будет осуществляться без изменений в штатном режиме.
3. Установите флаг **Ограничить трафик обновлений**, чтобы ограничить объем сетевого трафика при передаче обновлений между Сервером и Агентами. В поле **Максимальная скорость передачи (КБ/с)** задайте значение максимальной скорости передачи обновлений.
4. Установите флаг **Получать все последние обновления**, чтобы станция получала все обновления компонентов, вне зависимости от ограничений, заданных в разделе Детальная конфигурация репозитория.

   Если флаг снят, станция будет получать только обновления, помеченные в качестве текущих обновлений для распространения.
5. В таблице **Расписание обновления станций** 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.



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.

6. После завершения редактирования, нажмите кнопку **Сохранить** для принятия внесенных изменений.

На панели инструментов также доступны следующие опции для управления содержимым раздела:

Установить все параметры в начальные значения – восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).

Установить все параметры в значения по умолчанию – установить для всех параметров данного раздела значения, заданные по умолчанию.

Распространить эти настройки на другой объект – скопировать настройки из данного раздела в настройки другой станции, группы или нескольких групп и станций.

Установить наследование настроек от первичной группы – удалить персональные настройки станций и установить наследование настроек данного раздела от первичной группы.

Скопировать настройки из первичной группы и установить их в качестве персональных – скопировать настройки данного раздела из первичной группы и задать их для выбранных станций. Наследование при этом не устанавливается и настройки станции считаются персональными.

Экспортировать настройки из данного раздела в файл – сохранить все настройки из данного раздела в файл специального формата.

Импортировать настройки в данный раздел из файла – заменить все настройки в данном разделе настройками из файла специального формата.

9.6. Обновление мобильных Агентов Dr.Web

Если компьютер, ноутбук или мобильное устройство пользователя долгое время не будет иметь связи с Сервером Dr.Web, для своевременного получения обновлений с серверов ВСО Dr.Web рекомендуется установить мобильный режим работы Агента Dr.Web на станции.

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.

Включение мобильного режима в настройках Агента будет доступно при условии, что использование мобильного режима разрешено в Центре управления в разделе **Антивирусная сеть** → **Права** → <*операционная_система*> → **Общие** → **Запуск в мобильном режиме**.

Во время функционирования Агента в мобильном режиме связь Агента с Сервером Dr.Web 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.

Описание настроек мобильного режима работы на стороне Агента приведено в **Руководстве пользователя**.

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 Сервера Dr.Web и Агентов Dr.Web в случае невозможности организации прямого доступа (например, если Сервер Dr.Web и Агенты Dr.Web расположены в различных сетях, между которыми отсутствует маршрутизация пакетов).

Для установки соединения между Сервером и клиентами через Прокси-сервер рекомендуется отключить шифрование трафика. Для этого достаточно установить значение **нет** для параметра **Шифрование** в разделе Конфигурация Сервера Dr.Web → Общие.

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).
3. Пересылка данных между Сервером Dr.Web и Агентами Dr.Web 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 рис. 10-1.

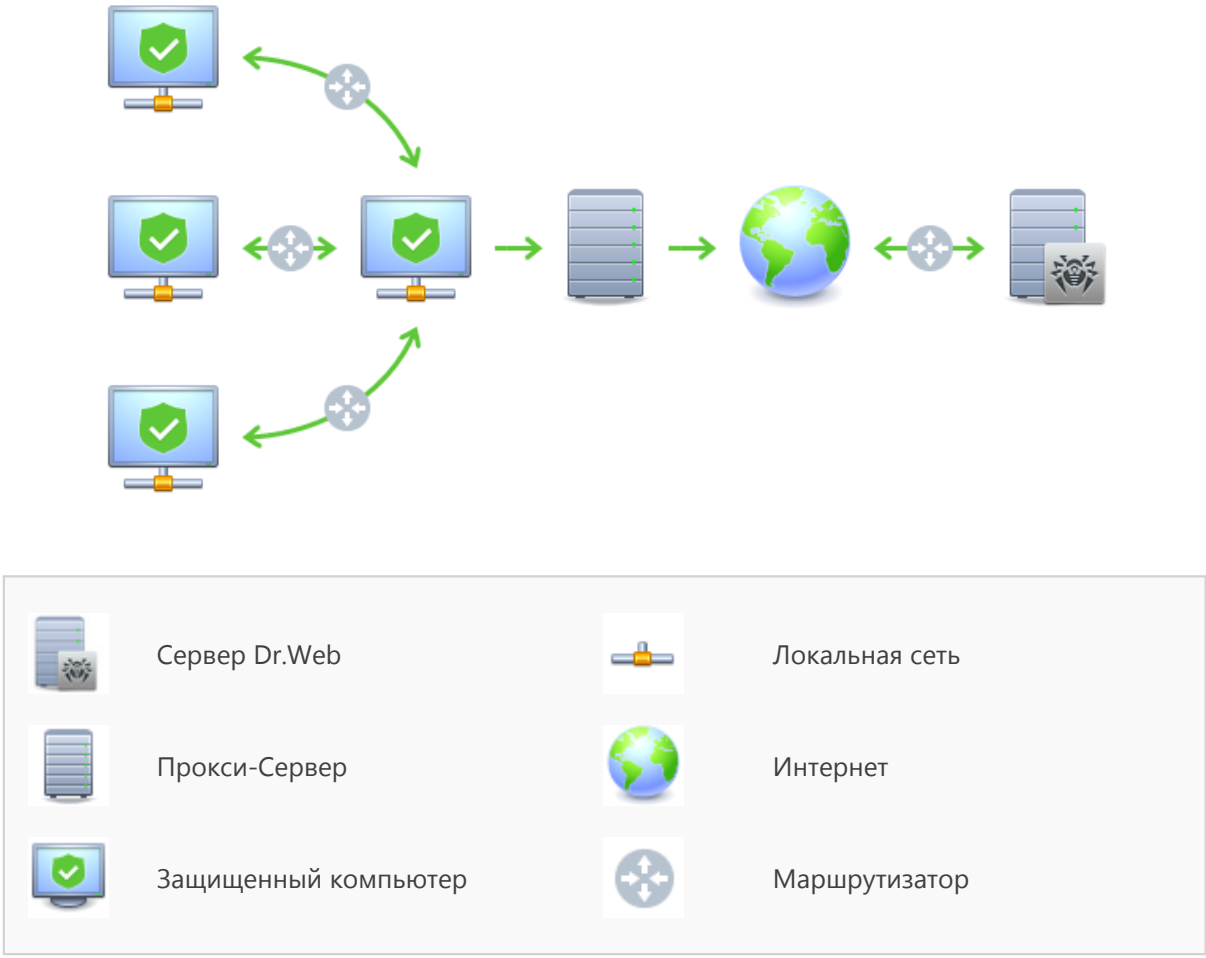


Рисунок 10-1. Схема антивирусной сети при использовании Прокси-сервера

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 Сервера Dr.Web. 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 Сервером Dr.Web.

Алгоритм переадресации при наличии списка Серверов Dr.Web:

1. Прокси-сервер загружает в оперативную память список Серверов Dr.Web из конфигурационного файла `drwcsd-proxy.xml` (см. документ **Приложения**, п. Приложение G4).
2. К Прокси-серверу подключается Агент Dr.Web.
3. Прокси-сервер переадресует Агента Dr.Web на первый Сервер Dr.Web из списка в оперативной памяти.
4. Прокси-сервер ротирует список, загруженный в оперативную память, и перемещает Сервер Dr.Web из первого элемента списка в конец списка.

   Прокси-сервер не сохраняет измененный порядок Серверов в свой файл конфигурации. При перезапуске Прокси-сервера список Серверов Dr.Web 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 Сервер Dr.Web 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 компьютере 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 Сервером Dr.Web 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, кэширование 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.

Параметры, задаваемые в конфигурационном файле, позволяют настроить следующие действия при кэшировании:

- Осуществлять периодическую очистку устаревших ревизий. По умолчанию – раз в час.
- Хранить только последние ревизии. Все остальные, более ранние ревизии, считаются устаревшими и удаляются. По умолчанию хранятся три последние ревизии.
- Периодически осуществлять выгрузку неиспользуемых *memory mapped* файлов. По умолчанию – каждые 10 минут.

Настройки

Прокси-сервер не имеет графического интерфейса. Задание настроек осуществляется при помощи конфигурационного файла. Формат конфигурационного файла Прокси-сервера приведен в документе **Приложения**, п. Приложение 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. **Руководство по установке**, 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 H9. 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 на сайте компании Microsoft.

Использование NAP в Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite 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 Агента Dr.Web на рабочую станцию.
- Сервер Dr.Web 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.
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 Серверу Dr.Web, 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. **Руководство по установке**, 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 выберите пункт **Client passed all SHV checks**, чтобы признавать станцию 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 выберите пункт **Client fail one or more SHV checks**, чтобы признавать станцию неработоспособной, если она не соответствует хотя бы одному из элементов заданной политики.

Предметный указатель

Предметный указатель

Предметный указатель

Т

У

Ф

Ц

Ш

Я